

Quantum circuit synthesis via a random combinatorial search


Sahel Ashhab¹, Fumiki Yoshihara^{1,2}, Miwako Tsuji³, Mitsuhsa Sato³, and Kouichi Semba^{1,4}

¹*Advanced ICT Research Institute, National Institute of Information and Communications Technology (NICT), 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan*

²*Department of Physics, Tokyo University of Science, 1-3 Kagurazaka, Shinjuku-ku, Tokyo 162-8601, Japan*

³*RIKEN Center for Computational Science, Kobe, Hyogo 650-0047, Japan*

⁴*Institute for Photon Science and Technology, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan*

 (Received 28 November 2023; revised 2 February 2024; accepted 16 April 2024; published 6 May 2024)

We use a random search technique to find quantum gate sequences that implement perfect quantum state preparation or unitary operator synthesis with arbitrary targets. This approach is based on the recent discovery that there is a large multiplicity of quantum circuits that achieve unit fidelity in performing a given target operation, even at the minimum number of single-qubit and two-qubit gates needed to achieve unit fidelity. We show that the fraction of perfect-fidelity quantum circuits increases rapidly as soon as the circuit size exceeds the minimum circuit size required for achieving unit fidelity. This result implies that near-optimal quantum circuits for a variety of quantum information processing tasks can be identified relatively easily by trying only a few randomly chosen quantum circuits and optimizing their parameters. In addition to analyzing the case where the CNOT gate is the elementary two-qubit gate, we consider the possibility of using alternative two-qubit gates. In particular, we analyze the case where the two-qubit gate is the B gate, which is known to reduce the minimum quantum circuit size for two-qubit operations. We apply the random search method to the problem of decomposing the four-qubit Toffoli gate and find a 15-CNOT-gate decomposition.

DOI: [10.1103/PhysRevA.109.052605](https://doi.org/10.1103/PhysRevA.109.052605)

I. INTRODUCTION

One of the important steps in implementing a quantum algorithm or performing a multiqubit operation on a quantum computing device is designing a sequence of elementary quantum gates to perform the desired multiqubit transformation [1–7] or prepare the desired multiqubit state [8–12]. This step can be thought of as compiling the quantum code from a high-level language to the low level of single- and two-qubit gates. The elementary quantum gate sequence is often called the quantum circuit.

Different technologies are currently being investigated for future quantum computing devices [13,14]. The specific technology used in an experimental setup often dictates how the qubits are addressed. For example, the most natural way to manipulate trapped ions [15–17] is different from the most natural way to manipulate superconducting qubits [18–20], and each technology has its own set of constraints on the allowed qubit control tools. Physical constraints on control signals can lead to technology-specific preferences in the elementary gate set used in the compilation step, i.e., in quantum circuit design [21]. While these experimental considerations must be considered in practical settings, past theoretical studies on quantum circuit synthesis have generally focused on elementary gate sets based on the controlled-NOT (CNOT) gate as the two-qubit entangling gate, combined with the set of all possible single-qubit unitary operators. We follow this convention and focus on the CNOT gate. It should be noted that the CNOT gate is a natural gate for numerous superconducting device architectures in use today [19,20].

An important question in the study of quantum circuit synthesis is quantum circuit size or complexity, which is quantified by the number of entangling gates N . In particular, it is highly desirable to find quantum circuits that have the minimum number of entangling gates needed for a perfect implementation of arbitrary multiqubit operations, including both state preparation and unitary operator synthesis. For this purpose, it is of great value to know in advance the minimum required circuit size. This question has been studied in numerous previous studies, typically by either devising recipes for quantum circuit synthesis [22–28] or by using mathematical arguments to derive lower and upper bounds for the required circuit size [3,11]. In Ref. [6], we investigated this question by numerically analyzing all the possible gate sequences up to a certain size for few-qubit tasks. Our results provided definite values for the minimum number of gates needed for various tasks, hence serving as tests and benchmarks to assess previously calculated lower bounds and recipe-based circuit sizes. There have been a few other recent studies on computer-based quantum circuit synthesis [29–38].

One of the remarkable results that we found in Ref. [6] is the large multiplicity of quantum circuits that can be used to perform the same task. In particular, even at the minimum number of CNOT gates needed for perfect state preparation of an arbitrary four-qubit state or unitary operator synthesis of an arbitrary three-qubit operator, we found that 20% of all possible CNOT gate configurations allow performing the desired task perfectly, i.e., with unit fidelity. This result naturally points to a possibly very efficient method to find optimal or near-optimal quantum circuits for various tasks. Although the

enormous number of different gate configurations limited our previous study to small numbers of qubits, if a finite fraction of all possible configurations give unit fidelity, it suffices to analyze a few randomly chosen quantum circuits. One will then, with a high probability, find at least one quantum circuit that performs the desired task perfectly.

In this work, we demonstrate this probabilistic approach to quantum circuit synthesis and treat cases that are intractable using the exhaustive search method. Our results indicate that the large multiplicity of unit-fidelity quantum circuits continues to hold for larger numbers of qubits than those investigated previously. Furthermore, we show that finding a unit-fidelity quantum circuit via a random search becomes increasingly easy if we increase the number of gates only slightly above the minimum required circuit size.

Since one of our main goals is reducing the gate count, we also consider the so-called *B* gate [39]. The reason behind this choice is that arbitrary two-qubit operations require shorter gate sequences if one uses the *B* gate instead of the CNOT gate [39]. We show that the *B* gate allows constructing shorter gate sequences than the CNOT gate for larger numbers of qubits. This result can be understood intuitively based on commutation relations and simple parameter-counting arguments. We emphasize, however, that experimental difficulties in implementing the *B* gate could outweigh any benefits that it provides, as we shall discuss below.

The remainder of this paper is organized as follows: in Sec. II, we provide some background information about quantum circuit synthesis and our computational approach. In Sec. III, we present the results of our numerical calculations and discuss their implications for practical quantum circuit synthesis. In Sec. IV, we give some concluding remarks.

II. BACKGROUND

A. Theoretical background

As mentioned in Sec. I, implementing a multiqubit operation on a quantum computer is typically achieved by finding a decomposition of the desired operation into a sequence of one- and two-qubit gates and then implementing that sequence. The CNOT gate, which is readily implementable on several quantum computing platforms, is the standard two-qubit gate used in most theoretical studies on the subject of quantum circuit synthesis.

Synthesizing a quantum circuit that implements an arbitrary n -qubit operation is analogous to reaching an arbitrary target point in the space of quantum operations [6]. Each added quantum gate adds adjustable control parameters that allow us to access more regions in the space of quantum operations. Lower bounds for the number of CNOT gates needed to perform an arbitrary n -qubit operation perfectly can be obtained by counting the free parameters in an arbitrary target and the number of adjustable parameters in the quantum circuit. The quantum circuit parameters must be at least equal to the number of free target parameters to be able to cover the space of all targets. This parameter-counting calculation gives the lower bounds (LB)

$$N_{\text{LB,SP,CNOT}} = \left\lceil \frac{2^n - 1 - n}{2} \right\rceil \quad (1)$$

for state preparation (SP) and

$$N_{\text{LB,U,CNOT}} = \left\lceil \frac{4^n - 1 - 3n}{4} \right\rceil \quad (2)$$

for unitary operator (*U*) synthesis. Here, the function $\lceil x \rceil$ is the ceiling function, i.e., the smallest integer larger than or equal to x .

Another important quantity in the present context is the number of different configurations for a single CNOT gate, i.e. the number of distinct ways that we can select a pair out of n qubits. Since reversing the control and target qubits in a CNOT gate gives the same CNOT gate, up to single-qubit rotations, the number of distinct CNOT gate configurations for a single gate is $n(n-1)/2$. As a result, the total number of CNOT gate configurations for a quantum circuit of size N is

$$N_{\text{config}} = \left(\frac{n(n-1)}{2} \right)^N. \quad (3)$$

In Ref. [6] we performed calculations in which we evaluated the maximum achievable fidelity for all possible CNOT gate configurations for n qubits, with $n \leq 4$ for state preparation and $n \leq 3$ for unitary operator synthesis. In the latter case, the computation time was on the order of a few years if the computations were run on a single core of a present-day computer. We now consider what would happen if we try to perform the same calculations for a larger number of qubits. Table I shows the number of CNOT gate configurations for different system sizes. If we go from $n = 3$ to $n = 4$ in the case of unitary operator synthesis, a number of factors change and dramatically increase the computation time. The Hilbert space size doubles, and the number of CNOT gates needed to achieve unit fidelity roughly quadruples. More importantly, the number of gate configurations N_{config} increases by a factor of $\sim 10^{41}$, which is a result of the superexponential scaling described by Eqs. (1)–(3). It is therefore impossible to extend the calculations of Ref. [6] to larger systems.

B. Computational approach

Since it is practically impossible to analyze all the gate configurations for the system sizes that we investigate in this work, we use a probabilistic approach. We analyze a number (N_{samples}) of randomly generated quantum circuits, each defined by the CNOT gate configuration. The number N_{samples} is a small fraction of the total number of possible gate configurations. Importantly, it does not scale with system size, and hence we avoid the superexponential scaling mentioned in the previous subsection. As a general rule, for each set of parameters n and N , we set $N_{\text{samples}} = 100$. The reason why we choose this number is that it is sufficiently large to allow us to perform statistical analysis for the purposes of the present study.

The target operation is generated randomly, as described in Ref. [6]. This target can be thought of as a random point in the space of operations or a random sample from a Haar-measure uniform distribution of quantum states or unitary operators.

Once we have specified the target, we generate gate sequences with the aim of reaching the target from a fixed

TABLE I. Estimates for the quantum circuit size N_{CNOT} , the total number of possible gate configurations N_{config} , and computation time per configuration as functions of system size, i.e., the number of qubits n . The number N_{CNOT} for each case is calculated from the appropriate lower bound formula, i.e., Eq. (1) or (2). The number N_{config} is calculated from Eq. (3), with N given by the appropriate value of N_{CNOT} . The computation times are specific to our computational environment: each calculation was run on a single core up to $n = 4$ and on about ten cores for $n \geq 5$. The calculations for $n \leq 7$ were performed on workstations, while those for $n = 8$ were performed on the Fugaku supercomputer. By far, the quantity that grows the fastest with increasing n is N_{config} .

No. of qubits	State preparation			Unitary operator synthesis		
	N_{CNOT}	N_{config}	Comp. time per config.	N_{CNOT}	N_{config}	Comp. time per config.
2	1	1	~0.1 s	3	1	~1 s
3	2	9	~2 s	14	4.8×10^6	~10 min
4	6	4.7×10^4	~1 min	61	$\sim 10^{47}$	~1 h
5	13	$\sim 10^{13}$	~5 min	252	$\sim 10^{252}$	~10 h
6	29	$\sim 10^{34}$	~1 h			
7	60	$\sim 10^{79}$	~10 h			
8	124	$\sim 10^{179}$	~20 h			

starting point. Each gate sequence is defined by a CNOT gate configuration along with the appropriate single-qubit rotations surrounding the CNOT gates. For each such configuration, the single-qubit rotation parameters serve as adjustable parameters that are chosen based on the target. They are optimized using a modified version of the gradient ascent pulse engineering (GRAPE) algorithm [6,40]. In the numerical optimization calculations, the fidelity F is used as the quantity to be maximized. For state preparation,

$$F = \text{Tr}\{\rho_F U(T)\rho_0 U^\dagger(T)\}, \tag{4}$$

where ρ_0 is the initial density matrix (with all the qubits in the state $|0\rangle$), ρ_F is the target density matrix, and $U(T)$ is the evolution operator generated by the quantum circuit, whose parameters are being updated by the optimization algorithm. For unitary operator synthesis,

$$F = \left| \frac{\text{Tr}\{U_F^\dagger U(T)\}}{2^n} \right|^2, \tag{5}$$

where U_F is the target unitary matrix.

In each iteration of the GRAPE algorithm, the derivatives of the fidelity with respect to all possible variations in all single-qubit rotations are calculated, which results in a gradient of the fidelity with respect to the rotation parameters. The rotations are then updated such that the fidelity increases steadily as the algorithm progresses. The optimization procedure is repeated for up to 10^5 iterations. The algorithm is terminated early if the fidelity exceeds $1 - 10^{-12}$ or grows by less than 10^{-12} in 10^3 iterations.

If the optimization gives $1 - F < 10^{-8}$ for a given quantum circuit, we identify the quantum circuit as corresponding to $F = 1$, i.e., a quantum circuit that implements the target perfectly. The error threshold, i.e., the number 10^{-8} , is chosen because it is sufficiently small that any deviation from $F = 1$ below this threshold can be attributed to numerical errors. Besides, from the perspective of practical implementations, an error of 10^{-8} is almost certain to be much smaller than other realistic errors in the experimental setup.

Since we would like to establish a probabilistic approach to quantum circuit synthesis, we use a probability-based interpretation of our results. The probability (p) that a random quantum circuit will give $F = 1$ in a given setting is straightforwardly inferred from the fraction (p_{num}) of the circuits that give $F = 1$ in our simulations, i.e., $p = p_{\text{num}}$. To determine the uncertainty in the calculated value of p , we need to evaluate the statistical variations in the results of the numerical calculations. We can do so by calculating the standard deviation σ in the data. Since each randomly generated circuit is classified as either having $F = 1$ or not, we need to use the formula for a binomial distribution. A quick and simple estimate for σ can be obtained by treating the value of p_{num} obtained from the simulations as the actual probability p in the binomial distribution. We then substitute this value in the formula for the binomial distribution standard deviation,

$$\sigma = \sqrt{\frac{p(1-p)}{N_{\text{samples}}}}. \tag{6}$$

This simple formula gives accurate results for large values of N_{samples} and p not too close to the end points $p = 0$ or $p = 1$. Since some of our data sets give $p_{\text{num}} = 0$, we avoid the simple calculation above and instead perform a Bayesian probability calculation to determine the size of the error bars and evaluate the uncertainty in p . We divide the range of p values, i.e., the range $[0, 1]$, into a large number of bins, which results in a statistical ensemble that we call ‘bins,’ with each bin characterized by a p value. For each data set, with a given fraction p_{num} of perfect-fidelity quantum circuits, we calculate the probability of obtaining p_{num} for each value of p in the ensemble. We refer to this conditional probability as $P(p_{\text{num}}|p)$. Using Bayes’ rule, the probability distribution for p values for a numerically obtained value of p_{num} is given by

$$P(p|p_{\text{num}}) = \frac{P(p_{\text{num}}|p)}{\sum_{p \in \text{Bins}} P(p_{\text{num}}|p)}. \tag{7}$$

To extract the extent of the error bars below and above p_{num} we determine the p values at which the distribution $P(p|p_{\text{num}})$ crosses the value $1/\sqrt{e}$. The error bars determined by this

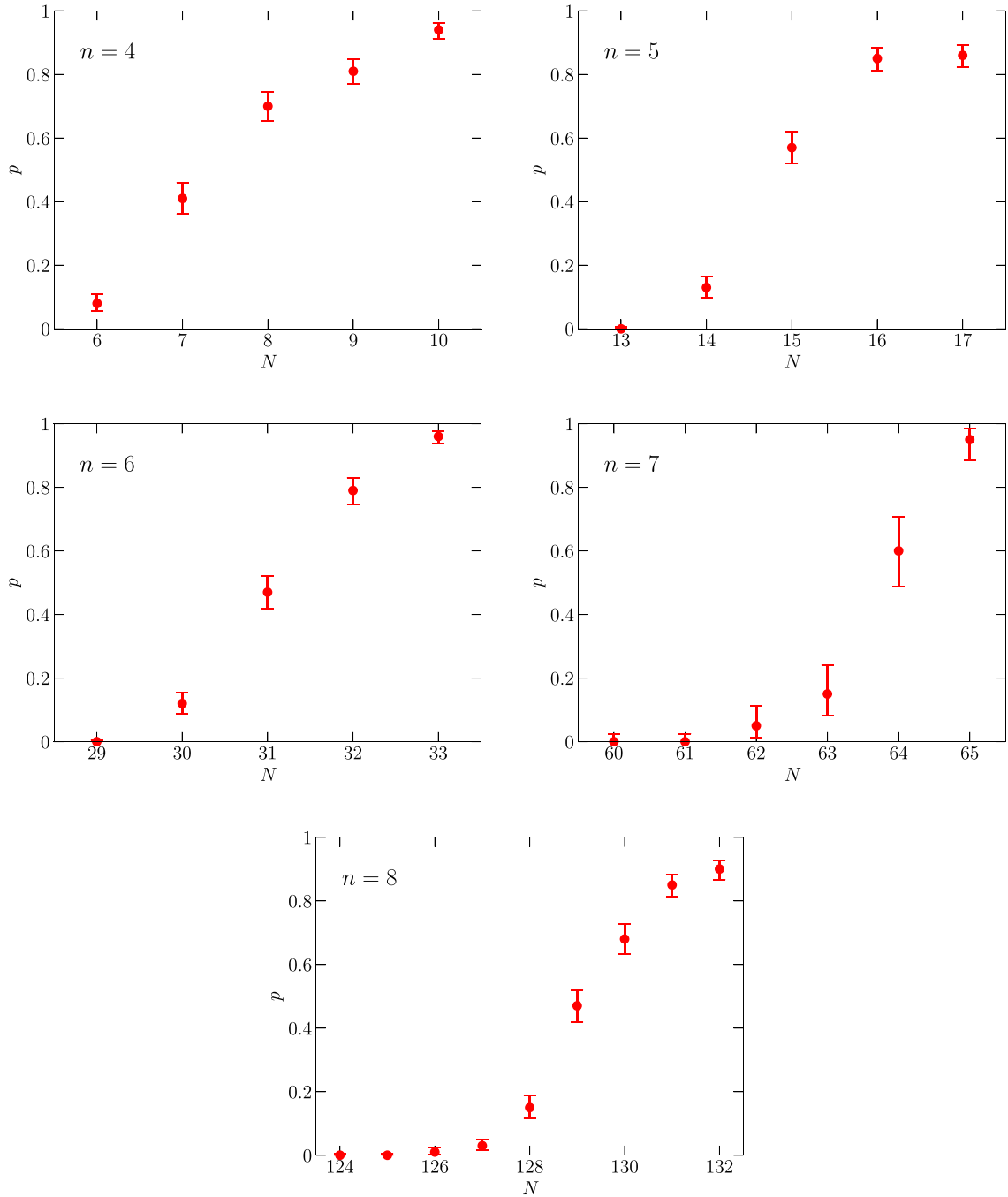


FIG. 1. Probability p that a random quantum circuit gives $F = 1$ as a function of circuit size N for the case of state preparation of an n -qubit system using the CNOT gate as the entangling gate. The $F = 1$ probability rises rapidly from zero to almost 1 even when N corresponds to just a few gates more than the theoretical lower bound $N_{\text{LB,SP,CNOT}}$. The error bars account for the uncertainty in inferring the probability p from the fraction p_{num} obtained in the random sampling calculation.

approach coincide with the standard deviation σ calculated from Eq. (6) in that equation's range of validity.

III. RESULTS

We now present the results of our numerical calculations. We analyze the statistical properties of randomly sampled quantum gate sequences, and we demonstrate how these

results can be used to establish a probabilistic approach to quantum circuit synthesis.

A. Establishing multiplicity of equivalent quantum circuits for small systems

As a starting point for the present study, we consider the small system sizes treated in Ref. [6]. In most of the figures in this manuscript, we plot the probability (p) of unit-fidelity

quantum circuits as a function of N . In each plot, the x axis starts from the relevant lower bound, i.e., Eq. (1), (2), (9), or (10).

The results for the case of state preparation are shown in Fig. 1. For four qubits ($n = 4$), the minimum number of CNOT gates needed to achieve $F = 1$ is $N = 6$. Even at the minimum required value of N , i.e., $N = 6$, 8% of the quantum circuits have $F = 1$. If we increase N , p increases rapidly, such that at $N = 10$, we find that 94% of the quantum circuits have $F = 1$. In other words, if we randomly generate a quantum circuit with $n = 4$ and $N = 10$ and optimize the single-qubit rotation parameters, the quantum circuit will almost certainly give $F = 1$. In the unlikely case that the first attempt does not succeed, a second random quantum circuit can be generated. The probability of finding at least one $F = 1$ quantum circuit approaches unity very rapidly with increasing number of trial quantum circuits. Specifically, the success probability after N_{trial} is given by

$$P_{\text{success}} = 1 - (1 - p)^{N_{\text{trial}}}, \quad (8)$$

such that the failure probability decreases exponentially with N_{trial} .

We obtain similar results for the case of unitary operator synthesis, as shown in Fig. 2. For $n = 3$, the minimum number of CNOT gates needed to achieve $F = 1$ is $N = 14$. The $F = 1$ probability in Fig. 2 ($n = 3$) rises from 26% at $N = 14$ to 90% at $N = 17$. As in the case of state preparation, the fraction of

quantum circuits that give $F = 1$ increases rapidly as soon as the number of CNOT gates exceeds the minimum required number.

B. Larger systems with the CNOT gate as the entangling gate

For state preparation with $n = 5$, the parameter-counting lower bound in Eq. (1) is $N_{\text{LB,SP,CNOT}} = 13$. However, none of the 100 random trial quantum circuits that we tried gave $F = 1$. For $N = 14$, 13% of the quantum circuits gave $F = 1$, and the fraction increased rapidly to 86% at $N = 17$. This result suggests that the minimum number of CNOT gates needed for perfect state preparation is $N = 14$, slightly higher than the value $N_{\text{LB,SP,CNOT}} = 13$ given by Eq. (1). Similarly, for $n = 6$, our numerical calculations suggest that the minimum number of CNOT gates is higher than that of Eq. (1) by one CNOT gate. For $n = 7$, we find a minimum number of CNOT gates that is higher than that of Eq. (1) by two CNOT gates. We note here that, because of the significant computational cost (as described in Table I), we used only 20 random quantum circuits for each parameter set in the case of $n = 7$. For $n = 8$, we also obtain a minimum number ($N = 126$) that is higher than that of Eq. (1) by two CNOT gates. In all cases shown in Fig. 1, the fraction of $F = 1$ quantum circuits increases rapidly from zero to near one. This result gives us confidence that the premise of this work, i.e., that there is large multiplicity in the unit-fidelity quantum circuits even at or

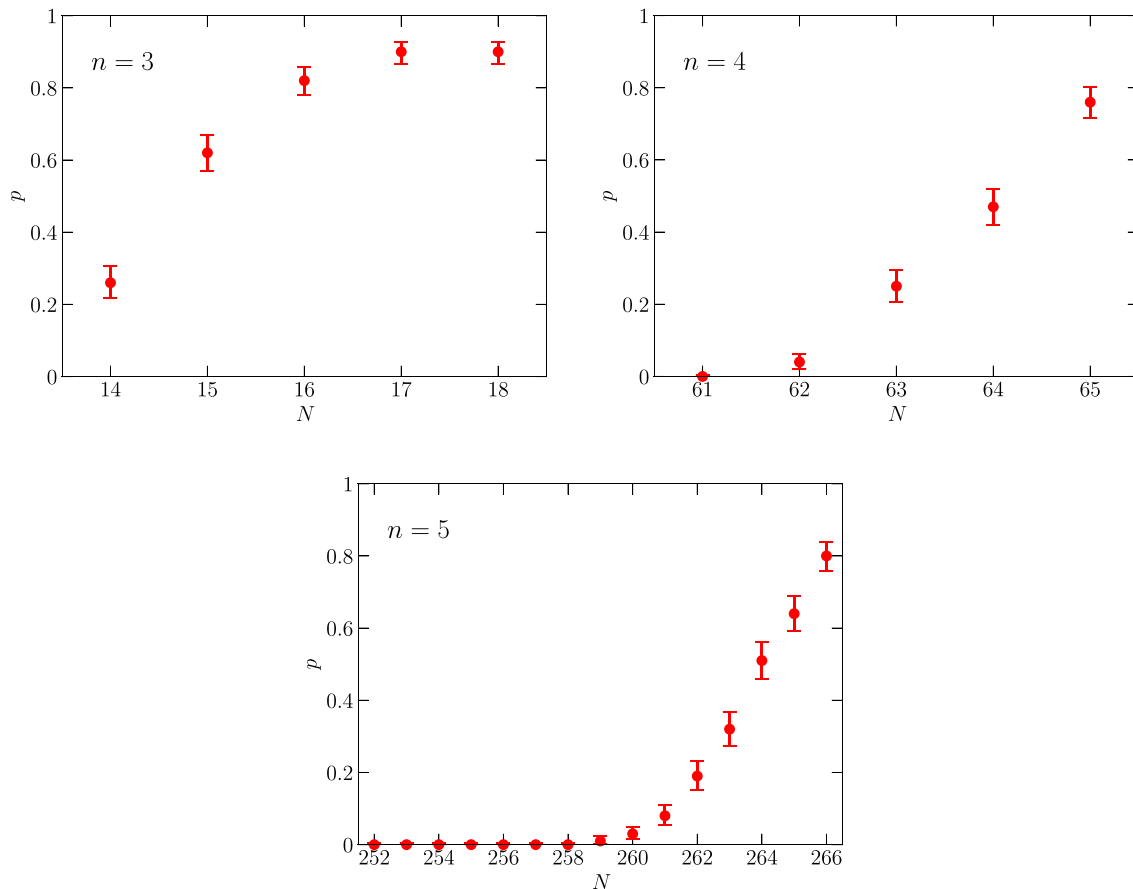


FIG. 2. Same as in Fig. 1, but for the case of unitary operator synthesis.

close to the minimum required circuit size, is valid. Although Eq. (1) is consistently not tight for $n \geq 5$, it provides a very good estimate even when $N \sim 100$. The deviation between the formula and our numerically obtained values of N grows much more slowly than N .

As alluded to in the previous subsection, in addition to the question of identifying the smallest value of N at which we obtain at least one quantum circuit with $F = 1$, another important question is the value of N at which the probability p becomes on the order of 1. In this context, we define the threshold number N_{th} as the smallest value of N at which $p > 50\%$. The value of N_{th} can be inferred from a plot of p as a function of N . The results for the cases of Figs. 1 and 2 are shown in Fig. 3. Equation (8) indicates that above N_{th} it should be easy to find a unit-fidelity quantum circuit with just a few attempts, since the success probability in each attempt is above 50%.

For the case of unitary operator synthesis (Fig. 2), for $n = 4$, the $F = 1$ fraction is zero at the lower bound $N_{\text{LB},U,\text{CNOT}} = 61$. However, it is 4% at $N = 62$ and rises rapidly to reach 76% at $N = 65$. For $n = 5$, the lower bound $N_{\text{LB},U,\text{CNOT}} = 252$. However, we obtain the first $F = 1$ quantum circuit at $N = 259$, i.e., seven more CNOT gates than $N_{\text{LB},U,\text{CNOT}}$. Considering that $N_{\text{LB},U,\text{CNOT}} = 252$, seven gates is under 3% of $N_{\text{LB},U,\text{CNOT}}$.

This result strongly suggests that the lower bound is not tight in this case. It is also remarkable that the probability p rises to 80% at $N = 266$, such that N_{th} is only a few steps above the smallest value of N that gives $F = 1$, even though $N \approx 260$.

It should be noted that there is a possibility that larger values of n lead to slower convergence, which could in turn lead to lowering the $F = 1$ fraction and an overestimation of the minimum number of gates needed to achieve $F = 1$. Our past experience with these optimization calculations does not indicate that such a slow convergence effect occurs. In fact, the increased number of control parameters can speed up the convergence. Nevertheless, as is the case with many search algorithms, we cannot completely rule out this possibility. It should also be noted that the optimization algorithm occasionally gives somewhat lower values, e.g., $F = 0.999$, for quantum circuits that correspond to $F = 1$. This property was observed in Ref. [6]; it manifests itself when the algorithm is run multiple times for the same CNOT gate configuration. However, this effect should only reduce the $F = 1$ fraction by a finite factor and should therefore not affect our conclusions about the minimum value of N that allows achieving $F = 1$.

One might also wonder if it is possible that for large quantum circuit sizes, e.g., in the case of unitary operator synthesis with $n = 5$ and $N \approx 260$, it might be possible to obtain

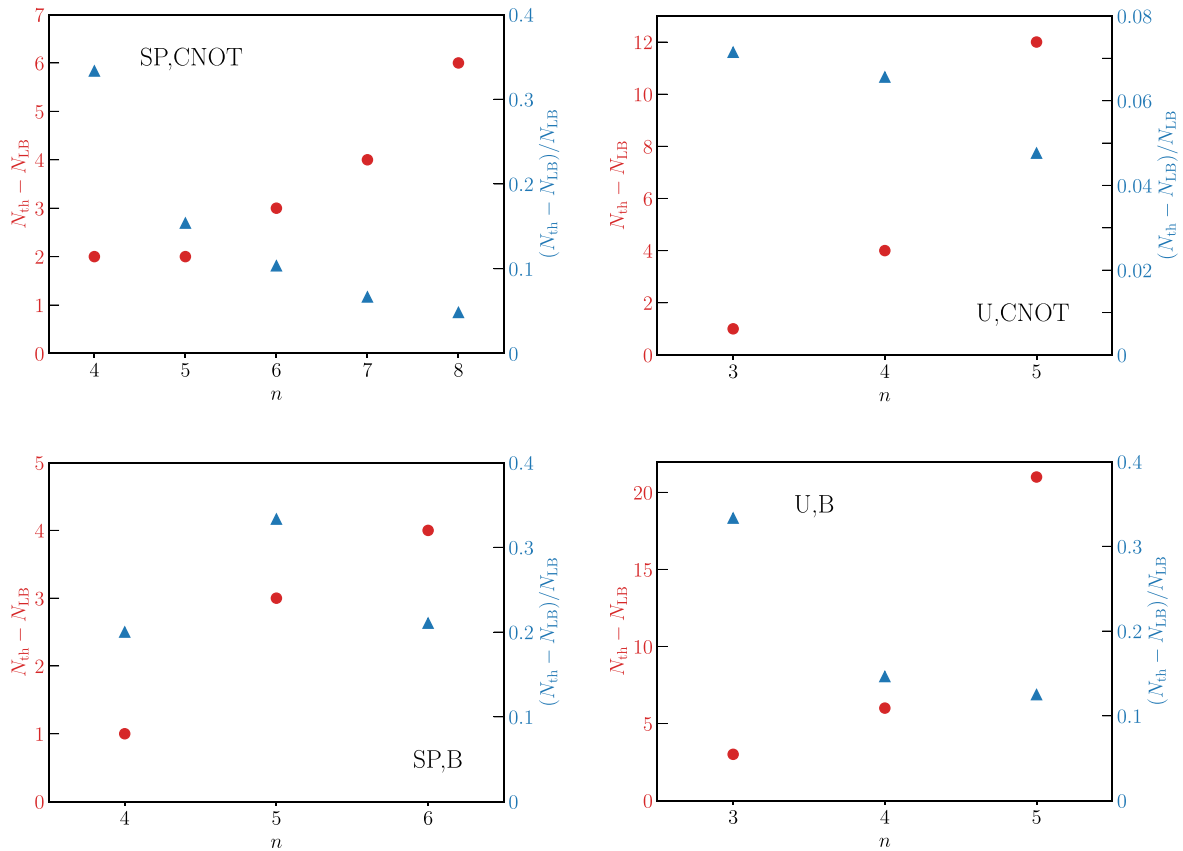
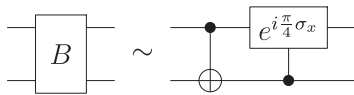


FIG. 3. Threshold at which the success probability exceeds 50%. The different panels are identified by their legends: SP corresponds to state preparation, while U corresponds to unitary operator synthesis. Similarly, CNOT corresponds to using the CNOT gate, while B corresponds to using the B gate, which is discussed in Sec. III C. The red circles show $N_{\text{th}} - N_{\text{LB}}$ (y axis on the left-hand side), while the blue triangles show $(N_{\text{th}} - N_{\text{LB}})/N_{\text{LB}}$ (y axis on the right-hand side). In almost all cases, $(N_{\text{th}} - N_{\text{LB}})/N_{\text{LB}}$ decreases with increasing n , which means that the ratio $N_{\text{th}}/N_{\text{LB}}$ gradually approaches 1, which means that in relative terms N_{th} approaches N_{LB} with increasing system size.

fidelities higher than our threshold of $1 - 10^{-8}$ even if the gate configuration in question does not allow achieving $F = 1$. In other words, 260 CNOT gates along with the single-qubit gates in the circuit allow so much freedom that one can get a very good approximation for the target. We do not expect that this possibility is affecting our calculations, because in our results the threshold is exceeded only for N values higher than the theoretical lower bounds in Eqs. (1) and (2). In other words, if false positives occur for $N \approx 260$, we would expect them to occur for $N \approx 250$ as well, considering the small relative difference between $N = 250$ and $N = 260$. We have not seen any such false positives below the lower bounds for N .

C. Using the B gate as the entangling gate

Although the CNOT gate is the standard entangling gate used in quantum algorithm design, the so-called B gate [39]



has one important advantage over the CNOT gate for the purpose of our study. Using the B gate can lead to smaller quantum circuit sizes to achieve the same result as using the CNOT gate. This point can be understood by considering the parameter-counting calculation used to determine the lower bounds for N . The CPHASE gate, which is equivalent to the CNOT gate up to single-qubit rotations, commutes with single-qubit rotations about the z axis. This property means that all z -axis rotations acting on the same qubit can be merged into one rotation. As a result, the number of independent quantum circuit parameters is reduced. If we use an entangling gate that does not commute with any single-qubit rotations, we maximize the number of free adjustable parameters in a quantum circuit of size N , thus increasing the number of free parameters per single-qubit rotation from 2 to 3 (excluding the first layer of single-qubit rotations). The B gate does not commute with any single-qubit rotations. The parameter-counting calculation then gives the lower bounds

$$N_{LB,SP,B} = \left\lceil \frac{2^n - 1 - n}{3} \right\rceil \tag{9}$$

for state preparation and

$$N_{LB,U,B} = \left\lceil \frac{4^n - 1 - 3n}{6} \right\rceil \tag{10}$$

for unitary operator synthesis. It is indeed well known that the B gate allows the synthesis of arbitrary two-qubit gates more efficiently than the CNOT gate: two B gates compared to three CNOT gates. With this point in mind, we perform similar calculations to those presented above but using the B gate as the entangling gate, along with the set of all single-qubit rotations.

As in the case of the CNOT gate, we can use the brute-force approach in which we analyze all possible gate configurations for state preparation up to $n = 4$ and for unitary operator synthesis up to $n = 3$. The results are shown in Figs. 4 and 5. These figures show that the B gate is more efficient than

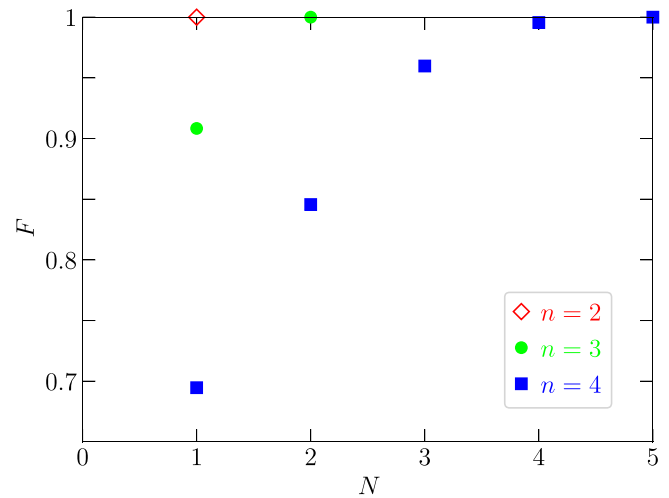


FIG. 4. Maximum achievable fidelity F as a function of the number of B gates for state preparation with $n = 2$ (red diamond), 3 (green circles), and 4 (blue squares). By comparing these results with those of Ref. [6], we can see that the B gate allows achieving the same results as the CNOT gate with smaller values of N . In the case of the CNOT gate, $F = 1$ is achieved for $N = 1, 3$, and 6 instead of 1, 2, and 5, respectively.

the CNOT gate in the sense that it allows quantum circuits with smaller values of N to perform the same operations. In the case of state preparation, the minimum numbers of CNOT gates needed for $n = 2, 3$, and 4 are 1, 3, and 6, respectively. Using the B gate, we obtain the values 1, 2, and 5, respectively. The theoretical lower bounds are $N_{LB,SP,B} = 1, 2$, and 4, respectively. In other words, $N_{LB,SP,B}$ in Eq. (9) is achieved for $n = 2$ and 3 but not for $n = 4$. In the case of unitary operator synthesis, the minimum numbers of CNOT gates needed for $n = 2$ and 3 are 3 and 14, respectively. Using the B gate, the numbers

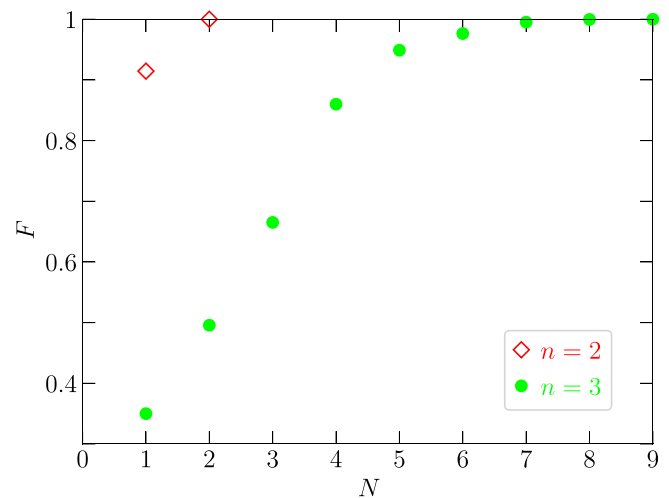


FIG. 5. Maximum achievable fidelity F as a function of the number of B gates for unitary operator synthesis with $n = 2$ (red diamonds) and 3 (green circles). In the case of the CNOT gate analyzed in Ref. [6], $F = 1$ is achieved for $N = 3$ and 14 instead of 2 and 9, respectively.

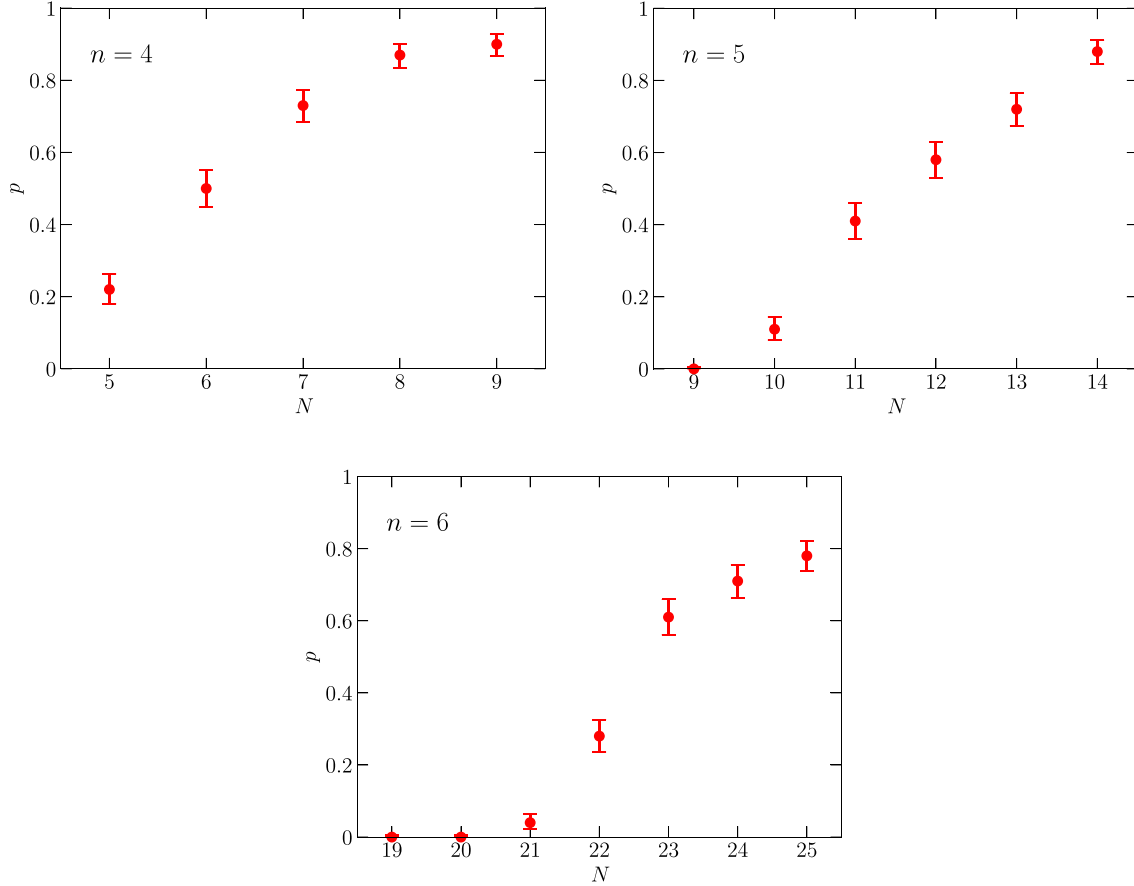


FIG. 6. Same as in Fig. 1, but for the case where the B gate is used as the entangling gate. The B gate allows achieving the same results as the CNOT gate with smaller values of N .

are 2 and 9, respectively, both matching the theoretical lower bounds given by Eq. (10).

The results of the probabilistic search calculations using the B gate are shown in Figs. 6 and 7. In all cases, the x axis starts at the lower bound given by Eq. (9) or (10). The results are generally similar to those obtained using the CNOT gate. The probability p rises above zero either at the lower bound value or slightly above it, and p reaches close to one after just a few additional steps, i.e., for a slightly higher value of N . Here, it is worth taking a closer look at the cases $n = 4$, $N = 42, 43$ and $n = 5$, $N = 180$. Considering that only one quantum circuit gave $F = 1$ in each one of the cases, one might wonder if these were cases in which the fidelity was slightly higher than $1 - 10^{-8}$, giving false positive counts of perfect quantum circuits. However, in two out of these three cases $1 - F$ was below 10^{-12} . In the case $n = 4$, $N = 42$, the quantum circuit identified as having $F = 1$ in fact had $1 - F \sim 10^{-9}$. However, we reran the optimization algorithm for this quantum circuit five times, and two of these reruns gave $1 - F < 10^{-12}$, which strongly suggests that these cases were not false positives. These results suggest that the fraction of quantum circuits that give $F = 1$ at the minimum required number of entangling gates decreases with increasing system size. This behavior differs from our observation for small systems, where a significant fraction of quantum circuits gave $F = 1$ even at the theoretical lower bound for circuit size. Nevertheless, our probabilistic approach remains a good

method to find quantum circuits with small numbers of gates and high fidelities.

D. Practical considerations

One important question when comparing different entangling gates, e.g., the CNOT and B gate, is the ability to perform the entangling gate in a real setup. The CNOT gate between two neighboring qubits can be implemented in realistic systems with a simple control pulse [18–20]. Even if we include technical difficulties such as coupling to nearby qubits and weak anharmonicity, one can still implement the CNOT gate with relatively simple pulses, as explained in Refs. [41,42]. To assess the ease of implementing the B gate, we first express it in matrix form as

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{2} & i\sqrt{2} & 0 \\ 0 & 0 & 0 & 1 \\ 0 & i\sqrt{2} & \sqrt{2} & 0 \end{pmatrix}, \quad (11)$$

where the rows and columns are ordered as in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. If we would like to implement this operation in a single step using Hamiltonian evolution of the form e^{-iHt} , where H is the Hamiltonian and t is the evolution time, the Hamiltonian will need to have

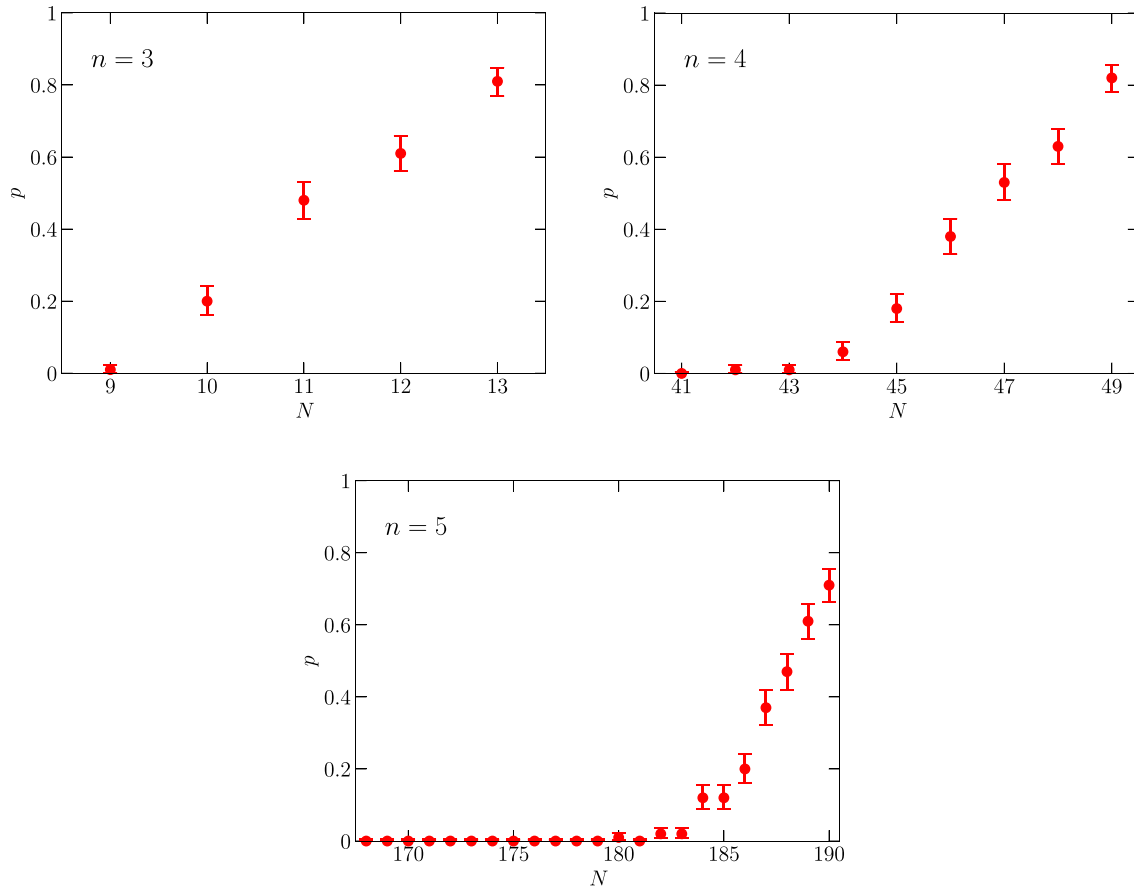


FIG. 7. Same as in Fig. 2, but for the case where the B gate is used as the entangling gate. The B gate allows achieving the same results as the CNOT gate with smaller values of N .

the form

$$H \propto i \log B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -0.243 + 0.625i & -0.508 + 0.715i & -0.265 - 0.492i \\ 0 & -0.265 - 0.492i & -1.449 + 0.381i & 0.997 + 0.095i \\ 0 & -0.508 + 0.715i & 2.106 - 0.24i & -1.449 + 0.381i \end{pmatrix}. \quad (12)$$

This Hamiltonian describes couplings with very specific strength ratios between all pairings of the states $|01\rangle$, $|10\rangle$, and $|11\rangle$. There is no simple physical mechanism that corresponds to this Hamiltonian and naturally implements the B gate. As a result, the B gate would likely have to be implemented in a two-step process as illustrated in the diagram at the beginning of Sec. III C. If we perform the gate count with each B gate counting as two controlled operations, and we compare the resulting numbers to the corresponding numbers for the CNOT gate, we find that using the CNOT gate is more efficient in practice. Furthermore, in a real setup, the naturally occurring interactions play a crucial role in determining the most natural entangling gate. Any other entangling gate can then be constructed from that platform-specific natural entangling gate.

Another important point relates to finding quantum circuits for different targets. As demonstrated in Ref. [6], if a CNOT-gate-based quantum circuit allows perfect implementation of one arbitrary target, i.e., a target that is not coincidentally easy to prepare, the same CNOT gate configuration allows perfect

implementation of any other target. Only the single-qubit rotation parameters need to be calculated for each new target. In other words, once we identify one unit-fidelity quantum circuit via the random combinatorial search technique, we do not need to run the same random search again for the same system size.

Another point relates to the high fidelity threshold in our calculations. In a practical setting, especially in present-day or near-future applications, there might not be any need to design extremely high-fidelity operations. Indeed, realistic decoherence considerations favor short quantum circuit. One might therefore find it advantageous to use a quantum circuit that has a theoretical fidelity below 1, if this quantum circuit is substantially shorter than the $F = 1$ quantum circuit. Our probabilistic approach can be used in this case as well. It is also possible to include decoherence in the GRAPE algorithm [40]. In this case, we can expect to obtain a maximum in F as a function of N . When N becomes too large, decoherence disrupts the dynamics and results in low fidelities.

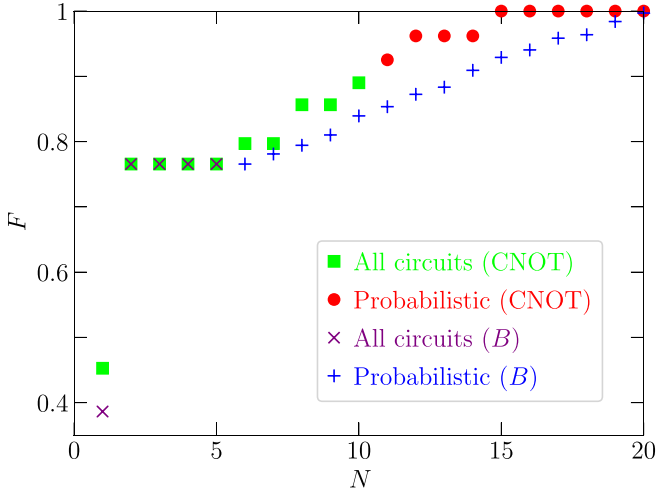


FIG. 8. Maximum achievable fidelity F as a function of the number of entangling (CNOT or B) gates used to synthesize a four-qubit Toffoli gate. The green squares correspond to the results obtained in Ref. [6], where all possible CNOT gate configurations were analyzed. The purple \times symbols are obtained by analyzing all possible B gate configurations. The red circles and blue $+$ symbols correspond to the random search approach for the CNOT gate and B gate, respectively. The four-qubit Toffoli gate can be perfectly synthesized using 15 CNOT gates. Unlike what we found for the case of arbitrary n -qubit gate synthesis, the B gate seems to be less efficient than the CNOT gate in this case. At $N = 20$, the B gate gives $F = 0.997$.

E. Constructing the n -qubit Toffoli gate

In the previous subsections we considered the case of arbitrary target operations. As such, the target states and unitary operators were generated using random number generators. In this subsection, we consider synthesizing multiqubit Toffoli gates. Specifically, we search for quantum circuits that implement the four-qubit Toffoli gate using two-qubit entangling gates. The lower bounds according to Eqs. (2) and (10) are $N_{LB,U,CNOT} = 61$ and $N_{LB,U,B} = 41$. However, considering that the n -qubit Toffoli gate has a special and simple structure, we can expect that it can be obtained using quantum circuits of smaller sizes. The results of our numerical calculations are shown in Fig. 8. The green squares show the results of Ref. [6], which were limited to $N \leq 10$ because larger values of N would have taken many years of single-core computation time. Using the random search approach (with 10^4 random quantum circuits for each set of parameters), we find that the four-qubit Toffoli gate can be decomposed into 15 CNOT gates. We note here that the $F = 1$ fraction was very low: for $N = 15, 16, \dots, 20$, we found, respectively, 1, 2, 7, 31, 56, and 133 perfect-fidelity circuits out of 10^4 random circuits in each set. The low $F = 1$ fraction in this case contrasts with the situation for the three-qubit Toffoli gate. In Ref. [6], we found that about 7% of all gate configurations with $N = 6$ gave $F = 1$. The CNOT gate configuration in the quantum circuit that gave $F = 1$ for $N = 15$ is described by the diagram

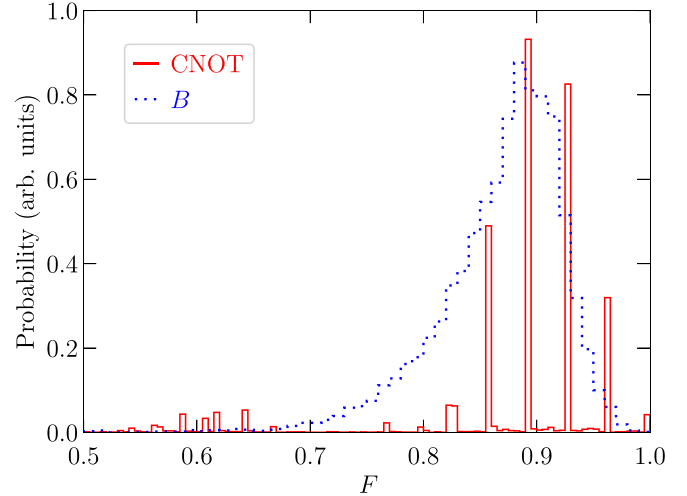
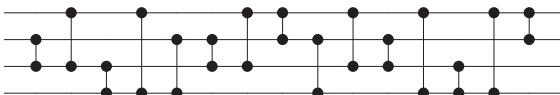


FIG. 9. Histograms for the fidelity F values for $N = 20$ when using the CNOT gate (red solid line) or the B gate (blue dotted line) to synthesize a four-qubit Toffoli gate. The y -axis scale is not the same for the two curves. For the CNOT gate there are special values of F that dominate the distribution, while for the B gate there is a continuous, broad distribution of F values.

where single-qubit rotations are not included in the diagram. This circuit does not have any easily discernible pattern. The circuit is slightly larger than the one in Ref. [43], which gave a decomposition of the four-qubit Toffoli gate into 14 CNOT gates, along with single-qubit gates. Hence, the random search approach produced an almost optimal decomposition of the gate. Besides, while the quantum circuit of Ref. [43] was constructed partly using intuition, the random search approach should work even for target gates that do not have a simple structure. We also performed random search calculations using the B gate. In contrast to the case of an arbitrary target unitary operator, the B gate does not outperform the CNOT gate for any value of N . On the contrary, it almost consistently gives lower fidelities for the same number of entangling gates. Even at $N = 15$, where the CNOT gate gives $F = 1$ up to numerical errors, the B gate gives $F = 0.93$. At $N = 20$, the B gate gives $F = 0.997$.

Here, it is also interesting to inspect the distribution of fidelity values obtained with the CNOT gate and the B gate. The histograms plotted in Fig. 9 show that the CNOT gate gives a set of sharp peaks. The peak locations, i.e., the F values at which the peaks occur, seem to be independent of N , at least between 1 and 20. Only the heights of the different peaks change with N . In contrast, the B gate gives continuous broad distributions of F values. The entire distribution shifts to larger values of F with increasing N .

IV. CONCLUSION

In conclusion, we have demonstrated the possibility of efficient quantum circuit synthesis using a random combinatorial search. This method allows us to analyze multiqubit systems of sizes that do not allow an analysis of all possible gate configurations. We find that, as long as the quantum circuit size is larger than the theoretical lower bound for perfect implementation of an arbitrary quantum operation,

a randomly generated quantum circuit has a high probability of performing an arbitrary operation after the circuit parameters are optimized. It should be noted that the circuit sizes needed to implement arbitrary n -qubit operations scale exponentially with n . Specific quantum gates can be implemented with smaller circuits. For the case of the n -qubit Toffoli gate, the circuit size is expected to scale quadratically with n . We applied the random search method to the four-qubit Toffoli gate and found a perfect fidelity quantum circuit with 15 CNOT gates. In addition to the CNOT gate, we applied our method to the B gate. The B gate consistently showed better performance for arbitrary targets but worse performance for the four-qubit Toffoli gate. This contrast sheds light on the utility of the B gate as an alternative to the CNOT gate in quantum circuit synthesis. It should of course be kept in mind that the naturally occurring physical interactions determine which gate to use in a real device. Our results demonstrate that the random

search approach provides one more powerful tool that can be used to optimize the implementation of quantum information processing tasks.

ACKNOWLEDGMENTS

We would like to thank Shunsuke Daimon, Norbert Schuch, and Naoki Yamamoto for useful discussions. This work was supported by Japan's Ministry of Education, Culture, Sports, Science and Technology (MEXT) Quantum Leap Flagship Program Grant No. JPMXS0120319794, and by the Center of Innovations for Sustainable Quantum AI [Japan Science and Technology Agency (JST), Grant No. JPMJPF2221]. The research used computational resources of the supercomputer Fugaku provided by the RIKEN Center for Computational Science.

-
- [1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. A* **52**, 3457 (1995).
 - [2] E. Knill, Approximation by quantum circuits, [arXiv:quant-ph/9508006](https://arxiv.org/abs/quant-ph/9508006).
 - [3] V. V. Shende, I. L. Markov, and S. S. Bullock, Minimal universal two-qubit controlled-NOT-based circuits, *Phys. Rev. A* **69**, 062321 (2004).
 - [4] V. Bergholm, J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Quantum circuits with uniformly controlled one-qubit gates, *Phys. Rev. A* **71**, 052330 (2005).
 - [5] M. Möttönen and J. J. Vartiainen, Decompositions of general quantum gates, in *Trends in Quantum Computing Research*, edited by S. Shannon (NOVA Publishers, New York, 2006).
 - [6] S. Ashhab, N. Yamamoto, F. Yoshihara, and K. Semba, Numerical analysis of quantum circuits for state preparation and unitary operator synthesis, *Phys. Rev. A* **106**, 022426 (2022).
 - [7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, New York, 2000).
 - [8] L. K. Grover, Synthesis of quantum superpositions by quantum computation, *Phys. Rev. Lett.* **85**, 1334 (2000).
 - [9] B. Kraus and J. I. Cirac, Optimal creation of entanglement using a two-qubit gate, *Phys. Rev. A* **63**, 062309 (2001).
 - [10] P. Kaye and M. Mosca, Quantum networks for generating arbitrary quantum states, in *Proceedings of the International Conference on Quantum Information* (Rochester, New York, 2001).
 - [11] V. V. Shende and I. L. Markov, Quantum circuits for incompletely specified two-qubit operators, *Quantum Inf. Comput.* **5**, 49 (2005).
 - [12] A. N. Soklakov and R. Schack, Efficient state preparation for a register of quantum bits, *Phys. Rev. A* **73**, 012307 (2006).
 - [13] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, Quantum computers, *Nature (London)* **464**, 45 (2010).
 - [14] I. Buluta, S. Ashhab, and F. Nori, Natural and artificial atoms for quantum computation, *Rep. Prog. Phys.* **74**, 104401 (2011).
 - [15] A. Sørensen and K. Mølmer, Quantum computation with ions in thermal motion, *Phys. Rev. Lett.* **82**, 1971 (1999).
 - [16] E. A. Martinez, T. Monz, D. Nigg, P. Schindler, and R. Blatt, Compiling quantum algorithms for architectures with multi-qubit gates, *New J. Phys.* **18**, 063029 (2016).
 - [17] T. Goubault de Brugière, M. Baboulin, B. Valiron, and C. Allouche, Synthesizing quantum circuits via numerical optimization, *Proceedings of ICCS, LNCS* **11537**, 3 (2019).
 - [18] G. S. Paraoanu, Microwave-induced coupling of superconducting qubits, *Phys. Rev. B* **74**, 140504(R) (2006).
 - [19] C. Rigetti and M. Devoret, Fully microwave-tunable universal gates in superconducting qubits with linear couplings and fixed transition frequencies, *Phys. Rev. B* **81**, 134507 (2010).
 - [20] P. C. de Groot, J. Lisenfeld, R. N. Schouten, S. Ashhab, A. Lupascu, C. J. P. M. Harmans, and J. E. Mooij, Selective darkening of degenerate transitions demonstrated with two superconducting quantum bits, *Nat. Phys.* **6**, 763 (2010).
 - [21] S. Ashhab, P. C. de Groot, and F. Nori, Speed limits for quantum gates in multi-qubit systems, *Phys. Rev. A* **85**, 052327 (2012).
 - [22] M. Žnidarič, O. Giraud, and B. Georgeot, Optimal number of controlled-NOT gates to generate a three-qubit state, *Phys. Rev. A* **77**, 032320 (2008).
 - [23] M. Plesch and C. Brukner, Quantum-state preparation with universal gate decompositions, *Phys. Rev. A* **83**, 032302 (2011).
 - [24] G. Vidal and C. M. Dawson, Universal quantum circuit for two-qubit transformations with three controlled-not gates, *Phys. Rev. A* **69**, 010301(R) (2004).
 - [25] F. Vatan and C. Williams, Optimal quantum circuits for general two-qubit gates, *Phys. Rev. A* **69**, 032315 (2004).
 - [26] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Efficient decomposition of quantum gates, *Phys. Rev. Lett.* **92**, 177902 (2004).
 - [27] T. Goubault de Brugière, M. Baboulin, B. Valiron, and C. Allouche, Quantum circuit synthesis using Householder transformations, *Comput. Phys. Commun.* **248**, 107001 (2020).

- [28] P. Rakyta and Z. Zimborás, Approaching the theoretical limit in quantum gate decomposition, *Quantum* **6**, 710 (2022).
- [29] D. Camps and R. Van Beeumen, Approximate quantum circuit synthesis using block encodings, *Phys. Rev. A* **102**, 052411 (2020).
- [30] S.-X. Zhang, C.-Y. Hsieh, S. Zhang, and H. Yao, Neural predictor based quantum architecture search, *Mach. Learn.: Sci. Technol.* **2**, 045027 (2021).
- [31] T. Shirakawa, H. Ueda, and S. Yunoki, Automatic quantum circuit encoding of a given arbitrary quantum state, [arXiv:2112.14524](https://arxiv.org/abs/2112.14524).
- [32] S.-X. Zhang, C.-Y. Hsieh, S. Zhang, and H. Yao, Differentiable quantum architecture search, *Quantum Sci. Technol.* **7**, 045023 (2022).
- [33] P. Wang, M. Usman, U. Parampalli, L. C. L. Hollenberg, and C. R. Myers, Automated quantum circuit design with nested Monte Carlo tree search, *IEEE Trans. Quantum Eng.* **4**, 1 (2023).
- [34] A. Szasz, E. Younis, and W. de Jong, Numerical circuit synthesis and compilation for multi-state preparation, in *IEEE International Conference on Quantum Computing and Engineering (QCE)*, Bellevue, WA, USA (IEEE, Piscataway, NJ, 2023).
- [35] M. Weiden, E. Younis, J. Kalloor, J. Kubiawicz, and C. Iancu, Improving quantum circuit synthesis with machine learning, [arXiv:2306.05622](https://arxiv.org/abs/2306.05622).
- [36] B. Rosenhahn and T. J. Osborne, Monte Carlo graph search for quantum circuit optimization, *Phys. Rev. A* **108**, 062615 (2023).
- [37] S. Daimon, K. Tsunekawa, R. Takeuchi, T. Sagawa, N. Yamamoto, and E. Saitoh, Quantum circuit distillation and compression, *Jpn. J. Appl. Phys.* **63**, 032003 (2024).
- [38] H. Wang, B. Tan, J. Cong, and G. De Micheli, Quantum state preparation using an exact CNOT synthesis formulation, [arXiv:2401.01009](https://arxiv.org/abs/2401.01009).
- [39] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Minimum construction of two-qubit quantum operations, *Phys. Rev. Lett.* **93**, 020502 (2004).
- [40] N. Khaneja, T. Reiss, C. Kehlet, T. S. Herbrüggen, and S. J. Glaser, Optimal control of coupled spin dynamics: Design of NMR pulse sequences by gradient ascent algorithms, *J. Magn. Reson.* **172**, 296 (2005).
- [41] P. C. de Groot, S. Ashhab, A. Lupascu, L. DiCarlo, F. Nori, C. J. P. M. Harmans, and J. E. Mooij, Selective darkening of degenerate transitions for implementing quantum controlled-NOT gates, *New J. Phys.* **14**, 073038 (2012).
- [42] S. Ashhab, F. Yoshihara, T. Fuse, N. Yamamoto, A. Lupascu, and K. Semba, Speed limits for two-qubit gates with weakly anharmonic qubits, *Phys. Rev. A* **105**, 042614 (2022).
- [43] N. Schuch, *Implementation of Quantum Algorithms with Josephson Charge Qubits* (Regensburg University, Regensburg, 2002); N. Schuch and J. Siewert, Programmable networks for quantum algorithms, *Phys. Rev. Lett.* **91**, 027902 (2003).