Phase-context decomposition of diagonal unitaries for higher-dimensional systems

Kerstin Beer and Friederike Anna Dziemba*

Institut für Theoretische Physik, Leibniz Universität Hannover, D-30060 Hannover, Germany

(Received 8 December 2015; published 25 May 2016)

We generalize the efficient decomposition method for phase-sparse diagonal operators of J. Welch *et al.* [Quantum Info. Comput. **16**, 87 (2016)] to qudit systems. The phase-context-aware method focuses on cascaded entanglers, whose decomposition into multicontrolled INC gates can be optimized by the choice of a proper signed base-d representation for the natural numbers. While the gate count of the best-known decomposition method for general diagonal operators on qubit systems scales with $O(2^n)$, the circuits synthesized by the Welch algorithm for diagonal operators with k distinct phases are upper-bounded by $O(n^2k)$, which is generalized to $O(dn^2k)$ for the qudit case in this paper.

DOI: 10.1103/PhysRevA.93.052333

I. INTRODUCTION

Diagonal unitary operators form a very restricted class among all unitary quantum gates. Despite this it has been proven that an efficient quantum circuit consisting of diagonal gates in the conjugate input basis cannot be efficiently classically simulated unless the polynomial hierarchy collapses at the third level [1]. Hence the complexity class IQP formed by these quantum circuits has attracted attention during recent years [2–5].

Indeed diagonal operators play a central role in many quantum algorithms, for example, in

(i) the oracle query in Grover's algorithm [[6], 6.1.2],

(ii) quantum optimization [7],

(iii) simulation of quantum dynamics [8,9], and

(iv) decoupling–the important primitive of quantum Shannon theory can be achieved by random diagonal unitaries [10,11].

Implementation of quantum algorithms motivates the study of decomposition methods for diagonal unitaries. Moreover, this decomposition raises interest as a subroutine within the compilation of an arbitrary quantum operation V based on the following.

(i) Spectral decomposition [12,13].

(ii) Givens' QR method [14]: $V = QR$, with Q Givens rotations and R the diagonal.

(iii) Real quantum computation [15]: $V = O_1 D O_2$, with O_1 and O_2 orthogonals and D the diagonal.

(iv) Cosine-sine decomposition [16,17]: $V = (U_1 \oplus U_2)W(U_3 \oplus U_4)$, with $D := (SH \otimes \mathbb{I})W(HS^\dagger \otimes \mathbb{I})$ the diagonal.

(v) Conditioned computation, where the circuits for the conditional operations are already known up to a relative phase.

While circuits decomposing arbitrary unitaries scale with $O(n^2 2^{2n})$ [[6], 4.5.1–4.5.2], the best-known compiling algorithm for diagonal unitaries provides circuits of size $O(2^n)$ [17]. The exponential growth is avoided in the setting of phase-sparse unitaries with k distinct phases. This setting is studied by the decomposition method in [18], which we generalize in this paper from qubit to qudit systems, resulting in a circuit scaling of $O(dn^2k)$.

Qudit systems and their advantages have been studied in [19–21], while extensive work on the synthesis of qudit operations has been done in [12,13,19,22,23]. Extending compiling methods to qudit systems is significant since many implementation architectures exhibit a natural qudit form.

Most of the previously mentioned algorithms containing diagonal unitary operators can be easily adapted for qudit systems. For example, higher-dimensional generalizations of Grover's algorithm have been studied in [24–27]. The aim of quantum optimization–finding the ground state of the Hamiltonian $H = -\sum_x g(x) |x\rangle \langle x|$ to determine the maximum of the function $g(x)$–requires the implementation of $e^{-iHt} = \sum_x e^{itg(x)} |x\rangle \langle x|$, which does not favor any specific underlying dimension structure. Using a binary encoding of the discrete grid for the originally continuous wave function in the simulation of quantum dynamics [8,9] is not physically motivated but rather arbitrary as well. There is no obstacle in considering a qudit encoding of the grid. Only the above-mentioned decoupling method is proven specifically for diagonal unitaries on qubits. But since the underlying realization of decoupling by approximate unitary 2-designs has been proven for arbitrary-dimensional systems [28] it would actually be interesting to study whether a sufficiently approximate 2-design can also be realized by diagonal unitaries in higher-dimensional systems.

All these examples motivate us to consider diagonal unitaries on general qudit structures and study suitable compiling algorithms for them.

II. OVERVIEW OF THE ALGORITHM

Throughout this paper we use the variable d for the dimension of a single qudit and the variable n for the number of qudits the diagonal operator acts on. The presented algorithm considers the *phase context* of a diagonal operator by splitting it into gate blocks for each of its distinct phases. Each block is built from a single-qudit phase gate and two so-called *cascaded entanglers*, which can be decomposed into single-qudit multiplication and addition operations and $\wedge_1$ and $\wedge_2$ gates. The latter are defined as singly and doubly controlled INC operations, where INC is a single-qudit gate with INC $|t\rangle = |t+1\rangle$ (operations on the labels of basis states are considered mod$d$ throughout this paper).

*friederike.dziemba@itp.uni-hannover.de

It is known that already $\wedge_1$, together with all single-qudit gates, forms a universal gate set for higher-dimensional quantum computation [29]. Thus one could apply a method like [13] to decompose the $\wedge_2$ operations even further, which can be regarded as higher-dimensional generalization of the Toffoli gate. But consideration of $\wedge_2$ gates as elementary allows us to end the decomposition of the cascaded entanglers at a point that reveals their basic structure and that is exact even if the single-qudit operations should be restricted to some finite gate set. Experimental realizations of $\wedge_2$ have been proposed [19].

The decomposition of the cascaded entanglers into controlled INC gates is based on a number-theoretical approach. At this point the authors of [18] focus on the binary representation of integers and mention a signed binary expansion as an alternative method. In this paper the central theorem is directly formulated for any signed base-d expansion. In many cases this allows further reduction of the number of required $\wedge_1$ and $\wedge_2$ gates.

III. PHASE-CONTEXT DECOMPOSITION OF DIAGONAL UNITARIES

We generalize the method in [18] for the decomposition of diagonal unitary operators to qudit systems. This method takes into consideration the phase context of an operator, i.e., a diagonal unitary,

$$U = \text{diag}(\underbrace{\phi_1,\ldots\phi_1}_{l_1},\underbrace{\phi_2,\ldots,\phi_2}_{l_2},\ldots,\underbrace{\phi_k,\ldots,\phi_k}_{l_k}),$$

on n qudits with k distinct phases is initially decomposed into a product of a global phase and $k-1$ similar operator blocks:

$$U = \phi_1 \prod_{i=1}^{k-1} \text{diag}(1,\ldots 1,\underbrace{\phi_{i+1}/\phi_i,\ldots\phi_{i+1}/\phi_i}_{\sum_{j=i+1}^{k} l_j}).$$

For the implementation of each block a phase gate,

$$P(\phi) := |0\rangle\langle 0| + \phi\,|1\rangle\langle 1| + \sum_{i=2}^{d-1}\alpha_i\,|i\rangle\langle i|$$

(with arbitrary higher phases α_i), assigns the desired phase $\phi = \phi_{i+1}/\phi_i$ to an ancillary target qudit if and only if its initial state $|0\rangle$ was changed to $|1\rangle$ beforehand by the so-called cascaded entangler CINC(l), which checks whether the original n-qudit register is in a computational basis state $|j\rangle$ with $j \geqslant d^n - l$:

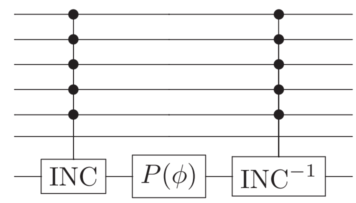
$$\text{CINC}(l)\,|j\rangle\,|t\rangle := \begin{cases} |j\rangle\,|t+1\rangle & \text{if} \quad j \geqslant d^n - l, \\ |j\rangle\,|t\rangle & \text{if} \quad j < d^n - l. \end{cases}$$

The operator diag$(1,\ldots,1,\phi,\ldots\phi)$, with the last l diagonal entries having value ϕ, can hence be realized on an $n+1$–qudit system by

$$V(\phi,l) = \text{CINC}(l)^\dagger(\mathbb{I}_n \otimes P(\phi))\,\text{CINC}(l).$$

In the case of qubits a cascaded entangler CINC(l) is its own inverse. For $d > 2$ one can realize the inverse by CINC$(l)^\dagger = (\mathbb{I}_n \otimes M)\,\text{CINC}(l)(\mathbb{I}_n \otimes M)$ with the single-qudit multiplication gate $M\,|t\rangle = |-t\rangle$.

The following circuit shows the decomposition of $V(\phi,l)$ for $d = 2$, $n = 6$, and $l = 2$:



In this paper the most significant dit always occurs at the left of a written string and at the top of a drawn quantum circuit.

In the special case above, the cascaded entangler corresponds to a single multicontrolled INC gate (NOT gate). This is due to the special choice of l and is not, in general, true. In the next section we show how to decompose a general cascaded entangler into several multicontrolled INC gates.

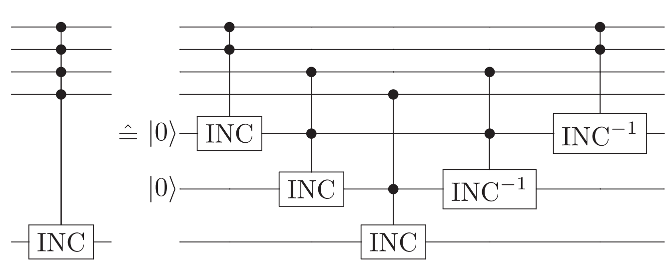
IV. DECOMPOSITION OF CASCADED ENTANGLERS

A. Multicontrolled INC operations

The aim here is to decompose a cascaded entangler CINC(l) into elementary single-qudit gates and cotrolled INC operations with maximally two control levels. In the first step the cascaded entangler is decomposed into multicontrolled INC$^{\pm 1}$ operations that increase or decrease the ancillary target qudit iff the computational basis state $|j\rangle = |j_1 \ldots j_n\rangle$ in the original n-qudit register corresponds in the first m qudits to a specific state $|b\rangle = |b_1 \ldots b_m\rangle$, $b_i \in \{0,1,\ldots,d-1\}$. These operations are denoted

$$\wedge_m^{n[b]}(\text{INC}^{\pm 1})\,|j\rangle\,|t\rangle := \begin{cases} |j\rangle\,|t \pm 1\rangle & \text{if} \quad b = j_1\ldots j_m, \\ |j\rangle\,|t\rangle & \text{otherwise.} \end{cases}$$

Note that it is easy to change a $\wedge_m^{n[b]}(\text{INC}^{-1})$ into a $\wedge_m^{n[b]}(\text{INC})$ operation by padding it by multiplication gates M on the target qubit. By padding suitable addition gates $\text{INC}_k\,|t\rangle = |t+k\rangle$ on each control level it is, furthermore, possible to replace any $\wedge_m^{n[b]}(\text{INC})$ operator by a $\wedge_m^{n[11\ldots 1]}(\text{INC})$ operator. Afterwards the operator with $m > 2$ control levels can be decomposed into linearly many doubly controlled INC gates denoted $\wedge_2$. The concrete parameters of the linear scaling depend on the chosen method. Here we exemplify the decomposition of a multicontrolled INC operation with $m = 4$ control levels according to a generalization of the method of [30] using $m-2$ ancilla qudits initialized to $|0\rangle$:



This specific decomposition method needs $2m-3$ $\wedge_2$ gates. The task of the last $m-2$ gates is to set the ancilla qudits back to $|0\rangle$. We could do without them, but most of them would cancel anyway with the $\wedge_2$ gates belonging to the next $\wedge_n^{m[b]}(\text{INC})$ operation, and additionally, they allow us to reuse the ancilla qudits and hence to keep the number of overall ancilla qudits small.

Since it is clear how to decompose $\wedge_m^{n[b]}(\text{INC}^{\pm 1})$ operations into $\wedge_2$ gates, it only remains to study the decomposition of a cascaded entangler $\text{CINC}(l)$ into $\wedge_m^{n[b]}(\text{INC}^{\pm 1})$ operations.

B. Results from classical logic synthesis

In the qubit case the remaining decomposition task has a classical analog in the $\{\wedge, \vee, \neg\}$ synthesis of the Boolean function $\phi : \{0,1\}^n \to \{0,1\}$ corresponding to the $\text{CINC}(l)$ operation with the ancilla qubit interpretated as output. Let $\{s_i\}_{1 \leqslant i \leqslant l} = \{x \in \{0,1\}^n | \phi(x) = 1\}$ be the set of inputs satisfying ϕ. A standard procedure in classical logic synthesis is to realize the circuit by the disjunctive normal form or sum-of-product form [[31], 4.3]:

$$\phi = \bigvee_{i=1}^{l} \bigwedge_{j=1}^{n} \neg^{s_{i,j} \oplus 1} x_j.$$

This general method obviously scales with $O(n2^n)$, since $l \in O(2^n)$ in the worst case. Many heuristic optimization methods are known making use of Karnaugh maps, BDDs, prime implicants, and more [[31], II], resulting in practical algorithms such as ESPRESSO. However, none of these methods is actually capable of avoiding the exponential scaling in the general case. This is not surprising since synthesizing the optimal circuit for an arbitrary Boolean formula is NP-hard.

Of course Boolean functions corresponding to $\text{CINC}(l)$ operations have a particular structure. They fall, for example, into the class of threshold functions obeying $\phi(x_1 \dots x_n) = 1$ iff $\sum_{i=1}^n w_i x_i$ greater than some threshold. For these functions [32] demonstrated a polynomially sized synthesis method and a scaling of $O(n^2)$ in particular examples.

This coincides with the scaling of $O(dn^2)$ obeyed by the decomposition method for cascaded entanglers presented in the next section. The method is an expansion of [18] to qudit systems but is also directly formulated with another number-theoretical degree of freedom: the choice of a signed base-d expansion for the natural numbers.

C. Decomposition of a cascaded entangler into multicontrolled INC operations

With the generalization

$$\text{CINC}(p,q)\,|j\rangle\,|t\rangle := \begin{cases} |j\rangle\,|t+1\rangle & \text{if} \quad p \leqslant j < q, \\ |j\rangle\,|t-1\rangle & \text{if} \quad q \leqslant j < p, \\ |j\rangle\,|t\rangle & \text{otherwise,} \end{cases}$$

one can easily find the trivial decomposition of a cascaded entangler corresponding to the classical disjunctive normal form, namely,

$$\text{CINC}(l) = \prod_{i=d^n-l}^{d^n-1} \text{CINC}(i,i+1),$$

where each $\text{CINC}(i,i+1)$ already equals a desired multicontrolled INC operation, $\wedge_n^{n[i]}(\text{INC})$. However, the number of l multicontrolled INC gates, each with n control levels, can be significantly reduced in many cases; e.g., consider the operation $\text{CINC}(2^{n-1})$ on a qubit system. In this example the cascaded entangler corresponds already to a single controlled INC gate with the first qubit as the only control level. This feature, based on the structure of the binary representation of the number l, is exploited in the decomposition method by [18], which we generalize in this section to qudit systems. We start with two helpful lemmata concerning the operator $\text{CINC}(p,q)$:

Lemma 1. $\text{CINC}(p,q) = \text{CINC}(p,r) \cdot \text{CINC}(r,q)$ for any $p,q,r \in \{0,1,\dots,d^n\}$.

Proof. The different cases depending on the order relation of p, q, and r can all be directly verified from the definition. Note that $\text{CINC}(p,p) = \mathbb{I}_{n+1}$ and $\text{CINC}(p,q) = \text{CINC}(q,p)^{-1}$. ■

Lemma 2. Suppose $p = bd^m$, $b \in \mathbb{N}_0$, $q = p + d^m$, and $p,q \in [0,d^n]$. Then $\text{CINC}(p,q) = \wedge_{n-m}^{n[b]}(\text{INC})$.

Proof. Since $q = (b+1)d^m \leqslant d^n$, it holds that $b < d^{n-m}$. Let $b_1 b_2 \dots b_{n-m}$ be the d-ary representation of b. Then the d-ary representations of p and $q-1$ turn out to be

$$p = bd^m = b_1 b_2 \dots b_{n-m} \underbrace{0 \dots 0}_{m \text{ times}},$$

$$q - 1 = p + d^m - 1 = b_1 b_2 \dots b_{n-m} \underbrace{(d-1) \dots (d-1)}_{m \text{ times}}.$$

$\text{CINC}(p,q)$ increases the ancillary target qubit iff the original n-qudit register is found in a computational state $|j\rangle$ with $p \leqslant j \leqslant q-1$. According to the above d-ary representations this is exactly the case when the first $n-m$ qudits are in the state $|b\rangle$. Hence $\text{CINC}(p,q)$ corresponds to a multicontrolled INC gate conditioned on the first $n-m$ qudits being in state $|b\rangle$. This is directly the definition of $\wedge_{n-m}^{n[b]}(\text{INC})$. ■

Corollary 3. Suppose $p = bd^m$, $b \in \mathbb{N}_0$, $q = p - d^m$, and $p,q \in [0,d^n]$. Then $\text{CINC}(p,q) = \wedge_{n-m}^{n[b-1]}(\text{INC}^{-1})$.

Proof. It holds that $q = b'd^m$ with $b' = b - 1 \in \mathbb{N}_0$. Exchanging the roles of p and q in Lemma 2 leads to $\text{CINC}(p,q) = \text{CINC}(q,p)^{-1} = \wedge_{n-m}^{n[b-1]}(\text{INC}^{-1})$. ■

The authors of [18] originally formulated their decomposition method for a cascaded entangler $\text{CINC}(l)$ in a qubit system based on the binary representation of the parameter l. Later they adapted the method for a signed bit binary expansion of l. Here we formulate the method not just for qudit systems but also directly for any *signed base-d expansion* of l. Such an expansion has the form $l = \sum_{i=1}^h s_i d^{m_i}$ with $0 \leqslant m_1 \leqslant m_2 \leqslant \dots m_h \in \mathbb{N}_0, s_i = \pm 1$, and $d^n \geqslant \sum_{i=r}^h s_i d^{m_i} > 0$ for all $1 \leqslant r \leqslant h$. We require the bounds for the partial sums because they guarantee proper parameters for the $\text{CINC}(p,q)$ gates used in the decomposition method.

Theorem 4. Let $\sum_{i=1}^h s_i d^{m_i}$ be a signed base-d expansion of l. Then $\text{CINC}(l) = \prod_{i=1}^h \wedge_{n-m_i}^{n[b_i]}(\text{INC}^{s_i})$.

Proof. Define $p_i := d^n - \sum_{r=i}^h s_r d^{m_r}$ for all $i \in \{1,2,\dots,h\}$ and $p_{h+1} := d^n$. It obviously holds that $p_1 = d^n - l$ and $p_i \in [0,d^n]$ for all $i \in \{1,2,\dots,h+1\}$. According to Lemma 1 we can decompose

$$\text{CINC}(l) = \text{CINC}(p_1,p_{h+1}) = \prod_{i=1}^h \text{CINC}(p_i,p_{i+1}).$$

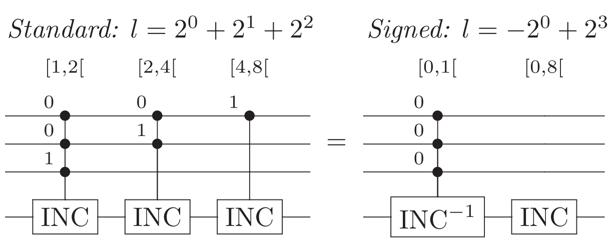
Because p_i is divisible by d^{m_i} for all $1 \leqslant i \leqslant h$, we can write $p_i = b_i' d^{m_i}$ with $b_i' \in \mathbb{N}_0$ and $p_{i+1} = p_i + s_i d^{m_i}$. Since the requirements of Lemma 2 and Corollary 3 are fulfilled it follows that

$$\text{CINC}(p_i, p_{i+1}) = \wedge_{n-m_i}^{n[b_i]}(\text{INC}^{s_i}),$$

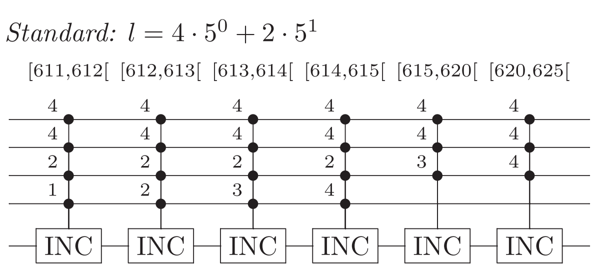
with $b_i = b_i'$ in the case $s_i = 1$ and $b_i = b_i' - 1$ in the case $s_i = -1$. This completes the proof. ∎

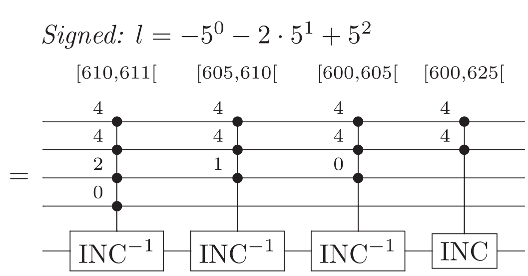
With the previous theorem we completed the decomposition of an arbitrary diagonal operator into $\wedge_1$, $\wedge_2$, and basic single-qudit gates. If we assume the setting of few distinct phases $k \in O(\text{poly}(n))$ and apply the previous theorem based on the standard d-ary expansion, the decomposition is even efficient. However, for many cascaded entanglers CINC(l) there exists an alternative signed base-d expansion of l leading to a decomposition into multicontrolled INC gates with a significantly smaller number of overall control levels and hence of required $\wedge_1$ and $\wedge_2$ gates due to the linear dependence. We close the section by demonstrating this in two examples.

Example 5. $d = 2, n = 3, l = 7$.



Example 6. $d = 5, n = 4, l = 14$.





V. CONCLUSION

A. Summary

We have generalized an efficient decomposition algorithm for diagonal phase-sparse unitaries presented in [18] to qudit systems. While this generalization is interesting from a number-theoretical point of view, it might also be advantageous for practical implementations since it allows decompositions into multicontrolled INC gates with fewer control levels compared to the qubit case (though higher-dimensional).

An advantage of the presented algorithm over other decomposition methods is its consideration of the phase context of the unitary, which leads to the small number k of required single-qudit phase gates. Hence the decomposition of an n-qubit operator with $k = 2$ distinct phases only requires two single-qubit gates, while previous methods decompose into $\Omega(2^n)$ phase gates, as pointed out in [18]. The number of required phase gates is of particular interest since they form the accuracy-dependent part in this decomposition (in contrast to the exactly decomposable cascaded entanglers) in the case where the single-qudit operations are further decomposed into some approximating, eventually finite set.

In the worst case–e.g. a signed base-d expansion $\sum_{j=0}^{n-1}(d-1)d^j$–a cascaded entangler is decomposed into multicontrolled INC$^{\pm 1}$ with a total number of $(d-1)\sum_{j=1}^{n} j = O(dn^2)$ control levels. This results in a total number of $O(dn^2k)$ $\wedge_1$ and $\wedge_2$ gates in the decomposition as well as $O(dn^2k)$ many single-qubit operations.

One accomplishment of this paper is the formulation of the decomposition algorithm based on arbitrary signed base-d extensions of natural numbers which may allow a significant reduction in the number of required gates over the standard d-ary extension as shown in Examples 5 and 6.

B. Outlook and open questions

It was verified by brute force that the signed base-d expansions in Examples 5 and 6 are indeed those that lead to the minimum of overall control levels as well as the simultaneous minimum of required $\wedge_1$ and $\wedge_2$ gates according to the presented further $\wedge_2$ decomposition scheme. Unfortunately there is no efficient algorithm known for the computation of an optimal signed base-d expansion. This is an open question even for the qubit case [18]. In the higher-dimensional case the trade-off between the summands (multicontrolled INC gates) and their exponents (control levels) depends, moreover, on the qudit dimension d and hence turns into an even more complicated multiparameter optimization problem.

Of course one can at least improve the performance over the standard d-ary representation by considering other efficiently computable signed base-d expansion schemes in comparison. In this spirit, Ref. [18] proposes a specific recursive algorithm and numerically confirms that it outperforms the standard binary expansion for most natural numbers. This algorithm is easy to adapt for the qudit case.

It seems plausible that the way over multicontrolled INC operations leads to the minimal number of $\wedge_1$ and $\wedge_2$ gates required for the decomposition of a cascaded entangler (taking canceling effects into consideration). Thinking about the optimal decomposition of cascaded entanglers into multicontrolled INC operations, it seems, moreover, intuitively reasonable to consider only those schemes which directly correspond to a signed base-d expansion of the represented number. If this intuition should be confirmed, the question in [18] about the complexity of cascaded entanglers is equivalent to the question of the optimal signed base-d expansion of natural numbers.

Beyond the reduction of the problem to cascaded entanglers it remains to study other decomposition methods for diagonal unitaries under the aspect of phase spareness in order to improve the scaling of $O(dn^2k)$. A compelling but nontrivial candidate for this is the best-known qubit algorithm [17] with a scaling of $O(2^n)$ without phase-context consideration.

ACKNOWLEDGMENTS

We thank Tobias J. Osborne for discussions and assistance with the original idea that led to this work. The work was supported by ERC grants QFTCMPS and SIQS and by the DFG through cluster of excellence EXC 201, Quantum Engineering and Space-Time Research, and Research Training Group 1991.

[1] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy, Proc. R. Soc. London A **467**, 459 (2011).

[2] Y. Nakata and M. Murao, Diagonal quantum circuits: Their computational power and applications, Eur. Phys. J. Plus **129**, 1 (2014).

[3] X. Ni and M. V. den Nest, Commuting quantum circuits: Efficient classical simulations versus hardness results, Quantum Info. Comput. **13**, 54 (2013).

[4] K. Fujii and T. Morimae, Quantum commuting circuits and complexity of Ising partition functions, arXiv:1311.2128.

[5] A. Matsuo, K. Fujii, and N. Imoto, A quantum algorithm for additive approximation of Ising partition functions, Phys. Rev. A **90**, 022304 (2014).

[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, Cambridge, UK, 2010).

[7] J. Welch, D. Greenbaum, S. Mostame, and A. Aspuru-Guzik, Efficient quantum circuits for diagonal unitaries without ancillas, New J. Phys. **16**, 033040 (2014).

[8] C. Zalka, Simulating quantum systems on a quantum computer, Proc. R. Soc. London A **454**, 313 (1998).

[9] I. Kassal, S. P. Jordan, P. J. Love, M. Mohseni, and A. Aspuru-Guzik, Polynomial-time quantum algorithm for the simulation of chemical dynamics, Proc. Natl. Acad. Sci. U.S.A. **105**, 18681 (2008).

[10] Y. Nakata, C. Hirche, C. Morgan, and A. Winter, Decoupling with random diagonal-unitary matrices, arXiv:1509.05155.

[11] Y. Nakata, C. Hirche, C. Morgan, and A. Winter, Implementing unitary 2-designs using random diagonal-unitary matrices, arXiv:1502.07514.

[12] S. S. Bullock, D. P. OLeary, and G. K. Brennen, Asymptotically Optimal Quantum Circuits for d-Level Systems, Phys. Rev. Lett. **94**, 230502 (2005).

[13] G. K. Brennen, S. S. Bullock, and D. P. OLeary, Efficient circuits for exact-universal computations with qudits, Quantum Info. Comput. **6**, 436 (2006).

[14] G. Cybenko, Reducing quantum computations to elementary unitary operations, Comput. Sci. Eng. **3**, 27 (2001).

[15] Y. Shi, Both Toffoli and controlled-NOT need little help to do universal quantum computation, Quantum Info. Comput. **3**, 84 (2003).

[16] R. R. Tucci, A rudimentary quantum compiler, arXiv:quant-ph/9902062.

[17] S. S. Bullock and I. L. Markov, Asymptotically optimal circuits for arbitrary n-qubit diagonal computations, Quantum Info. Comput. **4**, 27 (2004).

[18] J. Welch, A. Bocharov, and K. M. Svore, Efficient approximation of diagonal unitaries over the Clifford + T basis, Quantum Info. Comput. **16**, 87 (2016).

[19] Y. M. Di and H. R. Wei, Synthesis of multivalued quantum logic circuits by elementary gates, Phys. Rev. A **87**, 012325 (2013).

[20] A. D. Greentree, S. G. Schirmer, F. Green, L. C. L. Hollenberg, A. R. Hamilton, and R. G. Clark, Maximizing the Hilbert Space for a Finite Number of Distinguishable Quantum States, Phys. Rev. Lett. **92**, 097901 (2004).

[21] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. OBrien, A. Gilchrist, and A. G. White, Quantum computing using shortcuts through higher dimensions, Nature Phys. **5**, 134 (2009).

[22] A. Muthukrishnan and J. Stroud, Multivalued logic gates for quantum computation, Phys. Rev. A **62**, 052309 (2000).

[23] D. Rosenbaum and M. Perkowski, Efficient implementation of controlled operations for multivalued quantum logic, in *Proceedings of the IEEE 39th International Symposium on Multiple-Valued Logic, Naha, Okinawa, Japan, 21–23 May 2009* (IEEE, New York, 2009), pp. 86–91.

[24] S. S. Ivanov, H. S. Tonchev, and N. V. Vitanov, Time-efficient implementation of quantum search with qudits, Phys. Rev. A **85**, 062321 (2012).

[25] Y. Fan, Applications of multi-valued quantum algorithms, arXiv:0809.0932v4.

[26] H. Y. Li, C. W. Wu, W. T. Liu, P. X. Chen, and C. Z. Li, Fast quantum search algorithm for databases of arbitrary size and its implementation in a cavity QED system, Phys. Lett. A **375**, 4249 (2011).

[27] Y. Wang and M. Perkowski, Improved complexity of quantum oracles for ternary Grover algorithm for graph coloring, in *Proceedings of the IEEE 41st International Symposium on Multiple-Valued Logic, Tuusula, Finland, May 2011* (IEEE, New York, 2011), pp. 294–301.

[28] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner, Decoupling with unitary approximate two-designs, New J. Phys. **15**, 053022 (2013).

[29] J.-L. Brylinski and R. K. Brylinski, Universal quantum gates, in *Mathematics of Quantum Computation*, edited by R.-K. Brylinski and G. Chen (Chapman and Hall/CRC, London, 2002).

[30] 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).

[31] G. D. Hachtel and F. Somenzi, *Logic Synthesis and Verification Algorithms*, 1st softcover ed. (Springer, Berlin, 2006).

[32] V. Annampedu and M. D. Wagh, Decomposition of threshold functions into bounded fan-in threshold functions, Info. Comput. **227**, 84 (2013).