Asymptotically Optimal Circuits for Arbitrary n-qubit Diagonal Computations*

Stephen S. Bullock and Igor L. Markov
N.I.S.T.-Gaithersburg & The University of Michigan
stephen.bullock@nist.gov imarkov@eecs.umich.edu

September 14, 2018

Abstract

A unitary operator $U = \sum_{j,k} u_{j,k}|k\rangle\langle j|$ is called *diagonal* when $u_{j,k} = 0$ unless $j = k$. The definition extends to quantum computations, where j and k vary over the 2^n binary expressions for integers $0, 1 \cdots, 2^n - 1$, given n qubits. Such operators do not affect outcomes of the projective measurement $\{\langle j| \; ; \; 0 \leq j \leq 2^n - 1\}$ but rather create arbitrary relative phases among the computational basis states $\{|j\rangle \; ; \; 0 \leq j \leq 2^n - 1\}$. These relative phases are often required in applications.

Constructing quantum circuits for diagonal computations using standard techniques requires either $O(n^2 2^n)$ controlled-not gates and one-qubit Bloch sphere rotations or else $O(n2^n)$ such gates and a work qubit. This work provides a recursive, constructive procedure which inputs the matrix coefficients of U and outputs such a diagram containing $2^{n+1} - 3$ alternating controlled-not gates and one-qubit z-axis Bloch sphere rotations. Up to a factor of two, these circuits are the smallest possible. Moreover, should the computation U be a tensor of diagonal one-qubit computations of the form $R_z(\alpha) = e^{-i\alpha/2}|0\rangle\langle 0| + e^{i\alpha/2}|1\rangle\langle 1|$, then a cancellation of controlled-not gates reduces our circuit to that of an n-qubit tensor.

1 Introduction

Let $U(N) = \{V \text{ an } N \times N \text{ matrix} \; ; \; VV^* = \mathbf{1}\}$, where $\mathbf{1}$ is an identity matrix and $V^* = \bar{V}^t$ is the mathematical notation for the adjoint. One may view $U(N)$ as the set of all reversible quantum computations acting on n qubits. Then our usual convention is that algorithms for *quantum circuit synthesis* input such a $V \in U(N)$ and output a quantum circuit diagram for V, up to global phase. Several distinct quantum circuits may realize the same computation V. Thus, one seeks circuits for which the total number of gates is small. This work focuses on the case where the input computation is diagonal.

Gate counts for quantum circuits are often made in terms of *basic gates* [1], i.e., the set of all controlled-not gates and one-qubit computations. Our gate counts will be made with respect to the following gate library. We refer to elements as *elementary gates*, in contrast to basic gates.

1. For $1 \leq j \leq n$, apply $R_y(\theta) \in U(2^1)$ on line j, where

$$\begin{aligned} R_y(\theta) \;=\; & \cos\tfrac{\theta}{2}\,|0\rangle\langle 0| + \sin\tfrac{\theta}{2}\,|0\rangle\langle 1| \\ & - \sin\tfrac{\theta}{2}\,|1\rangle\langle 0| + \cos\tfrac{\theta}{2}\,|1\rangle\langle 1|,\; 0 \leq \theta < 2\pi \end{aligned} \tag{1}$$

is a y-axis Bloch sphere rotation [12, §4.2].

2. For $1 \leq j \leq n$, apply $R_z(\alpha) \in U(2^1)$ on line j, where

$$R_z(\alpha) = e^{-i\alpha/2}\,|0\rangle\langle 0| + e^{i\alpha/2}|1\rangle\langle 1|, \quad 0 \leq \theta < 2\pi \tag{2}$$

is a z-axis Bloch sphere rotation [12, §4.2].

3. Let $1 \leq j,k \leq n$, let $b_1, b_2, \cdots, b_n$ be n variables varying in the field of two elements $\mathbb{F}_2$, and let $x, y \mapsto x \oplus y$ denote the exclusive-or (XOR) operator which is addition in $\mathbb{F}_2$. The final type of elementary gate is the j-controlled-not gate acting on line k. We denote it by C_j^k. In case $j < k$,

$$C_j^k = \sum_{0 \leq b_1 \cdots b_n \leq N-1} |b_1 \cdots b_j \cdots (b_j \oplus b_k) \cdots b_n\rangle\langle b_1 \cdots b_j \cdots b_k \cdots b_n| \tag{3}$$

The other case $k < j$ is similar.

The elementary gate library is universal because any $V \in U(N)$ factors into basic gates [1] and any one-qubit computation W can be decomposed into $W = e^{i\Phi} R_y(\theta_1) R_z(\alpha) R_y(\theta_2)$ for $e^{i\Phi}$ an unmeasurable global phase [1, Lemma4.1] [12, §4.2]. Moreover, the asymptotics $\Omega(-)$, $O(-)$, and $\Theta(-)$ of the counts in either gate library are identical, since every elementary gate is basic while every basic gate factors into at most three elementary gates.

We next set some conventions. Throughout, U is a diagonal quantum computation on n qubits. Thus, for $N = 2^n$, U acts on

*Partially supported by the University of Michigan mathematics department VIGRE grant and the DARPA QuIST program. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing official policies or endorsements, either expressed or implied, of employers and funding agencies.

the n-qubit state space which is the $\mathbb{C}$ span of the computational basis $\{|j\rangle\,;\,0 \le j \le N-1\}$. The j are typically written as binary integers. As U is diagonal, $U = \sum_{j=0}^{N-1} u_j |j\rangle\langle j|$. Moreover, U unitary implies $|u_j|^2 = 1$.

We denote the Lie group [9] of all diagonal computations on n-qubit states by A. The notation $A(n)$ may be used for emphasis. Observe that A is abelian, i.e., commutative.

Circuit synthesis algorithms that provably produce minimal gate counts are rare, difficult to construct, and have been published for special cases only [14]. Before stating our main result, we formalize a sense in which it is best possible.

Definition 1.1 Let $H \subset U(N)$ be an analytic subgroup. An n-qubit quantum circuit synthesis algorithm with inputs restricted to H is said to stably output to H iff i) it outputs at most a countably infinite number of quantum circuit topologies containing only elementary gates as inputs are varied over all of H and ii) for each such circuit topology τ, the corresponding computations remain in H for every variation of parameter on any $R_y(\theta)$, $R_z(\alpha)$ gate within τ. If ς is such a synthesis algorithm accepting any input from H and outputting stably to H, we put $\#\varsigma = \max\{\#\tau\,;\,\tau \text{ is a diagram output by } \varsigma\}$, where $\#\tau$ refers to the number of elementary gates in τ. We finally put

$$\ell(H) = \min\{\#\varsigma\,;\,\varsigma \text{ outputs stably to } H\} \tag{4}$$

Definition 1.2 Consider now a family $\{H(n) \subset U(2^n)\,;\,n \ge 1\}$ of analytic subgroups [9, p. 47]. A family of n-qubit synthesis algorithms $\{\varsigma(n)\,;\,n \ge 1\}$, each allowing for any input in $H(n)$ and outputting stably to $H(n)$, will be called *stably asymptotically optimal* iff $\#\varsigma(n) \in O(\ell[H(n)])$.

Theorem 1.3 *Any n-qubit diagonal computation $U \in A(n)$ may be realized by a quantum circuit holding $2^{n+1} - 3$ alternating controlled-not gates and z-axis Bloch sphere rotations $R_z(\theta)$. The construction is stably asymptotically optimal for $A(n)$.*

Remark 1.4 Two other comments should be made about the construction. First, it requires neither a work qubit [1] nor any $R_y(\theta)$ elementary gates. Second, should a n-qubit tensor of the form $\otimes_{j=1}^n R_z(\alpha_j)$ be input to the algorithm, the output will hold several cancelling controlled-not gates. After cancellation, the output will match the input. $\diamond$

As a benchmark, we describe in Section 2 a diagram for a given diagonal U using standard techniques. The technique hinges on a well-known circuit diagram for an $(n-1)$-qubit controlled element of $A(1)$. In the presence of one ancilla (work) qubit, this diagram holds $O(n2^n)$ basic or equivalently elementary gates. The cost rises to $O(n^2 2^n)$ when there is no ancilla qubit. Thus, the asymptotic cost of $O(2^n)$ of the synthesis algorithm of the Theorem (see Section 4) compares favorably with known results. Moreover, dimension counts during the argument for stably asymptotically optimal will make clear that synthesizing large subsets of A requires $\ge 2^n - 1$ elementary gates. In this specialized sense, $\Omega(2^n)$ gates are required, and the diagram of Section 4 proves that diagrams for generic diagonal computations cost $\Theta(2^n)$ elementary (or basic) gates.

See Figure 1 for the overall circuit topology in the case $n = 3$ qubits. We defer a description of the algorithm for computing the R_z angles to the body and next discuss potential applications.

The first application is in conjunction with the standard synthesis algorithm [1, 3] [12, §4.5], which may be formalized using the QR matrix decomposition [4, 3]. For $V \in U(N)$, the algorithm uses a matrix factorization $V = QR$, where Q is a product of Givens rotations [3] realizable as $(n-1)$-controlled one-qubit computations and R is diagonal. Should the projective measurement $\{\langle j|\,;\,0 \le j \le N-1\}$ follow V, one need not apply R.

Consider instead the following situation. For $p << n$, a desired computation $V \in U(N)$ is known to arise from $V_1, V_2, \cdots, V_{n-p+1} \in U(2^p)$ as follows. First V_1 is applied on lines $1, 2, \cdots, p$, after which V_2 is applied on lines $2, 3, \cdots, p+1$, and so on until finally V_{n-p+1} is applied on lines $n-p+1, n-p+2, \cdots n$. If quantum computing technology has progressed so that $O(np2^p)$ elementary gates may be realized directly, one may factor each $V_1 = Q_1R_1, V_2 = Q_2R_2, \ldots V_{n-p+1} = Q_{n-p+1}R_{n-p+1}$ and apply the standard synthesis algorithm on each subblock. However, with the convention that $\{\langle j|\,;\,0 \le j \le N-1\}$ is only applied after the entire computation V, we now need quantum circuits realizing each of the $R_1, R_2, \cdots, R_{n-p+1}$. The synthesis algorithms proposed in this paper provide these. Moreover, note that essential part of the argument is merely the overlap of the smaller blocks, not their pattern.

Two further instances commonly arise where one needs to be careful about relative phases of computational basis states.

- Suppose that for $V \in U(2^{n-1})$, one wishes to build a circuit for the computation $(\mathbf{1} \oplus V) \in U(2^n)$ which applies V iff the top line carries $|1\rangle$. Suppose one has a circuit for V, correct up to relative phase. For example, such results from the factorization of Q into Givens rotations using $V = QR$ [3]. A straightforward approach is to condition every gate in Q, so that e.g. conditioned-not gates in Q correspond to Toffoli computations in $\mathbf{1} \oplus Q$. Yet $\mathbf{1} \oplus R$ will affect measurements in the n-qubit computational basis, unlike the diagonal computation R in $(n-1)$ qubits. One even needs a conditioned gate for the *global* phase of the original V.
- Moreover, circuits for diagonal computations are required whenever the final projective measurement [12, §2.2.5] is not $\{\langle j|\,;\,0 \le j \le N-1\}$.

Another possible application of circuits for diagonal quantum computations is to reduce the synthesis of arbitrary quantum computations to the synthesis of real quantum computations [13], i.e., of those $V \in O(N) = \{V \in U(N)\,;\,V = \bar{V}\}$. For there is a matrix decomposition $U(N) = O(N)\ A\ O(N)$. Indeed,

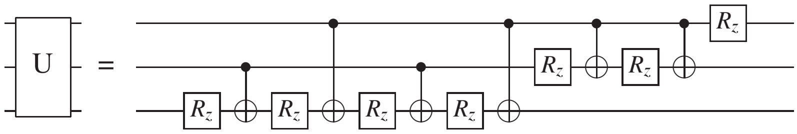

Figure 1: This diagram shows the circuit structure realizing a three qubit diagonal computation using our circuit synthesis algorithm. The general algorithm applies in n rather than merely three qubits and extends the construction of Section 2.2 of a previous work [2]. Should the input diagonal be of the form $U = R_z(\alpha_1) \otimes R_z(\alpha_2) \otimes R_z(\alpha_3)$, the second, third, fourth, and sixth R_z gates of the output diagram are trivial, implying that all controlled-not gates cancel. The output then coincides with the input.

this is a special case of the KAK metadecomposition [9, 8, 2]. Thus if $V \in U(N)$ is arbitrary, we may write $V = O_1 U O_2$ for $O_1, O_2 \in O(N)$ real quantum computations and $U \in A(n)$. The present work produces a circuit for $U \in A(n)$, reducing the question of a circuit for $V \in U(N)$ to circuits for $O_1, O_2 \in O(N)$.

Finally, we expect further applications to other quantum circuit synthesis algorithms relying on other examples of the KAK matrix metadecomposition. Another such example is the `Cosine-Sine` decomposition[17]. This decomposition states that one may write any $V \in U(N)$ as $V = (U_1 \oplus U_2) W (U_3 \oplus U_4)$ for $U_1, U_2, U_3, U_4 \in U(N/2)$ and W a sparse matix whose nonzero entries are paired cosines and sines. A quantum circuit for the matrix W may be synthesized using the algorithm of this paper. Indeed, let $S = |0\rangle\langle 0| + i|1\rangle\langle 1|$ and H denote the Hadamard gate, costing one and two elementary gates respectively [2]. Then for $\mathbf{1}$ an $(N/2) \times (N/2)$ identity matrix, one may compute that $U = [SH \otimes \mathbf{1}] W [(SH)^* \otimes \mathbf{1}] \in A$ is a diagonal computation. Hence, one may implement the nonrecursive portion of `Cosine-Sine` synthesis using the methods of this paper and six extra elementary gates.

We briefly outline the body of the paper. Section 2 describes an algorithm for building quantum circuits for diagonal computations which is analogous to an unoptimized version of classical two-level synthesis of logic functions. This algorithm produces $O(n2^n)$ gates with a single ancilla qubit and $O(n^2 2^n)$ gates else. Section 3 outlines how to use Lie theory [9] to recognize when $U_n \in A(n)$ factors as a tensor on line n, i.e., case $U_n = U_{n-1} \otimes R_z(\alpha)$ for $U_{n-1} \in A(n-1)$. Section 4 motivates and describes the recursive construction of the circuits of Theorem 1.3. Finally, Section 5 discusses dimension counts required for the lower bounds proving that our circuit diagrams are generically asymptotically optimal. Appendix A gives a construction similar to that of the Theorem, using $(n-1)$-controlled R_z gates.

Finally, some mathematical background beyond that usually associated to the quantum computing literature [12] is required to understand the arguments in this manuscript. The constructive synthesis algorithm makes use of the Lie theory of commutative matrix groups [9]. The argument for stable lower bounds makes use of the theory of smooth manifolds as is commonly treated in differential topology [5].

2 Prior Work

Circuits with measurement gates of Hogg et al.

Hogg et al. [7] consider synthesis of quantum circuits for diagonal computations from a much different perspective. Their main result is polynomial-size circuits, but in somewhat different circumstances compared to our work.

- The diagonal computations $U = \sum_{j=0}^{N-1} u_j |j\rangle\langle j|$ to which the prior result applies are required to have many u_j repeat. Indeed, accounting for the global phase, one supposes a family of diagonal computations $\{U_n = \sum_{j=0}^{N-1} u_{n,j} |j\rangle\langle j| \; ; n \geq 1\}$ where $\#\{u_{n,j} \neq 1 \; ; 0 \leq j \leq 2^n - 1\}$ scales as some polynomial $p(n)$.

- Moreover, the algorithm chosen in later steps depends on outputs of measurements of the quantum memory state in earlier steps. In the construction of classical circuits, the gate count would be increased by at least one `MUX` (if-then-else) gate for each classical branching, and each unique u_j contributes such a branching. The presense of measurement gates moreover takes their algorithm out of the present context of reversible gate libraries.

- The circuits ibid. would be large on a generic input of $\otimes_{j=1}^{n} R_z(\alpha_j)$ due to little repetition in the input phases. Thus, a separate section [7, §4] describes a precomputation to determine whether an input is of the form $\otimes_{j=1}^{n} R_z(\alpha_j)$. If this is the case, one should instead choose the tensor diagram. In contrast, given an input $U = \otimes_{j=1}^{n} R_z(\alpha_j)$, our output circuits automatically contain several cancelling controlled-nots's. After cancellation, one recovers the input tensor.

Despite these caveats, the citation above does include some of the discussion of the next subsection.

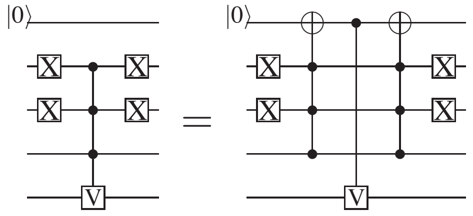

Figure 2: For $S = \{1,2\} \subset \{1,2,3\}$, this figure shows at left $[X^{\delta_S} \otimes \mathbf{1}] \circ \Lambda_{\{1,2,3\}}(V) \circ [X^{\delta_S} \otimes \mathbf{1}]$. At right is the first reduction of this circuit in a common implementation [1].

Analogies to classical two-level logic

We briefly recall classical two-level synthesis in order to contrast our circuits with this technique. Thus, let $\mathbb{F}_2$ denote the field of two elements, and $b \in \mathbb{F}_2$ also denote either a Boolean value or an integer of $\{0,1\}$. In this section, let $\bar{b} = b_1 b_2 \cdots b_n \in (\mathbb{F}_2)^n$ denote an n-bit string. Suppose $\varphi : (\mathbb{F}_2)^n \to \mathbb{F}_2$ describes an n-to-1 Boolean function we wish to realize with a circuit in the classical, irreversible AND-OR-NOT gate library. A textbook technique [6] is the two-level approach. Briefly, take $b_1, b_2, \cdots b_n$ as variables, and let $\bar{c} = c_1 c_2 \cdots c_n \in (\mathbb{F}_2)^n$ be a fixed bit string with $\varphi(\bar{c}) = 1$. Denote by $\delta_{\bar{c}}$ the indicator function of $\bar{c}$, i.e., $\delta_{\bar{c}} : (\mathbb{F}_2)^n \to \mathbb{F}_2$ has $\delta_{\bar{c}}(\bar{c}) = 1$ and $\delta_{\bar{c}}(\bar{b}) = 0$ for $\bar{b} \neq \bar{c}$. Then we have

$$\delta_{\bar{c}} = [\mathtt{NOT}^{c_1 \oplus 1}(b_1)]\mathtt{AND}[\mathtt{NOT}^{c_2 \oplus 1}(b_2)]\mathtt{AND} \cdots [\mathtt{NOT}^{c_n \oplus 1}(b_n)], \quad (5)$$

where the AND gates are equivalently multiplication in $\mathbb{F}_2$. Moreover, if $\{\bar{c}_1, \bar{c}_2, \cdots, \bar{c}_\ell\} = \{\bar{b} \in (\mathbb{F}_2)^n \; ; \; \varphi(\bar{b}) = 1\}$, then the expression

$$\varphi = \; \delta_{\bar{c}_1} \; \mathtt{OR} \; \delta_{\bar{c}_2} \; \mathtt{OR} \cdots \mathtt{OR} \; \delta_{\bar{c}_\ell} \quad (6)$$

provides an AND $-$ OR $-$ NOT circuit. For generic φ with $\ell \approx 2^{n-1}$, note this classical two-level circuit requires $O(2^{n-1})$ gates.

Optimizing such two-level circuits is NP-hard [6], and the problem has been studied extensively since the late 1960s. Algorithms and tools for this problem, e.g. Espresso, are widely known, and some are used in commercial circuit design tools. More recently, two-level decompositions in the AND-XOR-NOT gate library have been introduced. This is still universal, as any $b_1, b_2 \in \mathbb{F}_2$ have $(b_1 \; \mathtt{OR} \; b_2) = b_1 \oplus b_2 \oplus (b_1 \; \mathtt{AND} \; b_2)$. Publicly available tools for such ESOP-decomposition include EXORCISM-4 [11, 15]. We mention this transition OR $\mapsto$ XOR as it is loosely analogous to our change in strategy from Section A to Section 4. Other work on ROM-based quantum computation [16] has also made use of XOR based two-level synthesis.

We extend these ideas to build a simple circuit for $U = \sum_{j=0}^{N-1} u_j |j\rangle\langle j|$ costing $O(n2^n)$ elementary (or basic) gates. Recall standard notation uses $\Lambda_k(V)$ to denote a $k-$controlled V gate for $V \in U(2^1)$ [1]. We extend this notation slightly, in view of this section and Appendix A.

Definition 2.1 In n-qubits, let $S \subset \{1,2,\cdots n-1\}$ and $V \in U(2^1)$. Then $\Lambda_S(V)$ denotes the particular instance of $\Lambda_{\#S}(V)$ controlled by lines $\{j \in S\}$ and acting on line n.

Definition 2.2 In n qubits, let $S \subset \{1,2,\cdots n-1\}$. Then $\delta_S : (\mathbb{F}_2)^n \to \mathbb{F}_2$ is given by $\delta_S(j) = 1$ iff $[(j \neq n)$ and $(j \in S)]$. For $X = |1\rangle\langle 0| + |0\rangle\langle 1|$ a Pauli-X gate, we write $X^{\delta_S} = \otimes_{j=1}^n X^{\delta_S(j)}$. If $0 \leq j \leq N/2-1$, then $S(j) \subset \{1,2,\cdots n-1\}$ is the subset

$$S(j) = \{0 \leq k \leq N/2-1 \; ; \; c_k = 1 \text{ for } j = \bar{c} = c_1 c_2 \cdots c_{n-1}\}$$

Finally, for $S \subset \{1,2,\cdots n-1\}$, the number $k(S)$ is that integer k such that $S = S(k)$.

We now detail one construction of a circuit for $U = \sum_{j=0}^{N-1} u_j |j\rangle\langle j|$. Let $0 \leq k \leq N-1$, and $k \equiv 0 \bmod 2$. Let $V_k = u_k|0\rangle\langle 0| + u_{k+1}|1\rangle\langle 1|$, a one-qubit computation. Label

$$U_k = u_k|k\rangle\langle k| + u_{k+1}|k+1\rangle\langle k+1| + \sum_{j \neq k, j \neq k+1} |j\rangle\langle j| \quad (7)$$

Then we have the following expression.

$$U_k = [X^{\delta_{S(k/2)}} \otimes \mathbf{1}] \; \Lambda_{\{1,2,\cdots,n-1\}}(V_k) \; [X^{\delta_{S(k/2)}} \otimes \mathbf{1}] \quad (8)$$

Moreover, all such U_k commute. Thus for any enumeration of subsets $S_1, \cdots, S_{N/2} \subset \{1,2,\cdots n-1\}$,

$$\begin{aligned} U \;\; = \;\; & [X^{\delta_{S_1}} \otimes \mathbf{1}] \; \Lambda_{\{1,2,\cdots,n-1\}}(V_{k(S_1)}) \; [X^{\delta_{S_1}} \otimes \mathbf{1}] \circ \\ & [X^{\delta_{S_2}} \otimes \mathbf{1}] \; \Lambda_{\{1,2,\cdots,n-1\}}(V_{k(S_2)}) \; [X^{\delta_{S_2}} \otimes \mathbf{1}] \circ \cdots \circ \\ & [X^{\delta_{S_{N/2}}} \otimes \mathbf{1}] \; \Lambda_{\{1,2,\cdots,n-1\}}(V_{k(S_{N/2})}) \; [X^{\delta_{S_{N/2}}} \otimes \mathbf{1}] \end{aligned} \quad (9)$$

This directly produces a quantum circuit built out of subblocks such as the one illustrated in Figure 2.

Before passing to the asympotitcs, we note an optimization. A *Grey code* [12, §4.5.2] produces a sequence $S_1, S_2, S_3 \cdots S_{N/2}$ with $\#(S_k \cap S_{k+1}) = 1, 1 \leq k \leq N/2-1$. Sample Grey codes are recalled with $n-1 = 1,2,3$, where we write $k(S)$ for each subset:

$$\begin{array}{l} 0,1 \\ 00,01,10,11 \\ 000,001,010,011,111,110,101,100 \end{array} \quad (10)$$

By using a Grey code in the choice of enumeration of the subset for equation 9, we obtain a massive cancellation of inverters leaving only $N/2$ such X gates.

Figure 2 recalls the remaining facts justifying the $O(n2^n)$ gate count for this synthesis algorithm. Namely, each of the $N/2$ computations $\Lambda_{n-1}(V)$ require $O(n^2)$ basic gates absent an ancilla qubit or $48n-164$ basic gates with an ancilla qubit present [1]. Summing produces asymptotics of $O(n2^n)$ elementary or basic gates with the ancilla present and $O(n^2 2^n)$ gates without the ancilla present. In contrast, the circuits of Theorem 1.3 described in Section 4 require no ancilla and cost $O(2^n)$ gates.

3 Tensors and characters

The recursive proccess of the two new synthesis algorithms for diagonal quantum computations in Section 4 and Appendix A both rely on well-known ideas from Lie theory [9]. Specifically, it is typical to study Lie groups and most especially commutative Lie groups using their character functions. For G a Lie group, a character is a function $\chi : G \to \mathbb{C} - \{0\}$ with $\chi(gh) = \chi(g)\chi(h)$. The motivating example is the following group and character.

$$\begin{aligned} G &= GL(n,\mathbb{C}) = \{M \ n\times n \text{ complex matrix} \ ; \ \exists\, M^{-1}\} \\ \chi &= \det : GL(n,\mathbb{C}) \to \mathbb{C} - \{0\} \end{aligned}$$

Note that for any character, $\log\chi(gh) = \log\chi(g) + \log\chi(h)$ and by continuity $\log\chi(g^a) = a\log\chi(g)$ for $g,h \in G, a \in \mathbb{R}$. This will be useful in the sequel.

We seek an obstruction η to writing $U_n \in A(n)$ as $U_{n-1} \otimes R_z(\alpha)$, written in terms of characters. First, let us classify which diagonal U_n may be written in this way.

Proposition 3.1 (cf. [2, §2.2]) *Let $U = \sum_{j=0}^{N-1} u_j |j\rangle\langle j|$. Then there exists $V = \sum_{j=0}^{N/2-1} v_j|j\rangle\langle j|$ in $A(n-1)$ and $W = w_0|0\rangle\langle 0| + w_1|1\rangle\langle 1|$ a one-qubit diagonal so that $U = V\otimes W$ if and only if*

$$u_0u_1^{-1} = u_2u_3^{-1} = u_4u_5^{-1} = \cdots = u_{N-2}u_{N-1}^{-1} \tag{11}$$

Proof: The check that such a tensor satisfies the chain of equalities is routine. For the opposite implication, let $U = \sum_{j=0}^{N-1} u_j|j\rangle\langle j|$. Then define the $W = u_0|0\rangle\langle 0| + u_1|1\rangle\langle 1|$. Now U being unitary demands $u_0 \neq 0$. Thus, choose in the expression for V that $v_0 = 1, v_1 = u_2/u_0, v_2 = u_4/u_0, \cdots, v_{N/2-1} = u_{N-2}/u_0$. The chain equality then implies $U = V\otimes W$. □

We now introduce the language for our obstruction η. Note that corollary 3.3 motivates these technical terms and is crucial to the constructions of Section 4 and Appendix A.

Definition 3.2 Let $U = \sum_{j=0}^{N-1} u_j|j\rangle\langle j|$ define coordinates on $A(n)$. For $1 \leq j \leq N/2-1$, we define character functions $\chi_j : A(n) \to \mathbb{C} - \{0\}$ by $\chi_j(U) = u_{2j-2}u_{2j-1}^{-1}u_{2j}^{-1}u_{2j+1}$. For $U \in A(n)$, we define the vector valued function $\eta : A(n) \to \mathbb{R}^{N/2-1}$ by $\eta(U) = -i\,[\log\chi_1(U) \ \log\,\chi_2(U) \ \cdots \ \log\chi_{N/2-1}(U)]^t$. Here, the superscript denotes the transpose of the typeset row vector, so that we follow that the usual convention of linear algebra that vector-valued functions output column vectors.

Corollary 3.3 *The function $\eta : A(n) \to \mathbb{R}^{N/2-1}$ has the following properties.*

- *$[U = V\otimes W$ for $V \in A(n-1), W \in A(1)] \iff [\eta(U) = \vec{0}]$*
- *For $U_1, U_2 \in A(n)$, we have $\eta(U_1U_2) = \eta(U_1) + \eta(U_2)$.*
- *For $U \in A(n)$, $a \in \mathbb{R}$, we have $\eta(U^a) = a\,\eta(U)$.*

Hence, the function $\eta(-)$ is a quantitative obstruction to writing U as a tensor on the last line. A heuristic for the algorithms of Sections 4 and A would then be the following.

1. Define a large enough set of parameter dependent circuit blocks in $A(n)$ so as to control all $N/2-1$ degrees of freedom of η. Note this number of degrees of freedom coincides with the number of nonempty subsets of the top lines $\{1,2,\cdots,n-1\}$.
2. Use the previous construction and the properties of η to append circuit blocks to U so that $\eta = \vec{0}$. Then the composition $\tilde{U} = V\otimes W$, with W some $R_z(\alpha)$ gate up to global phase.
3. Recurse on V.

In terms of this heuristic, the circuit blocks of Section A are the usual conditioned gates $\Lambda_k[R_z(\alpha)]$ [1], while Section 4 requires a variant XOR-controlled rotation. We denote this $\bigoplus_k[R_z(\alpha)]$, in analogy to the Λ of $\Lambda_k[V]$ being an enlarged version of the propositional logic symbol $\wedge$ for AND.

4 Synthesis using $\bigoplus_k[R_z(\alpha)]$

This section describes our main synthesis algorithm. Certain proofs are omitted due to their similarity to results of Appendix A. This appendix may be read first independently in order to motivate the constructions in this section.

Circuit blocks for $\bigoplus_k[R_z(\alpha)]$

We begin by making precise the notion of a k-fold XOR-controlled one-qubit computation $V \in U(2^1)$. Several circuits blocks holding $2k+1$ elementary gates are associated with this for $V = R_z(\alpha)$. Thus we first describe the $(k+1)$-qubit computation, then highlight a circuit optimized for cancellation in our application, and finally describe possible variant circuit blocks.

Definition 4.1 Let $k \geq 1$, $V \in U(2^1)$ a one-qubit quantum computation, and for $b_1, b_2, \cdots, b_{k+1} \in \mathbb{F}_2$ let the bit-string $b_1b_2\cdots b_{k+1}$ also denote the element of $\mathbb{Z}$ with this binary representation. Then the XOR-controlled V-computation controlled on lines $1,2,\cdots,k$ and acting on line $k+1$ is that $\bigoplus_k(V) \in U(2^{k+1})$ which extends linearly from

$$[\bigoplus_k(V)]|b_1b_2\cdots b_{k+1}\rangle = \begin{cases} |b_1\cdots b_k\rangle \otimes V|b_{k+1}\rangle, \text{ if} \\ \quad b_1\oplus b_2\oplus\cdots\oplus b_k = 0 \in \mathbb{F}_2 \\ |b_1b_2\cdots b_k\rangle\otimes \mathbf{V}^*|b_{k+1}\rangle, \text{ if} \\ \quad b_1\oplus b_2\oplus\cdots\oplus b_k = 1\in\mathbb{F}_2 \end{cases} \tag{12}$$

Here, $\mathbf{V}^* \in U(2^1)$ is the inverse or adjoint operator to V and the symbol $\oplus$ denotes the exclusive-OR operation which is also addition in $\mathbb{F}_2$. We take the convention that $\bigoplus_0(V)|b_1b_2\cdots b_n\rangle = |b_1b_2\cdots b_{n-1}\rangle\otimes V|b_n\rangle$. In n qubits, should $S \subset \{1,2,\cdots,n-1\}$

be a possibly empty subset, we write $\bigoplus_S(V)$ for the instance of $\bigoplus_{\#S}(V)$ conditioned on lines $\{j \in S\}$ and acting on line n.

In the application, we will use the circuit diagram for $\bigoplus_k[R_z(\alpha)]$ which follows from the following equation. Let $S \subset \{1,2,\cdots,n-1\}$, say nonempty, label $S=\{s_1,s_2,\cdots,s_k\}$, and finally let $\mathbf{1} \in U(N/2)$ denote an $(n-1)$-qubit identity computation. Recalling the controlled-not notation C_j^k from the Introduction one has

$$\bigoplus_S[R_z(\alpha)] = C_{s_1}^n C_{s_2}^n \cdots C_{s_{k-1}}^n C_{s_k}^n [\mathbf{1} \otimes R_z(\alpha)] C_{s_k}^n C_{s_{k-1}}^n \cdots C_{s_2}^n C_{s_1}^n \tag{13}$$

All controlled-not gates to either side of the $\mathbf{1} \otimes R_z(\alpha)$ term commute. The right hand side of figure 3 illustrates the corresponding circuits. These circuits require $2k+1$ elementary gates and are the implementation of $\bigoplus_k[R_z(\alpha)]$ used in our final circuit diagrams. For completeness, we briefly note possible variant circuit blocks of the same size.

Let $S \subset \{1,\cdots,n-1\}$ and $S \neq \emptyset$. Suppose $S=\{s_1,\cdots s_k\}$ with $s_1 < s_2 < \cdots < s_k$. Then another quantum circuit for $\bigoplus_S[R_z(\alpha)]$ arises from

$$\bigoplus_S[R_z(\alpha)] = \begin{array}{c} C_{s_1}^{s_2} C_{s_2}^{s_3} \cdots C_{s_{k-1}}^{s_k} C_{s_k}^n \; [\mathbf{1} \otimes R_z(\alpha)] \\ C_{s_k}^n C_{s_{k-1}}^{s_k} \cdots C_{s_2}^{s_3} C_{s_1}^{s_2} \end{array} \tag{14}$$

This is illustrated to the left in Figure 3.

Finally, although the controlled-not gates in the second diagram corresponding to the alternate Equation certainly do *not* commute, one may reorder the circuit in a certain sense. Let σ be a permutation of $\{1,\cdots,k\}$, retaining $S=\{s_1<s_2<\cdots<s_k\}$.

$$\bigoplus_S[R_z(\alpha)] = \begin{array}{c} C_{s_{\sigma(1)}}^{s_{\sigma(2)}} C_{s_{\sigma(2)}}^{s_{\sigma(3)}} \cdots C_{s_{\sigma(k-1)}}^{s_{\sigma(k)}} C_{s_{\sigma(k)}}^n \; [\mathbf{1} \otimes R_z(\alpha)] \\ C_{s_{\sigma(k)}}^n C_{s_{\sigma(k-1)}}^{s_{\sigma(k)}} \cdots C_{s_{\sigma(2)}}^{s_{\sigma(3)}} C_{s_{\sigma(1)}}^{s_{\sigma(2)}} \end{array} \tag{15}$$

See the left hand side of Figure 3.

Computation of $\eta(\bigoplus_S[R_z(\alpha)])$

We find it more convenient to use mathematical notation for vectors such as values of η rather than the `bra-ket` notation. We briefly recall the appropriate conventions, treated in more detail in Appendix A.

Definition 4.2 For $1 \leq j \leq N/2-1$, let e_j denote is the column vector in $\mathbb{R}^{N/2-1}$ with a single entry of 1 in the j^{th} row and all other entries 0. The vectors $v_j = e_j - e_{j+1}$ if $1 \leq j \leq N/2-2$, while $v_0 = -e_1$ and $v_{N/2-1} = e_{N/2-1}$.

The vectors $\{v_j\,; 1 \leq j \leq N/2-1\}$ form a basis for $\mathbb{R}^{2^{n-1}-1}$. We need one more definition before computing $\eta(\oplus_S[R_z(\alpha)])$.

Definition 4.3 Let $S=\{s_1,s_2,\cdots,s_k\} \subset \{1,2,\cdots,n-1\}$ be nonempty. In n qubits with $N=2^n$, let $1 \leq j \leq N/2-1$ with binary representation $j=b_1b_2\cdots b_{n-1}$ for $b_1,b_2,\cdots,b_{n-1} \in \mathbb{F}_2$. Then we say the integer j is XOR-S-conditioned iff $b_{s_1} \oplus b_{s_2} \oplus \cdots \oplus b_{s_k} = 1$. We further define the set

$$\mathcal{F}(S) = \{1 \leq j \leq N/2-1\,;\ j \text{ is XOR-}S\text{-conditioned}\} \tag{16}$$

By a *flip state* of S, we mean any $j \in \mathcal{F}(S)$, i.e., S-flip is an abbreviation of XOR-S-conditioned.

Example 4.4 Consider the special case of $n=4$ qubits. The flip states of each nonempty subset of $\{1,2,3\}$ of the top three lines are given in the table below, in binary.

subset	flip states
$\{1\}$	100, 101, 110, 111
$\{1,2\}$	010, 011, 100, 101
$\{1,3\}$	001, 011, 100, 110
$\{1,2,3\}$	001, 010, 100, 111
$\{2\}$	010, 011, 110, 111
$\{2,3\}$	001, 010, 101, 110
$\{3\}$	001, 011, 101, 111

Note that for any $S \neq \emptyset$, exactly half of the eight integers $0,1,\cdots,7$ are elements of $\mathcal{F}(S)$. ◇

Proposition 4.5 *Let $\mathcal{F}(S)$ be the set of flip states of any nonempty $S \subset \{1,2,\cdots,n-1\}$. Then*

$$\eta(\bigoplus_S[R_z(\alpha)]) = -2\alpha \sum_{j \in \mathcal{F}(S)} v_j \tag{17}$$

Also, for $S=\emptyset$, $\eta[\mathbf{1} \otimes R_z(\alpha)] = \vec{0}$.

The proof is similar to that of Proposition A.3. However, $\oplus_S[R_z(\alpha)]$ never leaves any computational basis state fixed, which accounts for the factor of two.

Example 4.6 Consider $n=4$ qubits for the subset $S=\{1,3\}$ and α arbitrary. For convenience, label $\phi=-\alpha/2$, so that $R_z(\alpha) = e^{i\phi}|0\rangle\langle 0| + e^{-i\phi}|1\rangle\langle 1|$. We leave it to the reader to check that $V=\bigoplus_S[R_z(\alpha)]$ is diagonal and merely describe the multiples on each computational basis state.

state	mult	state	mult	state	mult	state	mult
$\|0000\rangle$	$e^{i\phi}$	$\|0100\rangle$	$e^{i\phi}$	$\|1000\rangle$	$e^{-i\phi}$	$\|1100\rangle$	$e^{-i\phi}$
$\|0001\rangle$	$e^{-i\phi}$	$\|0101\rangle$	$e^{-i\phi}$	$\|1001\rangle$	$e^{i\phi}$	$\|1101\rangle$	$e^{i\phi}$
$\|0010\rangle$	$e^{-i\phi}$	$\|0110\rangle$	$e^{-i\phi}$	$\|1010\rangle$	$e^{i\phi}$	$\|1110\rangle$	$e^{i\phi}$
$\|0011\rangle$	$e^{i\phi}$	$\|0111\rangle$	$e^{i\phi}$	$\|1011\rangle$	$e^{-i\phi}$	$\|1111\rangle$	$e^{-i\phi}$

Thus, $\chi_1(V)=e^{4i\phi}$, $\chi_2(V)=e^{-4i\phi}$, $\chi_3(V)=e^{4i\phi}$, $\chi_4(V)=1$, $\chi_5(V)=e^{-4i\phi}$, $\chi_6(V)=e^{4i\phi}$, and $\chi_7(V)=e^{-4i\phi}$. Thus we have computed $\eta(\bigoplus_{\{1,3\}}[R_z(\alpha)]) = 4\phi i[1\ -1\ 1\ 0\ -1\ 1\ -1]^t$.

On the other hand, flip states for $\{1,3\}$ are given in binary by $j=001,011,100$, and 110. So $\mathcal{F}(S)=\{1,3,4,6\}$ and

$$(e_1-e_2)+(e_3-e_4)+(e_4-e_5)+(e_6-e_7) = [1\ -1\ 1\ 0\ -1\ 1\ -1]^t.$$

This concludes the example. ◇

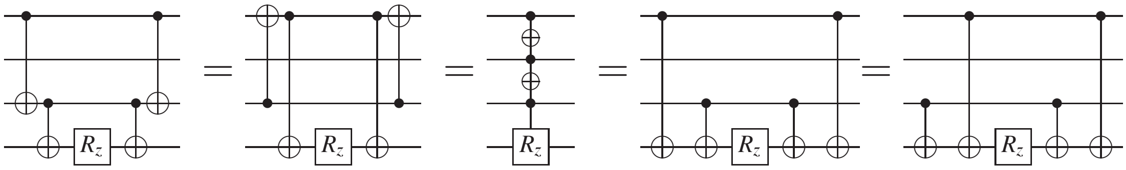

Figure 3: Shown at center is a symbol due to the authors for denoting XOR control. At right are circuits for $\bigoplus_S[R_z(\alpha)]$ per Equation 13, as used in the circuits diagonal computations. Here, $n = 4$ qubits and $S = \{1,3\} \subset \{1,2,3\}$, so this is an instance of $\bigoplus_2[R_z(\alpha)]$. At left are possible variaint circuits per Equations 14 and 15, where σ is an identity permutation and σ is the flip permutation of two elements.

$\bigoplus_k[R_z(\alpha)]$-block synthesis algorithm

The -0.5 radians in the Definition of the following matrix cancels the 2 coefficient in Equation 17, so that the resulting matrix has all entires in $\mathbb{Z}$. It is similar to Definition A.5.

Definition 4.7 The matrix $\eta^\oplus$ is the $(N/2-1)\times(N/2-1)$ real matrix defined as follows. Order nonempty subsets $S_1, S_2, \cdots, S_{N/2-1}$ in *Grey order*, omitting the empty set. Then for $1 \le j \le N/2-1$, the j^{th} column of $\eta^\oplus$ is $\eta(\bigoplus_{S_j}[R_z(-0.5 \text{ radians})])$.

Example 4.8 Computing the four-qubit case of $\eta^\oplus$ is most quickly accomplished using the table of example 4.4 and Proposition 4.5. The Grey order of nonempty subsets of $\{1,2,3\}$ is $\{3\},\{2,3\},\{2\},\{1,2\},\{1,2,3\},\{1,3\},\{1\}$. Thus the Definition in this case states

$$\eta^\oplus = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ -1 & 0 & 1 & 1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & -1 & 0 \\ -1 & 0 & -1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & -1 & -1 & 0 \\ -1 & 0 & 1 & -1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & -1 & 1 & 0 \end{pmatrix} \quad (18)$$

The fifth column recalls example 4.6. ◇

The matrix $\eta^\oplus$ has the following application. Note the right hand side is matrix multiplication with the column vector $\vec{\alpha}$.

Lemma 4.9 *Fix n qubits, with $N = 2^n$. Let $\vec{\alpha} = [\alpha_1 \cdots \alpha_{N/2-1}]^t$ be a vector of angles, $0 \le \alpha_j < 2\pi$, $1 \le j \le N/2-1$. Then for $S_1, S_2, \ldots S_{N/2-1}$ the Grey ordering of the nonempty subsets of the set of top lines $\{1,\cdots,n-1\}$,*

$$\eta(\oplus_{S_1}[R_z(\alpha_1)]\cdots\oplus_{S_{N/2-1}}[R_z(\alpha_{N/2-1})]) = -2\,\eta^\oplus\vec{\alpha} \quad (19)$$

The proof is quite similar to Lemma A.6. It uses Proposition 4.5 and properties of $\eta(-)$ following from each component being a character.

We now state the synthesis algorithm. It is critical in the following that $\eta^\oplus$ be invertible. This result will be proven in the next subsection.

XOR-Controlled Rotation Synthesis Algorithm Let $U = \sum_{j=0}^{N-1} u_j|j\rangle\langle j|$, for which we wish to synthesize a circuit diagram using $\bigoplus_k[R_z(\alpha)]$ blocks. Label $S_1, S_2, S_3 \ldots S_{N/2-1}$ the nonempty subsets of the top lines $\{1,\cdots,n-1\}$ in the *Grey order*.

1. Compute $\vec{\psi} = \eta(U)$.
2. Compute the inverse matrix $(\eta^\oplus)^{-1}$.
3. Compute $\vec{\alpha} = (-1/2)(\eta^\oplus)^{-1}\vec{\psi}$, treating $\vec{\psi}$ as a column vector. Label $\vec{\alpha} = [\alpha_1 \cdots \alpha_{N/2-1}]^t$.
4. Compute the diagonal quantum computation $\tilde{U} = \bigoplus_{S_1}[R_z(-\alpha_1)] \cdots \bigoplus_{S_{N/2-1}}[R_z(-\alpha_{N/2-1})]\ U$ As is verified below, $\tilde{U}$ is a tensor.
5. Use the argument of Proposition 3.1 to compute $\tilde{U} = V \otimes W$ for $V \in A(n-1)$ and $W = e^{i\Phi}R_z(\alpha_0)$ for some angle α_0.
6. Given prior computations, the following expression holds:
$$U = \bigoplus_\emptyset[R_z(\alpha_0)]\bigoplus_{S_1}[R_z(\alpha_1)]\cdots \bigoplus_{S_{N/2-1}}[R_z(\alpha_{N/2-1})]\ [V\otimes\mathbf{1}] \quad (20)$$
Here, $\mathbf{1}$ denotes the trivial computation of $U(2^1)$. Also, $\bigoplus_\emptyset[R_z(\alpha_0)]$ means $\mathbf{1}\otimes R_z(\alpha_0)$ for $\mathbf{1}\in U(2^{N/2})$.
7. Decompose each $\bigoplus_k R_z(\alpha)$ into elementary gates using the circuit diagrams at the right of Figure 3.
8. Using the Grey order and $C_j^nC_k^n = C_k^nC_j^n$, cancel all but one controlled-not between consecutive $R_z(\alpha)$ gates in the resutling diagram.
9. The algorithm terminates by recursively producing a circuit diagram for $V \in A(n-1)$.

Example 4.10 Consider the following 3-qubit computation:

$$\begin{aligned} U = {} & e^{4\pi i/12}|0\rangle\langle 0| + e^{2\pi i/12}|1\rangle\langle 1| + \\ & e^{9\pi i/12}|2\rangle\langle 2| + e^{7\pi i/12}|3\rangle\langle 3| + \\ & e^{3\pi i/12}|4\rangle\langle 4| + e^{8\pi i/12}|5\rangle\langle 5| + \\ & e^{11\pi i/12}|6\rangle\langle 6| + e^{10\pi i/12})|7\rangle\langle 7| \end{aligned} \quad (21)$$

We apply the synthesis algorithm above to U.

We begin by computing the 3-qubit case of $\eta^{\oplus}$. The Grey order is $\{1\},\{1,2\}$, and $\{2\}$.

$$\eta^{\oplus} = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix} \tag{22}$$

The inverse matrix appears in the algorithm and may be reused for multiple diagonal computations.

$$(\eta^{\oplus})^{-1} = (1/2) \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 1 & 2 & 1 \end{pmatrix} \tag{23}$$

Now $\vec{\psi} = \eta(U) = -i[\log\chi_1(U) \quad \log\chi_2(U) \quad \log\chi_3(U)]^t = [0 \;\; 7\pi/12 \;\; -6\pi/12]^t$. Thus computing the parameters for the $\bigoplus_S[R_z(\alpha)]$ blocks,

$$\vec{\alpha} = (-1/2)(\eta^{\oplus})^{-1}\vec{\psi} = [3\pi/24 \;\; -3\pi/24 \;\; -4\pi/24]^t \tag{24}$$

It should be the case that the computation $\tilde{U}$ given by

$$\bigoplus\nolimits_{\{1\}}[R_z(-3\pi/24)] \bigoplus\nolimits_{\{1,2\}}[R_z(3\pi/24)] \bigoplus\nolimits_{\{2\}}[R_z(4\pi/24)]\, U \tag{25}$$

has $\tilde{U} = V \otimes W$ for V a two-qubit diagonal and W a one-qubit diagonal. We verify this by computing matrix coefficients for $\tilde{U}$.

In the following computation, for given $R \in A$ we abbreviate $R = \sum_{j=0}^{N-1} r_j |j\rangle\langle j|$ as $R = \mathrm{diag}(r_0, r_1, \cdots, r_{N-1})$ in order to save space. The first step in computing $\tilde{U}$ is to compute $\bigoplus_{\{1\}}[R_z(4\pi/24)]$. Begin by noting that

$$\begin{aligned} \mathbf{1}\otimes\mathbf{1}\otimes R_z(4\pi/24) \;=\; & \mathrm{diag}(e^{-4\pi i/48}, e^{4\pi i/48}, e^{-4\pi i/48}, e^{4\pi i/48}, \\ & e^{-4\pi i/48}, e^{4\pi i/48}, e^{-4\pi i/48}, e^{4\pi i/48}) \end{aligned} \tag{26}$$

Associating the entries with $|000\rangle$, $|001\rangle$, etc., we reverse those pairs $|b_1b_2b_3\rangle$ with the binary integer $b_1b_2 \in \mathcal{F}(\{1\})$.

$$\begin{aligned} \oplus_{\{1\}}[R_z(4\pi/24)] \;=\; & \mathrm{diag}(e^{-4\pi i/48}, e^{4\pi i/48}, e^{-4\pi i/48}, e^{4\pi i/48}, \\ & e^{4\pi i/48}, e^{-4\pi i/48}, e^{4\pi i/48}, e^{-4\pi i/48}) \end{aligned} \tag{27}$$

We may similarly construct $\oplus_{\{1,2\}}[R_z(3\pi/24)]$.

$$\begin{aligned} \oplus_{\{1,2\}}[R_z(3\pi/24)] \;=\; & \mathrm{diag}(e^{-3\pi i/48}, e^{3\pi i/48}, e^{3\pi i/48}, e^{-3\pi i/48}, \\ & e^{3\pi i/48}, e^{-3\pi i/48}, e^{-3\pi i/48}, e^{3\pi i/48}) \end{aligned} \tag{28}$$

Finally, the flip states of $\{2\}$ are $j = 1, 3$. Thus

$$\begin{aligned} \oplus_{\{2\}}[R_(-3\pi/24)] \;=\; & \mathrm{diag}(e^{3\pi i/48}, e^{-3\pi i/48}, e^{-3\pi i/48}, e^{3\pi i/48}, \\ & e^{3\pi i/48}, e^{-3\pi i/48}, e^{-3\pi i/48}, e^{3\pi i/48}) \end{aligned} \tag{29}$$

Collecting all terms, we arrive at

$$\begin{aligned} \tilde{U} \;=\; & \mathrm{diag}(e^{-4\pi i/48}, e^{4\pi i/48}, e^{-4\pi i/48}, e^{4\pi i/48}, \\ & e^{4\pi i/48}, e^{-4\pi i/48}, e^{4\pi i/48}, e^{-4\pi i/48}) \circ \\ & \mathrm{diag}(e^{-3\pi i/48}, e^{3\pi i/48}, e^{3\pi i/48}, e^{-3\pi i/48}, \\ & e^{3\pi i/48}, e^{-3\pi i/48}, e^{-3\pi i/48}, e^{3\pi i/48}) \circ \\ & \mathrm{diag}(e^{3\pi i/48}, e^{-3\pi i/48}, e^{-3\pi i/48}, e^{3\pi i/48}, \\ & e^{3\pi i/48}, e^{-3\pi i/48}, e^{-3\pi i/48}, e^{3\pi i/48}) \circ \\ & \mathrm{diag}(e^{4\pi i/12}, e^{8\pi i/48}, e^{36\pi i/48}, e^{28\pi i/48}, \\ & e^{12\pi i/48}, e^{32\pi i/48}, e^{44\pi i/48}, e^{40\pi i/48}) \\ =\; & \mathrm{diag}(e^{12\pi i/48}, e^{12 i\pi/48}, e^{32\pi i/48}, e^{32 i\pi/48}, \\ & e^{22\pi i/48}, e^{22 i\pi/48}, e^{42\pi i/48}, e^{42 i\pi/48}) \end{aligned} \tag{30}$$

Thus $\tilde{U} = \mathrm{diag}(e^{12\pi i/48}, e^{32\pi i/48}, e^{22\pi i/48}, e^{42\pi i/48}) \otimes \mathrm{diag}(1,1)$. The odd happenstance that the latter tensor factor is an identity saves one gate.

Next, write out circuit diagrams for each $\bigoplus_S[R_z(\alpha)]$ per the right hand side of Figure 3. Since the chose the Grey order $\{1\},\{1,2\}$, $\{2\}$, cancelling controlled not gates produces the leftmost 8 elementary gates of figure 1. Finally, call the algorithm recursively on V. The two-qubit case coincides with other work [2, §2.2]. $\diamond$

Proof of Correctness

We briefly verify that $\tilde{U} = V \otimes W$. First use Proposition 4.5 for

$$\eta\big(\bigoplus\nolimits_{S_1}[R_z(-\alpha_1)] \cdots \bigoplus\nolimits_{S_{N/2-1}}[R_z(-\alpha_{N/2-1})]\,\big) = 2\eta^{\oplus}\vec{\alpha} \tag{31}$$

Now by definition $\vec{\alpha} = (-1/2)(\eta^{\oplus})^{-1}\vec{\psi}$, so that $2\eta^{\oplus}\alpha = -\vec{\psi}$.

$$\eta\big(\bigoplus\nolimits_{S_1}[R_z(-\alpha_1)] \cdots \bigoplus\nolimits_{S_{N/2-1}}[R_z(-\alpha_{N/2-1})]\,\big) = -\vec{\psi} \tag{32}$$

Then the property $\eta(U_1U_2) = \eta(U_1) + \eta(U_2)$ demands

$$\eta\big(\bigoplus\nolimits_{S_1}[R_z(-\alpha_1)] \cdots \bigoplus\nolimits_{S_{N/2-1}}[R_z(-\alpha_{N/2-1})]\, U\,\big) = -\vec{\psi} + \vec{\psi} = \vec{0} \tag{33}$$

So by the restatement of Proposition 3.1, we have $\tilde{U} = V \otimes W$.

There is one remaining unjustified (subtle) statement to check.

Proposition 4.11 $\eta^{\oplus}$ *is an invertible* $(N/2-1)\times(N/2-1)$ *real matrix for* $n \geq 1$.

Sketch: It is equivalent to consider the question for an alternate basis of $\mathbb{R}^{N/2-1}$. Thus, choose instead the vectors $\{v_j\,;\,1 \leq j \leq \mathbb{R}^{N/2-1}\}$ of Definition 4.2. In this alternate basis, the similar matrix M corresponding to $\eta^{\oplus}$ has an entry of 1 for the v_j component whenever j is a flip state for the j^{th}-set in Grey order.

Fix an nonempty subset S of $\{1,2,\cdots,n-1\}$, thus fixing a column of $\eta^{\oplus}$. We first claim there precisely 2^{n-2} flip states for S. To see this, observe that the equation $\oplus_{k\in S} b_k = 1$ satisfied by S-flip states defines an affine linear $\mathbb{F}_2$ subspace of the finite-dimensional vector space $(\mathbb{F}_2)^{2^{n-1}}$. Then this number of elements corresponds to the dimension count, since any ℓ dimensional vector space with $\mathbb{F}_2$-scalars must contain 2^ℓ elements.

Next, fix $S_1 \neq S_2$ distinct nonempty subsets. Then the associated columns of M share precisely 2^{n-3} positions in which each has a nonzero, unit entry. This is again a dimension count. Note that since S-flip states satisfy $\oplus_{k\in S} b_k = 1$, $S_1 \neq S_2$. Thus the codimension one subspaces corresponding to S_1 and S_2 intersect transversally in a codimension two subspace.

Given these claims, label $M = (m_{jk})$ and recall δ_j^k the Kronecker delta which is 1 for $j = k$ and zero else. Now considerations of the last two paragraphs demand that for the transpose (real adjoint) M^t, $M^t M = (m_{kj})(m_{j\ell}) = 2^{n-2}(\delta_j^\ell + 1)$. An omitted argument then shows $0 \neq \det(M^t M)$, demanding $(\det M)^2 \neq 0$. As M is invertible and $\eta^\oplus$ is similar to M, we must have $\eta^\oplus$ invertible. □

Gate Counts

Our circuit diagrams are built from blocks realizing $\bigoplus_S [R_z(\alpha)]$ at the right of Figure 3, and the choice of subsets in the Grey order causes a large cancellation of controlled-not gates which is required for the $O(2^n)$ asymptotic. We now justify the gate count of $2^{n+1} - 3$, which for $n = 2$ coincides with 5 gates [2, §2.2].

Except for the recursive call to V, the synthesis algorithm writes elementary gates realizing the following compution.

$$\bigoplus_\emptyset [R_z(\alpha_0)] \bigoplus_{S_1} [R_z(\alpha_1)] \cdots \bigoplus_{S_{N/2-1}} [R_z(\alpha_{N/2-1})] \tag{34}$$

Here, $\bigoplus_\emptyset [R_z(\alpha_0)] = (\mathrm{e}^{-i\Phi})(\mathbf{1} \otimes W)$ is the one-qubit gate resulting on the last tensor factor due to zeroing the obstruction $\eta(-)$. We have used the commutativity of $A(n)$ to move this computation to the front to preserve the full Grey order including $\emptyset$.

Now realize each of the $\bigoplus_S [R_z(\alpha)]$ blocks using the circuits at the right of Figure 3. Due to the Grey order, all but one controlled-not gate will cancel between any two consecutive R_z gates on the bottom line. Thus the gate count in terms of elementary gates from the Introduction should account for the following.

- 2^{n-1} controlled rotations R_z, since this is the number of possibly empty subsets of $\{1, 2, \cdots, n-1\}$.
- 2^{n-1} controlled-not gates, since one lies to the right of each R_z gate.

Thus prior to the recursive call, in $n \geq 2$ qubits the algorithm will place 2^n elementary gates.

To obtain the exact count, stop the recursive count at $n = 2$ qubits.

$$2^n + 2^{n-1} + \cdots + 8 + 4 = 2^{n+1} - 4 \tag{35}$$

The end case of recursion is for $n = 1$. Since any one-qubit diagonal may be written $\mathrm{e}^{i\Phi} R_z(\alpha)$, the remaining one-qubit diagonal requires one elementary gate. Thus the grand total is $2^{n+1} - 3$ elementary gates.

5 Stable Lower Bounds

The section justifies the claim of stably-asymptotical optimality in Theorem 1.3 using an argument similar to one by E. Knill [10, Theorem 3.4]. We provide a greater level of detail and tailor the discussion to synthesis within a subgroup $H \subset U(N)$. Our argument is what simpler because we are dealing with *elementary* gates from the Introduction while Knill uses *basic* gates [1].

Thus let $S \subset U(N)$. We introduce the following convention:

$$\tilde{S} = \{\mathrm{e}^{i\Phi} V \; ; \; 0 \leq \Phi < 2\pi, V \in S\} \tag{36}$$

This will allow us to ignore global phases in the following discussion. Note that $\tilde{A} = A$.

We now expand on comments made briefly in Definition 1.2 of the Introduction. A *circuit topology*[1] τ is an n-line diagram on which is marked a sequence of gate-holders. These gate-holders are either controlled-not gates joining any two lines or boxes labelled either Y or Z. To specialize the circuit topology τ to an actual circuit, one chooses paramaters for either an $R_y(\theta)$ gate or an $R_z(\alpha)$ gate to place into boxes labelled Y or Z respectively. We define $\#\tau$ to be the total of the number of controlled-nots and boxes, while $\dim\tau$ denotes the number of boxes. Label S_τ to be the subset of all $V \in U(N)$ that result from choosing particular parameters for a $R_y(\theta)$ gate in each Y box and an $R_z(\alpha)$ gate in each Z box. We say that τ specializes stably to an analytic subgroup $H \subset U(N)$ when $\tilde{S}_\tau \subset H$.

Lemma 5.1 *Suppose τ specializes stably to H and $\dim\tau + 1 < \dim H$. Then $\tilde{S}_\tau$ is a measure zero subset of H.*

Proof: We appeal to Sard's theorem from differential topology [5, p.39]. Consider the map $f : \mathbb{R}^{\dim\tau+1} \to U(N)$ which carries a tuple $(\Phi, t_1, t_2, \cdots, t_{\dim\tau+1})$ to the $\mathrm{e}^{i\Phi} V$ which is the phase $\mathrm{e}^{i\Phi}$ multiplied by the specialization of τ corresponding to $t_1, t_2, \cdots, t_{\dim\tau}$. This map is smooth.

By Sard's theorem [5, p.39], for all but a measure zero subset of $h \in H$ one of the following two cases hold:

- There is no choice of parameter v with $f(v) = h$.
- For each v with $f(v) = h$, the derivative linear map at the parameter v denoted $df_v : \mathbb{R}^{\dim\tau+1} \to T_h(H)$ is onto.

The second possibility is absurd by the dimension hypothesis. Thus $f(\mathbb{R}^{\dim\tau+1})$ is a measure zero subset of H. □

Proposition 5.2 *Fix n, and let ς be a quantum circuit synthesis algorithm inputting $a \in A(n)$ and outputting stably to $A(n)$. Then $\#\varsigma \geq 2^n - 1 = N - 1$.*

[1] We discuss here circuit topologies in the elementary gate library.

Proof: Let C be a countable set with $\{\tau(c)\ ;\ c \in C\}$ the set of topologies output by ς. Now $\dim A(n) = N$. Thus assume by way of contradiction $\#\varsigma < N-1$. Then we may write

$$A(n) = \cup_{c \in C} \tilde{S}_{\tau(c)} \tag{37}$$

This is impossible by Lemma 5.1. Indeed, a countable union of measure zero subsets is still measure 0 and hence can not cover $A(n)$. $\square$

Corollary 5.3 *Let $\{\varsigma(n)\}$ be a family of synthesis algorithms, each of which accepts all inputs from $A(n)$ and outputs stably to $A(n)$ per Definition 1.2. If $\#\varsigma(n) \in O(2^n)$, then $\{\varsigma(n)\}$ is stably asymptotically optimal.*

6 Conclusions and On-Going Work

We realize quantum circuits for any diagonal $U = \sum_{j=0}^{N-1} u_j |j\rangle\langle j|$ consisting of at most $2^{n+1}-3$ alternating controlled-not gates and z axis Bloch sphere rotations on individual qubits. The construction uses a new circuit block, the `XOR`-controlled rotation. This $O(2^n)$ construction is optimal in the following sense. In the worst-case and also the generic case, at least $2^n - 1$ one-qubit rotations are required to construct such a diagonal U. Thus our constructive algorithm shows that the synthesis of quantum circuits for diagonal computations is in fact $\Theta(2^n)$. Note that special-case computations such as tensors of one-qubit diagonal computations may require fewer gates.

The circuits above have several common applications. For example, they are useful when constructing a circuit for a top-conditioned V computation given a circuit diagram for V correct up to relative phase. They are also needed when applying projective measurements other than the typical $\{\langle j|\ ;\ 0 \le j \le N-1\}$. In our ongoing work, we will explore applications relating to the synthesis of real quantum computations and also exotic quantum circuit synthesis algorithms relying on *KAK* metadecompositions of $U(2^n)$.

A Synthesis via Controlled Rotations

This appendix describes a synthesis algorithm using the $\Lambda_k[R_z(\alpha)]$ circuit subblocks. Recall our constructive proof of the upper bound on gate counts of Theorem 1.3 used $\bigoplus_k[R_z(\alpha)]$ subblocks instead. Several technical issues arising in our main algorithm also arise here. Thus, this appendix may serve as an introduction of how to use the obstruction $\eta(-)$ of Definition 3.2 to form a recursive synthesis algorithm reducing n-qubit diagonals to $(n-1)$-qubit diagonals.

Computation of $\eta(\ \Lambda_S[R_z(\alpha)]\ )$

Recall from the Introduction $U = \sum_{j=0}^{N-1} u_j |j\rangle\langle j|$ for $N = 2^n$ a fixed n-qubit diagonal quantum computation. Further recall that

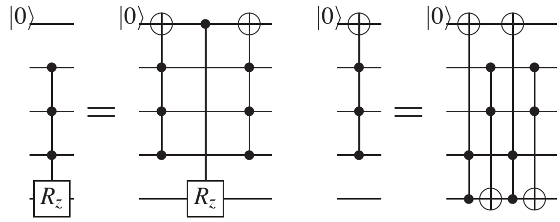

Figure 4: This diagram [1, Lemma 7.11] illustrates how to realize a $\Lambda_k[R_z(\alpha)]$ via a singly controlled rotation and k-controlled-nots. The latter may be synthesized using $O(k)$ elementary gates, *given the ancilla qubit shown as the top line*. Without the ancilla, a $O(k^2)$ gates would be required per corollary 7.6 ibid. The diagram at right recalls the next step of the decomposition.

for $S \subset \{1,2,\cdots,n-1\}$, by $\Lambda_S(V)$ for $V \in U(2^1)$ we mean that instance of the $\#S$-conditioned computation $\Lambda_{\#S}(V)$ which is conditioned on lines $\{j \in S\}$ and acts on line n.

Every computation $\Lambda_S[R_z(\alpha)]$ is also diagonal. We seek an explicit formula for $\eta(\ \Lambda_S[R_z(\alpha)]\ )$. With sufficient understanding of how $\Lambda_S[R_z(\alpha)]$ affects $\eta(-)$, we will be able to choose exact angles α so that preprending the conditioned blocks to U forces the composite to have $\eta = \vec{0}$. Thus the composite will be a tensor by corollary 3.3, allowing for recursion. The following language is useful for expressing and computing $\eta(\ \Lambda_S[R_z(\alpha)]\ )$. It is slightly more convenient to use the mathematical notation for vectors rather than `bra-ket`.

Definition 1.1 For $1 \le j \le N/2-1$, let e_j denote the standard basis column vectors for $\mathbb{R}^{N/2-1}$, i.e., e_j has a single entry of 1 in the j^{th} row and all other entries 0. We further define the vectors $v_j = e_j - e_{j+1}$ if $1 \le j \le N/2-2$, also setting $v_0 = -e_1$ and $v_{N/2-1} = e_{N/2-1}$.

Observe that the vectors $\{v_j\ ; 1 \le j \le N/2-1\}$ form a basis for $\mathbb{R}^{2^{n-1}-1}$. We need one further convention to describe $\eta(\ \Lambda_S[R_z(\alpha)]\ )$.

Definition 1.2 Let $1 \le j \le N/2-1$, with binary representation $j = b_1 b_2 \cdots b_{n-1}$ for $b_1, b_2, \cdots, b_{n-1} \in \mathbb{F}_2$. Let $S \subset \{1,2,\cdots,n-1\}$, $S \neq \emptyset$. We say that j is S-conditioned iff $\prod_{j \in S} b_j = 1$. We label $\mathcal{C}(S) = \{j\ ;\ j \text{ is } S \text{ conditioned}\}$.

Proposition A.3 *Let $\mathcal{C}(S)$ denote the S-conditioned set for some nonempty $S \subset \{1,\cdots,n-1\}$. Then*

$$\eta(\ \Lambda_S[R_z(\alpha)]\ ) = \alpha \sum_{j \in \mathcal{C}(S)} v_j \tag{38}$$

Proof: Label $V = \Lambda_S[R_z(\alpha)] = \sum_{j=0}^{N-1} \lambda_j |j\rangle\langle j|$. We recall that $\eta(V)$ is defined in terms of $\chi_j(V) = \lambda_{2j-2}\lambda_{2j-1}^{-1}\lambda_{2j}^{-1}\lambda_{2j+1}$. Now if $j \in \mathcal{C}(S)$, then $\lambda_{2j} = \mathrm{e}^{-i\alpha/2}$ and $\lambda_{2j+1} = \mathrm{e}^{i\alpha/2}$. If the binary expression for j is not S-conditioned, then $\lambda_{2j} = \lambda_{2j+1} = 1$. Continuing in this manner, say the binary expression for $j+1 \in \mathcal{C}(S)$.

Then $\lambda_{2j+2} = e^{-i\alpha/2}$ and $\lambda_{2j+3} = e^{i\alpha/2}$, else $\lambda_{2j+2} = \lambda_{2j+3} = 1$. Thus letting $\delta_{C(S)}$ denote the indicator function of $C(S)$,

$$-i \log \chi_j(V) = \alpha \delta_{C(S)}(j) - \alpha \delta_{C(S)}(j+1) \quad (39)$$

This expression agrees componentwise with the result of the proposition, given Definition 3.2. □

Example 1.4 Consider $n = 4$ qubits for the subset $S = \{1,3\}$ and $0 \le \alpha < 2\pi$ arbitrary. Label $\phi = -\alpha/2$, so that $R_z(\alpha) = e^{i\phi}|0\rangle\langle 0| + e^{-i\phi}|1\rangle\langle 1|$. Since $V = \Lambda_S[R_z(\alpha)]$ is diagonal, we describe the quantum computation by specifying multiples on each computational basis state.

state	mult	state	mult	state	mult	state	mult
$\|0000\rangle$	1	$\|0100\rangle$	1	$\|1000\rangle$	1	$\|1100\rangle$	1
$\|0001\rangle$	1	$\|0101\rangle$	1	$\|1001\rangle$	1	$\|1101\rangle$	1
$\|0010\rangle$	1	$\|0110\rangle$	1	$\|1010\rangle$	$e^{i\phi}$	$\|1110\rangle$	$e^{i\phi}$
$\|0011\rangle$	1	$\|0111\rangle$	1	$\|1011\rangle$	$e^{-i\phi}$	$\|1111\rangle$	$e^{-i\phi}$

Thus, $\chi_1(V) = 1$, $\chi_2(V) = 1$, $\chi_3(V) = 1$, $\chi_4(V) = 1$, $\chi_5(V) = e^{-2i\phi}$, $\chi_6(V) = e^{2i\phi}$, and $\chi_7(V) = e^{-2i\phi}$. Thus we have directly computed that $\eta(\,\Lambda_S[R_z(\alpha)]\,) = -2\phi i[0\;0\;0\;0\;1\;-1\;1]^t$.

On the other hand, $C(\{1,3\}) = \{101_b, 111_b\} = \{5,7\}$, where the subscript denotes binary. Thus

$$v_5 + v_7 = (e_5 - e_6) + e_7 = [0\;0\;0\;0\;1\;-1\;1]^t \quad (40)$$

Thus we computed the right-hand side of Proposition A.3. ◇

A.1 $\Lambda_k[R_z(\alpha)]$-block synthesis algorithm

Before the following definition, we note a happy accident. There are $N/2-1$ nonempty subsets of the top lines $\{1,\cdots,n-1\}$, and moreover $N/2-1$ characters $\chi_j : A(n) \to U(1)$ which must be zeroed within the components of the obstruction $\eta(-)$ to form a tensor. Thus, the following matrix is square.

Definition 1.5 The $(N/2-1) \times (N/2-1)$ real matrix $\eta^\wedge$ is defined as follows. Order nonempty subsets $S_1, S_2, \dots S_{2^{n-1}-1}$ in dictionary order. Then for $1 \le j \le N/2-1$, the j^{th} column of $\eta^\wedge$ is $\eta(\,\Lambda_{S_j}[R_z(1 \text{ radian})]\,)$.

Lemma A.6 *Let $\vec{\alpha} = [\alpha_1 \;\cdots\; \alpha_{N/2-1}]^t$. Then for S_1, S_2, $\dots S_{N/2-1}$ the dictionary ordering of nonempty subsets of $\{1,\cdots,n-1\}$,*

$$\eta(\,\Lambda_{S_1}[R_z(\alpha_1)]\,\Lambda_{S_2}[R_z(\alpha_2)]\,\cdots\,\Lambda_{S_{N/2-1}}[R_z(\alpha_{N/2-1})]\,) = \eta^\wedge \vec{\alpha} \quad (41)$$

Here, the right hand side denotes matrix multiplication by the column vector $\vec{\alpha}$.

Sketch: Recall that for any character $\chi : A \to \mathbb{C} - \{0\}$, one has $\log \chi(VW) = \log \chi(V) + \log \tilde{\chi}(W)$ and $\log \chi(V^a) = a \log \chi(V)$ for $V, W \in A$, $a \in \mathbb{R}$. Recall Definition 3.2 and apply these properties to the entries $-i \log \vec{\chi}_j$ of the vector valued function $\eta(-)$. □

We now state $\Lambda_k[R_z(\alpha)]$-block synthesis algorithm for a diagonal unitary computations. The proof of correctness follows in the next subsection and includes a proof of the subtle fact that the matrix $\eta^\wedge$ is inveritble.

Controlled Rotation Synthesis Algorithm Let $U = \sum_{j=0}^{N-1} u_j |j\rangle\langle j|$, for which we wish to synthesize a circuit diagram in terms of $\Lambda_k[R_z(\alpha)]$ blocks. Label S_1, S_2, S_3 $\dots S_{2^{n-1}-1}$ the nonempty subsets of the top $n-1$ lines $\{1,\cdots,n-1\}$ in dictionary order.

1. Compute the obstruction $\vec{\psi} = \eta(U)$.
2. Compute the inverse matrix $(\eta^\wedge)^{-1}$.
3. Compute $\vec{\alpha} = (\eta^\wedge)^{-1}\vec{\psi}$, treating $\vec{\psi}$ as a column vector. Label $\vec{\alpha} = [\alpha_1 \cdots \alpha_{N/2-1}]^t$.
4. Compute the diagonal quantum computation $\tilde{U} = \Lambda_{S_1}[R_z(-\alpha_1)] \;\cdots\; \Lambda_{S_{N/2-1}}[R_z(-\alpha_{N/2-1})]\; U$. As is verified below, $\tilde{U}$ is a tensor.
5. Use the argument of prop. 3.1 to compute $\tilde{U} = V \otimes W$ for $V \in A(n-1)$ and $W = e^{i\Phi} R_z(\alpha_0)$ for some angle α_0.
6. Given prior computations, the following expression holds:
$$U = \Lambda_\emptyset[R_z(\alpha_0)]\,\Lambda_{S_1}[R_z(\alpha_1)]\,\cdots\,\Lambda_{S_{N/2-1}}[R_z(\alpha_{N/2-1})]\,[V \otimes \mathbf{1}] \quad (42)$$
Here, $\mathbf{1}$ denotes the trivial computation of $U(2^1)$. Also, $\Lambda_\emptyset[R_z(\alpha_0)]$ means $\mathbf{1} \otimes R_z(\alpha_0)$ for $\mathbf{1} \in U(2^{N/2})$.
7. Techniques from the literature are then used to decompose each $\Lambda_{S_j}[R_z(\alpha_j)]$ into elementary gates per Figure 4.
8. The algorithm terminates by recursively producing a circuit diagram for $V \in A(n-1)$.

Example 1.7

In three qubits, consider the following diagonal computation.

$$\begin{aligned} U \;=\; & e^{6\pi i/6}|0\rangle\langle 0| + e^{3\pi i/6}|1\rangle\langle 1| + e^{9\pi i/6}|2\rangle\langle 2| + e^{8\pi i/6}|3\rangle\langle 3| \\ & + e^{5\pi i/6}|4\rangle\langle 4| + e^{1\pi i/6}|5\rangle\langle 5| + e^{6\pi i/6}|6\rangle\langle 6| + 1|7\rangle\langle 7| \end{aligned} \quad (43)$$

Then one has $\chi_1(U) = e^{2\pi i/6}$, $\chi_2(U) = e^{-3\pi i/6}$, $\chi_3(U) = e^{-2\pi i/6}$ so that $\vec{\psi} = \eta(U) = [2\pi/6 \;\, -3\pi/6 \;\, -2\pi/6]^t$.

We now must compute $\vec{\alpha}$ by computing the inverse matrix $(\eta^\wedge)^{-1}$. For this matrix, first compute the following.

$$\eta^\wedge = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} \quad (44)$$

The following inverse matrix results, and it may be reused for multiple specific diagonals U.

$$(\eta^\wedge)^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad (45)$$

So $\vec{\alpha} = (\eta)^{-1}\vec{\psi} = [-\pi/6 \;\; -4\pi/6 \;\; 2\pi/6]^t$. Hence $\tilde{U}$ as defined below is a tensor.

$$\tilde{U} = \Lambda_{\{1\}}[R_z(\pi/6)]\,\Lambda_{\{1,2\}}[R_z(4\pi/6)]\,\Lambda_{\{2\}}[R_z(-\pi/6)]\,U \tag{46}$$

In order to verify this directly, we compute the eight diagonal matrix coefficients of each of $\Lambda_S[R_z(\alpha)]$. To save space, we write $\mathrm{diag}(\lambda_0,\cdots,\lambda_7)$ for $\lambda_0|0\rangle\langle 0| + \cdots + \lambda_7|7\rangle\langle 7|$.

$$\begin{aligned} \Lambda_{\{1\}}[R_z(\pi/6)] &= \mathrm{diag}(1,1,1,1,e^{-\pi i/12}, \\ &\qquad e^{\pi i/12}, e^{-\pi i/12}, e^{\pi i/12}) \\ \Lambda_{\{1,2\}}[R_z(4\pi/6)] &= \mathrm{diag}(1,1,1,1,1,1,e^{-4\pi i/12},e^{4\pi i/12}) \\ \Lambda_{\{2\}}[R_z(-2\pi/6)] &= \mathrm{diag}(1,1,e^{2\pi i/12},e^{-2\pi i/12}, \\ &\qquad 1,1,e^{2\pi i/12},e^{-2\pi i/12}) \end{aligned} \tag{47}$$

Then multiplying, the expression demonstrates $\tilde{U} = V \otimes W$.

$$\begin{aligned} \tilde{U} &= \mathrm{diag}(e^{12\pi i/12}, e^{6\pi i/12}, e^{20\pi i/12}, e^{14\pi i/12}, \\ &\qquad e^{9\pi i/12}, e^{3\pi i/12}, e^{9\pi i/12}, e^{3\pi i/12}) \end{aligned} \tag{48}$$

Since $\tilde{U}$ is a tensor, we obtain the following decomposition of U.

$$\begin{aligned} U &= \Lambda_{\{1\}}[R_z(-\pi/6)]\,\Lambda_{\{1,2\}}[R_z(-4\pi/6)]\,\Lambda_{\{2\}}[R_z(\pi/6)] \\ &\qquad [\mathrm{diag}(1,e^{8\pi i/12},e^{-3\pi i/12},e^{-3\pi i/12}) \otimes \mathrm{diag}(e^{12\pi i/6},e^{6\pi i/6})] \end{aligned} \tag{49}$$

The algorithm then recursively synthesizes the 2-qubit diagonal $V = 1|0\rangle\langle 0| + e^{8\pi i/12}|1\rangle\langle 1| + e^{-3\pi i/12}|2\rangle\langle 2| + e^{-3\pi i/12})|3\rangle\langle 3|$. ◇

Proof of correctness of $\Lambda_k[R_z(\alpha)]$-block synthesis

We briefly verify that $\tilde{U} = V \otimes W$. First use proposition A.6 for

$$\eta(\,\Lambda_{S_1}[R_z(-\alpha_1)]\,\cdots\,\Lambda_{S_{N/2-1}}[R_z(-\alpha_{N/2-1})]\,) = -\vec{\psi} \tag{50}$$

Then the property $\eta(U_1U_2) = \eta(U_1) + \eta(U_2)$ demands

$$\eta(\,\Lambda_{S_1}[R_z(-\alpha_1)]\,\cdots\Lambda_{S_{N/2-1}}[R_z(-\alpha_{N/2-1})]\,U\,) = -\vec{\psi} + \vec{\psi} = \vec{0} \tag{51}$$

So by the restatement of Proposition 3.1, we have $\tilde{U} = V \otimes W$.

The algorithm also uses the following proposition.

Proposition A.8 *The matrix $\eta^\wedge$ per Definition A.5 is an invertible $(2^{n-1}-1) \times (2^{n-1}-1)$ matrix.*

Sketch: It suffices instead to consider the similar matrix corresponding to a change of basis to v_j, $1 \leq j \leq N/2-1$ of Definition 4.2. Thus, if $B = [v_1\; v_2\; \cdots\; v_{N/2-1}]$ is the change of basis matrix, the matrix similar to $\eta^\wedge$ is $M = B^{-1}\eta^\wedge B = (m_{jk})$. Now $m_{jk} = 0$ if j is not S_k-conditioned and $m_{jk} = 1$ if j is S_k-conditioned.

M is invertible since column operations reduce M to a permutation matrix. Indeed, the last $e_{N/2-1}$ column may be used to clear all other nonzero entries in the last row. Then each of the columns corresponding to $n-2$ element subsets retain a single nonzero entry, and the corresponding rows may be cleared. □

References

[1] A. Barenco et al., "Elementary Gates For Quantum Computation," *Physical Review A* vol. 52, 1995, 3457-3467.

[2] S.S.Bullock and I.L. Markov, "An Elementary Two-Qubit Quantum Computation In Twenty-Three Elementary Gates," *Physical Review A* vol. 68, 2003, 012318-012325, quant-ph/0211002.

[3] G. Cybenko, "Reducing Quantum Computations to Elementary Unitary Operations," *Comp. in Sci. and Engin.*, March/April 2001, pp. 27-32.

[4] G. H. Golub and C. F. Van Loan, *Matrix Computations*, Johns Hopkins Press, Baltimore, 1996.

[5] V. Guillemin and A. Pollack, *Differential Topology*, Prentice-Hall, Inc., Englewoods Cliffs New Jersey, 1974.

[6] G. Hachtel and F. Somenzi, *Synthesis and Verification of Logic Circuits*, 3rd ed., Kluwer, 2000.

[7] T. Hogg, C. Mochon, W. Polak, and E. Rieffel, "Tools For Quantum Algorithms," *International Journal of Modern Physics C*, (10) 1999, 1347-1361, quant-ph/9811073.

[8] N. Khaneja, R. Brockett and S. J. Glaser, "Time Optimal Control In Spin Systems," 2001 quant-ph/0006114.

[9] A. W. Knapp, *Lie Groups Beyond an Introduction*, Progress in Mathematics, vol. 140, *Birkhäuser*, 1996.

[10] E. Knill, "Approximation by Quantum Circuits," 1995, quant-ph/9508006.

[11] A. Mishchenko and M.Perkowski, "Fast Heuristic Minimization of Exclusive Sum-of-Products," *Reed-Muller Workshop* 2001, pp. 242-250.

[12] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, 2000.

[13] Y.Shi, "Both Toffoli and Controlled-NOT need little help to universal quantum computing," *Quantum Information and Computing*, vol. 3, no. 1, pp84-92, quant-ph/0205115.

[14] "Optimal realizations of controlled unitary gates," G. Song and A. Klappenecker, *Quantum Information and Computing*, vol. 3, no. 2, pp139-155 quant-ph/0301078.

[15] B. Steinbach and A. Mishchenko, "A New Approach to Exact ESOP Minimization", *Reed-Muller Workshop* '01, pp. 66-81.

[16] B. Travaglione et al. "ROM-based Computation: Quantum Versus Classical," *Quantum Information and Computation* Vol. 2, No. 4, 2002 quant-ph/0109016.

[17] R. Tucci, "A Rudimentary Quantum Compiler," 1999, quant-ph/9902062.