Shorter quantum circuits

Vadym Kliuchnikov[1,2], Kristin Lauter[3], Romy Minko[4,5], Adam Paetznick[1], and Christophe Petit[6,7]

[1]Microsoft Quantum, Redmond, WA, US
[2]Microsoft Quantum, Toronto, ON, CA
[3]Facebook AI Research, Seattle, WA, US
[4]University of Oxford, Oxford, UK
[5]Heilbronn Institute for Mathematical Research, University of Bristol, Bristol, UK
[6]University of Birmingham, Birmingham, UK
[7]Université Libre de Bruxelles, Brussels, Belgium

We give a novel procedure for approximating general single-qubit unitaries from a finite universal gate set by reducing the problem to a novel magnitude approximation problem, achieving an immediate improvement in sequence length by a factor of 7/9. Extending the work of [Has17; Cam17], we show that taking probabilistic mixtures of channels to solve fallback [BRS15a] and magnitude approximation problems saves factor of two in approximation costs. In particular, over the Clifford+$\sqrt{\mathrm{T}}$ gate set we achieve an average non-Clifford gate count of $0.23\log_2(1/\varepsilon)+2.13$ and T-count $0.56\log_2(1/\varepsilon)+5.3$ with mixed fallback approximations for diamond norm accuracy ε.

This paper provides a holistic overview of gate approximation, in addition to these new insights. We give an end-to-end procedure for gate approximation for general gate sets related to some quaternion algebras, providing pedagogical examples using common fault-tolerant gate sets (V, Clifford+T and Clifford+$\sqrt{\mathrm{T}}$). We also provide detailed numerical results for Clifford+T and Clifford+$\sqrt{\mathrm{T}}$ gate sets. In an effort to keep the paper self-contained, we include an overview of the relevant algorithms for integer point enumeration and relative norm equation solving. We provide a number of further applications of the magnitude approximation problems, as well as improved algorithms for exact synthesis, in the Appendices.

Romy Minko: This work was supported by the CDT in Cyber Security at the University of Oxford (EP/P00881X/1) and the Additional Funding Programme for Mathematical Sciences, delivered by EPSRC (EP/V521917/1) and the Heilbronn Institute for Mathematical Research.

Contents

1 Introduction

In the quantum circuit model, quantum algorithms are expressed as sequences of unitary operations and measurements. Any n-qubit unitary can be implemented by a circuit of elementary gates, comprising controlled-NOT (CNOT) gates and single-qubit gates [Bar+95]. Fault tolerant quantum computers require that the single-qubit gates belong to a finite set. Such a set is called universal if it generates a dense covering of $SU(2)$. That is, if any unitary $U \in SU(2)$ can be approximated to any accuracy by a finite sequence of gates from the set. Of particular interest is the subject of approximating single-qubit diagonal unitaries, as a Euler decomposition guarantees that any single-qubit unitary can be decomposed into diagonal R_z- and R_x-rotations. In addition, diagonal R_z rotations are directly used in many quantum algorithm.

The cost of an approximation is quantified by the gate complexity, or gate cost. Associating each gate g_i in a sequence with a weight w_i, the gate cost of that sequence is $\sum_i w_i$. The gate cost of approximating U to within ε is then taken as the minimum gate cost of all possible approximating sequences. Note that select gates, such as the Pauli or Clifford gates, are considered cheap to implement and so take zero weight. Typically, expensive gates will be given a weight of 1, so that the gate cost of an approximation corresponds to the number of expensive gates in the sequence. Consequently, minimizing the length of an approximating sequence is a problem integral to the subject of gate synthesis. A fundamental and general result is the Solovay-Kitaev theorem, which states that a universal gate-set G can approximate any unitary $U \in SU(2)$ to accuracy ε by a finite sequence of gates from G of length $O(\log^c(1/\varepsilon))$, where c is a constant. Significant progress has been made since Solovay-Kitaev for specific gate-sets associated with fault-tolerant quantum computers. Bourgain and Gamburd [BG11] showed that universal gate-sets of unitaries with algebraic entries give approximating sequences with lengths $O(\log(1/\varepsilon))$. This result was quickly applied to find efficient constructive algorithms for the Clifford+T gate set [KMM13a; Sel15] and, later, the V basis [BGS13b]. Constructive algorithms for optimal diagonal approximations for both gate sets followed soon thereafter [RS15; Ros15; BBG15a]. Many of these algorithms adopted a common framework of integer point enumeration followed by a solving a norm equation. Measurements were also introduced to aid gate synthesis [PS13], culminating in the fall-back circuit [BRS15b], although this work was a departure from the common framework. Sarnak [Sar] noted a connection between gate synthesis and quaternion algebras in his letter to Aaronson and Pollington, which has been used to build frameworks for both exact [KY15][1] and approximate synthesis [Kli+15b]. The letter also characterizes 'golden gate sets', of which the Clifford+T and V gates are examples, that achieve optimal sequence lengths. For approximations of diagonal unitaries, this is shown to be $3\log_\ell(1/\varepsilon)$. These results are further expanded and generalizations of two-step approach to diagonal approximations from [RS15] to other gate sets also discussed in [PS18]. Recent research [Cam17; Has17] shows that approximation with quantum channels, rather than unitaries, achieves quadratic improvement in ε and reduces the length by factor of two.

The quality of an approximation V for some desired unitary U is captured by the accuracy parameter ε. The distance between two unitaries is computed by evaluating some norm of $U - V$. Typically, this is the operator (or spectral) norm, where $\|A\| = \max \lambda_k$, where λ_k are the singular values of A. In order to measure distance for quantum channels, that is, completely-positive trace-preserving linear maps on density matrices, we refer to the diamond norm. For quantum channels $\mathcal{U}$ and $\mathcal{V}$ corresponding to unitaries U and V,

[1] This work has been developed independently of [Sar].

the diamond norm of their difference is defined by

$$\|\mathcal{U}-\mathcal{V}\|_\diamond = \max_\rho\{\|((\mathcal{U}-\mathcal{V})\otimes\mathcal{I}_d)(\rho)\|_1\},\ \text{where}\ \|A\|_1 = \mathrm{Tr}\sqrt{A^\dagger A} \tag{1}$$

and $\mathcal{I}_d$ is the identity map, and the maximum is taken over all probability density matrices ρ. The diamond norm thus allows for accurate measurement of errors in unitaries constituting a quantum algorithm, independent of the algorithm itself.

We consider three universal gate sets associated with fault-tolerant quantum computation: the V basis, the Clifford+T basis and the Clifford+$\sqrt{\mathrm{T}}$ basis. The Clifford+T gate set is commonly used for fault tolerant quantum computation, and is known to be efficiently universal [Sel15], with gate cost depending solely on the number of T gates used. The V basis was shown to be efficiently universal in [HRC02], and provides a simple pedagogical example of approximation. The Clifford+$\sqrt{\mathrm{T}}$ gate set is an alternative to the Clifford+T gate set for fault tolerant computing. The merits of these gate sets with regard to fault tolerant computing are discussed in greater detail in Section **??**.

The rest of this paper is organized as follows. Section **??** summarizes our main results. In Section **??**, we briefly discuss connections between gate synthesis and cryptography. Section **??** defines the five approximation problems that are the focus of this paper. We detail a complete method for solving these problems in Section **??**, with examples for the V, Clifford+T and Clifford +$\sqrt{\mathrm{T}}$ gate sets, in addition to a general solution. We provide extensive numerical results for our method in Section **??** for Clifford+T and Clifford+$\sqrt{\mathrm{T}}$. Section **??** and Section **??** recall algorithms for solving two problems that arise in our solution method: integer point enumeration and norm equation solving.

1.1 Fault tolerant gate sets

Unitary synthesis translates the description of a quantum algorithm into a sequence of operations ("gates") that can be implemented on the target quantum computer. The set of operations permitted by a particular quantum computing platform are limited by physical constraints and may not match the operations prescribed in the algorithm. Moreover, even if the operations offered by the quantum computer match the operations in the algorithm, the accuracy to which the quantum computer can perform each operation is likely to be limited. Loosely speaking, existing quantum computing systems offer single-qubit unitary operations with accuracy up to 10^{-4} (see Fig. S.17 in [Aru+19] for the accuracy of one and two qubit gates) whereas useful quantum algorithms require accuracy of 10^{-10} or better (see Table I in [Bur+21] for the typical number of gates in useful quantum algorithms).

Fault-tolerant quantum computation bridges the accuracy gap by encoding many physical qubits into a smaller number of logical qubits. To guarantee accuracy, logical qubits must be encoded at all times. Operations of the quantum algorithm must be performed on the logical qubits *while* they are encoded. Each logical operation must both preserve the code structure and carefully limit the spread of errors. Those requirements restrict the available set of logical quantum operations.

The cheapest form of logical operations involves executing the same physical operation to each of the physical qubits in the code. For example, some codes admit the logical Hadamard operation by executing the physical Hadamard operation to each physical qubit. Unfortunately, these so-called "transversal" gates can yield only a sparse discrete set within a single quantum code [EK09; BK13; WB20].

Stabilizer codes, the most widely studied class of quantum error correcting codes, typically admit transversal implementation of some or all of the Clifford group—the group

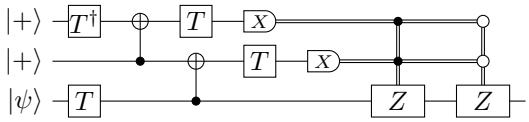


Figure 1: A Clifford+T circuit implementation of $V_Z = (I+2iZ)/\sqrt{5}$ proposed in [PS14]. Conditioned on X-basis measurement outcomes of zero on the top two qubits, the circuit outputs $V_Z|\psi\rangle$. For any other measurement outcome the circuit outputs $|\psi\rangle$. Repeating the circuit until obtaining the 00 measurement outcome yields $V_Z|\psi\rangle$ using approximately 5.26 T gates, in expectation.

generated by $\{H, S, \text{CNOT}\}$. A broad and widely studied subset of stabilizer codes called CSS support transversal implementation of the CNOT operation, for example.[2] Circuits composed of Clifford group operations have the added benefit of being efficiently simulable, an essential feature for the study of fault tolerant quantum computing schemes.

At least one operation outside of the Clifford group is required for universal quantum computation (see Theorem 6.7.3 in [NRS06]). In most fault-tolerant quantum computing proposals, that non-Clifford operation is the T gate. The logical T operation is typically implemented by "distillation" which combines many (noisy) physical T gates with (less noisy) logical Clifford operations [BK05]. Distillation is regarded as the most efficient known technique for non-Clifford gates, but remains roughly an order of magnitude more expensive than transversal operations despite much study [BKS21]. Distillation can be used to construct other operations, but known distillation protocols are limited to operations that belong to the so-called "Clifford hierarchy" introduced in [GC99]. Of the known distillation techniques the most cost competitive operations are T and the three qubit double-controlled-Z (CCZ) [GF19].

To the best of our knowledge, there are no operations outside of the Clifford hierarchy that admit implementation through distillation of the corresponding resource states. However, by including measurement it is possible to construct other kinds of circuits out of fault tolerant Clifford+T gates. For example, $V_Z = (I + 2iZ)/\sqrt{5}$ can be implemented with the circuit shown in Figure **??**. The idea then is to approximate a unitary U with a sequence of Clifford+V_Z gates then substitute Figure **??** for each V_Z in the sequence. Unfortunately, that strategy yields higher number of T gates than synthesis with Clifford+T alone. The strategy could be redeemed with cheaper Clifford+T implementations of V_Z or similar non-Clifford gates. But finding such circuits is difficult,and the best known circuits do not produce better resource requirements overall. Though we consider the V-basis gate set in this paper, it is largely for instructional purposes.

Incorporation of measurements into Clifford+T circuits can be used to emulate other gates *within* the Clifford hierarchy, as well. For example, the gate $\sqrt{T}$ can be implemented with Clifford+T and measurements [Bev+20]. Approximations with the set Clifford+$\sqrt{T}$, through emulation, use the the same number of T gates as direct Clifford+T sequences. Using Clifford+$\sqrt{T}$ gates, however, yields approximating sequences that are half the length of corresponding Clifford+T sequences, offering an advantage when rotations must be executed as fast as possible.

Table 1: Scaling of the approximation cost for random angles. Approximation accuracy ε is measured using diamond distance. Linear fit of the cost is based on the numerical results reported in Figure **??** and Figure **??**. Mixed diagonal rows contain results for our new and improved version of a mixed diagonal approximation protocol first introduced in [Cam17; Has17]. Results from [Cam17; Has17] apply to any gate set for which diagonal approximation is available. Fallback rows correspond to our improved and generalized fallback synthesis method (**??**) first introduced in [BRS15a]. For power cost, the cost of T is two and the cost of $T^{1/2}, T^{3/2}$ is three. Our algorithms are optimal with respect to this cost. For gate count cost, the cost of T, $T^{1/2}, T^{3/2}$ is one. For T-count cost, the cost of T is one and the cost of $T^{1/2}, T^{3/2}$ is four. Clifford gate costs are always zero. Different costs are discussed in **??**. Heuristic cost estimates are discussed in **??**. Applications of magnitude approximation are illustrated in **??**.

Gate set (cost)	Approximation protocol	Linear fit of the cost ($\varepsilon < 10^{-4}$)		Heuristic cost estimate	Novelty
		Mean	Max		
Clifford+T (T-count) **??**	Diagonal [RS15]	$3.02\log_2(1/\varepsilon) + 1.77$	$3.02\log_2(1/\varepsilon) + 9.19$	$3.0\log_2(1/\varepsilon) + O(1)$	Known
	Fallback [BRS15b]	$1.03\log_2(1/\varepsilon) + 5.75$	$1.05\log_2(1/\varepsilon) + 11.83$	$1.0\log_2(1/\varepsilon) + O(1)$	Improved
	Magnitude	–	–	$1.0\log_2(1/\varepsilon) + O(1)$	New
	Mixed diagonal	$1.52\log_2(1/\varepsilon) - 0.01$	$1.54\log_2(1/\varepsilon) + 6.85$	$1.5\log_2(1/\varepsilon) + O(1)$	Improved
	Mixed fallback	$0.53\log_2(1/\varepsilon) + 4.86$	$0.57\log_2(1/\varepsilon) + 8.83$	$0.5\log_2(1/\varepsilon) + O(1)$	New
	Mixed magnitude	–	–	$0.5\log_2(1/\varepsilon) + O(1)$	New
Clifford+$\sqrt{T}$ (power) **??**	Diagonal	$3.02\log_2(1/\varepsilon) + 2.80$	$3.01\log_2(1/\varepsilon) + 8.53$	$3.0\log_2(1/\varepsilon) + O(1)$	New
	Fallback	$1.04\log_2(1/\varepsilon) + 6.61$	$1.02\log_2(1/\varepsilon) + 11.83$	$1.0\log_2(1/\varepsilon) + O(1)$	New
	Magnitude	–	–	$1.0\log_2(1/\varepsilon) + O(1)$	New
	Mixed diagonal	$1.53\log_2(1/\varepsilon) + 1.06$	$1.58\log_2(1/\varepsilon) + 4.98$	$1.5\log_2(1/\varepsilon) + O(1)$	New*
	Mixed fallback	$0.56\log_2(1/\varepsilon) + 5.32$	$0.62\log_2(1/\varepsilon) + 7.66$	$0.5\log_2(1/\varepsilon) + O(1)$	New
	Mixed magnitude	–	–	$0.5\log_2(1/\varepsilon) + O(1)$	New
Clifford+$\sqrt{T}$ (gate count) **??**	Diagonal	$1.21\log_2(1/\varepsilon) + 1.18$	$1.26\log_2(1/\varepsilon) + 3.86$	$1.2\log_2(1/\varepsilon) + O(1)$	New
	Fallback	$0.42\log_2(1/\varepsilon) + 2.68$	$0.44\log_2(1/\varepsilon) + 5.13$	$0.4\log_2(1/\varepsilon) + O(1)$	New
	Magnitude	–	–	$0.4\log_2(1/\varepsilon) + O(1)$	New
	Mixed diagonal	$0.61\log_2(1/\varepsilon) + 0.43$	$0.64\log_2(1/\varepsilon) + 2.52$	$0.6\log_2(1/\varepsilon) + O(1)$	New*
	Mixed fallback	$0.23\log_2(1/\varepsilon) + 2.13$	$0.25\log_2(1/\varepsilon) + 3.85$	$0.2\log_2(1/\varepsilon) + O(1)$	New
	Mixed magnitude	–	–	$0.2\log_2(1/\varepsilon) + O(1)$	New
Clifford+$\sqrt{T}$ (T count) **??**	Diagonal	$3.03\log_2(1/\varepsilon) + 2.48$	$3.25\log_2(1/\varepsilon) + 14.40$	$3.0\log_2(1/\varepsilon) + O(1)$	New
	Fallback	$1.04\log_2(1/\varepsilon) + 6.43$	$1.18\log_2(1/\varepsilon) + 14.01$	$1.0\log_2(1/\varepsilon) + O(1)$	New
	Magnitude	–	–	$1.0\log_2(1/\varepsilon) + O(1)$	New
	Mixed diagonal	$1.53\log_2(1/\varepsilon) + 1.02$	$1.68\log_2(1/\varepsilon) + 7.30$	$1.5\log_2(1/\varepsilon) + O(1)$	New*
	Mixed fallback	$0.56\log_2(1/\varepsilon) + 5.30$	$0.67\log_2(1/\varepsilon) + 9.85$	$0.5\log_2(1/\varepsilon) + O(1)$	New
	Mixed magnitude	–	–	$0.5\log_2(1/\varepsilon) + O(1)$	New

2 Summary of main results

In Section **??** we define six approximation problems: diagonal unitary approximation, fallback approximation, magnitude approximation and their versions with probabilistic mixing. The first two of these problems have been the subject of research for some time, with many results pertaining to specific gate sets [RS15; KMM13b; BGS13a; BRS15b; KY15; Kli+15b]. The magnitude approximation problem is new. One of its applications is solving the general unitary approximation problem, which exploits the connection between unitary approximation and LPS graphs (See Section **??**). Explicitly, we adapt the path-finding algorithm of Carvalho Pinto and Petit [CP18] to the quantum setting, requiring only two diagonal approximations and one more efficient magnitude approximation. The sequence costs obtained using our method improve on the standard Euler decomposition, which requires three diagonal approximations, by roughly one-third. Stier [Sti20] has concurrently and independently produced a similar result. We discuss additional ap-

[2]CSS is an initialism that comes from the three authors that first defined the codes: Calderbank, Shor and Steane.

Figure 2: Cost of approximating a set of random diagonal rotation gates with Clifford+T gates using four approximation protocols. Diagonal rotation angles are random angles drawn from the uniform distribution on $[0, 2\pi]$. We fix a set of approximation accuracy values. For each value in the set we compute mean cost over all target angles. Vertical bars show the cost standard deviation for the given accuracy value. Shaded regions indicate range of costs from min to max over all angles for the given accuracy value. For the diagonal approximation protocol the cost for a given angle and given accuracy is equal to number of T gates in the approximating sequence. For the other protocols the cost is the expectation of T-count. For example, if the first step of fall-back protocol requires 10 T gates and fails with probability 0.01 and the step to correct failure requires 30 T gates, the expected cost is 10.3. In all reported fallback protocols the probability of fallback is at most 0.01.

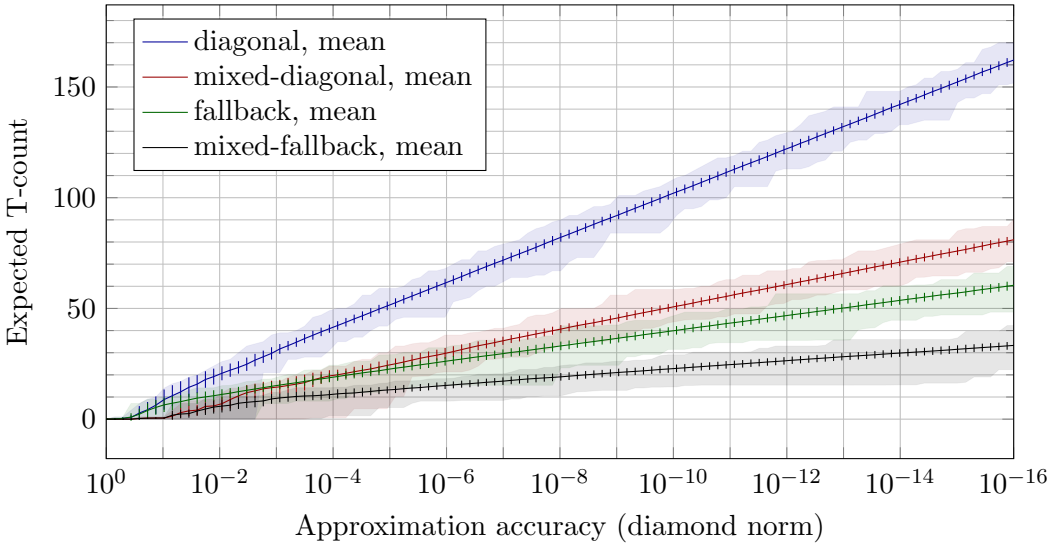


Table 2: Examples of problems that benefit from magnitude approximation. The case of a general qubit unitary approximation is described in **??** and **??**. Solutions to qubit approximation and general $\mathrm{SU}(4)$ approximation are outlined in **??**. More generally, the magnitude approximation problem can be used when compiling CNOT and rotation circuits for isometries produced by UniversalQCompiler [Ite+16; Ite+21; MIC21] for fault-tolerant quantum computers.

Problems that benefit from magnitude approximation		Qubit state preparation	General SU(2) approximation	General SU(4) approximation
Problem properties	Number of real parameters	2	3	15
	Number of magnitude approximation instances	1	1	6
	Number of diagonal approximation instances	1	2	9
Gate set	Approximation method	Heuristic T-count scaling with diamond norm accuracy ε		
Clifford+T	Diagonal (known)	$6\log_2(1/\varepsilon) + O(1)$	$9\log_2(1/\varepsilon) + O(1)$	$45\log_2(1/\varepsilon) + O(1)$
	Diagonal + Magnitude (new)	$4\log_2(1/\varepsilon) + O(1)$	$7\log_2(1/\varepsilon) + O(1)$	$33\log_2(1/\varepsilon) + O(1)$
	Mixed Diagonal (improved)	$3\log_2(1/\varepsilon) + O(1)$	$4.5\log_2(1/\varepsilon) + O(1)$	$22.5\log_2(1/\varepsilon) + O(1)$
	Mixed Diag. + Mag. (new)	$2\log_2(1/\varepsilon) + O(1)$	$3.5\log_2(1/\varepsilon) + O(1)$	$11.5\log_2(1/\varepsilon) + O(1)$

plications of the magnitude approximation problem in **??**.

The latter three problems are defined by applying the concept of channel mixing to diagonal, fallback and magnitude approximation, expanding on the ideas of [Cam17; Has17]. Channel mixing employs a probabilistic combination of sequences of unitaries to approximate the target. The key idea is to use probabilistic combination of under-rotated and over-rotated approximations of a given target. We combine channel mixing with fallback and magnitude approximation to achieve a roughly two-fold improvement in cost compared to non-mixed problem variants. To account for the fact that we are approximating with channels rather than unitaries, we use the diamond norm to measure the accuracy of approximation. We introduce the use of diagonal Clifford twirling, which ensures that the difference between the ideal and approximating channel is a Pauli channel. Because of this, we obtain a closed-form expression for the diamond distance which improves on analysis in [Cam17; Has17] and results in lower approximation costs. The method in [Cam17] uses diagonal approximation algorithms as black-boxes and finds under-rotations and over-rotations by modifying target rotation angle. In contrast, we modify synthesis algorithms to directly find under and over-rotated approximations and further reduce approximations costs.

We provide a uniform approach to the six approximation problems and various gate sets. For each problem, we show that a constraint on the diamond norm can be reduced to a constraint on a single complex number. In contrast to [BRS15a], our approach to fallback approximation ensures desired success probability and approximation accuracy. The set of feasible solutions is represented geometrically as a region in $\mathbb{R}^2$, illustrated in Section **??**. Figure **??** compares the areas of the regions associated to the approximation problems with respect to varying approximation accuracy ε and success probability q. The scaling of the region area with epsilon determines the scaling of the approximation sequence cost with accuracy ε, as illustrated in **??**. To establish dependence between region area scaling and cost scaling we use several heuristic assumptions as discussed in **??**. We also provide experimental justification of relation between the cost and region scaling.

The results of our numerical experiments for Clifford+T and Clifford+$\sqrt{T}$ gate sets are summarized in **??**. More detailed numerical results for Clifford+T are provided in **??**, in particular they show that linear fits for cost scaling with accuracy are well justified. Even more detailed results for Clifford+T and for Clifford+$\sqrt{T}$ are in Section **??**. We show numerical results for approximating uniformly random diagonal rotations and angles and rotations by Fourier angles $\pi/2^k$. The study of uniformly random diagonal rotations is motivated by the use of diagonal rotations in quantum algorithm for chemistry, material science applications [Chi+21] and the rotations used in Quantum Signal Processing [LC17]; rotations by Fourier angles appear in the Quantum Fourier Transform [NSM20] and preparation of Phase Gradient states [Gid18].

We find that Clifford+$\sqrt{T}$ is a promising gate-set for approximation when executing rotations as fast impossible. In this case the execution speed is limited by the gate count, in particular when executing rotations using a circuit from Figure 33 in [Lit19]. We achieve average gate-count scaling $0.23\log_2(1/\varepsilon) + 2.13$ when using mixed fallback protocol with Clifford+$\sqrt{T}$ and T-count similar to Clifford+T approximations. We assume that each $\sqrt{T}$ gate requires four T gates, which is justified in **??**. These are the first numerical studies of approximation cost scaling for Clifford+$\sqrt{T}$ gates that include additive constants, which are practically important because the $\log_2(1/\varepsilon)$ prefactor is small. These are also the first numerical results for mixed fallback and mixed diagonal approximations for Clifford+T. We also provide more detail on approximate synthesis for general gate sets than the high-level approach outlined in [PS18].

In Section **??** we describe a complete method for solving the six approximation problems, restricting the scope to considering gate sets that can be represented by quaternion algebras. The general solution method is described in Section **??**, and includes a process for constructing quaternion gate sets, as defined in [Kli+15a]. To summarize, a gate set is defined by a complex field L, its maximal totally real subfield K and a fixed set of elements in K. A solution to an approximation problem involves finding a matrix $M = \left(\begin{smallmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{smallmatrix}\right)$ with entries in the integer ring of L. Our approach to finding M can be summarized in two steps: point enumeration in a region defined by the approximation problem to find m_1, followed by solving a relative norm equation to recover m_2. To guide the reader, we work through three pedagogical examples: the V basis (Section **??**), the Clifford+T basis (Section **??**), and the Clifford+$\sqrt{\mathrm{T}}$ basis (Section **??**). A worked example for the V basis is given here in Section **??**.

2.1 Example: V basis diagonal approximation of $e^{i\frac{\pi}{4}Z}$

We use the notation I, X, Y, Z for Pauli matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Recall that the V basis consists of the following six matrices:

$$V_{\pm Z} = \frac{1}{\sqrt{\ell}}\left(I \pm 2iZ\right), \qquad V_{\pm Y} = \frac{1}{\sqrt{\ell}}\left(I \pm 2iY\right), \qquad V_{\pm X} = \frac{1}{\sqrt{\ell}}\left(I \pm 2iX\right),$$

where $\ell = 5$. Let $\theta = \frac{\pi}{4}$ and suppose we want to approximate $U = e^{i\theta Z} = \left(\begin{smallmatrix} e^{i\pi/4} & 0 \\ 0 & e^{-i\pi/4} \end{smallmatrix}\right)$ using the V basis within accuracy $\varepsilon = 0.1$ with respect to the diamond norm. In other words, we look for V, a product of unitaries from the V basis, which satisfies $\|\mathcal{Z}_\theta - \mathcal{V}\|_\diamond \leq \varepsilon$, where $\mathcal{Z}_\theta$ and $\mathcal{V}$ are the channels[3] induced by $e^{i\theta Z}$ and V, respectively.

Writing V as $\left(\begin{smallmatrix} u & -v^* \\ v & u^* \end{smallmatrix}\right)$, with $u, v \in \mathbb{C}$, we obtain the following:

$$\left|\mathrm{Re}(ue^{-i\pi/4})\right| \geq 1 - \varepsilon^2/8 \implies \left\|\mathcal{Z}_{\pi/4} - \mathcal{V}\right\|_\diamond \leq \varepsilon. \tag{2}$$

For the full derivation of this constraint see Problem **??**, Section **??**. The constraint on u is represented geometrically by the region in Figure **??**.

Since V is a product of V basis matrices, there exists $N \in \mathbb{N}$ such that $V = \frac{1}{\sqrt{5^N}}\left(\begin{smallmatrix} u' & -(v')^* \\ v' & (u')^* \end{smallmatrix}\right)$, with $u', v' \in \mathbb{Z}[i]$. It follows that $u = u'/\sqrt{5^N}$ and $v = v'/\sqrt{5^N}$. Hence, we scale the region in Figure **??** by $\sqrt{5^N}$ and look for integer points $(a, b) \in \mathbb{Z}^2$, each corresponding to a candidate $u' = a + ib$. We initialize $N := 1$, and iterate over N until a solution is found.

We find that there are no integer solutions for $N = 1, 2, 3, 4$. At $N = 5$, there are four candidates for u', namely $\{38{+}41i, 39{+}40i, 40{+}39i, 41{+}38i\}$, shown in Figure **??**. Since V is unitary, we require $\det(V) = uu^* {+} vv^* = 1$ or, equivalently, $u'(u')^* {+} v'(v')^* = 5^5 = 3125$. So we must have $0 \leq v'(v')^* = 3125 - u'(u')^*$. Then,

$$u' = 38 + 41i \implies u'(u')^* = 38^2 + 41^2 = 3125 \tag{3}$$
$$u' = 39 + 40i \implies u'(u')^* = 39^2 + 40^2 = 3121 \tag{4}$$
$$u' = 40 + 39i \implies u'(u')^* = 3121 \tag{5}$$
$$u' = 41 + 38i \implies u'(u')^* = 3125. \tag{6}$$

[3] The channel induced by a unitary U is an action of U on a density matrix ρ: $\mathcal{U}(\rho) = U\rho U^\dagger$. Channels and density matrices are defined fully in Section **??**.

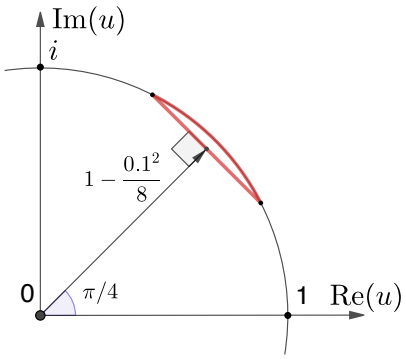


Figure 3: Geometric interpretation of constraint on complex number u in Equation (**??**). The region with the red boundary contains candidate points $(a, b) \in \mathbb{Z}^2$, such that $u = a+ib$ and $\left|\mathrm{Re}(ue^{-i\pi/4})\right| \geq 1-(0.1)^2/8$.

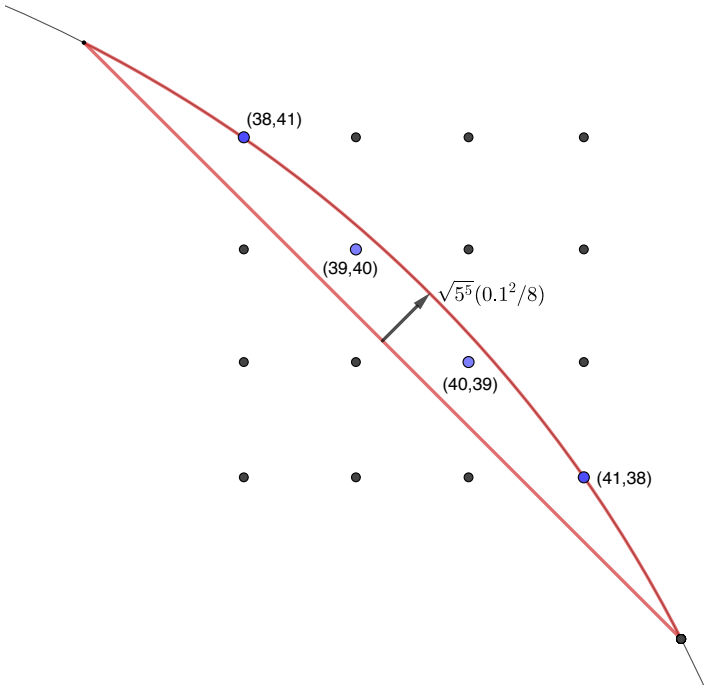


Figure 4: Geometric interpretation of the constraint on complex number u', such that $V = \frac{1}{\sqrt{5^5}}\begin{pmatrix} u' & -(v')^* \\ v' & (u')^* \end{pmatrix}$ approximates $e^{i\frac{\pi}{4}Z}$ to accuracy $\varepsilon = 0.1$. The region with the red boundary contains four candidate complex numbers satisfying $\left|\mathrm{Re}(u'e^{-i\pi/4})\right| \geq \sqrt{5^5}(1-(0.1)^2/8)$.

Let $v' = c + id$, so

$$v'(v')^* = c^2 + d^2 = 5^5 - (a^2 + b^2). \tag{7}$$

For Equations (**??**) and (**??**), we have $v'(v')^* = 0$ so $v = 0$ is the only solution. Equations (**??**) and (**??**) yield $v'(v')^* = 4$, so $c^2 + d^2 = 4 = 2^2$ then either $c = \pm 2, d = 0$ or $c = 0, d = \pm 2$. The two corresponding values for v' are ± 2 and $\pm 2i$. In general, Equation (**??**) admits a solution for $v \in \mathbb{Z}[i]$ if and only if all terms p^k in the prime factorization of $5^5 - (a^2 + b^2)$, with $p \equiv 3 \bmod 4$, have even exponent k. Each candidate pair (u', v') defines an approximation unitary $V = \frac{1}{\sqrt{3125}}\begin{pmatrix} u' & -(v')^* \\ v' & (u')^* \end{pmatrix}$, which is factorized over the V

basis. These factorizations are given in Table **??**.

u'	v'	V basis factorization
$41+38i$	0	$(V_{-Z})^5$
$38+41i$	0	$iZ \cdot (V_{+Z})^5$
$39+40i$	$2i$	$e^{i\pi} \cdot V_{-X}V_{-Y}V_{+X}V_{+Y}V_{-X}$
	2	$e^{i\pi} \cdot V_{+Y}V_{-X}V_{-Y}V_{+X}V_{+Y}$
	$-2i$	$e^{i\pi} \cdot V_{+X}V_{+Y}V_{-X}V_{-Y}V_{+X}$
	-2	$e^{i\pi} \cdot V_{-Y}V_{+X}V_{+Y}V_{-X}V_{-Y}$
$40+39i$	$2i$	$-iZ \cdot V_{-Y}V_{-X}V_{+Y}V_{+X}V_{-Y}$
	2	$-iZ \cdot V_{+X}V_{-Y}V_{-X}V_{+Y}V_{+X}$
	$-2i$	$-iZ \cdot V_{+Y}V_{+X}V_{-Y}V_{-X}V_{+Y}$
	-2	$-iZ \cdot V_{-X}V_{+Y}V_{+X}V_{-Y}V_{-X}$

Table 3: V basis factorizations of unitaries $V := \frac{1}{\sqrt{5^5}} \begin{pmatrix} u' & -(v')^* \\ v' & (u')^* \end{pmatrix}$, satisfying $\left\| e^{i\frac{\pi}{4}Z} - V \right\|_\diamond \leq \varepsilon = 0.1$.

3 Connections to cryptography and hash functions

In this section we will recall some definitions and results about cryptographic hash functions. In particular, we explain the connection between the Charles, Goren and Lauter hash construction [CLG09], built from LPS graphs, to unitary synthesis problems.

A *hash function* $h : \{0,1\}^* \to \{0,1\}^m$ is a function which takes bitstrings of arbitrary length as inputs, and outputs bitstrings of fixed length. A hash function is required to be *preimage resistant*; that is, given a value $y \in \{0,1\}^m$ in the image of h, it must be computationally infeasible to find a bitstring x which hashes to that value. This is formalized in Problem **??**.

Problem 3.1 (Preimage Finding Problem)**.** *Given a hash function h and a value $y \in \mathrm{Im}(h)$, find x such that $h(x) = y$.*

There are several constructions of hash functions built on Cayley graphs. Given a group $\mathcal{G}$ with generating set $S = \{s_0, \ldots, s_k\}$, the corresponding Cayley graph has vertices associated with elements g in $\mathcal{G}$ and directed edges (g, h) if and only if $gh^{-1} \in S$. Writing a message $m = m_1 m_2 \ldots m_k$ with $m_i \in \{0, \ldots, k\}$, the hash function is defined by $H(m) = s_{m_1} s_{m_2} \ldots s_{m_n}$. For such constructions, called Cayley hash functions, Problem **??** can be reformulated as the group theoretic problem below.

Problem 3.2 (Constructive Membership Problem)**.** *Let $\mathcal{G}$ be a group with generating set $S = \{s_1, \ldots, s_k\}$ and let $N \in \mathbb{Z}$ be small. Given an element $g \in \mathcal{G}$, find a sequence $m_1, \ldots, m_N$ such that $g = \prod_i s_{m_i}$.*

In [CLG09], Charles, Goren and Lauter (CGL) proposed a Cayley hash function based on LPS graphs. LPS graphs were introduced by Lubotsky, Phillips and Sarnak in [LPS88]. Let p, ℓ be distinct primes congruent to 1 mod 4, where $\left(\frac{\ell}{p}\right) = 1$. Let $\mathbb{F}_p$ denote the finite field with p elements and let ι such that $\iota^2 = -1 \mod p$. An LPS graph $X_{p,\ell}$ is the Cayley graph with $\mathcal{G} = PSL(2, \mathbb{F}_p)$, the projective special linear group of 2×2 matrices over $\mathbb{F}_p$,

and generating set $S = \left\{ \begin{pmatrix} a+\iota b & c+\iota d \\ -c+\iota d & a-\iota b \end{pmatrix} : a^2+b^2+c^2+d^2 = \ell \right\}$, where $a > 0$ and b, c, d even. We can write $g \in \mathcal{G}$ as $\begin{pmatrix} a+\iota b & c+\iota d \\ -c+\iota d & a-\iota b \end{pmatrix}$ with $a, b, c, d \in \mathbb{F}_p$ and define the norm function $n(g) = a^2 + b^2 + c^2 + d^2$. The preimage problem for the CGL hash function amounts to path finding on an LPS graph. Since these are Cayley graphs, the preimage problem is equivalent to Problem **??**.

Recall that the unitary synthesis problem is the search for a circuit, or sequence, of unitaries from a specified gate set that is equivalent to some target unitary. Clearly, this problem is highly related to Problem **??**. Unitaries are represented by matrices over $\mathbb{C}$ and vertices in $X_{p,\ell}$ correspond to matrices over $\mathbb{F}_p$, and both problems look for 'short' sequences in a subset of matrices. Remarkably, algorithms developed independently to solve the constructive membership problem for LPS graphs [PLQ08; Sar17] and the quantum unitary synthesis problem [Ros15; BBG15b] have many similarities. Petit, Lauter and Quisquater [PLQ08] proposed an algorithm for finding short paths in LPS graphs in which a matrix from the group $\mathcal{G}$ is decomposed into the product of four diagonal matrices with square determinant and graph generators, up to multiplication by a unit. Each diagonal matrix is factorized into elements from S using an extension of the Tillich-Zémor algorithm [TZ08] for collision finding in an LPS graph. This diagonal decomposition method is reminiscent of the Euler decomposition method for unitary synthesis, described in greater detail in Section **??**, in which the target unitary is decomposed into the product of Z-axis rotations. Notably, Z-axis rotations can be expressed as diagonal matrices. Carvalho Pinto and Petit [CP18] later improved upon the algorithm in [PLQ08], by decomposing the target matrix into the product of two diagonal matrices and a third non-diagonal, easily-factorizable matrix, resulting in path lengths of $7\log_\ell(p)$. In Section **??** we translate the algorithm to the continuous setting of general unitary approximation, achieving a similar improvement in sequence length. We obtain an additional constant factor improvement by implementing approximation via quantum channel mixing.

We deal with the problem of approximating unitaries to some chosen accuracy ε. The algorithms described in [PLQ08] and [CP18] both involve 'lifting' a matrix $M \in PSL(2, \mathbb{F}_p)$ to a matrix $M' \in GL(\mathbb{Z}[i])$, such that the corresponding entries of each matrix are congruent modulo p. In other words, for some well-defined p-adic norm the distance between M and M' is $O(p^{-1})$. The matrix M' is then factorized over $GL(\mathbb{Z}[i])$, with some conditions regarding the determinant size, with each factor mapped back to $PSL(2, \mathbb{F}_p)$ via a group homomorphism. The lifting step is analogous to approximation in the quantum setting, using p^{-1} as a measure of accuracy. Clearly, p^{-1} is analogous to ε. Of course, in the LPS hash setting p is fixed, whereas in the quantum setting we have some control over the value ε. The length of a sequence indicates the cost of approximating the target unitary in the context of gate synthesis. For the CGL hash function, the sequence length will equal the length of the corresponding path in the LPS graph, and is similarly used as measure of performance for path-finding algorithms. The length of a sequence is determined by taking the norm of the target matrix. For matrices over $\mathbb{C}$, we can use some some complex matrix norm, while matrices in $PSL(2, \mathbb{F}_p)$ use some p-adic norm. For instance, the six unitary approximation problems defined in Section **??** use the diamond norm to measure accuracy. Note, however, that despite the similarities just described, not all of these approximation problems have natural analogues in cryptography. In particular, those problems that utilize fall-back and channel mixing techniques do not translate to the classical setting. Moreover, the other properties required of cryptographic hash functions - collision resistance and second preimage resistance - do not yet have quantum approximation analogues, either.

The gate sets considered in this paper are quaternion gate sets, so-called due to their

relationship to quaternion algebras (see Section **??**). Sarnak first observed the connection between LPS graphs, quaternion orders and quantum gate sets in his letter to Aaronson and Pollington on the Solvay-Kitaev Theorem and golden gates [Sar]. For instance, synthesis over the V basis is analogous to path finding in an LPS graph $X_{p,\ell}$, where $p \equiv 1 \bmod 4$ and $\ell = 5$. We return to the V basis in Section **??**, as an example of a quaternion gate set, along with the Clifford $+T$ basis and the Clifford$+\sqrt{\mathrm{T}}$ basis.

4 Approximation problems

In this section we introduce six problems that address the approximation of qubit unitaries. Recall that in this paper we follow a two-step approach to solving approximation problems. First, in this section, we relate each problem to one-dimensional or two-dimensional regions. Second, in **??**, we find sequences of gates $g_1, \ldots, g_n$ over gate-set G such that for a unitary computed by the sequence $g_1 \ldots g_n = \left(\begin{smallmatrix} u & -v^* \\ v & u^* \end{smallmatrix}\right)$ the top-left entry u belongs to a two-dimensional region of the complex plain, or the absolute values $|u|$ belongs to an interval, that is one-dimensional region. In this section we also show that these sequences $g_1, \ldots, g_n$ then can be used to construct solutions to the approximation problems.

We begin by establishing some notation and key definitions [KLM07; NC00; Wat18]. An arbitrary two-by-two unitary matrix with determinant one (i.e., a special unitary matrix) can be written as:

$$U = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}, \text{ for } u, v \in \mathbb{C} \text{ such that } |u|^2 + |v|^2 = 1$$

Using the polar form of complex numbers we can write $u = r_1 \exp(i\psi_1)$ and $v = ir_2 \exp(i\psi_2)$. Let us introduce $r_1 = \cos(\theta)$ and $r_2 = \sin(\theta)$ for some $\theta \in [0, \pi/2]$ because $r_1^2 + r_2^2 = 1$. The unitary U can then be expressed as

$$U = \cos(\theta) e^{i\psi_1 Z} + \sin(\theta) i X e^{i\psi_2 Z} \text{ for } \psi_1, \psi_2, \theta \in \mathbb{R} \tag{8}$$

We will interchangeably use both parameterizations of a special unitary U. We denote the special unitary group, that is the group of all two by two unitary matrices with determinant equal to 1, by SU(2). We will also frequently use the fact that Pauli matrices are Hermitian and equal to their inverses.

A probabilistic ensemble of pure quantum states is represented as a trace-one positive semidefinite operator called a *density matrix*. The most general type of transformation on quantum state is a *channel*, a linear completely positive trace-preserving map on the space of density matrices. The action of a unitary U on density matrix ρ is given by

$$\mathcal{U}(\rho) = U \rho U^\dagger \tag{9}$$

and we refer to $\mathcal{U}$ as the "channel induced by U". For diagonal unitaries of the form $e^{i\phi Z}, e^{i\theta X}$ we denote the induced channel by

$$\mathcal{Z}_\phi(\rho) = e^{i\phi Z} \rho e^{-i\phi Z}, \; \mathcal{X}_\theta(\rho) = e^{i\theta X} \rho e^{-i\theta X} \tag{10}$$

To measure the distance between channels we use the diamond norm

$$\|\Phi\|_\diamond := \max_\rho \|(\Phi \otimes \mathcal{I})(\rho)\|_1 \tag{11}$$

where $\mathcal{I}$ is the channel induced by the identity matrix. For additional discussion and facts about the diamond norm see Appendix **??**.

Our main goal in this paper is to solve single-qubit unitary approximation problems. The most general form is:

Problem 4.1 (General qubit unitary approximation)**.** *Given:*

- *target unitary* $U \in \mathrm{SU}(2)$*,*
- *gate set* G*, a finite set of unitary matrices with determinant one*
- *accuracy* ε*,*[4] *a positive real number*

Find a channel $\mathcal{V}$ *implemented using elements of* G *and computational basis measurements such that*

$$\|\mathcal{U} - \mathcal{V}\|_\diamond \leq \varepsilon,$$

where $\mathcal{U}$ *is the channel induced by* U*.*

In a simpler case, when channel $\mathcal{V}$ corresponds to unitary V equal to the product $g_1 \dots g_n$ of two-by-two matrices from gate set G, the diamond norm is tightly bounded by twice the minimum spectral norm distance between $\pm U$ and V (see **??**). To avoid frequent explicit references to channels $\mathcal{U}$ and $\mathcal{V}$ induced by unitaries U and V we introduce distance between unitaries U and V as:

$$\mathcal{D}_\diamond(U, V) = \|\mathcal{U} - \mathcal{V}\|_\diamond. \tag{12}$$

Of particular interest is the case where U is a diagonal unitary, namely $U = e^{i\phi Z}$ for real ϕ. This case is very common in many quantum algorithms. In addition, the state-of-the-art way of solving the general unitary approximation problem is to use *Euler angle decomposition* to reduce the problem to three diagonal unitary approximation problems. Recall that $e^{i\theta X} = \cos(\theta)I + i\sin(\theta)X$. Euler decomposition is performed by solving for ϕ_1, ϕ_2 in the equation below:

$$U = \cos(\theta)e^{i\psi_1 Z} + \sin(\theta)iXe^{i\psi_2 Z} = e^{i\phi_1 Z}e^{i\theta X}e^{i\phi_2 Z} = \cos(\delta)e^{i(\phi_1+\phi_2)Z} + \sin(\theta)iXe^{i(\phi_2-\phi_1)Z} \tag{13}$$

To obtain the last equality we used the fact that $e^{i\phi Z}X = Xe^{-i\phi Z}$, since $XZX = -Z$ and for any invertible matrix A and any matrix B, it is the case that $Ae^B A^{-1} = e^{ABA^{-1}}$.

In this section, we demonstrate how the general unitary approximation problem reduces to two diagonal approximations and a search for elements in a one-dimensional (1D) region, that we call magnitude approximation problem, improving on the traditional Euler angle decomposition approach. We then introduce a series of four problems for approximating diagonal unitaries, corresponding to the combinations of using probabilistic mixing (or not) and using fallback protocols [BRS14] (or not). For each problem we give a reduction to the search for elements in two-dimensional (2D) regions. We conclude the section with applying mixing to the magnitude approximation. **??** summarizes this section.

4.1 Magnitude approximation

In the general unitary approximation problem (Problem **??**), the task is to approximate an arbitrary unitary U. The standard approximation strategy is to use the Euler angle decomposition $U = e^{i\phi_1 Z}e^{i\theta X}e^{i\phi_2 Z}$ and independently approximate the three elements of the product. Our new approach is to first approximate $e^{i\theta X}$ up to phases, that is finding a unitary V equal to $e^{i\phi_1' Z}e^{i\theta' X}e^{i\phi_2' Z}$ such that θ and θ' are close. In other words only magnitudes of entries of U and V are close, and phases ϕ_1' and ϕ_2' are arbitrary. We then re-express U as:

$$U = e^{i(\phi_1-\phi_1')Z}\underline{e^{i\phi_1' Z}e^{i\theta X}e^{i\phi_2' Z}}e^{i(\phi_2-\phi_2')Z}. \tag{14}$$

[4] The parameter ε is commonly referred to as the *precision* in the literature. Since we use ε as a measure of approximation error from a target, we believe the term accuracy is more appropriate.

Table 4: Summary of the qubit unitary approximation protocols. Each protocol corresponds to a "key problem" for which the top-left entry of matrix $\left(\begin{smallmatrix} u & -v^* \\ v & u^* \end{smallmatrix}\right)$ belongs to a two-dimensional region of complex plain, or the absolute value $|u|$ belongs to a one-dimensional interval. Some approximation protocols use others as sub-protocols. Combining the solution to the key problem(s) with the sub-protocols is described by the statements in "Full protocol analysis" column. Comparisons of the geometric regions are given in **??**, **??** and **??**. For cost scaling see **??** and **??**.

Approximation protocol	Section	Target unitary	Key problem definition	Key problem region	Full protocol analysis	Sub-protocols
General unitary	**??**	SU(2)	**??** (magnitude)	**??** **??**	**??**	Diagonal or Fallback
Mixed general unitary	**??**	SU(2)	**??** (magnitude)	**??** **??**	**??**	Mixed diagonal or mixed fallback
Diagonal unitary	**??**	$e^{i\varphi Z}$	**??** (diagonal)	**??** **??**	**??**	-
Mixed diagonal unitary	**??**	$e^{i\varphi Z}$	**??** (diagonal)	**??** **??**	**??**	-
Fallback (**??**)	**??**	$e^{i\varphi Z}$	**??** (projective)	**??** **??**	**??**	Diagonal
Mixed fallback	**??**	$e^{i\varphi Z}$	**??** (projective)	**??** **??**	**??**	Mixed diagonal

The underlined middle part of the product is approximated by V, so it remains to approximate two diagonal Z rotations.

The first main insight behind this strategy is that magnitude approximations have lower cost (see **??** and **??**) and are easier to find than diagonal approximations. The second insight is that, for a random angle θ, the approximation cost of a diagonal unitary $e^{i\theta Z}$ is independent of θ (see **??** and **??**). Therefore, we may freely adjust the angles of the Z-axis rotations in the Euler decomposition in order to compensate for phase inaccuracy of the X-axis rotation. This results in a circuit that is approximately one-third shorter, in terms of gate-count, than the solution resulting directly from Euler decomposition. An analogous strategy was developed by Carvalho Pinto and Petit in [CP18] for path finding in LPS graphs, and they noted that their method could be adapted to the quantum setting. This was also confirmed by Stier [Sti20], concurrent to the work done in this paper. To construct V, we use the following proposition, which determines the approximate synthesis of any unitary by imposing the condition that the norm of its upper left element lies in a given interval.

Proposition 4.2 (Magnitude approximation condition)**.** *Let θ be from $[0, \pi/2]$ and ε be a positive real number. Suppose that we have found a special unitary V*

$$V = g_1 \dots g_n = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}$$

over gate set G such that $|u|$ belongs to the interval $\{\cos(\theta'') : \theta'' \in [0, \pi/2], |\theta'' - \theta| \leq \delta\}$ for $\delta = \arcsin(\varepsilon/2)$.

*Then unitary V satisfies the inequality $\mathcal{D}_\diamond\left(V, e^{i\phi_1' Z}\underline{e^{i\theta X}}e^{i\phi_1' Z}\right) \leq \varepsilon$, for ϕ_1' and ϕ_2' defined by the equality $V = e^{i\phi_1' Z}e^{i\theta' X}e^{i\phi_1' Z}$ with $\theta' \in [0, \pi/2]$. We call such V a **magnitude ε-approximation** of $e^{i\theta X}$. For a geometric interpretation of the constraint see Figure **??**.*

Proof. By unitary invariance property of the diamond norm (see **??**), distance $\mathcal{D}_\diamond\left(V, e^{i\phi_1' Z}\underline{e^{i\theta X}}e^{i\phi_1' Z}\right)$ is equal to $\mathcal{D}_\diamond\left(e^{i\theta' X}, e^{i\theta X}\right)$. Now we use the the fact that diamond norm distance between

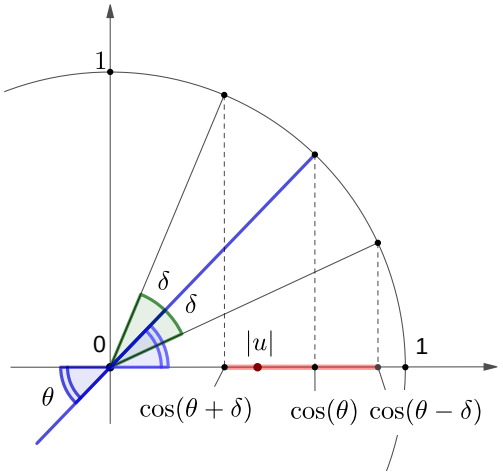


Figure 5: Geometric interpretation of the constraint on complex number u appearing in Proposition **??**. Possible absolute values $|u|$ belong to the interval $\{\cos(\theta'') : \theta'' \in [0, \pi/2], |\theta'' - \theta| \leq \delta\}$ for $\delta = \arcsin(\varepsilon/2)$ and are shown as blue and dashed blue segments on the horizontal axis.

unitaries U and V is equal to the diameter of the smallest disc containing eigenvalues of $U^\dagger V$ (see **??**). The eigenvalues of $e^{i(\theta'-\theta)X}$ are $e^{\pm i(\theta-\theta')}$ because Hadamard diagonalizes $e^{i\phi X} = He^{i\phi Z}H$. Because we only have two eigenvalues, the diameter of the disc containing them is equal to distance $|e^{i(\theta-\theta')} - e^{-i(\theta-\theta')}|$, which is equal to $2|\sin(\theta - \theta')|$. It remain to upper-bound this quantity. By definition of θ', $|u| = \cos(\theta')$. This implies that $|\theta' - \theta| \leq \delta$ because cosine is a bijection from $[0, \pi/2]$ onto $[0, 1]$. Using $\sin(\delta) = \varepsilon/2$ we get the required bound.

□

Note that when $\arcsin(\varepsilon/2) \leq \theta \leq \pi/2 - \arcsin(\varepsilon/2)$, the absolute value $|u|$ must simply belong to interval $[\cos(\theta - \arcsin(\varepsilon/2), \cos(\theta + \arcsin(\varepsilon/2))]$.

A simple way to leverage Proposition **??** for general unitary approximation is to split the accuracy ε evenly among the three factors of the Euler decomposition. Then, use Proposition **??** to find a magnitude $\epsilon/3$-approximation of the X-axis rotation. Finally, find $\varepsilon/3$-approximations of the two remaining Z-axis rotations, adjusting the angles to compensate for the phase inaccuracy of the X-axis rotation. This strategy is captured formally in the following proposition.

Proposition 4.3 (General unitary approximation)**.** *Suppose we are given a target unitary $U = e^{i\phi_1 Z}e^{i\theta X}e^{i\phi_2 Z}$ and target accuracy ε. Let V be a magnitude ε_0-approximation of $e^{i\theta X}$ (see **??**) and let $V = e^{i\phi_1' Z}e^{i\theta' X}e^{i\phi_2' Z}$. Let channels Ψ_k be within diamond norm distance ε_k from unitary $e^{i(\phi_k - \phi_k')Z}$, for $k = 1, 2$, and let $\varepsilon \geq \varepsilon_0 + \varepsilon_1 + \varepsilon_2$.*

Then channel $\mathcal{U}$ induced by U and composition $\Psi_1\mathcal{V}\Psi_2$ satisfy

$$\|\mathcal{U} - \Psi_1\mathcal{V}\Psi_2\|_\diamond \leq \varepsilon, \text{ where } \mathcal{V} \text{ is the channel induced by } V.$$

Proof. Let us write U as a product $U_1U_0U_2$, where $U_k = e^{i(\phi_k - \phi_k')Z}$ and $U_0 = e^{i\phi_1' Z}e^{i\theta X}e^{i\phi_2' Z}$. We then write channel $\mathcal{U}$ as composition of channels $\mathcal{U}_1\mathcal{U}_0\mathcal{U}_2$, where $\mathcal{U}_k$ is the channel induced by U_k. Using the chain rule for diamond norm we have:

$$\|\mathcal{U} - \Psi_1\mathcal{V}\Psi_2\|_\diamond = \|\mathcal{U}_1\mathcal{U}_0\mathcal{U}_2 - \Psi_1\mathcal{V}\Psi_2\|_\diamond \leq \|\mathcal{U}_1 - \Psi_1\|_\diamond + \|\mathcal{U}_0 - \mathcal{V}\|_\diamond + \|\mathcal{U}_2 - \Psi_2\|_\diamond \quad (15)$$

By **??** $\|\mathcal{U}_0 - \mathcal{V}\|_\diamond \leq \varepsilon_0$. Combining this bound with **??** completes the proof. □

One can optimize the choices of ε_k in the above **??**. For random diagonal approximation, the cost scales as $3\log_2(1/\varepsilon) + O(1)$ and for random magnitude approximation the cost scales as $\log_2(1/\varepsilon) + O(1)$ (see **??**). To minimize overall sequence length one can choose $\varepsilon_1 = \varepsilon_2 = 0.43\varepsilon$ and $\varepsilon_0 = 0.14\varepsilon$, however this improves the sequence length only by a small additive constant 0.95 in comparison to distributing errors equally.

4.2 Diagonal unitary approximation

The Euler angle decomposition **??** describes a qubit unitary as a product of two diagonal unitaries of the form $e^{i\theta Z}$ and one X rotation of the form $e^{i\theta X}$. Proposition **??** further reduces the X rotation to a one-dimensional search problem, leaving just the diagonal unitaries. Therefore, the special case of diagonal unitary approximation is relevant to the general unitary approximation problem. In this section we recall some of the known results regarding the diagonal approximation problem.

Problem 4.4 (Diagonal unitary approximation)**.** *Given:*

- *target angle θ, a real number,*
- *gate set G, a finite set of two by two unitary matrices with determinant one,*
- *accuracy ε, a positive real number,*

Find a sequence $g_1, \ldots, g_n$ of elements of G such that

$$\mathcal{D}_\diamond\left(\exp(i\theta Z), g_1 \ldots g_n\right) \leq \varepsilon.$$

Observe that Problem **??** is a special case of the general unitary approximation problem, where the target unitary is diagonal and approximating channel $\mathcal{V}$ is induced by unitary $g_1 \ldots g_n$. The diagonal unitary approximation problem is easier to solve because it admits the following bound on the diamond norm that depends only on the top left entry of $V = g_1 \ldots g_n$.

Lemma 4.5 (Diamond difference from a diagonal unitary)**.** *Given an angle θ and a unitary*

$$V = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix},$$

the distance

$$\mathcal{D}_\diamond(e^{i\theta Z}, V) = 2\sqrt{1 - \left(\mathrm{Re}(ue^{-i\phi})\right)^2} \leq 2\sqrt{2 - 2|\mathrm{Re}(ue^{-i\theta})|}.$$

Proof of this bound is in **??** in Appendix **??**. Lemma **??** immediately suggests a simple condition for solutions of the diagonal approximation problem.

Proposition 4.6 (Diagonal approximation condition)**.** *Let $g_1, \ldots, g_n$ be a sequence of gates from a gate set G and let*

$$g_1 \ldots g_n = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}.$$

Then $g_1, \ldots, g_n$ is a solution to the diagonal approximation problem for target angle θ, gate set G and accuracy ε if

$$\left|\mathrm{Re}\left(ue^{-i\theta}\right)\right| \geq \sqrt{1 - \varepsilon^2/4}. \tag{16}$$

*For a geometric interpretation of the constraints see Figure **??**.*

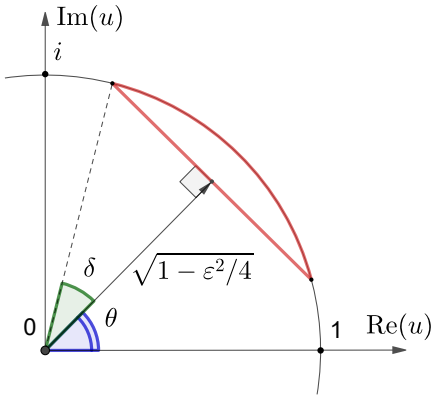


Figure 6: Geometric interpretation of constraints on complex number u appearing in Proposition **??**. The region with red boundary contains complex numbers u that satisfy constraints $\mathrm{Re}\big(ue^{-i\theta}\big) \geq \sqrt{1-\varepsilon^2/4}$ and $|u| \leq 1$. Note that the segment spans points with angular coordinates $[\theta-\delta, \theta+\delta]$ for $\delta = \arcsin(\varepsilon/2)$. Constraints in Proposition **??** lead to two regions: one with segment spanning points with angular coordinates $[\theta-\delta, \theta+\delta]$ and another one with $[\pi+\theta-\delta, \pi+\theta+\delta]$.

Proof. Let $\mathcal{V}$ be the channel induced by unitary $V = g_1 \dots g_n$. Then by Lemma **??**

$$\|\mathcal{Z}_\theta - \mathcal{V}\|_\diamond = 2\sqrt{1-|\mathrm{Re}(ue^{-i\theta})|^2} \leq 2\sqrt{\varepsilon^2/4} = \varepsilon. \tag{17}$$

□

4.3 Fallback approximation

Fallback protocols [BRS15a] offer a more efficient way to approximate diagonal unitaries by incorporating measurements. A fallback protocol is a non-deterministic single-qubit quantum channel consisting of two steps: a projective rotation and a conditional fallback. The projective rotation and fallback steps may be implemented in a variety of ways. We limit our discussion to fallback protocols with the form illustrated in Figure **??**.

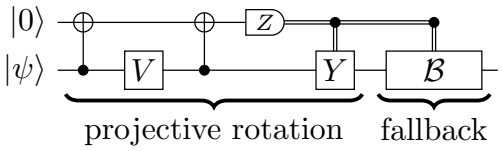


Figure 7: A fallback protocol circuit [BRS15a]. The circuit is composed of two steps, a projective rotation step and a fallback step. The projective rotation step effects one of two diagonal rotations on the input $|\psi\rangle$ depending on the Z-basis measurement outcome of the top ancilla qubit. The two rotation angles are determined by the matrix entries of the unitary V. If the measurement outcome is one, then a Pauli Y is applied followed by the fallback step $\mathcal{B}$.

For a fixed single-qubit unitary

$$V = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix} \tag{18}$$

the corresponding projective rotation effects one of two diagonal rotations on $|\psi\rangle$ depending on the measurement outcome. With probability $|u|^2$ the measurement outcome is zero,

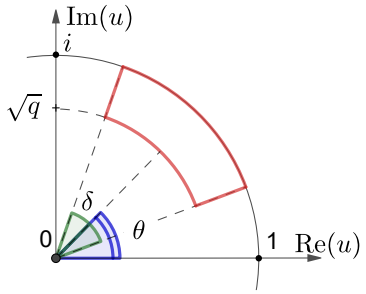


Figure 8: Geometric interpretation of constraint on complex number u appearing in Proposition **??**. The region with red boundary contains complex numbers u that satisfy constraints $\mathrm{Arg}(u) \in [\theta - \delta, \theta + \delta]$ and $|u| \geq q$, where $\delta = \arcsin(\varepsilon/2)$. Constraints in Proposition **??** lead to two regions: one with $\mathrm{Arg}(u) \in [\theta - \delta, \theta + \delta]$ and another one with $\mathrm{Arg}(u) \in [\pi + \theta - \delta, \pi + \theta + \delta]$

the projective rotation is said to have "succeeded" and the input state undergoes the transformation

$$|\psi\rangle \mapsto e^{i\theta_0 Z}|\psi\rangle = e^{i\mathrm{Arg}(u)Z}|\psi\rangle. \tag{19}$$

otherwise, the measurement outcome is one, the projective rotation is said to have "failed" and

$$|\psi\rangle \mapsto e^{i\theta_1 Z}|\psi\rangle = e^{i\mathrm{Arg}(v)Z}|\psi\rangle. \tag{20}$$

The projective rotation is intended to approximate a target diagonal unitary $e^{i\theta Z}$ so that $\theta_0 \approx \theta$. The constraints necessary to achieve that goal are captured by the following problem.

Problem 4.7 (Projective approximation)**.** *Given:*

- *target angle θ, a real number,*
- *success probability q, a positive real number between 0 and 1,*
- *gate set G, a finite set of two by two unitary matrices with determinant one,*
- *accuracy ε, a positive real number,*

find a sequence $g_1, \ldots, g_n$ of elements in G, such that for u, v defined via $g_1 \ldots g_n = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}$ the following holds:

- $|u|^2 \geq q$, *and*
- $\mathcal{D}_\diamond\left(e^{i\theta Z}, e^{i\mathrm{Arg}(u)Z}\right) \leq \varepsilon$.

Much like the case of the diagonal approximation problem (**??**), solutions to Problem **??** can be characterized entirely by conditions on the complex value u at the top-left entry of the circuit unitary $g_1 \ldots g_n$. These conditions are, however, less restrictive than those prescribed by Proposition **??**. For the detailed comparison of the conditions see **??** and **??**.

Proposition 4.8 (Projective approximation condition)**.** *Let $g_1, \ldots, g_n$ be a sequence of gates from a gate set G and $g_1 \ldots g_n = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}$. Then $g_1, \ldots, g_n$ is a solution to the projective approximation problem (Problem **??**) if u satisfies*

$$|u| \geq \sqrt{q} \text{ and } (\sin|\mathrm{Arg}(u) - \theta| \leq \varepsilon/2 \text{ or } \sin|\mathrm{Arg}(u) - (\theta + \pi)| \leq \varepsilon/2)$$

*For a geometric interpretation of these constraints see Figure **??**.*

Proof. The condition $|u| \geq \sqrt{q}$ is equivalent to $|u|^2 \geq q$ from Problem **??**.

It remains to show that $\left\|\mathcal{Z}_\theta - \mathcal{Z}_{\mathrm{Arg}(u)}\right\|_\diamond \leq \varepsilon$. According to **??**, we have $\left\|\mathcal{Z}_\theta - \mathcal{Z}_{\mathrm{Arg}(u)}\right\|_\diamond \leq 2\sin|\mathrm{Arg(u)}-\theta|$. This immediately implies that the channels are ε-close when $\sin|\mathrm{Arg}(u) - \theta| \leq \varepsilon/2$. Because $\mathcal{Z}_\theta = \mathcal{Z}_{\theta+\pi}$ inequality $\sin|\mathrm{Arg}(u) - (\theta + \pi)| \leq \varepsilon/2$ also ensures $\left\|\mathcal{Z}_\theta - \mathcal{Z}_{\mathrm{Arg}(u)}\right\|_\diamond \leq \varepsilon$. □

[BRS15a] constructs a solution to Problem **??** by first approximating the target phase factor $e^{i\theta}$ with a cyclotomic rational of the form z^*/z, then searching for a real-valued modifier to achieve the desired success probability q. The characterization of the fallback approximation problem given by Proposition **??** differs by addressing accuracy (ε) and success probability (q) conditions simultaneously, resulting in an intuitive geometric description as illustrated in Figure **??**.

Any solution to the diagonal approximation problem is also a solution to the corresponding projective approximation problem. The projective problem admits additional and possibly cheaper solutions.

Problem **??** constrains the action of a successful projective rotation but ignores the failure case. The difference $\theta - \theta_1$ between the target and failure angles may be large, in general. Therefore, in the case of failure (measurement outcome one), the fallback step is applied in order to recover and approximate the target rotation.

The problem of constructing a fallback step can be treated independently of the projective rotation. In [BRS15a], the fallback step is a unitary $B \approx e^{i(\theta-\theta_1)Z}$ chosen so that the net effect of the failure case is

$$|\psi\rangle \mapsto Be^{i\theta_1 Z}|\psi\rangle \approx e^{i\theta Z}|\psi\rangle. \tag{21}$$

This choice corresponds directly to the diagonal approximation **??** defined earlier. A complete fallback protocol of this form may be constructed by first solving Problem **??** and then solving Problem **??** for appropriate values of ε. This is captured by the following proposition that follows from standard properties of the diamond norm (see **??**).

Proposition 4.9 (Fallback approximation)**.** *Suppose we are given:*

- *target angle θ, a real number,*
- *success probability q, a positive real number between 0 and 1,*
- *gate set G, a finite set of two by two unitary matrices with determinant one*

and

- *real numbers $\varepsilon_1, \varepsilon_2$*
- *$g_1 \ldots g_n = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}$, a solution to Problem **??** for $\{\theta, q, G, \varepsilon_1\}$, and*
- *$b_1 \ldots b_m = B$, a solution to Problem **??** for $\{\theta - \mathrm{Arg}(v), G, \varepsilon_2\}$*

then overall fallback protocol accuracy is

$$\left\|\mathcal{Z}_\theta - |u|^2\mathcal{Z}_{\mathrm{Arg}(u)} - |v|^2\mathcal{B}\mathcal{Z}_{\mathrm{Arg}(v)}\right\|_\diamond \leq \varepsilon_1 + |v|^2\varepsilon_2 \tag{22}$$

where $\mathcal{B}(\rho) := B\rho B^\dagger$.

A simple approach to solving the above problem is to choose $\varepsilon_1 = \varepsilon/2$, solve **??**, then choose $\varepsilon_2 = \varepsilon/2/|v|^2$ and then solve the corresponding instance of **??**.

?? can be generalized to admit an arbitrary quantum channel (denoted by $\mathcal{B}$ in Figure **??**) as the fallback step. For example, the fallback may be simply to repeat the projective rotation until success is achieved [PS14; BRS14]. In Section **??** we consider fallbacks that are probabilistic mixtures of unitaries.

The cost of of fallback protocol is a random variable. When success probability is $q = 1 - p$ for small p, the average cost is equal to the cost of the projective rotation step plus p times the cost of the fallback step, which is the cost of a diagonal approximation. The worst case cost is the sum of the costs of the projective and the diagonal approximation. High worst case cost might become a problem when using N fallback approximations in parallel, however we can always ensure that the probability of at least one of them requiring a fallback step is p by choosing the success probability of each of them $q = 1 - p/N$.

4.4 Mixed diagonal unitary approximation

?? describes synthesis of a qubit unitary by construction and application of a deterministic sequence of elementary gates. An alternative approach, proposed by [Cam17] and [Has17], is to construct several sequences of elementary gates and apply one of them according to a probability distribution. Given the correct probabilistic mixture of unitaries the overall error of the approximation is reduced quadratically, cutting the approximation cost roughly in half. In this paper, we introduce the use of diagonal Clifford twirling to construct these sequences, which ensures that the difference between the ideal and approximating channel is a Pauli channel. Because of this, we obtain a closed-form expression for the diamond distance (see **??**) which improves on analysis in [Cam17; Has17] and results in lower approximation costs. Method in [Cam17] uses diagonal approximation algorithms as black-boxes and finds under-rotations and over-rotations by modifying target rotation angle. In contrast, we modify synthesis algorithms to directly find under and over-rotated approximations and further reduce approximations costs.

Problem 4.10 (Diagonal unitary approximation by unitary mixing)**.** *Given:*

- *target angle θ, a real number,*
- *gate set G, a finite set of two by two unitary matrices with determinant one,*
- *accuracy ε, a positive real number,*

Find

- *$G_1, \ldots, G_n$, a sequence of sequences G_k of elements of G and*
- *$p_1, \ldots, p_n$, a probability distribution*

such that

$$\left\| \mathcal{Z}_\theta - \sum_{k=1}^{n} p_k \mathcal{G}_k \right\|_\diamond \leq \varepsilon$$

where $\mathcal{G}_k$ is the channel obtained by applying the sequence G_k.

This problem generalizes Problem **??** by allowing a random choice among multiple gate sequences.

[Cam17] gives an algorithm for constructing the mixture by "Z twirling" two unitary approximations: an under-rotation and an over-rotation. The *twirl* of a unitary U over generators $\mathcal{G}$ is a channel obtained by uniformly selecting a random element V over the set generated by $\mathcal{G}$ and then applying $VUV^\dagger$. For example, the twirl of U over $\{Z, S = e^{-i\pi Z/4}\}$ which we denote by $\mathcal{T}_U$ is given by

$$\mathcal{T}_U(\rho) = \frac{1}{4} \sum_{V \in \{I,Z,S,S^\dagger\}} \left(VUV^\dagger\right) \rho \left(V^\dagger U^\dagger V\right). \tag{23}$$

We show that by twirling over the set $\{Z, S\}$, instead of Z alone, the approximation error of the unitary mixture is a probabilistic mixture of Pauli operators—i.e., a Pauli channel. This allows for an alternative proof of [Cam17] and [Has17] and yields a simple expression for the approximation error in terms of diamond distance.

The procedure is as follows. Find two unitaries (defined formally below): U_1 an under-rotation and U_2 an over-rotation. Calculate a probability p (also defined below) that depends on U_1 and U_2. With probability p select U_1 and otherwise select U_2. Then apply the $\{Z, S\}$ twirl to that selection. The resulting channel $p\mathcal{T}_{U_1} + (1-p)\mathcal{T}_{U_2}$ approximates a diagonal unitary $e^{i\theta Z}$ with an accuracy given by the following theorem.

Theorem 4.11 (Diamond difference of a twirled mixture)**.** *Let θ be an angle and let unitaries*

$$U_1 = \begin{pmatrix} r_1 e^{i(\theta+\delta_1)} & v_1^* \\ v_1 & r_1 e^{-i(\theta+\delta_1)} \end{pmatrix} \tag{24}$$

$$U_2 = \begin{pmatrix} r_2 e^{i(\theta+\delta_2)} & v_2^* \\ v_2 & r_2 e^{-i(\theta+\delta_2)} \end{pmatrix} \tag{25}$$

for real values r_1, r_2 and $\sin(\delta_1) < 0 < \sin(\delta_2)$. Define probability

$$p = \frac{r_2^2 \sin(2\delta_2)}{r_2^2 \sin(2\delta_2) - r_1^2 \sin(2\delta_1)}. \tag{26}$$

Then

$$||p\mathcal{T}_{U_1} + (1-p)\mathcal{T}_{U_2} - \mathcal{Z}_\theta||_\diamond = 2\left(1 - pr_1^2\cos^2(\delta_1) - (1-p)r_2^2\cos^2(\delta_2)\right). \tag{27}$$

The proof of the theorem in given in **??**. A simple way to leverage **??** is by splitting an approximation error ε evenly between U_1 and U_2 so that

$$\begin{aligned} 1 - r_1^2\cos^2(\delta_1) &\leq \varepsilon/2 \\ 1 - r_2^2\cos^2(\delta_2) &\leq \varepsilon/2. \end{aligned} \tag{28}$$

The synthesis task then is to find two unitary approximations, an "under rotation" U_1 and "over rotation" U_2 each such that

$$|r_k \cos(\delta_k)| \geq \sqrt{1 - \varepsilon/2} = 1 - \varepsilon/4 - \varepsilon^2/32 + o(\varepsilon^2), \text{ for } k = 1, 2. \tag{29}$$

This strategy is captured in the following Proposition.

Proposition 4.12 (Diagonal mixing approximation condition)**.** *Suppose we are given sequences $g_1, \ldots, g_n$ and $h_1, \ldots, h_m$ of gates from a gate set G. Define u_k, v_k from the equations below*

$$g_1 \ldots g_n = \begin{pmatrix} u_1 & -v_1^* \\ v_1 & u_1^* \end{pmatrix}, h_1 \ldots h_m = \begin{pmatrix} u_2 & -v_2^* \\ v_2 & u_2^* \end{pmatrix}.$$

Then

- *sequence $G_1, \ldots, G_4, H_1, \ldots, H_4$, where $G_k = \sigma_k, g_1, \ldots, g_m, \sigma_k^\dagger$, $H_k = \sigma_k, h_1, \ldots, h_m, \sigma_k^\dagger$, and $\sigma_1, \sigma_2, \sigma_3, \sigma_4 = I, S, Z, S^\dagger$.*
- *probability distribution $p/4, p/4, p/4, p/4, (1-p)/4, (1-p)/4, (1-p)/4, (1-p)/4$*

*is a solution to the diagonal unitary approximation Problem **??** with accuracy ε and target angle θ if*

- *u_1 satisfies $\left|\mathrm{Re}\left(u_1 e^{-i\theta}\right)\right| \geq \sqrt{1-\varepsilon/2}$, $\mathrm{Im}\left(u_1 e^{-i\theta}\right) < 0$, and*
- *u_2 satisfies $\left|\mathrm{Re}\left(u_2 e^{-i\theta}\right)\right| \geq \sqrt{1-\varepsilon/2}$, $\mathrm{Im}\left(u_2 e^{-i\theta}\right) > 0$.*

*For a geometric interpretation of these constraints see Figure **??**.*

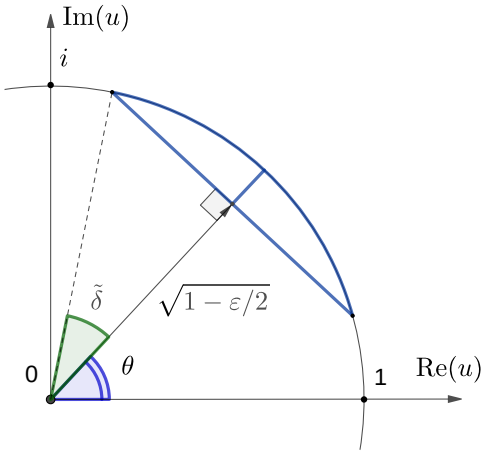


Figure 9: Geometric interpretation of constraints on complex numbers u_1 and u_2 appearing in Proposition **??**. The region with blue boundary contains complex numbers u that satisfy constraints $\mathrm{Re}\big(ue^{-i\theta}\big) \geq \sqrt{1-\epsilon/2}$ and $|u| \leq 1$. This region is split into two parts, an under-rotation region for u_1 with angular coordinates spanning $[\theta - \tilde{\delta}, \theta]$ and an over-rotation region for u_2 with angular coordinates spanning $[\theta, \theta + \tilde{\delta}]$ for $\tilde{\delta} = \arcsin(\sqrt{\varepsilon/2})$.

Proof. First, note that the sequences G_1, G_2, G_3, G_4 along with probabilities $\{p/4, p/4, p/4, p/4\}$ corresponds to the $\{Z, S\}$ twirl of $U_1 = g_1 \dots g_n$ with probability p,

$$p\mathcal{T}_{U_1}(\rho) = \frac{p}{4} \sum_{\sigma \in \{I,Z,S,S^\dagger\}} \Big(\sigma U_1 \sigma^\dagger\Big)\rho\Big(\sigma^\dagger U_1^\dagger \sigma\Big). \tag{30}$$

Similarly, the sequences H_1, H_2, H_3, H_4 along with probabilities $\{(1-p)/4, (1-p)/4, (1-p)/4, (1-p)/4\}$ corresponds to the $\{Z, S\}$ twirl of $U_2 = h_1 \dots h_m$ with probability $(1-p)$,

$$(1-p)\mathcal{T}_{U_2}(\rho) = \frac{1-p}{4} \sum_{\sigma \in \{I,Z,S,S^\dagger\}} \Big(\sigma U_2 \sigma^\dagger\Big)\rho\Big(\sigma^\dagger U_2^\dagger \sigma\Big). \tag{31}$$

We therefore seek to show that $\|p\mathcal{T}_{U_1} + (1-p)\mathcal{T}_{U_2} - \mathcal{Z}_\theta\|_\diamond \leq \varepsilon$. Let $r_1 = |u_1|, \delta_1 = \mathrm{Arg}(u_1) - \theta$ and similarly $r_2 = |u_2|, \delta_2 = \mathrm{Arg}(u_2) - \theta$. Then $\mathrm{Im}\Big(u_1 e^{-i\theta}\Big) = \sin(\delta_1) < 0$ and $\mathrm{Im}\Big(u_2 e^{-i\theta}\Big) = \sin(\delta_2) > 0$. Substituting $U_1 = \left(\begin{smallmatrix} u_1 & -v_1^* \\ v_1 & u_1^* \end{smallmatrix}\right)$, $U_2 = \left(\begin{smallmatrix} u_2 & -v_2^* \\ v_2 & u_2^* \end{smallmatrix}\right)$ into Theorem **??** and using $\Big|\mathrm{Re}(u_1 e^{-i\theta})\Big| \geq \sqrt{1-\varepsilon/2}$, $\Big|\mathrm{Re}(u_2 e^{-i\theta})\Big| \geq \sqrt{1-\varepsilon/2}$, we obtain

$$\begin{aligned}
\|p\mathcal{T}_{U_1} + (1-p)\mathcal{T}_{U_2} - \mathcal{Z}_\theta\|_\diamond &= 2\Big(1 - pr_1^2\cos^2(\delta_1) - (1-p)r_2^2\cos^2(\delta_2)\Big) \\
&= 2\Big(1 - p\mathrm{Re}\Big(u_1 e^{-i\theta}\Big)^2 - (1-p)\mathrm{Re}\Big(u_2 e^{-i\theta}\Big)^2\Big) \\
&\leq 2(1 - p(1-\varepsilon/2) - (1-p)(1-\varepsilon/2)) \\
&= \varepsilon.
\end{aligned} \tag{32}$$

□

As observed by [Cam17; Has17], the constraints imposed by Proposition **??** admit quadratically better scaling in ε as compared to approximation without mixing (Proposition **??**), which would require $|r\cos(\delta)| \geq \sqrt{1-\varepsilon^2/4}$.

Evenly splitting the error as in Proposition **??** does not yield optimal solutions in general. A better approach is to first find a cheap (but possibly poor) approximation of the

target. With the first approximation fixed, a search region for the second approximation can be defined. In particularly, this is useful when identity is a sufficiently good under-rotated or over-rotated approximation to the target rotation. This happens in practice when approximating Fourier angles. See **??** for a detailed treatment.

The main technical component of **??** is to show that the twirled mixture $p\mathcal{T}_{U_1}(\rho) + (1-p)\mathcal{T}_{U_2}(\rho)$ is equal to the target rotation $e^{i\theta Z}$ followed by a Pauli channel error.

Lemma 4.13 (Twirled mixture yields Pauli channel error)**.** *Let θ be an angle, U_1, U_2 be unitaries as in* **??** *and p be a probability as in* **??***. Then*

$$p\mathcal{T}_{U_1}(\rho) + (1-p)\mathcal{T}_{U_2}(\rho) = \mathcal{E}(\mathcal{Z}_\theta(\rho)) \tag{33}$$

where $\mathcal{E}$ is a qubit Pauli channel

$$\mathcal{E}(\rho) = p\mathcal{P}_{r_1,\delta_1}(\rho) + (1-p)\mathcal{P}_{r_2,\delta_2}(\rho) \tag{34}$$

and

$$\mathcal{P}_{r,\delta}(\rho) = r^2\cos^2(\delta)\rho + \frac{1-r^2}{2}(X\rho X + Y\rho Y) + r^2\sin^2(\delta)Z\rho Z. \tag{35}$$

This lemma can be proved by calculating the four by four process matrices for channels induced by U_1, U_2, channels $\mathcal{T}_{U_k}$ and $\mathcal{E}$. Recall that for a qubit channel Ψ the process matrix χ is given by

$$\Psi(\rho) = \sum_{P,Q\in\{I,X,Y,Z\}} \chi_{P,Q} P\rho Q.$$

The $\{Z, S\}$ twirl eliminates all but two off-diagonal elements and the mixture with probability p eliminates the remaining off-diagonal elements. We then see that the process matrix of $\mathcal{E}$ is a diagonal matrix and therefore $\mathcal{E}$ is a Pauli channel. Finally we apply the following result from Section V.A in [MGE12] to get a closed form expression for the diamond norm distance between $\mathcal{E}$ and the identity channel:

Theorem 4.14 (Diamond norm distance between Pauli channels)**.** *Suppose $\mathcal{E}_1$, $\mathcal{E}_2$ are n-qubit Pauli channels, that is*

$$\mathcal{E}_1(\rho) = \sum_{P\in\{I,X,Y,Z\}^{\otimes n}} q_P P\rho P^\dagger,\ \mathcal{E}_2(\rho) = \sum_{P\in\{I,X,Y,Z\}^{\otimes n}} r_P P\rho P^\dagger,$$

then $\|\mathcal{E}_1 - \mathcal{E}_2\|_\diamond = \sum_{P\in\{I,X,Y,Z\}^{\otimes n}} |q_P - r_P|$.

Detailed proofs of **??** and **??** are given in **??**.

4.5 Mixed fallback approximation

The results of [Cam17; Has17] halve the cost of qubit unitary approximation by taking probabilistic mixtures of unitaries. We show that an additional factor of two improvement in cost can be obtained by taking probabilistic mixtures of *channels*. In particular, we demonstrate a procedure for mixing fallback protocols (see Section **??**). The basic idea is to apply at random one of two projective rotations, one that approximates $e^{i\theta Z}$ by over-rotation and one that approximates $e^{i\theta Z}$ by under-rotation. If the projective rotation fails, then a corresponding fallback channel is applied.

Problem 4.15 (Diagonal unitary approximation by projective rotation mixing)**.** *Given:*

- *target angle θ, a real number,*
- *success probability q, a positive real number between 0 and 1,*

- *gate set G, a finite set of two by two unitary matrices with determinant one,*
- *accuracy ε, a positive real number.*

Find

- *$G_1, \ldots, G_n$, a sequence of sequences of elements of G and*
- *$p_1, \ldots, p_n$, a probability distribution*

such that

- *$|u_k|^2 \geq q$ for all $k \in [n]$, and*
- *the diamond norm of the channel below is at most ε*

$$\sum_{k=1}^{n} p_k |u_k|^2 \left(\mathcal{Z}_{\mathrm{Arg}(u_k)} - \mathcal{Z}_\theta \right)$$

where u_k is the top-left entry of the unitary $\begin{pmatrix} u_k & -v_k^* \\ v_k & u_k^* \end{pmatrix}$ corresponding to sequence G_k.

In analogy to Problem **??**, this problem generalizes the projective rotation approximation problem (Problem **??**) by allowing multiple projective rotation circuits in convex combination. Note that the elements of the probability distribution $p_1, \ldots, p_n$ are distinct from the success probabilities of the projective rotations.

In the analysis of the fall-back protocol in **??** we considered only unitary fallback steps. We now consider fallbacks that are probabilistic mixtures of unitaries. The channel $\mathcal{F}$ for a fallback protocol has the form

$$\mathcal{F}(\rho) = q\mathcal{Z}_{\theta_0}(\rho) + (1-q)\mathcal{B}'(\rho) \tag{36}$$

where $\mathcal{B}'$ is the composition of the failure rotation $e^{i\theta_1 Z}$ and the fallback step $\mathcal{B}$ and q is the probability of success (measurement outcome of zero).

The following theorem provides a simple closed form bound for the diamond distance of a mixture of fallback protocols, similar to the expression obtained from **??** for unitary mixtures. The proof is provided in **??**.

Theorem 4.16 (Diamond distance of a fallback mixture)**.** *Let θ be an angle and let fallback channels*

$$\mathcal{F}_1(\rho) = q_1 \mathcal{Z}_{\theta+\delta_1}(\rho) + (1-q_1)\mathcal{B}_1(\rho) \tag{37}$$

$$\mathcal{F}_2(\rho) = q_2 \mathcal{Z}_{\theta+\delta_2}(\rho) + (1-q_2)\mathcal{B}_2(\rho) \tag{38}$$

where $\sin(\delta_1) \leq 0 \leq \sin(\delta_2)$. Define probability

$$p = \frac{q_2 \sin(2\delta_2)}{q_2 \sin(2\delta_2) - q_1 \sin(2\delta_1)}. \tag{39}$$

Then

$$\|pq_1 \left(\mathcal{Z}_{\theta+\delta_1} - \mathcal{Z}_\theta\right) + (1-p)q_2 \left(\mathcal{Z}_{\theta+\delta_2} - \mathcal{Z}_\theta\right)\|_\diamond = 2\left(pq_1 \sin^2(\delta_1) + (1-p)q_2 \sin^2(\delta_2)\right) \tag{40}$$

and the total accuracy of the mixed fall-back approximation protocol is

$$\begin{aligned} ||p\mathcal{F}_1 + (1-p)\mathcal{F}_2 - \mathcal{Z}_\theta||_\diamond \leq{}& 2\left(pq_1 \sin^2(\delta_1) + (1-p)q_2 \sin^2(\delta_2)\right) \\ &+ p(1-q_1)||\mathcal{B}_1 - \mathcal{Z}_\theta||_\diamond + (1-p)(1-q_2)||\mathcal{B}_2 - \mathcal{Z}_\theta||_\diamond. \end{aligned} \tag{41}$$

The goal of a synthesis algorithm then is to bound **??**[5] by an approximation error ε. We have some flexibility in bounding the accuracy of the components of the two fallback protocols. We may set the accuracy of each term separately

$$\begin{aligned} 2\left(pq_1\sin^2(\delta_1)+(1-p)q_2\sin^2(\delta_2)\right) &= \varepsilon_1 \\ p(1-q_1)||\mathcal{B}_1-\mathcal{Z}_\theta||_\diamond &= \varepsilon_2 \\ (1-p)(1-q_2)||\mathcal{B}_2-\mathcal{Z}_\theta||_\diamond &= \varepsilon_3 \\ \varepsilon_1+\varepsilon_2+\varepsilon_3 &\leq \varepsilon. \end{aligned} \tag{42}$$

The first condition is ensured by solving **??**. The second two conditions are ensured by solving the mixed diagonal approximation problems. Note that for the two fallback terms $||\mathcal{B}_1-\mathcal{Z}_\theta||_\diamond$ and $||\mathcal{B}_2-\mathcal{Z}_\theta||_\diamond$, the accuracy is scaled by $1-q_1$ and $1-q_2$ thereby reducing the fallback step approximation T-count on average by $1.5\log_2(1/(p(1-q_1)))$ and $1.5\log_2(1/(1-p)/(1-q_2))$ when using mixed diagonal approximation with Clifford+T gate set. This is in comparison to the cost of mixed diagonal approximation with Clifford+T gate set of accuracy ε. As in previous sections, **??** is solved by finding gate sequences with certain constraints on the top-left entry of the unitaries they compute.

Proposition 4.17 (Projective rotation mixing approximation condition)**.** *Suppose that we are given two sequences $G=g_1,\ldots,g_n$ and $H=h_1,\ldots,h_m$ from a gate set G. Define*

$$g_1\ldots g_n=\begin{pmatrix} u_1 & -v_1^* \\ v_1 & u_1^* \end{pmatrix}, h_1\ldots h_n=\begin{pmatrix} u_2 & -v_2^* \\ v_2 & u_2^* \end{pmatrix}.$$

Suppose that for angle θ and accuracy ε

- *u_1 satisfies $|u_1|\geq\sqrt{q}$, $-\sqrt{\varepsilon/2}\leq\sin(\mathrm{Arg}(u_1)-\theta)\leq 0$, and*
- *u_2 satisfies $|u_2|\geq\sqrt{q}$, $0\leq\sin(\mathrm{Arg}(u_2)-\theta)\leq\sqrt{\varepsilon/2}$.*

Then sequence G,H and probability distribution $p,1-p$ for

$$p=\frac{q_2\sin(2\delta_2)}{q_2\sin(2\delta_2)-q_1\sin(2\delta_1)},\ \text{where } q_k=|u_k|^2,\delta_k=\mathrm{Arg}(u_k)-\theta \tag{43}$$

*is a solution to the projective rotation mixing approximation Problem **??**. For a geometric interpretation of the constraints on u_1,u_2 see Figure **??**.*

Proof. The conditions $|u_1|\geq\sqrt{q}$, $|u_2|\geq\sqrt{q}$ trivially ensure success probability conditions of Problem **??**. We need to bound diamond distance of the channel

$$p|u_1|^2\left(\mathcal{Z}_{\mathrm{Arg}(u_1)}-\mathcal{Z}_\theta\right)+(1-p)|u_2|^2\left(\mathcal{Z}_{\mathrm{Arg}(u_2)}-\mathcal{Z}_\theta\right).$$

By Theorem **??** it is equal to

$$\begin{aligned} &2\left(p|u_1|^2\sin^2(\delta_1)+(1-p)|u_2|^2\sin^2(\delta_2)\right)\leq 2\left(p\sin^2(\delta_1)+(1-p)\sin^2(\delta_2)\right) \\ &\leq\varepsilon \end{aligned} \tag{44}$$

□

The conditions $|\sin(\delta_k)|\leq\sqrt{\varepsilon/2}$ imposed by Proposition **??** are quadratically looser than the equivalent condition for projective rotations without mixing (**??**) which requires $|\sin(\delta)|\leq\varepsilon/2$. When combined with unitary mixing for the fallback step, this yields a

[5] When the composition $\mathcal{B}_k\mathcal{Z}_{-\theta}$ is a Pauli channel, we can replace inequality in **??** by an exact value

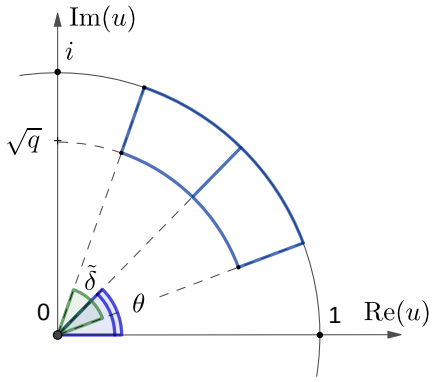


Figure 10: A geometric interpretation of constraints on the projective rotations given by Proposition **??**. The sector with blue boundary contains complex numbers u that satisfy constraints $\mathrm{Arg}(u) \in [\theta - \tilde{\delta}, \theta + \tilde{\delta}]$ and $|u| \geq \sqrt{q}$, where $\tilde{\delta} = \arcsin(\sqrt{\varepsilon/2})$. This sector is split into two parts, an over-rotation sector for one projective rotation and an under-rotation sector for the other projective rotation.

quadratic improvement in ε for the entire fallback protocol. The gate cost of a fallback protocol scales as $C \log_2(1/\varepsilon) + O(1)$. Thus the quadratic improvement in ε translates to a roughly two times savings in expected gate cost over conventional fallback protocols. For the more detailed cost comparisons see **??**.

For reasonable ranges of ε the $\log(1/\varepsilon)$ term is well below 100, making additive constants and higher order terms an important consideration. In that sense, solutions obtained by Proposition **??** are sub-optimal. The overall cost can be optimized by a more careful assignment of $\varepsilon_1, \varepsilon_2$ and ε_3 in **??**. This is discussed further in **??**.

4.6 Mixed magnitude approximation

We have shown that taking a probabilistic mixture of channels leads to improvement in accuracy for diagonal approximations with and without the fallback protocol. It is natural to then question whether a similar improvement can be achieved for general unitary approximation. We show that this is indeed the case, following the same strategy of finding approximations corresponding to under- and over- rotations of a target angle.

We begin by defining the following problem for approximating an arbitrary X-rotation up to phases.

Problem 4.18 (Magnitude approximation by mixing)**.** *Given:*

- *target angle θ,*
- *gate set G, a finite set of two by two unitary matrices with determinant one,*
- *accuracy ε, a positive real number.*

Find

- *$G_1, \ldots, G_n$, a sequence of sequences of elements of G and*
- *$p_1, \ldots, p_n$, a probability distribution on these sequences*

such that

$$\left\| \sum_{k=1}^{n} p_k \mathcal{X}_{\arccos(|u_k|)} - \mathcal{X}_\theta \right\|_\diamond \leq \varepsilon.$$

where u_k is the top-left entry of the matrix corresponding to sequence G_k and $\mathcal{X}_\theta$ is the channel induced by $e^{i\theta X}$.

As in Problem **??** and Problem **??**, Problem **??** allows for a solution comprising a probabilistic mixture of channels. We can further assume without loss of generality that $|\cos(\theta)| \geq 1/\sqrt{2}$, by the following remark.

Remark 4.19. Let $g_1 \dots g_n$ be a solution to Problem **??** for target angle θ. Then $iX \cdot g_n^\dagger \dots g_1^\dagger$ is a solution for target angle $\frac{\pi}{2} - \theta$, since $iX \cdot g_n^\dagger \dots g_1^\dagger = iXe^{-i\phi_2 Z}(-iX)iXe^{-i\theta X}e^{-i\phi_1 Z} = e^{i\phi_2 Z}e^{i(\pi/2-\theta)X}e^{i\phi_1 Z}$.

Hence, if $|\cos(\theta)| < 1/\sqrt{2}$ we can simply apply magnitude approximation to $\pi/2 - \theta$, noting that $\cos(\pi/2 - \theta) = \sin(\theta) \geq 1/\sqrt{2}$.

The following proposition shows that the error bound on the diamond norm in Problem **??** induces a constraint on the top-left entries of the matrices corresponding to sequences G_k. Our approach is to again find X-approximations corresponding to under- and over-rotations of the angle δ.

Proposition 4.20 (Mixed magnitude approximation condition)**.** *Suppose we are given sequences $g_1, \dots, g_n$ and $h_1, \dots, h_m$ of gates from a gate set. Define complex numbers u_k, v_k*

$$g_1 \dots g_n = \begin{pmatrix} u_1 & -v_1^* \\ v_1 & u_1^* \end{pmatrix}, h_1 \dots h_m = \begin{pmatrix} u_2 & -v_2^* \\ v_2 & u_2^* \end{pmatrix}$$

Suppose that for accuracy ε and target angle θ

- $|u_1| \in \{\cos(\theta'') : \theta'' \in [0, \pi/2], 0 \leq \theta - \theta'' \leq \arcsin\sqrt{\varepsilon/2}\}$*, and*
- $|u_2| \in \{\cos(\theta'') : \theta'' \in [0, \pi/2], 0 \leq \theta'' - \theta \leq \arcsin\sqrt{\varepsilon/2}\}$.

Define

$$p = \frac{\sin(2\delta_2)}{\sin(2\delta_2) - \sin(2\delta_1)}, \text{ where } \delta_k = \arccos(u_k) - \theta$$

*The the sequences $g_1, \dots, g_n$ and $h_1, \dots, h_m$ and probability distribution $p, 1-p$ is a a solution to the magnitude mixing approximation Problem **??** with $n = 2$, accuracy ε and target angle θ. For a geometric interpretation of the constraints on $|u_k|$ see Figure **??**.*

Proof. Let $g_1 \dots g_n = e^{i\phi_1 Z}e^{i\theta_u X}e^{i\phi_2 Z}$ with $\theta_u = \theta + \delta_1$ and $h_1 \dots h_m = e^{i\psi_1 Z}e^{i\theta_o X}e^{i\psi_2 Z}$ with $\theta_u = \theta + \delta_2$. Then

$$\|p\mathcal{X}_{\theta_u} + (1-p)\mathcal{X}_{\theta_o} - \mathcal{X}_\theta\|_\diamond = \|p\mathcal{Z}_{\theta_u} + (1-p)\mathcal{Z}_{\theta_o} - \mathcal{Z}_\theta\|_\diamond. \tag{45}$$

using the identity $He^{i\theta Z}H = e^{i\theta X}$ and unitary invariance of the diamond norm (**??**). The norm on the right hand side and the expression for p are of the form required for Theorem **??**, so we can conclude $\|p\mathcal{X}_{\theta_u} + (1-p)\mathcal{X}_{\theta_o} - \mathcal{X}_\theta\|_\diamond \leq \varepsilon$ when $2p(\sin^2(\delta_1)) + 2(1-p)(\sin^2(\delta_2)) \leq \varepsilon$. It remain to show that $\sin^2(\delta_k) \leq \varepsilon/2$.

Consider the under-rotated case. By definition $|u_1| = \cos(\theta_u)$ and so $\theta - \theta_u \leq \arcsin\sqrt{\varepsilon/2}$. So we have $\sin^2(\delta_1) \leq \varepsilon/2$ as required, and analogously for $|u_2|$. □

In comparison to Proposition **??**, the constraint on the top-left matrix entries in Proposition **??** is quadratically looser, thus admitting a greater possible number of candidate values. Analogously to the unmixed case, mixed magnitude approximations can be extended to approximations of arbitrary unitaries.

Proposition 4.21 (General unitary approximation with mixing)**.** *Let $U = e^{i\alpha Z}e^{i\theta X}e^{i\beta Z}$ be an arbitrary unitary in $SU(2)$. Let $g_1, \dots, g_n$ and $h_1, \dots, h_m$ be sequences from a gate set G that satisfy the constraints of Proposition **??**. Let probability p be defined as in Proposition **??**. Define angles ϕ_k, ψ_k from equations $g_1 \dots g_n = e^{i\phi_1 Z}e^{i\theta_u X}e^{i\phi_2 Z}$*

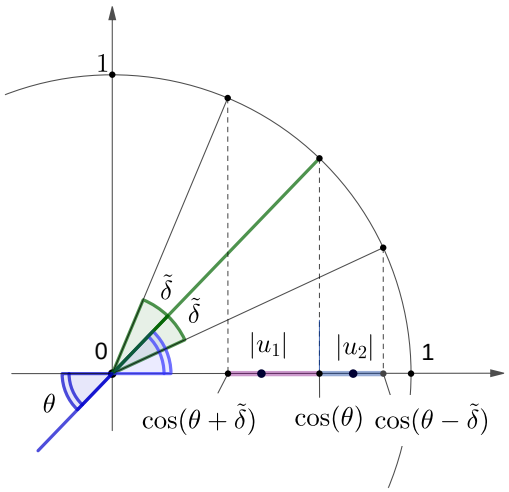


Figure 11: A geometric interpretation of constraints given by Proposition **??**. Absolute values $|u|$ belonging to the interval $\{\cos(\delta'') : \delta'' \in [0, \frac{\pi}{2}], |\delta'' - \theta| \leq \sqrt{\tilde{\delta}}\}$, for $\tilde{\delta} = \arcsin\sqrt{\varepsilon/2}$ are shown on the vertical axis. This interval is split into two parts, an over-rotation interval (blue) and an under-rotation interval (purple).

and $h_1 \dots h_m = e^{i\psi_1 Z} e^{i\theta_o X} e^{i\psi_2 Z}$. *Suppose* Φ_1, Φ_2, Ψ_1 *and* Ψ_2 *are* ε*-approximations of* $\mathcal{Z}_{\alpha-\phi_1}, \mathcal{Z}_{\beta-\phi_2}, \mathcal{Z}_{\alpha-\psi_1}$ *and* $\mathcal{Z}_{\beta-\psi_2}$*, respectively. Then*

$$\|p\Phi_1\mathcal{G}\Phi_2 + (1-p)\Psi_1\mathcal{H}\Psi_2 - \mathcal{U}\|_\diamond \leq 3\varepsilon,$$

where $\mathcal{G}$ *and* $\mathcal{H}$ *are channels induced by products* $g_1 \cdots g_n$ *and* $h_1 \cdots h_m$.

Proof. Using the Euler decomposition of U we have $\mathcal{U} = \mathcal{Z}_\alpha \mathcal{X}_\theta \mathcal{Z}_\beta$ and so

$$\|p\Phi_1\mathcal{G}\Phi_2 + (1-p)\Psi_1\mathcal{H}\Psi_2 - \mathcal{U}\|_\diamond = \|p\Phi_1\mathcal{G}\Phi_2 + (1-p)\Psi_1\mathcal{H}\Psi_2 - \mathcal{Z}_\alpha\mathcal{X}_\theta\mathcal{Z}_\beta\|_\diamond.$$

Applying the triangle inequality, we bound this norm from above by

$$p\|\Phi_1\mathcal{G}\Phi_2 - \mathcal{Z}_\alpha\mathcal{X}_{\theta_u}\mathcal{Z}_\beta\|_\diamond + (1-p)\|\Psi_1\mathcal{H}\Psi_2 - \mathcal{Z}_\alpha\mathcal{X}_{\theta_o}\mathcal{Z}_\beta\|_\diamond + \|\mathcal{Z}_\alpha(p\mathcal{X}_{\theta_u} + (1-p)\mathcal{X}_{\theta_o} - \mathcal{X}_\theta)\mathcal{Z}_\beta\|_\diamond.$$

Now, using unitary invariance of the diamond norm with $e^{-i\alpha Z}$ and $e^{-i\beta Z}$, we can simplify the three terms in the expression above and bound each by an accuracy measure. Concretely, we obtain the following set of equations

$$\begin{aligned} p\|\Phi_1\mathcal{G}\Phi_2 - \mathcal{Z}_\alpha\mathcal{X}_{\theta_u}\mathcal{Z}_\beta\|_\diamond &= p\left\|\Phi_1\underline{\mathcal{G}}\Phi_2 - \mathcal{Z}_\alpha\mathcal{Z}_{-\phi_1}\underline{\mathcal{Z}_{\phi_1}\mathcal{X}_{\theta_u}\mathcal{Z}_{\phi_2}}\mathcal{Z}_{-\phi_2}\mathcal{Z}_\beta\right\|_\diamond = \varepsilon_1 \\ (1-p)\|\Psi_1\mathcal{H}\Psi_2 - \mathcal{Z}_\alpha\mathcal{X}_{\theta_o}\mathcal{Z}_\beta\|_\diamond &= (1-p)\left\|\Psi_1\underline{\mathcal{H}}\Psi_2 - \mathcal{Z}_\alpha\mathcal{Z}_{-\psi_1}\underline{\mathcal{Z}_{\psi_1}\mathcal{X}_{\theta_o}\mathcal{Z}_{\psi_2}}\mathcal{Z}_{-\psi_2}\mathcal{Z}_\beta\right\|_\diamond = \varepsilon_2 \\ \|\mathcal{Z}_\alpha(p\mathcal{X}_{\theta_u} + (1-p)\mathcal{X}_{\theta_o} - \mathcal{X}_\theta)\mathcal{Z}_\beta\|_\diamond &= \varepsilon_3. \end{aligned}$$

such that the claim holds if $\varepsilon_1+\varepsilon_2+\varepsilon_3 \leq 3\varepsilon$. Consider the first norm $\|\Phi_1\mathcal{G}\Phi_2 - \mathcal{Z}_\alpha\mathcal{X}_{\theta_u}\mathcal{Z}_\beta\|_\diamond$ and apply the chain rule

$$\begin{aligned} \left\|\Phi_1\underline{\mathcal{G}}\Phi_2 - \mathcal{Z}_\alpha\mathcal{Z}_{-\phi_1}\underline{\mathcal{Z}_{\phi_1}\mathcal{X}_{\theta_u}\mathcal{Z}_{\phi_2}}\mathcal{Z}_{-\phi_2}\mathcal{Z}_\beta\right\|_\diamond &\leq \|\Phi_1 - \mathcal{Z}_{\alpha-\phi_1}\|_\diamond + \\ \|\mathcal{G} - \mathcal{Z}_{\phi_1}\mathcal{X}_{\theta_u}\mathcal{Z}_{\phi_2}\|_\diamond &+ \|\Phi_2 - \mathcal{Z}_{\beta-\phi_2}\|_\diamond \leq 2\varepsilon \end{aligned} \tag{46}$$

The same argument applies *mutatis mutandis* to $\|\Psi_1\mathcal{H}\Psi_2 - \mathcal{Z}_\alpha\mathcal{X}_{\theta_o}\mathcal{Z}_\beta\|_\diamond$. Since the sequences $g_1, \dots, g_n$ and $h_1, \dots, h_m$ and p satisfy Proposition **??** we also have

$$\|\mathcal{Z}_\alpha(p\mathcal{X}_{\theta_u} + (1-p)\mathcal{X}_{\theta_o} - \mathcal{X}_\theta)\mathcal{Z}_\beta\|_\diamond = \|p\mathcal{X}_{\theta_u} + (1-p)\mathcal{X}_{\theta_o} - \mathcal{X}_\theta)\| \leq \varepsilon.$$

Therefore $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 \leq 2\varepsilon p + 2\varepsilon(1-p) + \varepsilon = 3\varepsilon$.

□

Table 5: Region areas for unitary approximation problems with and without mixing. The geometric regions associated with each problem are illustrated in **??**. The diagonal and projective approximation problems result in two-dimensional regions, while the magnitude approximation problem results in a one-dimensional interval. In the latter case, *Region area* refers to the length of the interval. In all cases, it can be seen that the mixed version of the problem corresponds to a larger approximation region.

Approximation Problem	Region area (big-O)	Region area (with pre-factors)
Diagonal unitary approximation	$O(\varepsilon^3)$	$\varepsilon^3/12 + O(\varepsilon^5)$
Mixed diagonal approximation	$O(\varepsilon^{3/2})$	$(2/3)(\varepsilon/2)^{3/2} + O(\varepsilon^{5/2})$
Projective rotation approximation	$O(\varepsilon)$	$(1-q)\varepsilon/2 + O(\varepsilon^3)$
Mixed projective approximation	$O(\varepsilon^{1/2})$	$(1-q)(\varepsilon/2)^{1/2} + O(\varepsilon^{3/2})$
Magnitude approximation	$O(\varepsilon)$	$\varepsilon/\sqrt{2} + O(\varepsilon^3)$
Mixed magnitude approximation	$O(\varepsilon^{1/2})$	$\varepsilon^{1/2} + O(\varepsilon^{3/2})$

4.7 Geometric interpretations

In the sections above, we defined two methods for approximating diagonal unitaries: by direct unitary sequences (Problem **??**), or by fallback protocols (**??**). Both of these methods can be extended by using probabilistic mixtures (Problem **??** and Problem **??**). Each of these problems involves finding one or more sequences of gates that induce two-by-two unitary matrices of the form $\begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}$. In each case, solutions can be described by conditions on the top-left entry u. See Proposition **??**, Proposition **??**, Proposition **??**, and Proposition **??**. Those conditions can be illustrated geometrically by regions on the complex plane: Figure **??** and Figure **??**.

Figure **??** shows these regions overlayed one on top of another. This geometric illustration makes clear the progressive increase in solution space going from unitary approximation, to fallback approximation and then to probabilistic mixtures. The region areas for each approximation problem can be quickly computed using basic formulas for the areas of sectors and triangles. For instance, for diagonal approximation without mixing the region area is given by

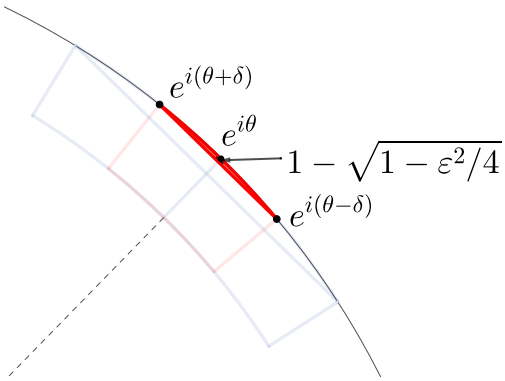
$$\delta - \frac{1}{2}\sin(2\delta)$$

where δ is the angle subtending the minimal sector containing the region. The region areas are given to leading order of ε in Table **??**.

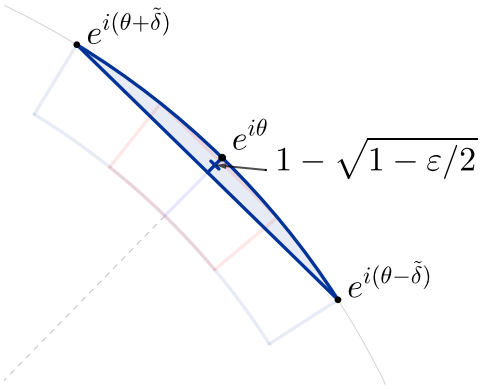
The projective approximation region encloses the unitary approximation region, provided that the probability of success q satisfies a modest $q \leq 1 - \varepsilon^2/4$. Loosely speaking, the condition $q = 1 - \varepsilon^2/4$ can be interpreted as the point at which the projection failure may be treated deterministically as an approximation error and no longer needs a fallback step.

Except for large values of ε, the unitary mixture region also encloses the (non-mixing) unitary approximation region. Finally, the projective mixing approximation region encloses all of the other regions, provided that $q \leq 1 - \varepsilon/2$.

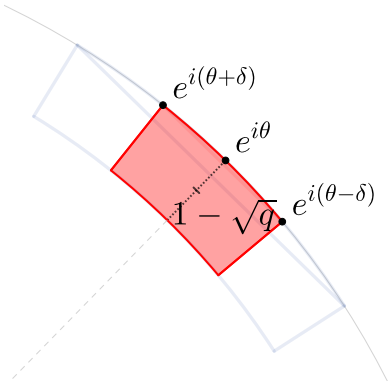
Indeed, for the chosen value of $\varepsilon = 0.1$, the illustration in Figure **??** under-represents the relative difference in region sizes. Practical values of ε are typically several orders of magnitude smaller, for which the relative difference in region sizes is dramatically larger. Figure **??** shows the areas of each of the approximation regions as a function of ε and q.



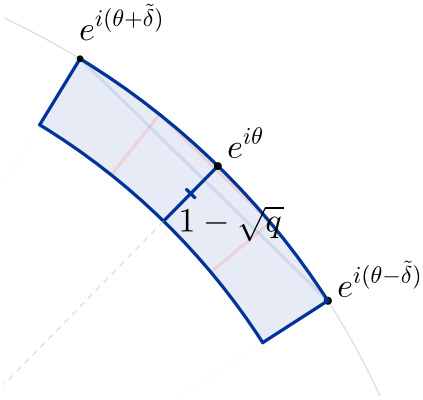
(a) Unitary region (Proposition **??**) with area in $O(\varepsilon^3)$



(b) Unitary mixing regions (Proposition **??**) with area in $O(\varepsilon^{3/2})$



(c) Projective rotation region (Proposition **??**) with area in $O(\varepsilon)$



(d) Projective rotation mixing regions (Proposition **??**) with area in $O(\varepsilon^{1/2})$

Figure 12: Approximation regions for target diagonal unitary $e^{i\theta Z}$. The figures above show close-ups of a section of the unit circle on the complex plane. Each colored highlight indicates a region of valid solutions for the corresponding approximation problem. For illustration, we have used (an impractical) approximation accuracy $\varepsilon = 0.1$ and projective rotation success probability $q = 0.9$. The unitary (a) and projective rotation (c) regions (without mixing) shown in red each subtend an angle of $2\delta = 2\arcsin(\varepsilon/2)$. The unitary mixing (b) and projective rotation mixing (d) regions shown in blue each subtend an angle of $2\tilde{\delta} = 2\arcsin(\sqrt{\varepsilon/2})$. The unitary mixing regions (b) fully encompasses the unitary region (a). Likewise, the projective rotation mixing region (d) fully encompasses the projective rotation region (c). For $q \leq 1-\varepsilon^2/4$, the projective rotation region (c) encompasses the unitary region (a). For $q \leq 1-\varepsilon/2$ the mixed projective regions encompasses all other regions.

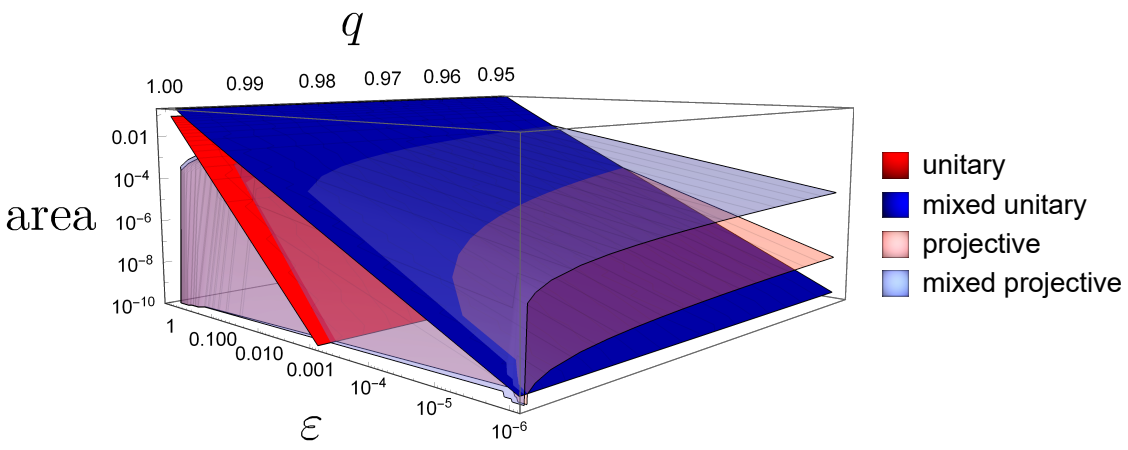


Figure 13: Areas of the solution regions prescribed by Proposition ?? (unitary), Proposition ?? (mixed unitary), Proposition ?? (projective) and Proposition ?? (mixed projective). Each curve shows the area of the region in the complex plane as a function of approximation accuracy ε and success probability q. The unitary and projective areas, highlighted in red, scale quadratically with ε. The mixed unitary and mixed projective areas, highlighted in blue, scale linearly with ε. For all values of ε and q the mixed unitary (resp. projective) region has larger area than the corresponding non-mixed unitary (resp. projective) region, thereby admitting more candidate solutions. Except for large values of ε and q, the projective and mixed projective regions have larger area then their respective unitary and mixed unitary regions.

5 Solutions to approximation problems for common gate sets

In Section ??, we related solutions to various approximation problems to specific geometric regions. In this section, we specialize these results to a few specific gate sets. Unitaries that can be synthesized exactly with these gate sets define discrete subsets within the above convex bodies, and this naturally leads to an enumeration strategy to solve approximation problems. We first describe this approach for the V basis, the Clifford+T basis and the Clifford+$\sqrt{T}$ basis, and we then generalize it to a family of gate sets introduced by [Kli+15b] for diagonal approximation problems.

Throughout this section, we introduce the following notation to highlight common methodology across our three illustrative examples. We use L to denote the field in which the entries of the unitaries defining a gate set lie, and O_L to denote the integer ring of L. We associate a *gate set determinant* $\ell \in K$ to each gate set, such that any element generated by the gate set can be written as $\frac{1}{\sqrt{\ell^N}} \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}$ with $u, v \in O_L$ and $N \in \mathbb{Z}$. The determinant of a unitary with elements in L lies in the maximal totally real subfield, which we denote by K. We have $L = K(i)$, where $i^2 = -1$. The norm of an element in L is a mapping from L to K defined by taking the product of an element of L with its complex conjugate. We denote the ring of integers of K by O_K.

5.1 V basis

5.1.1 Quaternion maximal order

We recall that the V basis consists of the following six matrices:

$$V_{\pm Z} = \frac{1}{\sqrt{\ell}} \begin{pmatrix} 1 \pm 2i & 0 \\ 0 & 1 \mp 2i \end{pmatrix}, \quad V_{\pm Y} = \frac{1}{\sqrt{\ell}} \begin{pmatrix} 1 & \mp 2 \\ \pm 2 & 1 \end{pmatrix}, \quad V_{\pm X} = \frac{1}{\sqrt{\ell}} \begin{pmatrix} 1 & \pm 2i \\ \pm 2i & 1 \end{pmatrix},$$

where $\ell = 5$. Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(i) = \{a_0 + ia_1 : a_0, a_1 \in \mathbb{Q}\}$, where $i^2 = -1$. Let $O_K = \mathbb{Z}$ and $O_L = \mathbb{Z}[i] = \{a_0 + ia_1 : a_0, a_1 \in \mathbb{Z}\}$ be the rings of integers of K and L respectively. Any element $t = a_0 + ia_1 \in O_L$ can be written as a 2-dimensional vector over O_K, namely (a_0, a_1). There are two homomorphisms of L into $\mathbb{C}$ related by complex conjugation. Denote by σ the homomorphism such that $\sigma(i) = i$.

Let $M_2(L)$ be the algebra of all 2×2 matrices with entries in L, and let $\mathcal{O}$ be an order in $M_2(L)$ that contains all the V basis elements scaled by $\sqrt{\ell}$. For concreteness we will set

$$\mathcal{O} := \mathbb{Z} \cdot I + \mathbb{Z} \cdot iX + \mathbb{Z} \cdot iY + \mathbb{Z} \cdot iZ. \tag{47}$$

We extend σ over $\mathcal{O}$ in a natural way, namely for $M \in \mathcal{O}$ we define $\sigma(M)$ as the matrix whose elements are the images of the elements of M under σ. As observed in [BGS13a; Kli+15b], elements of $\mathcal{O}$ with determinant ℓ^N correspond to unitaries that can be expressed as a product of N matrices from the V gate set via the map $\sigma'(M) = \frac{1}{\sqrt{\ell^N}}\sigma(M)$.

Example 5.1. Let $V = V_Z \cdot V_X = \frac{1}{5}\begin{pmatrix} 1+2i & 2i-4 \\ 2i+4 & 1-2i \end{pmatrix}$. Then, $M_V = \begin{pmatrix} 1+2i & 2i-4 \\ 2i+4 & 1-2i \end{pmatrix} = I + 2 \cdot iX - 4 \cdot iY + 2 \cdot iZ \in \mathcal{O}$ and $\sigma'(M_V) = V$. Since $\det(M_V) = 5^2$, we have $N = 2$ as expected, as V is the product of two V basis matrices. Note that the sequence $V_Z V_X$ cannot be simplified (over the V basis) so N is minimal.

Example 5.2. Let $V = V_Z V_X V_{-X} V_Y V_{-Z} = \frac{1}{\sqrt{3125}}\begin{pmatrix} 25 & 30-40i \\ -30-40i & 25 \end{pmatrix}$. Then,

$$M_V = \begin{pmatrix} 25 & 30-40i \\ -30-40i & 25 \end{pmatrix} = 25 \cdot I - 40 \cdot iX + 30 \cdot iY \in \mathcal{O}$$

and $\sigma'(M_V) = V$. Then $\det(M_V) = 3125 = 5^5$ so V can be expressed as the product of five V basis elements. However, $M'_V = \begin{pmatrix} 5 & 6-8i \\ -6-8i & 5 \end{pmatrix} = 5 \cdot I - 8 \cdot iX + 6 \cdot iY \in \mathcal{O}$, is also such that $\sigma'(M'_V) = V$. Here, $\det(M'_V) = 125 = 5^3$, giving $N = 3$. Since $V_P V_{-P} = V_{-P} V_P = I$, for $P \in \{X, Y, Z\}$, the sequence $V_Z V_X V_{-X} V_Y V_{-Z}$ simplifies to $V_Z V_Y V_{-Z}$, so V can in fact be expressed as a product of *three* V basis elements. The sequence cannot be simplified further, so this N is minimal.

5.1.2 Solving approximation problems

Finding a solution to any approximation problem over the V basis involves finding a matrix $M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix}$ with additional constraints on m_1 depending on the approximation problem, such that $\det(M) = \ell^N$. In essence, we seek matrices which can be achieved by the V basis, with elements falling in a particular region. Our approach is to first determine candidate values for m_1 via a specific enumeration problem, then to deduce the m_2 values that satisfy the determinant constraint by solving a norm equation. These two steps are repeated while iterating over N, beginning with $N = 1$, until a valid M is found. In the following, the point enumeration and norm equation steps are described for fixed N.

For the diagonal (Problem **??**, Problem **??**) and fallback (**??**, Problem **??**) approximation problems, M is such that $\sigma_1(m_1)/\sqrt{\sigma_1(\ell^N)} \in R_{\text{approx}}$, where R_{approx} is a specific region of $\mathbb{C}$ depending on the problem. Namely, we consider R_{approx} as one of the regions defined in Proposition **??**, Proposition **??**, Proposition **??** and Proposition **??**. For magnitude approximation (**??**, **??**) with our new decomposition, M must be such that $\sigma_1(m_1 m_1^*)/\sigma_1(\ell^N) \in I_{\text{approx}}$, where $I_{\text{approx}} \subset [0, 1]$ where I_{approx} is an interval of $\mathbb{R}$ as defined in Proposition **??**, **??**. Formally, we solve the following point enumeration problems.

Problem 5.3 (2D point enumeration (V basis)). *Let R_{approx} be a 2D region corresponding to a particular approximation problem and fix $N \in \mathbb{N}$.*

$$\textit{Find all } (a_0, a_1) \in \mathbb{Z}^2 \textit{ such that } \frac{1}{\sqrt{\ell^N}}(a_0, a_1) \in R_{\text{approx}}.$$

Problem 5.4 (1D point enumeration (V basis)). *Let $I_{\text{approx}} \subset [0, 1]$ be a real interval corresponding to a particular approximation problem and fix $N \in \mathbb{N}$.*

$$\textit{Find all } n \in \mathbb{Z} \textit{ such that } \frac{n}{\ell^N} \in I_{\text{approx}}.$$

In the first case we set $m_1 = a_0 + ia_1$ for every solution (a_0, a_1). In the second case we first solve the norm equation $n = a_0^2 + a_1^2$, and for every solution we obtain a candidate value $m_1 = a_0 + ia_1$.

To satisfy the determinant condition, solving the approximation problems requires that we keep only those m_1 for which the following problem is solvable.

Problem 5.5 (Norm equation (V basis)). *Given $m_1 \in \mathbb{Z}[i]$ and integer N, find $m_2 \in \mathbb{Z}[i]$ such that*

$$m_2 m_2^* = \ell^N - m_1 m_1^* \in \mathbb{Z}.$$

For every pair of solutions (m_1, m_2) we then deduce a matrix $M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix}$. Since m_2 is a solution to Problem **??** we have $\det(M) = \ell^N$ and the matrix $\sigma'(M) = \frac{1}{\sqrt{\ell^N}}\sigma_1(M) = \frac{1}{\sqrt{\ell^N}} \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix}$ is unitary.

In summary, given a target unitary and associated region or interval, the following procedure finds an approximation over the V basis. For a fixed value of N, an element $m_1 \in \mathbb{Z}[i]$ is obtained by solving an integer point enumeration problem defined by the target region. Together with N, m_1 defines a norm equation, which is solved to obtain an element $m_2 \in \mathbb{Z}[i]$. If no solution to either problem is found, the value of N is increased. The point enumeration and norm equation steps are repeated for each value of N until a valid pair (m_1, m_2) is obtained. Each pair defines a matrix $M \in \mathcal{O}$ as above with determinant ℓ^N. Then, the unitary $\sigma'(M)$ is factorized over the V basis using an existing exact synthesis algorithm (see Appendix **??**) to obtain a solution to the approximation problem.

5.2 Clifford+T basis

5.2.1 Gate set

The single-qubit Clifford group is defined as the set of unitaries that preserve the Pauli matrices under conjugation. That is, $\mathcal{C}$ is in the single-qubit Clifford group if and only if for any Pauli matrix P, the matrix $\mathcal{C}^* P \mathcal{C}$ is also a Pauli matrix.

We recall that the S, H and T gates are defined as follows:

$$S = e^{-i\pi/4Z} = \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad T = e^{-i\pi/8Z} = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}.$$

The single-qubit Clifford group is generated by the H and S gates, and the Clifford+T group is generated by the single-qubit Clifford group and the T gate. Moreover we have

$T^2 = S$, so the Clifford+T group is generated by H and T. We also recall the matrices T_x, T_y defining rotations by $\frac{\pi}{4}$ about the x and y axes, namely

$$T_x := \begin{pmatrix} \cos(\frac{\pi}{8}) & -i\sin(\frac{\pi}{8}) \\ -i\sin(\frac{\pi}{8}) & \cos(\frac{\pi}{8}) \end{pmatrix} = \frac{1}{\sqrt{\ell}}\left(I + \frac{I - iX}{\sqrt{2}}\right),$$
$$T_y := \begin{pmatrix} \cos(\frac{\pi}{8}) & -\sin(\frac{\pi}{8}) \\ \sin(\frac{\pi}{8}) & \cos(\frac{\pi}{8}) \end{pmatrix} = \frac{1}{\sqrt{\ell}}\left(I + \frac{I - iY}{\sqrt{2}}\right)$$

where $\ell = 2 + \sqrt{2}$. Note that T similarly defines the rotation of $\frac{\pi}{4}$ about the z axis and we can write $T = \frac{1}{\sqrt{\ell}}\left(I + \frac{I-iZ}{\sqrt{2}}\right)$. We can obtain T_x and T_y from T, and vice versa, by conjugation with single-qubit Clifford unitaries. Synthesis via a circuit of T_x, T_y, T and Hadamard gates therefore corresponds to synthesis in the Clifford+T basis, up to a global phase.

In evaluating the cost of approximate synthesis with Clifford+T gates, we assume that Clifford gates are low cost, and only count T gates, or equivalently the total number of T_x, T_y and T matrices. See Section **??** for a justification of this assumption.

5.2.2 Quaternion maximal order

Let $K = \mathbb{Q}(\sqrt{2})$ and let $L = \mathbb{Q}(\zeta_8)$, where $\zeta_8 = e^{2\pi i/8}$. The ring of integers of L is

$$O_L = \mathbb{Z}[\zeta_8] = \left\{a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3 : a_k \in \mathbb{Z}\right\} = \mathbb{Z}[\sqrt{2}] + \frac{1+i}{\sqrt{2}} \cdot \mathbb{Z}[\sqrt{2}].$$

The ring of integers of K is the real subring $O_K = \mathbb{Z}[\sqrt{2}] = \{b_0 + b_1\sqrt{2} : b_0, b_1 \in \mathbb{Z}\} \subset O_L$. We can identify any element m in O_L with a 4-dimensional vector $\boldsymbol{m} = (a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ using the integral basis above. There are four distinct injective field homomorphisms that embed L into $\mathbb{C}$, related to one another by complex conjugation and $\sqrt{2}$-conjugation. Define two such homomorphisms σ_1, σ_2 by

$$\sigma_1(\zeta_8) = \frac{1+i}{\sqrt{2}}, \quad \sigma_2(\zeta_8) = \frac{-(1+i)}{\sqrt{2}}. \tag{48}$$

We represent σ_1, σ_2 by the matrix

$$\Sigma := \begin{pmatrix} 1 & 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 0 & 1/\sqrt{2} & 1 & 1/\sqrt{2} \\ 1 & -1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & -1/\sqrt{2} & 1 & -1/\sqrt{2} \end{pmatrix}$$

where $(\operatorname{Re}\sigma_1(m), \operatorname{Im}\sigma_1(m), \operatorname{Re}\sigma_2(m), \operatorname{Im}\sigma_2(m))^T = \Sigma \boldsymbol{m}^T$.

Let $n = mm^*$ and write $n = b_0 + b_1\sqrt{2}$, $b_0, b_1 \in \mathbb{Z}$. We can identify n with the 2-dimensional vector $\boldsymbol{n} = (b, b_1)$ or with $(\sigma_1(n), \sigma_2(n))^T = \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix} \boldsymbol{n}^T$ through the above homomorphisms. We choose one homomorphism arbitrarily, say σ_1, to embed elements into Euclidean space. Both σ_1 and σ_2 are necessary to express the solvability constraints imposed by the norm equation for elements in L. Let $M_2(L)$ be the algebra of 2×2 matrices with entries in L, and let $\mathcal{O}$ be a maximal order in $M_2(L)$ which contains T_x, T_y and T. For concreteness we will set $\mathcal{O} = \sum_{i=1}^4 O_K \cdot \omega_i$ in what follows, where

$$\omega_1 = I, \qquad \omega_2 = \frac{I + iX}{\sqrt{2}}, \qquad \omega_3 = \frac{I + iY}{\sqrt{2}}, \qquad \omega_4 = \omega_3\omega_2 = \frac{I + iX + iY + iZ}{2}.$$

The homomorphisms σ_1, σ_2 extend over $\mathcal{O}$ in a natural way. Elements of $\mathcal{O}$ correspond to 2×2 unitaries via the map $\sigma'(M) = \frac{1}{\sqrt{\sigma_1(\det(M))}}\sigma_1(M)$. Elements of $\mathcal{O}$ with determinant equal to 1 correspond to Clifford gates, and elements of $\mathcal{O}$ with determinant ℓ^N correspond to unitaries that can be expressed as a product of N gates T_x, T_y and T (see Appendix **??**, [Gos+14]).

5.2.3 Solving approximation problems

Finding a solution to any approximation problem (as defined in Section **??**) over the Clifford+T gate set involves finding a matrix

$$M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix} = X_1\omega_1 + X_2\omega_2 + X_3\omega_3 + X_4\omega_4, \tag{49}$$

or equivalently finding $X_i \in O_K$, with additional constraints on m_1 depending on the approximation problem, such that $\det(M) = \ell^N$. Recall that these matrices will correspond to unitaries which are products of gates from the Clifford+T basis.

Let us first examine the sets M_{diag} and $M_{\text{off}-\text{diag}}$, in which we will look for elements m_1 and m_2, respectively. From Equation (**??**) we have

$$\begin{aligned} M_{\text{diag}} &= \left\{m_1 : \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix} \in \mathcal{O}\right\} = \left\{X_1 + \frac{X_2 + X_3}{\sqrt{2}} + \frac{X_4}{2} + \frac{X_4}{2}i : X_i \in O_K\right\} \\ &= \frac{1}{\sqrt{2}}O_K + \left(\frac{1+i}{2}\right)O_K \\ &= \frac{1}{\sqrt{2}}O_L. \end{aligned}$$

Let $M_{\mathcal{O}}$ denote the elements of L corresponding to diagonal elements of $\mathcal{O}$. That is elements m_1 such that $\begin{pmatrix} m_1 & 0 \\ 0 & m_1^* \end{pmatrix} \in \mathcal{O}$. By Equation (**??**), we can see $M_{\mathcal{O}} = O_L$.

Similarly, we have

$$\begin{aligned} M_{\text{off}-\text{diag}} &= \left\{m_2 : \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix} \in \mathcal{O}\right\} = \left\{\frac{\sqrt{2}X_1 - X_3}{2} + \frac{\sqrt{2}X_2 + X_3}{2}i : X_i \in O_K\right\} \\ &= \frac{1}{\sqrt{2}}O_K + \left(\frac{1+i}{2}\right)O_K \\ &= \frac{1}{\sqrt{2}}O_L. \end{aligned}$$

Hence, for all $m_1 \in M_{\text{diag}}, m_2 \in M_{\text{off}-\text{diag}}$ there exist $\hat{m_1}, \hat{m_2} \in O_L$, such that $m_1 = \frac{\hat{m_1}}{\sqrt{2}}$ and $m_2 = \frac{\hat{m_2}}{\sqrt{2}}$. For fixed m_1, $M_{\text{off}-\text{diag}}$ is restricted to the subset

$$M_{\text{off}-\text{diag}}^{m_1} = \left\{m_2 \in M_{\text{off}-\text{diag}} : \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix} \in \mathcal{O}\right\}.$$

Noticing that iY, $(iY)^{-1} \in \mathcal{O}$, we see that $m_2 \in M_{\text{off}-\text{diag}}^0 \iff m_2 \in M_{\mathcal{O}}$.

Our approach is to first determine candidate values for m_1 via a specific enumeration problem, then to deduce corresponding values for m_2 by solving a norm equation. These two steps are repeated while iterating over N, beginning with $N = 1$, until a valid M is found. This approach is analogous to that used in Section **??** for the V basis. In the following sections, the point enumeration and norm equation steps are described for fixed N. For every pair of solutions (m_1, m_2) we deduce a matrix $M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix}$. The unitary $\sigma'(M)$ is factorized over the Clifford+T basis to obtain a solution to the approximation problem.

5.2.4 Finding m_1: an enumeration problem

For the diagonal (Problem **??**, Problem **??**) and fallback (**??**, Problem **??**) approximation problems, we need $\sigma_1(m_1)/\sqrt{\sigma_1(\ell^N)} \in R_{\text{approx}}$, where $R_{\text{approx}} \subset D_1$ is a specific region of $\mathbb{C}$ depending on the problem, and D_1 denotes the disk of radius 1 about the origin. For magnitude approximation (**??**, **??**), m_1 must be such that $\sigma_1(m_1 m_1^*)/\sigma_1(\ell^N) \in I_{\text{approx}}$, where $I_{\text{approx}} \subset [0,1]$.

In order to satisfy the determinant condition we then naturally consider the following norm equation,

$$m_2 m_2^* = \ell^N - m_1 m_1^*, \tag{50}$$

which we would a priori need to solve for every candidate value of m_1 satisfying the previous constraints. We observe, however, that this problem can only have solutions if the right-hand side of the equation is totally positive. This means that we only need to consider values of m_1 which additionally satisfy $\sigma_2(m_1)/\sqrt{\sigma_2(\ell^N)} \in D_1$ or, equivalently, $\sigma_2(m_1 m_1^*)/\sigma_2(\ell^N) \in [0,1]$. Since $m_1 = \hat{m}_1/\sqrt{2}, m_2 = \hat{m}_2/\sqrt{2}$, there is an equivalent norm equation for a given $\hat{m}_1$:

$$\hat{m}_2 \hat{m}_2{}^* = 2\ell^N - \hat{m}_1 \hat{m}_1{}^*. \tag{51}$$

The conditions on $\hat{m}_1$ are scaled accordingly: $\hat{m}_1$ must satisfy $\sigma_2(\hat{m}_1)/\sqrt{\sigma_2(2\ell^N)} \in D_1$ or, equivalently, $\sigma_2(\hat{m}_1 \hat{m}_1^*)/\sigma_2(2\ell^N) \in [0,1]$.

We write $\hat{m}_1 = a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3$ and $\hat{n} = \hat{m}_1 \hat{m}_1{}^* = b_0 + b_1\sqrt{2}$, with all coefficients in $\mathbb{Z}$. Let Σ be as defined in Section **??** and let $\Sigma' = \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}$. The operation Σ (respectively Σ') embeds $\hat{m}_1$ (respectively $\hat{n}$) into the Euclidean space of the approximation regions. In order to satisfy the constraints imposed by both the approximation regions and the norm equation, we define normalization matrices Λ and Λ' for Σ and Σ', respectively. Let Λ and Λ' be the diagonal matrices with $\left(\sqrt{\sigma_1(2\ell^N)}, \sqrt{\sigma_1(2\ell^N)}, \sqrt{\sigma_2(2\ell^N)}, \sqrt{\sigma_2(2\ell^N)}\right)$ and $\left(\sigma_1(2\ell^N), \sigma_2(2\ell^N)\right)$ on their respective diagonals. Candidate values for $\hat{m}_1$ are obtained by solving the point enumeration problems below.

Problem 5.6 (2D point enumeration (Clifford+T basis)). *Let R_{approx} be a two-dimensional region corresponding to a particular approximation problem. Find $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ such that $\Lambda^{-1}\Sigma \cdot (a_0, a_1, a_2, a_3)^T \in R_{\text{approx}} \times D_1$.*

Problem 5.7 (1D point enumeration (Clifford+T basis)). *Let $I_{\text{approx}} \subset [0,1]$ be a real interval corresponding to a particular approximation problem. Find $(b_0, b_1) \in \mathbb{Z}^2$ such that $\Lambda'^{-1}\Sigma' \cdot (b_0, b_1)^T \in I_{\text{approx}} \times [0,1]$.*

In the first case, we immediately recover a candidate value for $\hat{m}_1$. In the second case, we recover a candidate value for $\hat{n}$, then solve the norm equation $\hat{m}_1 \hat{m}_1{}^* = \hat{n}$ and for every solution we obtain a candidate value $\hat{m}_1$. Then we set $m_1 = \frac{\hat{m}_1}{\sqrt{2}}$.

5.2.5 Finding m_2: solving a norm equation

Given a candidate value for m_1, we proceed to solve a norm equation problem (or determine there is no solution), restricting m_2 to $M_{\text{off-diag}}^{m_1}$:

Problem 5.8. *Given $m_1 \in \frac{1}{\sqrt{2}} O_L$ and integer N, find $m_2 \in M_{\text{off-diag}}^{m_1}$ such that*

$$m_2 m_2^* = \ell^N - m_1 m_1^* \in \frac{1}{2} O_K.$$

Fixing an arbitrary $m \in M^{m_1}_{\text{off}-\text{diag}}$, we have $M^{m_1}_{\text{off}-\text{diag}} = m + O_L$, since for any two $m, m' \in M^{m_1}_{\text{off}-\text{diag}}$ we have $m - m' \in M^0_{\text{off}-\text{diag}} = O_L$. Since $M_{\text{off}-\text{diag}} = M_{\text{diag}} = \frac{1}{\sqrt{2}} O_L$, Problem **??** can then be reformulated as

Problem 5.9. *Given $\hat{m}_1 \in \mathbb{Z}[\zeta_8]$, integer N, and $m \in \sqrt{2} M^{m_1}_{\text{off}-\text{diag}}$ find $\hat{m}_2 \in m + \sqrt{2}\mathbb{Z}[\zeta_8]$ such that*

$$\hat{m}_2 \hat{m}_2{}^* = 2\ell^N - \hat{m}_1 \hat{m}_1{}^* \in \mathbb{Z}[\sqrt{2}].$$

Solving Problem **??** for $\hat{m}_2$ then yields a solution to Problem **??**: $m_2 = \hat{m}_2/\sqrt{2}$.

5.3 Clifford+$\sqrt{T}$ basis

We now demonstrate how the solution framework applies to the Clifford+$\sqrt{T}$ basis. Note that the Clifford+T group is contained within the Clifford+$\sqrt{T}$ group and unitaries in the latter are defined over the complex field $\mathbb{Q}(\zeta_{16}) \supseteq \mathbb{Q}(\zeta_8)$. Clearly, the fields L and K defined for Clifford+$\sqrt{T}$ are of higher degree over $\mathbb{Q}$ than the respective Clifford+T fields. Accordingly, in this section we work with larger matrices for Σ, Λ and Σ', Λ'. The point enumeration problems are also higher dimensional. The framework otherwise proceeds as for the Clifford+T basis.

5.3.1 Gate set

Let $\ell = 2 + 2\cos(\frac{\pi}{8}) = 2 + (\zeta_{16} + \zeta_{16}^{-1})$, where $\zeta_{16} = e^{2\pi i/16}$. Let also $\theta = 2\cos(\frac{\pi}{8})$, $\beta = \theta^3 + 3\theta$ and $\mu = \theta^2 - 3$. We recall that the $\sqrt{T}$ gate is defined as follows:

$$\sqrt{T} = \begin{pmatrix} e^{-i\pi/16} & 0 \\ 0 & e^{i\pi/16} \end{pmatrix} = \frac{1}{\sqrt{2 + 2\cos(\frac{\pi}{8})}} \begin{pmatrix} 1 + e^{-i\pi/8} & 0 \\ 0 & 1 + e^{i\pi/8} \end{pmatrix}.$$

The $\sqrt{T}$ gate defines a rotation about the z axis by $\frac{\pi}{8}$. The Clifford+$\sqrt{T}$ group is generated by the single qubit Clifford group and the $\sqrt{T}$ gate. Note that we will use the notation $T^{1/2}$ interchangeably with $\sqrt{T}$ in the following discussion. We also recall the matrices $T_x^{1/2}, T_y^{1/2}$ defining rotations by $\frac{\pi}{8}$ about the x and y axes, namely

$$T_x^{1/2} = \begin{pmatrix} \cos(\frac{\pi}{16}) & -i\sin(\frac{\pi}{16}) \\ -i\sin(\frac{\pi}{16}) & \cos(\frac{\pi}{16}), \end{pmatrix} = \frac{1}{\sqrt{\ell}} \left(I + \frac{\theta(I - i\mu X)}{2} \right)$$

$$T_y^{1/2} = \begin{pmatrix} \cos(\frac{\pi}{16}) & -\sin(\frac{\pi}{16}) \\ \sin(\frac{\pi}{16}) & \cos(\frac{\pi}{16}) \end{pmatrix} = \frac{1}{\sqrt{\ell}} \left(I + \frac{\theta(I - i\mu Y)}{2} \right).$$

We can additionally write $\sqrt{T} = \frac{1}{\sqrt{\ell}} \left(I + \frac{\theta(I - \mu i Z)}{2} \right)$. Observe that $\sqrt{T}^2 = T$ and $\left(T_a^{1/2}\right)^2 = T_a$ with $a = x, y$, as suggested by the notation. We can obtain the unitaries $\mathrm{T}_x^{k/2}$ and $\mathrm{T}_y^{k/2}$ from $T^{k/2}$, for $k = 1, 2, 3$, and vice versa, by conjugation with single-qubit Clifford unitaries. Here $T_a^{3/2} = \left(T_a^{1/2}\right)^3$. Synthesis via a circuit of unitaries in $\{T^{k/2}, \mathrm{T}_a^{k/2} : a = x, y \quad k = 1, 2, 3\}$ and Clifford gates therefore corresponds to synthesis in the Clifford $+\sqrt{T}$ basis, up to a global phase.

5.3.2 Quaternion maximal order

Let K be the totally real number field $K = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$, and let L be the field $L = \mathbb{Q}(\zeta_{16})$. The ring of integers of L is

$$O_L = \mathbb{Z}[\zeta_{16}] = \left\{ \sum_{i=0}^{7} a_k \zeta_{16}^k : a_k \in \mathbb{Z} \right\} = \mathbb{Z}\left[2\cos\left(\frac{\pi}{8}\right) \right] + \zeta_{16}\mathbb{Z}\left[2\cos\left(\frac{\pi}{8}\right) \right]$$

and the ring of integers of K is the real subring

$$O_K = \mathbb{Z}\left[2\cos\left(\frac{\pi}{8}\right)\right] = \left\{b_0 + b_1 \cdot 2\cos\left(\frac{\pi}{8}\right) + b_2\sqrt{2} + b_3 \cdot 2\cos\left(\frac{3\pi}{8}\right) : b_k \in \mathbb{Z}\right\} \subset O_L.$$

We can identify any element m in O_L with an 8-dimensional vector $\boldsymbol{m} = (a_0, a_1, \ldots, a_7) \in \mathbb{Z}^8$ using the integral basis above. There are 8 distinct injective field homomorphisms that embed L into $\mathbb{C}$, which can be grouped into pairs depending on their images when restricted to K. Define four such homomorphisms $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ by

$$\sigma_1(\zeta_{16}) = \cos(\frac{\pi}{8}) + i\cos(\frac{3\pi}{8}), \quad \sigma_2(\zeta_{16}) = \cos(\frac{3\pi}{8}) + i\cos(\frac{\pi}{8}),$$
$$\sigma_3(\zeta_{16}) = -\cos(\frac{3\pi}{8}) + i\cos(\frac{\pi}{8}), \quad \sigma_4(\zeta_{16}) = \cos(\frac{\pi}{8}) + i\cos(\frac{3\pi}{8}).$$

We represent $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ by the matrix

$$\Sigma := \begin{pmatrix}
1 & \cos(\frac{\pi}{8}) & \frac{1}{\sqrt{2}} & \cos(\frac{3\pi}{8}) & 0 & -\cos(\frac{3\pi}{8}) & -\frac{1}{\sqrt{2}} & -\cos(\frac{\pi}{8}) \\
0 & \cos(\frac{3\pi}{8}) & \frac{1}{\sqrt{2}} & \cos(\frac{\pi}{8}) & 1 & \cos(\frac{\pi}{8}) & \frac{1}{\sqrt{2}} & \cos(\frac{3\pi}{8}) \\
1 & \cos(\frac{3\pi}{8}) & -\frac{1}{\sqrt{2}} & -\cos(\frac{\pi}{8}) & 0 & \cos(\frac{\pi}{8}) & \frac{1}{\sqrt{2}} & -\cos(\frac{3\pi}{8}) \\
0 & \cos(\frac{\pi}{8}) & \frac{1}{\sqrt{2}} & -\cos(\frac{3\pi}{8}) & -1 & -\cos(\frac{3\pi}{8}) & \frac{1}{\sqrt{2}} & \cos(\frac{\pi}{8}) \\
1 & -\cos(\frac{3\pi}{8}) & -\frac{1}{\sqrt{2}} & \cos(\frac{\pi}{8}) & 0 & -\cos(\frac{\pi}{8}) & \frac{1}{\sqrt{2}} & \cos(\frac{3\pi}{8}) \\
0 & \cos(\frac{\pi}{8}) & -\frac{1}{\sqrt{2}} & -\cos(\frac{3\pi}{8}) & 1 & -\cos(\frac{3\pi}{8}) & -\frac{1}{\sqrt{2}} & \cos(\frac{\pi}{8}) \\
1 & -\cos(\frac{\pi}{8}) & \frac{1}{\sqrt{2}} & -\cos(\frac{3\pi}{8}) & 0 & \cos(\frac{3\pi}{8}) & -\frac{1}{\sqrt{2}} & \cos(\frac{\pi}{8}) \\
0 & \cos(\frac{3\pi}{8}) & -\frac{1}{\sqrt{2}} & \cos(\frac{\pi}{8}) & -1 & \cos(\frac{\pi}{8}) & -\frac{1}{\sqrt{2}} & \cos(\frac{3\pi}{8})
\end{pmatrix}$$

where

$$(\operatorname{Re}\sigma_1(m), \operatorname{Im}\sigma_1(m), \operatorname{Re}\sigma_2(m), \operatorname{Im}\sigma_2(m), \operatorname{Re}\sigma_3(m), \operatorname{Im}\sigma_3(m), \operatorname{Re}\sigma_4(m), \operatorname{Im}\sigma_4(m))^T = \Sigma\boldsymbol{m}^T.$$

Let $n = mm^*$ and write $n = b_0 + b_1 \cdot 2\cos(\frac{\pi}{8}) + b_2\sqrt{2} + b_3 \cdot 2\cos(\frac{3\pi}{8})$. We can identify n with the 4-dimensional vector $\boldsymbol{n} = (b_0, b_1, b_2, b_3)$, or with $(\sigma_1(n), \sigma_2(n), \sigma_3(n), \sigma_4(n))^T = \Sigma'\boldsymbol{n}^T$ where

$$\Sigma' := \begin{pmatrix}
1 & 2\cos(\frac{\pi}{8}) & \sqrt{2} & 2\cos(\frac{3\pi}{8}) \\
1 & -2\cos(\frac{3\pi}{8}) & -\sqrt{2} & -2\cos(\frac{\pi}{8}) \\
1 & -2\cos(\frac{3\pi}{8}) & \sqrt{2} & 2\cos(\frac{\pi}{8}) \\
1 & -2\cos(\frac{\pi}{8}) & \sqrt{2} & -2\cos(\frac{3\pi}{8})
\end{pmatrix}$$

through the above homomorphisms. As for the Clifford+T basis, we choose a homomorphism arbitrarily, for example σ_1, to embed elements into Euclidean space.

Let $M_2(L)$ be the algebra of all 2×2 matrices with entries in L. Let $\mathcal{O}$ be a maximal order in $M_2(L)$ which contains $T_x^{1/2}$, $T_y^{1/2}$ and $T^{1/2}$, namely $\mathcal{O} = \sum_{i=1}^4 O_K \cdot \omega_i$, where

$$\omega_1 = I, \qquad \omega_2 = \frac{I + iX}{\sqrt{2}}, \qquad \omega_3 = \frac{I + iY}{\sqrt{2}}, \qquad \omega_4 = \omega_3\omega_2 = \frac{I + iX + iY + iZ}{2}.$$

The homomorphisms $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ extend over $\mathcal{O}$ in a natural way. Elements of $\mathcal{O}$ correspond to 2×2 unitaries via the map $\sigma'(M) = \frac{1}{\sqrt{\sigma_1(\det(M))}}\sigma_1(M)$. Elements of $\mathcal{O}$ with determinant ℓ^N correspond to unitaries that can be expressed as a product of N gates $\mathrm{T}_x^{k/2}$, $\mathrm{T}_y^{k/2}$ and $\mathrm{T}^{k/2}$ with $k = 1, 2, 3$ (see Appendix **??**, [Gos+14]), hence in the Clifford + $\sqrt{T}$ gates.

5.3.3 Solving approximation problems

Finding a solution to any approximation problem over the Clifford+$\sqrt{T}$ gate set involves finding a matrix

$$M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix} = X_1\omega_1 + X_2\omega_2 + X_3\omega_3 + X_4\omega_4 \in \mathcal{O}, \tag{52}$$

or equivalently finding $X_i \in O_K$, with additional constraints on m_1 depending on the approximation problem, such that $\det(M) = \ell^N$.

Let us first examine the sets M_{diag} and $M_{\text{off}-\text{diag}}$, in which we will look for elements m_1 and m_2, respectively. From Equation (**??**) we have

$$\begin{aligned} M_{\text{diag}} &= \left\{ m_1 : \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix} \in \mathcal{O} \right\} = \left\{ X_1 + \frac{X_2 + X_3}{\sqrt{2}} + \frac{X_4}{2} + \frac{X_4}{2} i : X_i \in O_K \right\} \\ &= \frac{1}{\sqrt{2}} O_K + \frac{1+i}{2} O_K. \end{aligned}$$

As before, let $M_{\mathcal{O}}$ denote the set of elements $m_1 \in L$ such that $\begin{pmatrix} m_1 & 0 \\ 0 & m_1^* \end{pmatrix} \in \mathcal{O}$. From Equation (**??**), we have $M_{\mathcal{O}} = O_K + \frac{1+i}{\sqrt{2}} O_K$ and so clearly $M_{\text{diag}} = \frac{1}{\sqrt{2}} M_{\mathcal{O}}$. Similarly, we have $M_{\text{off}-\text{diag}} = \frac{1}{\sqrt{2}} M_{\mathcal{O}}$. Note that $O_L \subsetneq M_{\mathcal{O}}$, since ζ_{16} is in O_L but not in $M_{\mathcal{O}}$.

As with the Clifford+T basis, our approach is to iterate over N, beginning with $N = 1$, and for each N to first determine candidate values for m_1 via a specific enumeration problem, then to deduce corresponding values for m_2 by solving a norm equation, until a valid M is found. In the following sections, the point enumeration and norm equation steps are described for fixed N. For every pair of solutions (m_1, m_2) we deduce a matrix $M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix}$. The unitary $\sigma'(M)$ is factorized over the Clifford+$\sqrt{\text{T}}$ basis.

5.3.4 Finding m_1: an enumeration problem

For both the diagonal and fallback approximation problems, we need $\sigma_1(m_1)/\sqrt{\sigma_1(\ell^N)} \in R_{\text{approx}}$, where $R_{\text{approx}} \subset D_1$ is a specific region of $\mathbb{C}$ defined by the problem.

For the general approximation problem, m_1 must be such that $\sigma_1(m_1 m_1^*)/\sigma_1(\ell^N) \in I_{\text{approx}}$, where $I_{\text{approx}} \subset [0, 1]$. In order to satisfy the determinant condition we then naturally consider the following norm equation,

$$m_2 m_2^* = \ell^N - m_1 m_1^*, \tag{53}$$

which we would a priori need to solve for every candidate value of m_1 satisfying the previous constraints. Again, we observe that this norm equation only has solutions if its right-hand side is totally positive. This means that we only need to consider those candidates m_1 that additionally satisfy $\sigma_k(m_1)/\sqrt{\sigma_k(\ell^N)} \in D_1$or, equivalently, $\sigma_k(m_1 m_1^*)/\sigma_k(\ell^N) \in [0, 1]$, for $k = 2, 3, 4$.

Writing any $m_1 = a_0 + a_1 i$ with $a_0, a_1 \in K$, we see that M_{diag} can be considered as a full rank O_K lattice in K^2. We therefore have a $\mathbb{Z}$-basis, $\{y_0, \ldots, y_7\}$, for M_{diag} and can write any element $m_1 \in M_{\text{diag}}$ as $m_1 = \sum_{i=0}^{7} a_0 y_0, a_0 \in \mathbb{Z}$.

Since $M_{\text{diag}} = \frac{1}{\sqrt{2}} O_K + \frac{1+i}{2} O_K$, we also have $n := m_1 m_1^* \in \frac{1}{2} O_K$. Since $m_1 \in \frac{1}{\sqrt{2}} M_{\mathcal{O}}$, there exists $\hat{m_1} \in M_{\mathcal{O}}$ such that $m_1 = \frac{\hat{m_1}}{\sqrt{2}}$ and furthermore, $\hat{m_1} {\hat{m_1}}^* = 2n := \hat{n} \in O_K$. We write $\hat{n} = b_0 + b_1 \cdot 2\cos(\frac{\pi}{8}) + b_2\sqrt{2} + b_3 \cdot 2\cos(\frac{3\pi}{8})$ with all coefficients in $\mathbb{Z}$.

Let $\Sigma_{\mathcal{O}}$ be defined as the matrix with rows:

$$\begin{aligned}\Sigma_{\mathcal{O}}^{(2j)} &= (\mathrm{Re}(\sigma_j(y_0)), \ldots, \mathrm{Re}(\sigma_j(y_7)) \\ \Sigma_{\mathcal{O}}^{(2j+1)} &= (\mathrm{Im}(\sigma_j(y_0)), \ldots, \mathrm{Im}(\sigma_j(y_7)),\end{aligned}$$

for $1 \leq j \leq 7$, where the σ_j are defined in Section **??**. Additionally, take Σ' as defined in Section **??**, and define normalization matrices Λ and Λ'. That is, Λ and Λ' are diagonal matrices with entries $(\sqrt{\sigma_1(\ell^N)}, \sqrt{\sigma_1(\ell^N)}, \ldots, \sqrt{\sigma_4(\ell^N)}, \sqrt{\sigma_4(\ell^N)})$ and $(\sigma_1(2\ell^N), (\sigma_2(2\ell^N), (\sigma_3(2\ell^N), \sigma_4(2\ell^N))$ on the main diagonal, respectively. Hence the operations $\Lambda\Sigma_{\mathcal{O}}$ and $\Lambda'\Sigma'$ first embed an element m_1 or $\hat{n}$ into the Euclidean space of our approximation regions, then normalizes it to satisfy the constraints.

Candidate values for m_1 are then obtained by solving point enumeration problems below.

Problem 5.10 (2D point enumeration (Clifford+$\sqrt{T}$ basis)). *Let R_{approx} be a 2D region corresponding to a particular approximation problem. Find $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7) \in \mathbb{Z}^8$ such that*

$$\Lambda^{-1}\Sigma_{\mathcal{O}} \cdot (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)^T \in R_{\mathrm{approx}} \times D_1 \times D_1 \times D_1.$$

Problem 5.11 (1D point enumeration (Clifford+$\sqrt{T}$ basis)). *Let $I_{\mathrm{approx}} \subset [0,1]$ be a real interval corresponding to a particular approximation problem. Find $(a'_0, a'_1, a'_2, a'_3) \in \mathbb{Z}^4$ such that*

$$\Lambda'^{-1}\Sigma' \cdot (b_0, b_1, b_2, b_3)^T \in I_{\mathrm{approx}} \times [0,1] \times [0,1] \times [0,1].$$

In the first case, we immediately recover a candidate value for m_1. In the second case, we recover a candidate value for $\hat{n}$, solve the norm equation $\hat{m_1}\hat{m_1}^* = \hat{n}$ for $\hat{m_1} \in M_{\mathcal{O}}$ and for every solution $\hat{m_1}$ we obtain a candidate value m_1 by setting $m_1 = \frac{\hat{m_1}}{\sqrt{2}}$.

5.3.5 Finding m_2: solving a norm equation

Given a candidate value for m_1, we proceed to solve a norm equation problem (or determine there is no solution), restricting m_2 to $M_{\mathrm{off-diag}}^{m_1}$:

Problem 5.12. *Given $m_1 \in \frac{1}{\sqrt{2}}M_{\mathcal{O}}$ and integer N, find $m_2 \in M_{\mathrm{off-diag}}^{m_1}$ such that*

$$m_2 m_2^* = \ell^N - m_1 m_1^* \in \frac{1}{2}O_K.$$

Fixing an arbitrary $m \in M_{\mathrm{off-diag}}^{m_1}$, we have $M_{\mathrm{off-diag}}^{m_1} = m + M_{\mathcal{O}}$, since for any two $m, m' \in M_{\mathrm{off-diag}}^{m_1}$ we have $m - m' \in M_{\mathrm{off-diag}}^{0} = M_{\mathcal{O}}$. Since $M_{\mathrm{off-diag}} = M_{\mathrm{diag}} = \frac{1}{\sqrt{2}}M_{\mathcal{O}}$, Problem **??** can then be reformulated as

Problem 5.13. *Given $\hat{m_1} \in M_{\mathcal{O}}$, integer N, and $m/\sqrt{2} \in M_{\mathrm{off-diag}}^{m_1}$ find $\hat{m_2} \in m + \sqrt{2}M_{\mathcal{O}}$ such that*

$$\hat{m_2}\hat{m_2}^* = 2\ell^N - \hat{m_1}\hat{m_1}^* \in O_K.$$

Solving Problem **??** for $\hat{m_2}$ then yields a solution to Problem **??**: $m_2 = \hat{m_2}/\sqrt{2}$.

5.4 General case

In this section, we extrapolate from the three preceding examples to outline a general method for solving approximate synthesis properties, and describe the properties required by gate sets to which this method applies.

5.4.1 Gate sets

We consider quaternion gate sets as defined by Kliuchnikov *et al.* in [Kli+15b]. Informally, these are gate sets which are described by *totally definite quaternion algebras*.

Let K be a totally real number field and take totally positive elements $a, b \in K$. Define L to be the extension $L := K(\sqrt{-a})$ and let $i \in L$ be such that $i^2 = -a$. There are $2d$ distinct injective field homomorphisms embedding L into $\mathbb{C}$, where $d = [K : \mathbb{Q}]$. Fix $\sigma_1, \ldots, \sigma_d$ as any d homomorphisms from L that are pairwise distinct when restricted to K.

A quaternion algebra $(\frac{-a,-b}{K}) := Q$ over the field K is an algebra of the form $K + K\mathbf{i} + K\mathbf{j} + K\mathbf{k}$ where $\mathbf{i}^2 = -a, \mathbf{j}^2 = -b$ and $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$. A totally definite quaternion algebra has $a, b >$ totally positive. An element in Q is written $q = q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$, $q_0, q_1, q_2, q_3 \in K$, with conjugate $\bar{q} = q_0 - q_1\mathbf{i} - q_2\mathbf{j} - q_3\mathbf{k}$. The reduced norm of q is $\mathrm{nrd}(q) = q\bar{q}$.

Let $M_2(L)$ be the set of 2×2 matrices with elements in L. Define the K-linear map $\kappa : Q \to M_2(L)$ by

$$\kappa(1) = I, \quad \kappa(\mathbf{i}) = \sqrt{-a}Z, \quad \kappa(\mathbf{j}) = -\sqrt{-b}Y, \quad \kappa(\mathbf{k}) = \sqrt{-ab}X, \tag{54}$$

where X, Y, Z are the Pauli matrices. Notice that κ defines an isomorphism of quaternion algebras, with $\kappa(\mathbf{k}) = \kappa(\mathbf{i})\kappa(\mathbf{j})$. Concretely, we have a correspondence between elements in Q and matrices in $M_2(L)$ of the form $M = \begin{pmatrix} q_0+q_1\sqrt{-a} & -q_2\sqrt{b}+q_3\sqrt{-ab} \\ q_2\sqrt{b}+q_3\sqrt{-ab} & q_0-q_1\sqrt{-a} \end{pmatrix}$, where the corresponding quaternion is $q := q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$, such that $\kappa(q) = M$. Observe that $\det(M) = \mathrm{nrd}(q) = q_0 - aq_1^2 - bq_2^2 + abq_3^2$. The set of matrices of this form corresponds to SU(2) via the map

$$\sigma'(M) = \frac{1}{\sqrt{\sigma_1(\det(M))}} \cdot \sigma_1(M), \tag{55}$$

where σ_1 is the natural extension over matrices of the homomorphism from L into $\mathbb{C}$. Let S be a set of elements from K. Consider the gate set to be those matrices with determinant in S.

For the V, Clifford+T and Clifford+$\sqrt{\mathrm{T}}$ bases, the corresponding fields and integer rings are given in Table **??**.

Table 6: Number field correspondences for the V, Clifford+T and Clifford+$\sqrt{T}$ gate sets.

Gate set	K	L	O_K	O_L
V basis	$\mathbb{Q}$	$\mathbb{Q}(i)$	$\mathbb{Z}$	$\mathbb{Z}[i]$
Clifford+T	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\zeta_8)$	$\mathbb{Z}[\sqrt{2}]$	$\mathbb{Z}[\zeta_8]$
Clifford+$\sqrt{\mathrm{T}}$	$\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$	$\mathbb{Q}(\zeta_{16})$	$\mathbb{Z}[\zeta_{16} + \zeta_{16}^{-1}]$	$\mathbb{Z}[\zeta_{16}]$

5.4.2 Quaternion maximal order

For a given gate set, K and L, there exists $\mathcal{O}$, an order of $M_2(L)$, containing the preimages of the gate set unitaries under σ'. We note here that while this order does not need to be maximal, maximal orders have several properties which allow for efficient factorization of elements [Kli+15b]. For a thorough background on quaternion orders, we direct the reader to [Voi05].

The order $\mathcal{O}$ is constructed as follows. The gate set elements are mapped to matrices in $M_2(L)$. Let $\mathcal{L}_\mathcal{K}$ be the O_K-lattice obtained by taking an O_K linear combination of the

elements of the ring generated by these matrices. Then, $\mathcal{O}$ can be taken as any order containing this lattice. Note that, due to the multiplicative properties of the determinant, elements in $\mathcal{O}$ with determinant equal to ℓ for some $\ell \in \langle S \rangle$ will correspond to gate set elements. Then $\ell = \prod s_i^{N_i}$ for some set of elements $s_i \in S$. Let $N := \sum N_i$, which gives the length of a sequence of basis elements that produces the corresponding gate set element (when the class number of the quaternion algebra is one). Observe that for the gate sets we consider, we have $S = \ell$ and so $\det(M) = \ell^N$ for some $N \in \mathbb{Z}^{\geq}$. Clifford+$\sqrt{T}$ is an example of a gate set for which the corresponding quaternion algebra has class number two. Recall that in Example **??**, two distinct elements in $\mathcal{O}$ corresponded to the same gate set element, each with a distinct N value. We look for minimal N, as this will correspond to the shortest possible basis sequence. This will be the N for which the entries of $M \in \mathcal{O}$ are integral and not all divisible by $s_i \in S$, for all i. Since the approximation method outlined here iterates over increasing N, the sequence obtained will be optimal.

Remark 5.14. In addition, we look for orders $\mathcal{O}$ in which gates that are considered 'low-cost' in the gate set behave as units. This forces the determinant of matrices corresponding to low-cost gates to be 1, ensuring that N is a count of 'expensive' gates in a sequence. In essence, this makes the determinant a useful cost measure for approximation. For the V-basis, these low-cost gates are the Pauli matrices; for Clifford+T and Clifford+$\sqrt{\text{T}}$ these are the Clifford unitaries.

The definitions for $\mathcal{O}$ and ℓ corresponding to the V, Clifford+T and Clifford+$\sqrt{\text{T}}$ bases are given in the Table **??**.

Table 7: Maximal orders for V, Clifford+T and Clifford+$\sqrt{T}$ gate sets.

Gate set	ℓ	$\mathcal{O}$
V basis	5	$O_K \cdot I + O_K \cdot iX + O_K \cdot iY + O_K \cdot iZ$
Clifford+T	$2+\sqrt{2}$	$O_K \cdot I + O_K \cdot \frac{I+iX}{\sqrt{2}} + O_K \cdot \frac{I+iY}{\sqrt{2}} + O_K \cdot \frac{I+iZ+iX+iY}{2}$
Clifford+$\sqrt{\text{T}}$	$2+2\cos\frac{\pi}{8}$	$O_K \cdot I + O_K \cdot \frac{I+iX}{\sqrt{2}} + O_K \cdot \frac{I+iY}{\sqrt{2}} + O_K \cdot \frac{I+iZ+iX+iY}{2}$

5.4.3 Solving approximation problems

For fixed $N \in \mathbb{N}$, finding a solution to any approximation problem over a gate set involves finding a matrix

$$M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix} \in \mathcal{O},$$

with additional constraints on m_1 depending on the approximation problem, such that $\det(m) = \ell^N$. Our approach to finding M can be summarized in two steps:

1. point enumeration in a target region to find m_1 (Section **??**), followed by
2. solving a relative norm equation to recover m_2 (Section **??**).

For the diagonal and fallback approximation problems, with and without mixing, we look for elements $M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix}$ of $\mathcal{O}$, such that

$$\sigma_1(m_1)/\sqrt{\sigma_1(\ell^N)} \in R_{\text{approx}} \subset D_1,$$

where R_{approx} is the region defined by the problem. For the general unitary approximation problem, m_1 is required to satisfy

$$\sigma_1(m_1 m_1^*)/\sigma_1(\ell^N) \in I_{\text{approx}} \subset [0,1],$$

where I_{approx} is the real interval defined by the parameters of the problem. We observe that for the relative norm equation

$$m_2 m_2^* = \ell^N - m_1 m_1^*.$$

to have a solution, it is necessary that, for all k, $\sigma_k(\ell^N - m_1 m_1^*) > 0$. This means we only need to consider those candidates m_1 that satisfy either

$$\sigma_k(m_1)/\sqrt{\sigma_k(\ell^N)} \in D_1 \text{ or, equivalently, } \sigma_k(m_1 m_1^*)/\sigma_k(\ell^N) \in [0,1]$$

for all $k > 1$.

From each pair (m_1, m_2) we can deduce a matrix $M = \begin{pmatrix} m_1 & -m_2^* \\ m_2 & m_1^* \end{pmatrix}$. The unitary $\sigma'(M)$ is factorized over the desired gate set to obtain a solution to the approximation problem. If no solution exists for the given N, set $N := N+1$ and repeat the process. Thus, iterating over N, initialized at 1, will give the solution corresponding to the shortest gate sequence.

5.4.4 Finding m_1: an enumeration problem

The problem of finding candidates $m_1 \in L$ satisfying the conditions of an approximation problem can be reduced to an integer point enumeration problem. To better understand the set to which the main diagonal entries, m_1, belong, we define the map h from L to Q by

$$h(a_0 + ia_1) = a_0 + a_1\mathbf{i}.$$

We see that $\kappa(h(m))$ sends an element from L to the diagonal matrix $\left(\begin{smallmatrix} m & 0 \\ 0 & m^* \end{smallmatrix}\right) \in M_2(L)$. Hence we are enumerating elements $m_1 \in L$ from the set

$$M_{\text{diag}} = \{m_1 : \exists m_2 \in L \text{ s.t. } \kappa(h(m_1)) + h(m_2)\mathbf{j}) \in \mathcal{O}\}.$$

We additionally define the set of diagonal matrices in $\mathcal{O}$:

$$M_{\mathcal{O}} := \{m \in L : \kappa(h(m)) \in \mathcal{O}\}.$$

Observe that enumerating m_1 from M_{diag} is equivalent to enumerating $a_0, a_1 \in K$ from the set

$$\mathcal{L}_{\mathcal{O}} = \{(a_0, a_1) : \exists a_2, a_3 \in K \text{ s.t. } a_0 I + a_1\sqrt{-a}Z - a_2\sqrt{-b}Y + a_3\sqrt{-ab}X \in \mathcal{O}\}.$$

We make use of the following lemma to find a $\mathbb{Z}$-basis for M_{diag}.

Lemma 5.15. *$\mathcal{L}_{\mathcal{O}}$ is a full rank O_K-lattice in K^2.*

Proof. Since $\mathcal{O}$ is closed under addition and scalar multiplication over O_K, so is $\mathcal{L}_{\mathcal{O}}$. Consider an O_K-linearly independent generating set G of $\mathcal{L}_{\mathcal{O}}$ and let $g_1, \ldots, g_r$ be the subset of these that are K-linearly independent. Then $r \leq 2$. We have $I \in \mathcal{O}$, so $(1,0) \in \mathcal{L}_{\mathcal{O}}$. Suppose for a contradiction that $\mathcal{L}_{\mathcal{O}}$ contains no elements of the form $(a_0, a_1), a_1 \neq 0$ in $\mathcal{L}_{\mathcal{O}}$. Let $\{\omega_i\}_{i=1,\ldots,4}$ be a basis for $\mathcal{O}$, with corresponding elements in $\mathcal{L}_{\mathcal{O}}$ denoted by $(\omega_{i,0}, \omega_{i,1})$. By assumption, $\omega_{i,1} = 0 \forall i$. Since κ is an isomorphism of quaternion algebras, we can write each basis element in the form $\omega_{i,0} I - \omega_{i,2}\sqrt{-b}Y + \omega_{i,3}\sqrt{-ab}X$. Then, we can see that at least two of the basis elements must be K-linearly dependent. Hence, we have a contradiction and so $r = 2$. So $\mathcal{L}_{\mathcal{O}}$ spans K^2 as a K vector space and clearly $\text{rank}(\mathcal{L}_{\mathcal{O}}) = 2d$. □

Hence, we can conclude that there exists a $\mathbb{Z}$-basis for $\mathcal{L}_{\mathcal{O}}$ and so also for M_{diag}, which we denote $\{y_i\}$, for $i = 0, \ldots, 2d-1$.

For the remainder of this section, let us consider orders of the form $\mathcal{O} = \sum_{i=1}^{4} O_K \omega_i$, with

$$\omega_1 = I, \quad \omega_2 = \frac{I + iZ}{\sqrt{2}}, \quad \omega_3 = \frac{I + iY}{\sqrt{2}}, \quad \omega_4 = \omega_3\omega_2 = \frac{I + iX + iY + iZ}{2}, \tag{56}$$

as for the Clifford+T and Clifford+$\sqrt{\text{T}}$ bases. In this case, we have

$$M_{\mathcal{O}} = O_K + \frac{1+i}{\sqrt{2}} O_K,$$

which allows us to establish M_{diag} as a fractional $M_{\mathcal{O}}$ ideal. Moreover, for the bases considered in this paper, we have that M_{diag} is also principal, so

$$M_{\text{diag}} = \frac{1}{\xi} M_{\mathcal{O}}, \quad \xi \in L. \tag{57}$$

The definitions for $M_{\mathcal{O}}$ and ξ corresponding to the V, Clifford+T and Clifford+$\sqrt{\text{T}}$ bases are given in the Table **??**.

Table 8: $\xi, M_{\mathcal{O}}$ for V, Clifford+T and Clifford+$\sqrt{T}$ gate sets.

Gate set	ξ	$M_{\mathcal{O}}$
V basis	1	O_L
Clifford+T	$\sqrt{2}$	O_L
Clifford+$\sqrt{\text{T}}$	$\sqrt{2}$	$O_K + \frac{1+i}{\sqrt{2}} O_K$

Case 1: Diagonal Approximation For diagonal approximation (with and without fallback and mixing) the first normalized embedding $\sigma_1(m_1)/\sigma_1(\ell^N)$ falls in a two dimensional region, R_{approx}. Define the $2d \times 2d$ matrix $\Sigma_{\mathcal{O}}$ with rows:

$$\begin{aligned} \Sigma_{\mathcal{O}}^{(2j)} &= (\text{Re}(\sigma_j(y_0)), \ldots, \text{Re}(\sigma_j(y_{2d-1}))) \\ \Sigma_{\mathcal{O}}^{(2j+1)} &= (\text{Im}(\sigma_j(y_0)), \ldots, \text{Im}(\sigma_j(y_{2d-1}))) \,. \end{aligned}$$

So $\Sigma_{\mathcal{O}}$ is the matrix with entries corresponding to the real and imaginary components of the images of the l_i under each of the d homomorphisms. Let Λ be the diagonal matrix with $\left(\sqrt{\sigma_1(\ell^N)}, \sqrt{\sigma_1(\ell^N)} \ldots, \sqrt{\sigma_d(\ell^N)}, \sqrt{\sigma_d(\ell^N)}\right)$ on the diagonal. Then the operation $\Lambda\Sigma_{\mathcal{O}} z$ first embeds z into the Euclidean space corresponding to M_{diag}, then normalizes the result with respect to the norm ℓ^N. Finding m_1 is now an integer point enumeration problem:

Problem 5.16. *Find* $z \in \mathbb{Z}^{2d}$ *such that* $\Lambda^{-1}\Sigma_{\mathcal{O}} z \in R_{\text{approx}} \times D_1^{d-1}$.

Each solution $z = (z_0, \ldots, z_{2d-1})$ yields a candidate for m_1 by setting $m_1 = z_0 y_0 + \cdots + z_{2d-1} y_{2d-1}$.

Case 2: Magnitude Approximation For general unitary approximation the first normalized embedding $\sigma_1(m_1 m_1^*)/\sigma_1(\ell^N)$ belongs to the interval I_{approx} and the remaining $d-1$ embeddings satisfy $\sigma_k(m_1 m_1^*)/\sigma_k(\ell^N) \in [0,1]$.

We are looking for values $n = m_1 m_1^*$ satisfying the above conditions, such that $m_1 \in M_{\text{diag}}$. Consider the set

$$\{n : \exists m_1 \in M_{\text{diag}} \text{ such that } m_1 m_1^* = n\}$$

and let M_{norm} be the set generated multiplicatively by the above set. From Equation (**??**), we see that

$$M_{\text{norm}} \subseteq \frac{1}{\xi\xi^*} O_K,$$

a fractional O_K ideal. For this reason we can enumerate points $\hat{n} = \xi\xi^* n \in O_K$. Let $k_0, \ldots, k_{d-1}$ be an integral basis for K and define Σ' as the $d \times d$ matrix with rows:

$$\Sigma'_j = (\sigma_j(k_0), \ldots, \sigma_j(k_{d-1}))\,.$$

Define Λ' as the diagonal normalization matrix with $\Big(\sigma_1(\xi\xi^*) \cdot \sigma_1(\ell^N), \ldots, \sigma_d(\xi\xi^*) \cdot \sigma_d(\ell^N)\Big)$ on the diagonal. Finding $\hat{n}$ is now an integer point enumeration problem in a parallepiped:

Problem 5.17. *Find $z \in \mathbb{Z}^d$ such that $\Lambda'^{-1}\Sigma' z \in I_{\text{approx}} \times [0,1]^{d-1}$.*

Each solution $z = (z_0, \ldots, z_{d-1})$ yields a candidate for $\hat{n}$ by setting $\hat{n} = z_0 k_0 + \cdots + z_{d-1} k_{d-1}$. Recovery of m_1 requires a solution to the norm equation

$$\hat{m_1}\hat{m_1}^* = \hat{n}, \quad \hat{m_1} \in M_{\mathcal{O}}.$$

Finally the candidate m_1 is defined as $m_1 = \hat{m_1}/\xi$.

5.4.5 Finding m_2: solving a norm equation

Finding a candidate for m_2 amounts to solving a norm equation, with the added constraint that the pair (m_1, m_2) corresponds to a matrix in the order $\mathcal{O}$. Given a candidate $m_1 \in M_{\text{diag}}$, we define the set containing valid candidates for m_2 as

$$M_{\text{off-diag}}^{m_1} = \{m_2 : \kappa(h(m_1) + h(m_2)\mathbf{j}) \in \mathcal{O}\}.$$

To satisfy the determinant condition, we require

$$m_2 m_2^* = \ell^N - m_1 m_1^*, \quad m_2 \in M_{\text{off-diag}}^{m_1}. \tag{58}$$

Any element $m_2 \in M_{\text{off-diag}}^{m_1}$ belongs to the larger set

$$M_{\text{off-diag}} = \{m_2 : \exists m_1 \text{ s.t. } \kappa(h(m_1) + h(m_2)\mathbf{j}) \in \mathcal{O}\},$$

which, as shown for M_{diag}, is a fractional $M_{\mathcal{O}}$ ideal. In the following discussion, we show that a solution for m_2 can be recovered from a related norm equation, in which we solve for elements in $M_{\mathcal{O}}$, under the assumption that $M_{\text{off-diag}}$ is moreover a principal fractional ideal. That is,

$$M_{\text{off-diag}} = \frac{1}{\xi'} M_{\mathcal{O}}, \quad \xi' \in L.$$

Fix $m \in M_{\text{off}-\text{diag}}^{m_1}$. For any other $m' \in M_{\text{diag}}^{m_1}$ we have $\kappa(h(m)\mathbf{j} - h(m')\mathbf{j}) \in \mathcal{O}$. Therefore, we write $M_{\text{off}-\text{diag}}^{m_1} = m + M_{\text{off}-\text{diag}}^{0}$, where $M_{\text{off}-\text{diag}}^{0}$ is the principal fractional $M_{\mathcal{O}}$ ideal $M_{\text{off}-\text{diag}}^{0} = \{m' : \kappa(h(m')\mathbf{j}) \in \mathcal{O}\}$. We take

$$M_{\text{off}-\text{diag}}^{0} = \frac{1}{\chi} M_{\mathcal{O}}, \quad \chi \in L.$$

Note that a representative m is found by considering the quotient lattice $M_{\text{off}-\text{diag}}/M_{\text{off}-\text{diag}}^{0}$. The definitions for ξ, ξ' and χ corresponding to the V, Clifford+T and Clifford+$\sqrt{\text{T}}$ bases are given in the Table **??**.

Table 9: Fractional ideal representatives for V, Clifford+T and Clifford+$\sqrt{T}$ gate sets.

Gate set	ξ	ξ'	χ	$M_{\mathcal{O}}$
V basis	1	1	1	O_L
Clifford+T	$\sqrt{2}$	$\sqrt{2}$	1	O_L
Clifford+$\sqrt{\text{T}}$	$\sqrt{2}$	$\sqrt{2}$	1	$O_K + \frac{1+i}{\sqrt{2}} O_K$

The norm equation in Equation (**??**) can now be reformulated to look for a solution in $M_{\mathcal{O}}$.

Problem 5.18. *Given* $\hat{z}/\xi' \in M_{\text{off}-\text{diag}}, m_1 \in M_{\text{diag}}$, *find* $z \in M_{\mathcal{O}}$ *such that*

$$\left|\frac{\hat{z}}{\xi'} + \frac{z}{\chi}\right|^2 = \ell^N - m_1 m_1^*.$$

A solution z yields a candidate for m_2 by setting $m_2 = \hat{z}/\xi' + z/\chi$. Since $m_1 = \hat{m_1}/\xi$ for some $m_1 \in M_{\mathcal{O}}$, if $\xi = \xi'$ and $\chi = 1$, then Problem **??** is simplified to:

Problem 5.19. *Find* $z \in M_{\mathcal{O}}$ *such that* $|\hat{z} + \xi z|^2 = \xi\xi^* \ell^N - \hat{m_1}\hat{m_1}^*$, *where* $\hat{z}, \hat{m_1} \in M_{\mathcal{O}}$.

Clearly the V, Clifford+T and Clifford+$\sqrt{\text{T}}$ bases admit this simplified case. Of course, solving the norm equation for the V basis is already straightforward, but is included here for completeness.

Remark 5.20. By applying the variable substitution $z' = \hat{z} + \xi z$, we see that Problem **??** is equivalent to solving

$$|z'|^2 = r \in O_K, \quad z' \in \hat{z} + \xi M_{\mathcal{O}}, \tag{59}$$

where $r = \xi\xi^* \ell^N - \hat{m_1}\hat{m_1}^*$. In other words, z' must lie in the same quotient in $M_{\mathcal{O}}/\xi M_{\mathcal{O}}$ as $\hat{z}$.

We discuss solving these norm equations in Section **??**. In particular, for the special case of fields with class number equal to 1, we suggest a simplified solution for Equation (**??**).

5.5 Heuristic approximation cost scaling with accuracy

We first establish heuristic scaling of the power cost function with the area of the 2D or 1D regions related to the the six approximation problems considered in **??**. All gate sets we consider are related to integral quaternion with norm ℓ^N for some ℓ fixed by the gate set and N being a power cost of the given approximating quaternion. Let $R_{\varepsilon,q}$ be a 2D or

1D region with ε being diamond norm accuracy and q being success probability, During the point enumeration step of our algorithms for 2D problems, we are looking for integer points of dimension $2d$ in the bounded subset of $\mathbb{R}^{2d}$ given by equation below:

$$(a_0, \ldots, a_{2d-1}) \in \Lambda \Sigma_{\mathcal{O}}^{-1} \left(R_{\varepsilon,q} \times D_1 \times \ldots D_{d-1}\right)$$

Now, applying the Gaussian heuristic, we assume that there exist an integer point in the subset of $\mathbb{R}^{2d}$ when the volume of the subset is 1. Taking into account that $\det \Lambda = \mathrm{Nrm}(\ell)^N$ we get the following condition for the existence of integer points:

$$N \log(\mathrm{Nrm}(\ell)) + \log(\mathrm{Area}(R_{\varepsilon,q})) + \log(\pi^{d-1} / \det(\Sigma_{\mathcal{O}})) = 0$$

Define $b = \mathrm{Nrm}(\ell)$, then the Gaussian heuristic implies power cost scaling:

$$N = -\log_b(\mathrm{Area}(R_{\varepsilon,q})) + \log_b(\det(\Sigma_{\mathcal{O}})/\pi^{d-1})$$

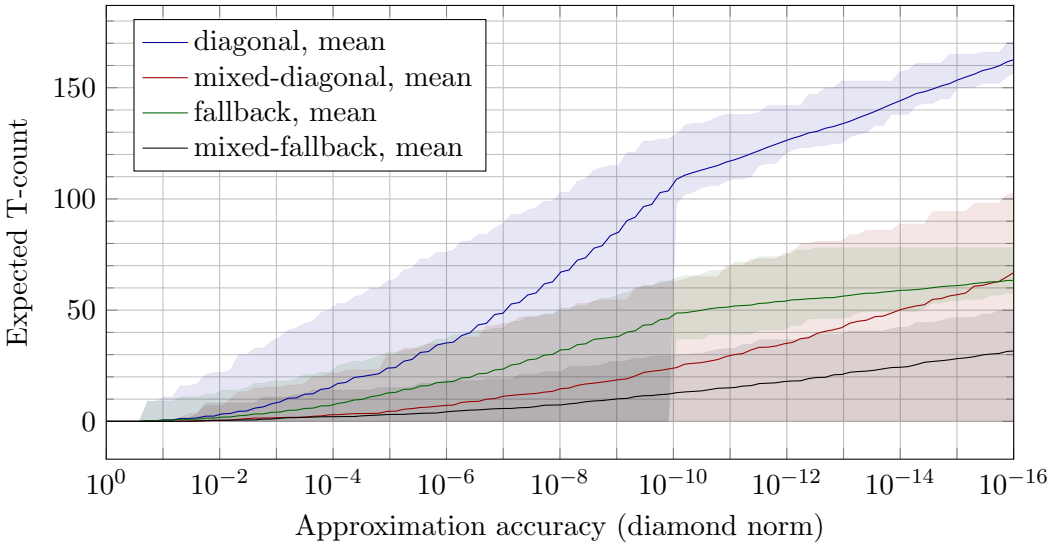
The relation between power cost and area for 1D problems is similarly

$$N = -\log_b(\mathrm{Length}(I_\varepsilon)) + O(1).$$

Now we specialize above calculation to Clifford+T and Clifford+$\sqrt{T}$ gate sets and specific approximation problems. Recalling that for Clifford+T and Clifford+$\sqrt{T}$ logarithm base $b = 2$ and using expression for the regions areas in **??**, we derive heuristic power cost scaling expression in the top half of **??**. We note that for projective (fallback) rotation approximation N is $\log_b(1/(1-q) \cdot 1/\varepsilon) + O(1)$, and for magnitude approximation N is $\log_b(1/\varepsilon) + O(1)$. We expect that magnitude approximations are shorter by the additive constant $\log_b(1/(1-q))$, where $1-q$ is the fall-back step probability of the fall-back protocol. Heuristically, we assume that increasing volume by a constant factor or $\log(1/\varepsilon)$ factor ensures that we can find integer points for which the corresponding norm equations are solvable. This does not affect constant in front of $\log_b(1/\varepsilon)$.

In applications we are interested in two other cost metrics for our gate sequences: non-Clifford gate count (that we simply call gate count) and T-count, that is the number of T states needed to executed given sequence. The gate count is a good proxy for how fast we can execute the sequence, where each non-Clifford gate is executed using circuit from Figure 33 in [Lit19]. The T-count is a good proxy for space-time volume needed to execute the sequence on a fault-tolerant quantum computer, because the space-time volume required is typically dominated by the space-time volume needed to distill T states. For Clifford+T approximations these two other cost metrics are equal to the power cost. It remains to estimate them for Clifford+$\sqrt{T}$ approximations. We assume that number of $\sqrt{T}, \sqrt{T}^3$ gates denoted by $N_{\sqrt{T}}$ in our sequences is the same as number of T gates. This is justified by our numerical results. Recall that $\sqrt{T}, \sqrt{T}^3$ contribute three to the power cost and T contributes 2. For this reason we have $N_{\sqrt{T}} = 0.2N$ and gate count is $0.4N$. To estimate T-count we assume that every $\sqrt{T}$ and $\sqrt{T}^3$ gate can be execute using four T states. This is because the circuit from Figure 33 in [Lit19]. consumes one $\sqrt{T}$ state and one T state. Producing one $\sqrt{T}$ state requires 3 T states in the worst case using catalysis protocol described in Figure 6a in [Bev+20]. We see that T-count for Clifford+$\sqrt{T}$ approximations heuristically scales the same way as power cost. Above implies heuristic cost scaling expressions in **??**.

Figure 14: Cost of approximating a set of Fourier angles rotations (see **??**) with Clifford+T gates using four approximation protocols. We fix a set of approximation accuracy values. For each value in the set we compute mean cost over all target angles. Shaded regions indicate range of costs from min to max over all angles for given accuracy value. In all reported fallback protocols the probability of the fallback step $1 - q$ is at most 0.01.



6 Numerical results

We have implemented algorithms described in the paper in Magma. For the numerical results we focus on four approximation protocols for diagonal unitaries (diagonal, mixed diagonal, fallback and mixed fallback) and two gate sets (Clifford+T and Clifford+$\sqrt{T}$). We target rotations by random angles and by Fourier angles $\pi/2^k$. The data-sets of angles for which we computed solutions numerically are summarized in **??**. We also provide the circuits for all approximations we have found in supplemental material.

Table 10: Sets of angles for which we computed solutions numerically. We approximate diagonal rotations using diagonal, mixed diagonal, fallback and mixed fallback protocols.

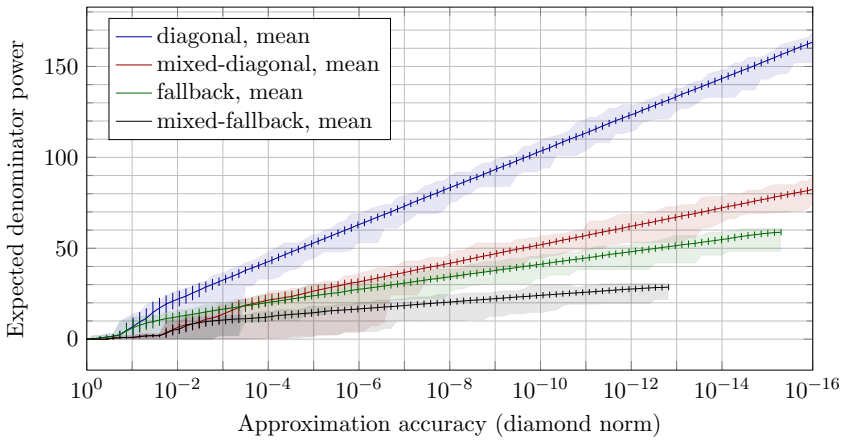
Gate set	Cost function	Data sets and corresponding figures			
		Random angles	Figure	Fourier angles	Figure
Clifford+T	T-count	1358 uniformly random angles from interval $[0, 2\pi]$	**??**	$\pi/2^n$ $n \in \{3, \ldots, 36\}$	**??**
Clifford+$\sqrt{T}$	Power	1221 uniformly random angles from interval $[0, 2\pi]$	**??**	$\pi/2^n$ $n \in \{3, \ldots, 45\}$	**??**
	Gate count		**??**		**??**
	T-count		**??**		**??**

Numerical results for random angles agree with the heuristic cost scaling derived in **??** as we can see from **??** and from **????**. Results for Fourier angles are a bit more complex. For many choices of angle and target accuracy, the Identity is a sufficient approximation. This is evident in the wide gap between minimum and maximum cost illustrated by the shaded regions of **??** and **??**. These low-cost Identity approximations have the effect of pulling down the overall mean cost as compared to random angles. However, once the Identity is no longer a viable option at high accuracy, the cost scaling is roughly the same as that of random angles.

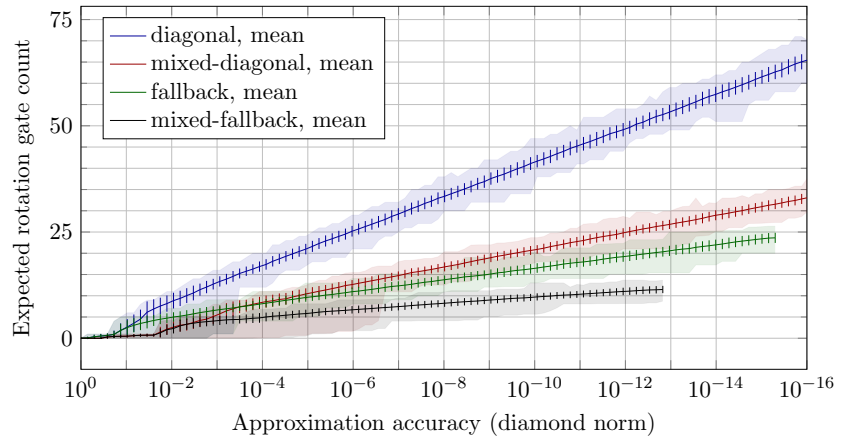
There is more variation in gate count and T-count when approximating using the

Figure 15: Cost of approximating a set of random rotations (see **??**) with Clifford+$\sqrt{T}$ gates using four approximation protocols. We fix a set of approximation accuracy values. For each value in the set we compute mean cost over all target angles. Vertical bars show the cost standard deviation for given accuracy value. Shaded regions indicate range of costs from min to max over all angles for given accuracy value. In all reported fallback protocols the probability of the fallback step $1 - q$ is at most 0.01. The linear fit results are in **??**.

(a) Scaling of denominator power with approximation accuracy. Denominator power of $\sqrt{T}$ and T is 3 and 2.



(b) Scaling of gate count with approximation accuracy. $\sqrt{T}$ gates and T gates contribute 1 to the gate count.



(c) Scaling of T-count with approximation accuracy. T-count of $\sqrt{T}$ gates is four.

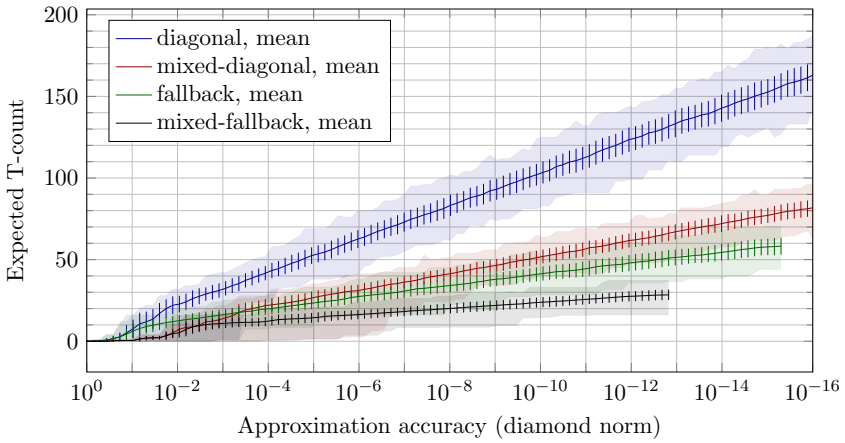
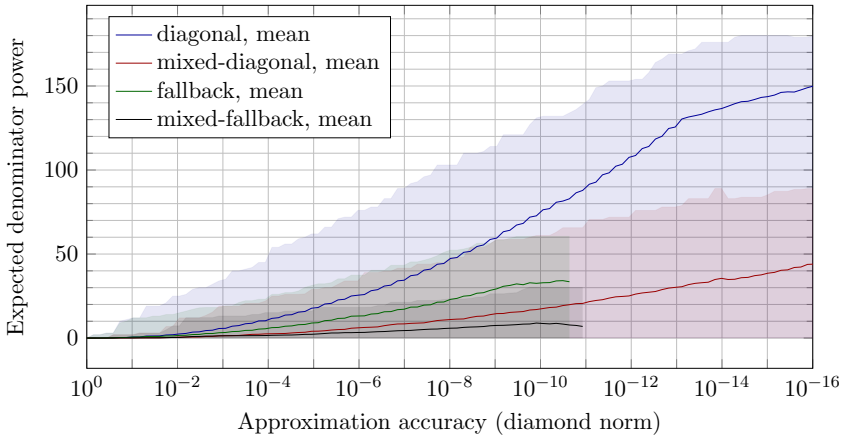
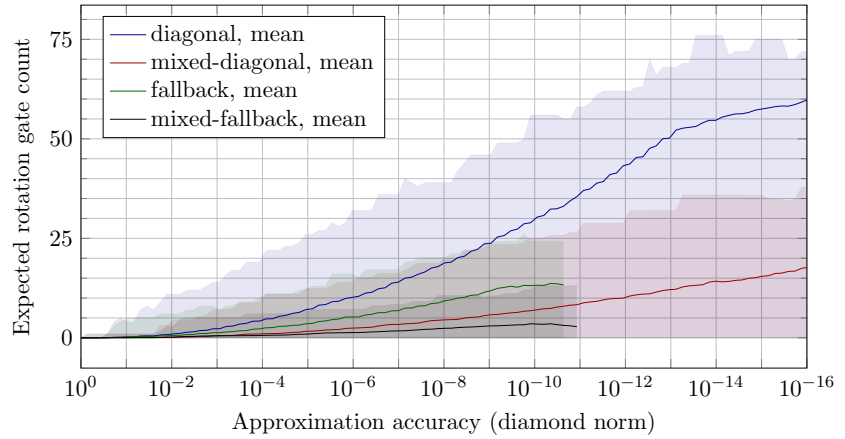


Figure 16: Cost of approximating a set of Fourier angles rotations (see **??**) with Clifford+$\sqrt{T}$ gates using four approximation protocols. We fix a set of approximation accuracy values. For each value in the set we compute mean cost over all target angles. Shaded regions indicate range of costs from min to max over all angles for given accuracy value. In all reported fallback protocols the probability of the fallback step $1 - q$ is at most 0.01.

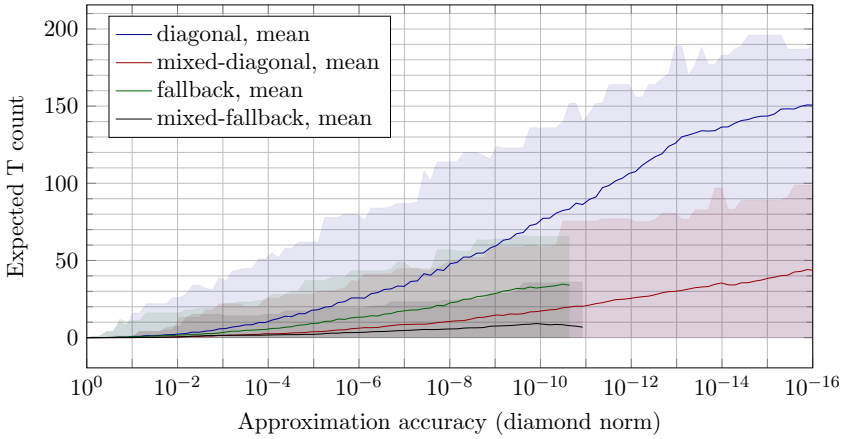
(a) Scaling of denominator power with approximation accuracy. Denominator power of $\sqrt{T}$ and T is 3 and 2.



(b) Scaling of gate count with approximation accuracy. $\sqrt{T}$ gates and T gates contribute 1 to the gate count.



(c) Scaling of T-count with approximation accuracy. T-count of $\sqrt{T}$ gates is four.



Clifford+$\sqrt{T}$ gate set than when approximating using Clifford+T, even for random rotations (**??** and **??**). This is because our algorithm finds optimal solutions to the subproblems only with respect to denominator power cost function. For Clifford+T gate set, the power cost function coincides with T-count and non-Clifford gate count. For Clifford+$\sqrt{T}$ gate set, the power cost function can be related to T-count and non-Clifford gate count using an additional assumption that the number of $\sqrt{T}, \sqrt{T}^3$ gates is the sequence roughly the same as the number of T gates. For this reason, we see that the variations in power cost function in **??** and **??** are similar. However, there is more variations in T-count and non-Clifford gate count in **??** and **??**.

7 Integer point enumeration problems

In Section **??**, we described a general method for solving approximate synthesis problems on quaternion gate sets, with three examples from commonly used gate sets. In this section, we focus on the first step in that method: integer point enumeration. Where relevant, we re-use the notations introduced in previous sections.

Recall that the conditions on m_1, as defined in Section **??**, define a target region in which we want to enumerate integer vectors. Section **??** outlines an algorithm for integer point enumeration in convex bodies of a particular form and shows how this can be applied to the target regions prescribed by approximate synthesis. In the case of magnitude approximation, the target region is a parallelotope. Section **??** gives an alternative method in that case, making use of the number-theoretic structure arising from the quaternion gate sets.

7.1 General point enumeration

In this section we describe an approach to solving integer point enumeration problems in a subset of convex bodies, and we apply this method to the regions arising from approximate synthesis. The algorithm is from Lenstra [Len83], and it applies to problems with the following general form.

Problem 7.1 (Integer point enumeration in a convex body). *Let R be a bounded convex body of positive volume satisfying $R = \{x \in \mathbb{R}^d : Ax \leq b\}$, where A is an invertible $d \times d$ matrix and b is a d-dimensional column vector. Find all $x \in R \cap \mathbb{Z}^d$.*

The inequality in Problem **??** denotes an element-wise comparison between two vectors.

Remark 7.2 (Target regions defined by approximate synthesis problems). The target regions defined by the approximation problems are not necessarily of the form in Problem **??**. For instance, the target region defined by **??**, illustrated in **??**, is *not* convex. In these cases, we can take the convex hull of R and apply Lenstra's algorithm, discarding any solutions not in R.

For the remainder of this section, we assume that R is of the form required by Problem **??**. In theory, we could find maximum and minimum bounds for R in each dimension, thus defining a d-dimensional box (hyperrectangle) C_R such that $R \subset C_R$. A solution to Problem **??** is then found by enumerating all integer points in the box and checking each point to see if it lies in R. In practice, this strategy is less than optimal, as there may be numerous points in the box, but the set R might contain no integer points. For an example, see **??**. Lenstra's algorithm circumvents this problem by using a constructive version of Khinchin's Flatness Theorem described below.

To state the Khinchin's Flatness Theorem we define the width of a convex body. For a non-empty convex body R, the *width* of R along a vector r is defined as $w_r(R) = \max_{x \in R}\{r^T x\} - \min_{x \in R}\{r^T x\}$. The width of R is $w(R) := \min_{r \in \mathbb{Z}^d, r \neq 0}\{w_r(R)\}$, the vector $r_{\min}(R)$ where the minimum is achieved is the flat direction of R. The Flatness Theorem (**??**) guarantees that the solution to Problem **??** is non-empty if $w(R)$ is above some constant $\omega(d)$. Banaszczyk proved that $\omega(d) = O(d)$ [Ban95].

Theorem 7.3 (Khinchin's Flatness Theorem, attributed to [Khi48]). *Let $R \in \mathbb{R}^d$ be a full-dimensional non-empty convex body. Either R contains an integer point, or $w(R) \leq \omega(d)$, where $\omega(d)$ is a constant depending on the dimension only.*

Above theorem shows that in the case of no integer points in R, convex body R must have small width. Suppose now that the flat direction is known $r_{\min}(R)$ and we width is small. Next we show how $r_{\min}(R)$ is used to find an integer in R.

Integer point enumeration in a d-dimensional convex body R to several instances of the integer point enumeration in a $(d-1)$-dimensional convex bodies. It is convenient to represent $\mathbb{Z}^d$ as disjoint union of $d-1$ dimensional lattices in $\mathbb{R}^d$

$$\mathbb{Z}^d = \bigcup_{k \in \mathbb{Z}} \{z : z^T r_{\min}(R') = k,\, z \in \mathbb{Z}^d\}$$

with each lattice $L_k = \{z : z^T r_{\min}(R') = k,\, z \in \mathbb{Z}^d\}$ contained in the hyperplane $H_k = \{x \in \mathbb{R}^d : r_{\min}(R')^T x = k\}$. The proposition below bounds the number of such hyperplanes intersecting R.

Proposition 7.4. *Let $R \in \mathbb{R}^d$ be a full-dimensional non-empty convex body. The number of hyperplanes of the form $H_k = \{x \in \mathbb{R}^d : r^T x = k\}$, $k \in \mathbb{Z}$ intersecting R is bounded by $w_r(R) + 1$.*

Using the flat direction of R, we have reduced finding an integer point in d-dimensional convex body R to finding an integer point in at most $w(R)+1$ $(d-1)$-dimensional convex bodies $R \cap H_k$. Using this approach the algorithm for finding an integer point in convex body R (or determining that R has no integer points) terminates in polynomial time when d is fixed. It remains to discuss an algorithm for finding the flat direction of R.

We discuss an efficient approach finding an approximation to the flat direction of R instead of the flat direction of R. More precisely, we will compute r from $\mathbb{Z}^d$ such that ratio $w_r(R)/w(R)$ is not too big. Such r can be used instead of $r_{\min}(R)$ for the reduction to $(d-1)$-dimensional integer point enumeration problems discussed above. Let us transform R so that it is roughly spherical in shape, via an invertible $d \times d$ matrix τ. Each point y in $\tau R \cap \tau\mathbb{Z}^d$ corresponds to a point $x \in R \cap \mathbb{Z}$ by $x = \tau^{-1} y$. More precisely, we can find τ such that τR satisfies

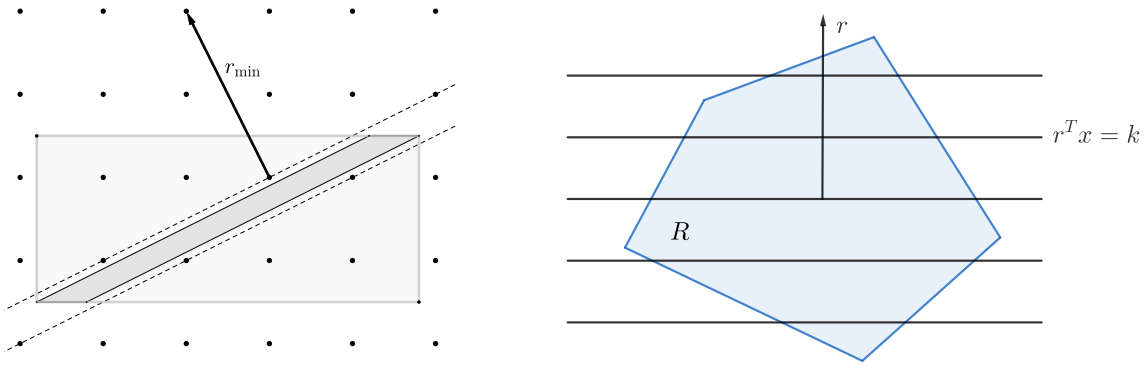
$$B(p, \delta) \subset \tau R \subset B(p, \Delta) \tag{60}$$

for balls with center point p and radii δ and Δ, such that the ratio $\frac{\Delta}{\delta}$ is bounded by a constant dependent only on d, $c_1(d)$; Lenstra takes $c_1(d) = 2d^{3/2}$. See Figure **??** for an illustration. For the regions considered in this work it is easy to find τ with a better ratio Δ/δ. Using above we see that R contains an ellipsoid $R' = \tau^{-1}B(p, \delta)$, for which width can be calculated more efficiently:

$$w(R') = w(\tau^{-1}B(0,\delta)) = \min_{r \in \mathbb{Z}^d, r \neq 0} 2\delta \cdot \max_{\|x\| \leq 1} r^T \tau^{-1} x = 2\delta \cdot \min_{r \in \mathbb{Z}^d, r \neq 0} \left\| (\tau^{-1})^T r \right\|$$

In other words, finding the flat direction $r'_{\min}$ of $\tau^{-1}B(p,\delta)$ is equivalent to finding the shortest vector of lattice $(\tau^{-1})^T\mathbb{Z}^d$ which is the dual lattice of $\tau\mathbb{Z}^d$. Then applying **??**

to R' determines whether an integer point in R, if it exists, lies in R' or the width of R' is bounded by $\omega(d)$. In the latter case, using **??**, we see that $w(R)$ is bounded by $\Delta/\delta \cdot w(R') \leq c_1(d)\omega(d)$, that is a constant dependent on the dimension only. Lenstra's algorithm (Algorithm **??**) uses approximation to the shortest vector of $(\tau^{-1})^T\mathbb{Z}^d$. More precisely, let $b_1, \ldots, b_d$ being an LLL-reduced basis of lattice $\tau\mathbb{Z}^d$, and let $b_1^*, \ldots, b_d^*$ be Gram-Schmidt orthogonalization of $b_1, \ldots, b_d$, then vector $b_d^*/\|b_d^*\|^2$ belongs to the dual lattice $(\tau^{-1})^T\mathbb{Z}^d$ and is an approximation to the shortest vector of the dual lattice.



(a) Parallelogram R with no integer points and bounding box C_R with many integer points. Vector $r_{\min}(R)$ is the flat direction of the parallelogram.

(b) The hyperplanes $\{x \in R : r^T x = k\}$ for $k \in \mathbb{Z}$ intersecting R.

Figure 17: Integer point enumeration in convex bodies and the flat direction.

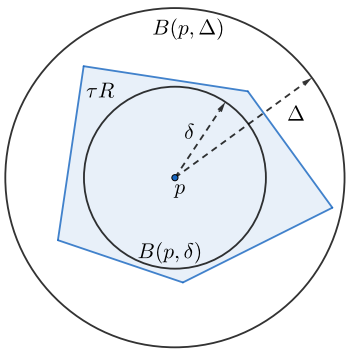


Figure 18: The concentric balls $B(p, \Delta)$ and $B(p, \delta)$, centered at p with radii Δ and δ, respectively, such that $B(p, \delta) \subset \tau R \subset B(p, \Delta)$ and $\Delta/\delta \leq c_1(d)$.

For fixed dimension d, Lenstra's algorithm (Algorithm **??**) runs in polynomial time in the length of the input [Len83]. This algorithm can be modified to enumerate integer points in R and require polynomial time per point. In practice, we use quadratic constraints $(x-p)^T Q(x-p) \leq 1$ for point p and symmetric matrix Q in **??** in addition to the linear constraints. The approach in this section can be modified to handle quadratic constraints. In this case, in Algorithm **??**, $k_{\min}, k_{\max}$ are found by solving quadratic optimization problems as opposed to using linear programming.

Input : A $n \times d$ real-valued matrix A and a d-dimensional column vector b defining the convex body $R := \{x \in \mathbb{R}^d : Ax \leq b\}$.
Output: A subset $X \subset \{x : x \in R \cap \mathbb{Z}^d\}$

$X \leftarrow \emptyset$;
Compute τ such that τR is "roughly spherical" with center p as in **??**;
$\mathcal{L} \leftarrow \tau\mathbb{Z}^d$, with LLL reduced basis $b_1, \ldots, b_d$ such that $|b_1| \leq \cdots \leq |b_d|$;
$b_1^*, \ldots, b_d^*$ is a Gram Schmidt Orthogonalised basis $b_1, \ldots, b_d$;
$r_{min} \leftarrow$ coordinates of $b_d^*/|b_d^*|^2$ in basis $(\tau^{-1})^T$, an approximation to $r_{\min}(R)$;
$k_{min} \leftarrow \left\lceil \min_{y \in R}\{(r_{\min})^T y\} \right\rceil$, using linear programming;
$k_{max} \leftarrow \left\lfloor \max_{y \in R}\{(r_{\min})^T y\} \right\rfloor$, using linear programming;
Let T be invertible integer matrix such that τT is matrix with columns $b_1, \ldots, b_d$, let $\tilde{A} = AT$;
for $k_{min} \leq k \leq k_{max}$ **do**
    $\tilde{x}_d \leftarrow k$;
    $A' \leftarrow \tilde{A}_{[1:d-1]}$, the $n \times (d-1)$ matrix consisting of the first $d-1$ columns of $\tilde{A}$;
    $b' \leftarrow b - \tilde{A}_{[d]}k$, where $\tilde{A}_{[d]}$ denotes the d^{th} column of $\tilde{A}$;
    Run Algorithm **??** on inputs A' and b' to obtain $X' \subset \{\tilde{x} := (\tilde{x}_1, \ldots, \tilde{x}_{d-1}) \in \mathbb{Z}^{d-1} : A'x' \leq b'\}$;
    $X \leftarrow X \cup T\{(\tilde{x}_1, \ldots, \tilde{x}_d) : (\tilde{x}_0, \ldots, \tilde{x}_{d-1}) \in X'\}$;
end
Output X;

Algorithm 1: Integer point enumeration in a bounded, positive-volume convex body satisfying $R = \{x \in \mathbb{R}^d : Ax \leq b\}$.

7.2 Point enumeration in a parallelotope

In this section, we will show how to exploit the number-theoretic structure present in the integer ring O_K for the instances of point enumeration relating to the magnitude approximation problems. These have a special shape: as described in Section **??**, point enumeration occurs in a d-dimensional box $I \times [0,1]^{d-1}$ where $d = [K : \mathbb{Q}]$. Specifically, we are interested in the following problem.

Problem 7.5 (Box Enumeration Problem). *Let K be a totally real number field of degree d and let O_K be its ring of integers. Given real numbers $\{g_j, h_j \mid g_j < h_j, j = 1, \ldots, d\}$, find n in O_K contained in the box, that is n such that $\sigma_j(n) \in [g_j, h_j]$ or determine that no such n exists.*

We rely on the same point enumeration approach as in the previous section, however in this special case it is easier to predict the number of integer points in the box. Interestingly the number of elements n from O_K in the box is proportional to the volume of the box $\prod_j (h_j - g_j)$. This observation was first made in [Sel15] and later generalized in [Kli+15b]. The lower-bound on the number of integer points is summarized by the following proposition.

Proposition 7.6. *Let K be a totally real number field, there exists a constant V_0 dependent only on K such that every box enumeration problem (**??**) with box volume at least V_0 has at least one solution.*

A corollary of the above proposition, is that any box contains at least $\lfloor \prod (h_j - g_j)/V_0 \rfloor$ elements of O_K. In the rest of this section we sketch the proof of the proposition. The proof proceeds in two steps. First we observe that if the box contains a certain parallelotope P centered at zero shifted by any vector t, then it must contain an element of O_K. Second we show that when the volume of the box is at least V_0, then the point enumeration problem is equivalent to point enumeration in another box $[g'_1, h'_1] \times \ldots \times [g'_d, h'_d]$ such that this box contains the parallelotope P translated by the center of the box.

Recall that the ring of integers O_K corresponds a d-dimensional lattice L in $\mathbb{R}^d$. Let k_i be an integral basis for O_K and σ_i be embedding of K into $\mathbb{R}$, the lattice basis is given by

$$b_j = (\sigma_1(k_j), \ldots, \sigma_d(k_j))^T, \text{ for } j = 1, \ldots, d$$

and the corresponding basis matrix B has columns b_j. Recall that the parallelotope

$$C(B) = \{Bx : x_k \in [-1/2, 1/2)\}$$

translated by lattice points from L defines partition of $\mathbb{R}^d$, that is for any point x in $\mathbb{R}^d$, there is a unique lattice point n, such that $x \in n + C(B)$. Equivalently, there is always a lattice point in $x - C(B)$. For this reason, if a box contains $P = -C(B)$, it must contain at least one lattice point. It is easy to find such a point by computing $B^{-1}x$ and rounding all the coordinates to the nearest integer. For the box to contain the shifted parallelotope $P = -C(B)$ the following constraints should hold:

$$h_j - g_j \geq \max_{x \in C(B)} x_j - \min_{x \in C(B)} x_j \text{ for all } j = 1, \ldots, d$$

This completes the first step of the proof.

For the second step of the proof we use units and the unit group of O_K. Let u be a unit of O_K, that is u^{-1} is also in O_K. First note that z from O_K is contained in the box $[g_1, h_1] \times \ldots \times [g_d, h_d]$, if and only if uz is contained in the transformed box $(\sigma_1(u)[g_1, h_1]) \times \ldots \times (\sigma_d(u)[g_d, h_d])$. Integers uz belong to the box with dimensions $|\sigma_j(u)|(h_j - g_j)$. Note that the overall volume of the box is the same because $\prod_j |\sigma_j(u)| = 1$.

The next step is to show that if the box has sufficiently big volume, we can always find a unit u, such that the transformed box contains shifted copy of $C(B)$, that is:

$$|\sigma_j(u)|(h_j - g_j) \geq \max_{x \in C(B)} x_j - \min_{x \in C(B)} x_j \text{ for all } j = 1, \ldots, d \tag{61}$$

For this we use the unit group of O_K. Recall that according to Dirichlet's Unit Group theorem, any unit of O_K can be written as:

$$u = \pm u_1^{m_1} \ldots u_{m_1}^{m_{d-1}}, \text{ for } m_j \in \mathbb{Z}$$

Substituting this expression for u in terms of u_k above into **??** and taking log of both sides of the inequality gives us:

$$\sum_{i=1}^{d-1} m_i \log |\sigma_j(u_i)| + \log(h_j - g_j) \geq \log(\max_{x \in C(B)} x_j - \min_{x \in C(B)} x_j) \text{ for all } j = 1, \ldots, d \tag{62}$$

Let us discuss the geometric interpretation of the above inequality. Vectors

$$b'_i = (\log |\sigma_1(u_i)|, \ldots, \log |\sigma_d(u_i)|)^T, \text{ for } i = 1, \ldots, d-1$$

define a $d-1$-dimensional lattice L' in $\mathbb{R}^d$ with basis matrix B' (known a the unit lattice of O_K), contained in sub-space $x_1 + \ldots + x_d = 0$. For the inequality to be true, the intersection between the shifted lattice

$$(\log(h_1 - g_1), \ldots, \log(h_1 - g_1))^T + L'$$

and the direct product of half-open intervals

$$R = [\log(\max_{x \in C(B)} x_1 - \min_{x \in C(B)} x_1), +\infty) \times \ldots \times [\log(\max_{x \in C(B)} x_d - \min_{x \in C(B)} x_d), +\infty)$$

must be non-empty. Note that the shifted lattice is contained in the subspace $x_1 + \ldots + x_d = \log \prod_j (h_j - g_j)$ which is determined by the box volume $V = \prod_j (h_j - g_j)$. To ensure that the inequalities in **??** have a solution, it is sufficient to ensure that the intersection of R and the subspace $x_1 + \ldots + x_d = \log V$ contains a shifted parallelotope $t + C(B')$ for some shift vector t. The bigger the volume $V = \prod_j (h_j - g_j)$, the bigger intersection between R and subspace $x_1 + \ldots + x_d = \log V$. In other words, there exists V_0, such for all $V \geq V_0$ intersection between R and subspace $x_1 + \ldots + x_d = \log V$ contains $t + C(B')$ for some shift vector t. This completes the proof.

In the above proof, the value V_0 depends on the choice of integral basis of O_K and fundamental units $u_1, \ldots, u_{d-1}$. Using reduced bases for O_K and the unit lattice can improve V_0. Further improvements can be achieve by using different fundamental domains for the lattices. One can replace $C(B)$ with $C(B^*)$, where B^* is the matrix corresponding to Gram-Schmidt orthogonalisation of basis $b_1, \ldots, b_d$. In this case rounding coordinates of $B^{-1}x$ is replaced by the Nearest-Plane algorithm. For further improvement, one can replace $C(B)$ with lattice's Voronoi cell and rounding with solving the Closest Vector Problem. Using an approach similar to the one described above one can also show the following:

Proposition 7.7. *Let K be a totally real number field, there exists a constant V_0' dependent only on K such that every box enumeration problem (**??**) with box volume at most V_0' has at most one solution.*

8 Relative norm equations

As explained in Section **??**, each solution to point enumeration gives rise to a relative norm equation, which is solved to complete a solution to some approximation problem. In this section, we provide a general approach for solving such relative norm equations. Specifically, we are interested in solving the following problem.

Problem 8.1. *Let K be a totally real number field with extension $L = K(i)$, such that $i^2 = -1$. Let O_K and O_L be the respective integer rings. Given r from O_K, compute m from O_L such that $mm^* = r$, or determine that no such m exists.*

Note that for this problem to have a solution, it is necessary (but not sufficient) that r is totally positive in O_K i.e. $\sigma_k(r) > 0$ for all homomorphisms from K into $\mathbb{R}$ [Coh93]. From now on we assume this is the case.

The algorithm for solving norm equations given here (Algorithm **??**) takes advantage of a number of properties specific to the examples of L and K that we consider. In particular, we look at fields L and K which are Galois fields, and whose rings of integers are principle ideal domains. For more general gate sets, Algorithm 7.5.15 of Cohen [Coh12] gives a method for solving relative norm equations, covering both Galois and non-Galois

extensions. We use the method from [KY15] and justify that for the fields we consider a solution to a relative norm equation can be found in polynomial time given factoring oracle. Examples of fields K and L of interest to us are provided in Table **??** (Section **??**). Our approach to solve Problem **??** uses common properties of these fields, which are captured in the following definition.

Definition 8.2 (Common properties of relevant fields). *Let i be such that $i^2 = -1$. We define K and $L = K(i)$ as fields having the following properties:*

1. *L/K is a cyclic Galois extension,*
2. *O_K and O_L are principal ideal domains,*
3. *$[O_L^\times : WO_K^\times] = 1$ or 2, where W is the group of roots of unity in L,*
4. *O_L is Euclidean with respect to the field norm of L (O_L is* norm-Euclidean*),*
5. *The generators of the unit group of O_L are known,*
6. *Given u a totally positive unit in O_K, there exists a unit $w \in O_L$ such that $ww^* = u$.*

The fields which we consider in Section **??**, (see Table **??**), are cyclotomic fields, and satisfy Definition **??** [Was97]. For the interested reader, Lemmermeyer provides a survey of cyclotomic fields known to be norm-Euclidean in [Lem95].

8.1 Solution overview

The correctness of Algorithm **??** is proved in Proposition **??**. Moreover, Proposition **??** shows that when a solution to the relative norm equation problem (Problem **??**) exists, we can write it as

$$m = w \prod_{\substack{j:\,\eta_j \\ \text{inert}}} \eta_j^{e_j/2} \prod_{\substack{j:\,\eta_j \text{ split/} \\ \text{ramified}}} \xi_j^{e_j}, \text{ where } r = \prod u\eta_j^{e_j}$$

where w is a unit of O_L, ξ_j are generators of prime ideals in O_L and η_j are primes in O_K and u is a unit in O_K. We will describe how to determine the existence of a solution and how to compute one when it exists.

Algorithm **??** summarizes the method for solving relative norm equations in O_K. First, we compute the prime factorization of the absolute norm $R = N(r) \in \mathbb{Z}$. Suppose $R = \prod_k p_k^{v_k}$. Each prime p_k is factored into prime O_L ideals $\mathfrak{p}_i^{(k)}$, for which we compute the ideal generators $\xi_i^{(k)}$ such that $\xi_i^{(k)} O_L = \mathfrak{p}_i^{(k)}$. The $\xi_i^{(k)}$ have corresponding primes $\eta_i^{(k)}$ in O_K. Through trial division of r by each prime $\eta_i^{(k)} \in O_K$, we compute a representation of r as a product of primes in O_K, $r = u \prod_j \eta_j^{e_j}$ (up to multiplication by a unit u). If e_j is even for all relatively inert η_j, the relative norm equation is solvable (Lemma **??**). Supposing a solution m exists, we compute w, a unit of O_L, such that $ww^* = u$ then write m in the form above.

Proposition 8.3. *Algorithm **??** returns, in polynomial time, a solution to Problem **??**, if one exists, and returns* No solution *otherwise.*

Remark 8.4. Algorithm **??** implicitly gives a description of all solutions, if more than one is needed. If $m_2 = w \prod_{\substack{i:\,\eta_i \\ \text{inert}}} \eta_i^{r_i/2} \prod_{\substack{i:\,\eta_i \text{ split/} \\ \text{ramified}}} \xi_i^{e_i}$ is a solution, then so is

$$w \prod_{\substack{i:\,\eta_i \\ \text{inert}}} \eta_i^{r_i/2} \prod_{\substack{i:\,\eta_i \text{ split/} \\ \text{ramified}}} (\xi_i^{e_i - e} (\xi_i^*)^e)$$

for each e between 0 and e_i.

Input : r in O_K
Output: m in O_L such that $mm^* = r$, or *No solutions.*

Compute $R \leftarrow N(r) \in \mathbb{Z}$;
Compute prime factorization $R = \prod_k p_k^{v_k}$;
For each p_k, apply Algorithm **??** to find all prime O_L ideals $\mathfrak{p}_i$ such that $p_k O_L \subset \mathfrak{p}_i$, corresponding ideal generators ξ_i and primes in O_K, η_i.;
Find integers $\{e_i\}$ and u, a unit of O_K, such that $r = u \prod_j \eta_i^{e_i}$;
if *all* e_i even for all relatively inert η_i **then**
    Compute $w \in O_L$ such that $ww^* = u$;
    Output solution $m = w \prod_{\substack{i:\,\eta_i \\ \text{inert}}} \eta_i^{e_i/2} \prod_{\substack{i:\,\eta_i \text{ split/} \\ \text{ramified}}} \xi_i^{e_i}$;
else
    Output *No solution.*
end

Algorithm 2: Algorithm for solving relative norm equations.

Input : p, prime
Output: The set $\{(\eta_i, \xi_i, \mathfrak{p}_i)\}$, where $p = \prod \mathfrak{p}_i$, $\xi_i O_L = \mathfrak{p}_i$ and $\eta_i \in O_K$ prime above p.

Factor p into prime O_L ideals $\mathfrak{p}_i$;
Compute ideal generators ξ_i such that $\xi_i O_L = \mathfrak{p}_i$;
if there exists v, a unit in $O_L^\times / O_K^\times$, such that $v\xi_i$ prime in O_K **then**
    Set $\eta_i := v\xi_i$;
else
    Set $\eta_i := \xi_i \xi_i^*$;
end
Output $(\eta_i, \xi_i, \mathfrak{p}_i)$ for each i.

Algorithm 3: Subroutine of Algorithm **??** for computing primes above p in O_K.

8.2 Subroutines of Algorithm ??

We now look at the subroutines of Algorithm **??** in more detail and prove Proposition **??**.

Step ??: Computing $R = N(r)$ Representing r in integer coordinates with respect to an integral basis of O_K gives a closed form multivariate polynomial expression for the absolute norm function.

Step ??: Computing the prime factorization of $R = N(r)$ Recall that in the application to approximate synthesis, the possible values for $R = N(r)$ are bounded above by ℓ^N. Using the Prime Number Theorem, we heuristically expect R to be prime with probability approximately $1/\log(\ell^N)$. Primality testing can be done with any polynomial time algorithm, such as Miller-Rabin or AKS. For composite R, variants of Miller-Rabin can be used to return factors under some conditions, for example when R is coprime to a Miller-Rabin witness.

If a candidate value for m_1 results in an R that is inefficient to factorize, it can be discarded, although one should note that this may result in a non-optimal unitary approximation. We certainly expect R to be easier to factorize than RSA integers, in general, recalling the relation between N and area given in Section **??**.

Step ??: Computing a set of primes in O_K dividing r For each prime factor p_k of R, Algorithm **??** is used to factorise p_k into a product of prime ideals $\mathfrak{p}_i$, compute corresponding ideal generators ξ_i, and, ultimately, find primes in O_K, η_i, which divide r.

A detailed description of Algorithm **??** is given in Section **??**.

Step ??: Representing r as a product of primes in O_K Algorithm **??** produces the set $\{\eta_i, \xi_i, \mathfrak{p}_i\}$ for each prime factor p_k of R. We have $N(\mathfrak{p}_i) = p_k^{f_i}$, where $f_i = [O_L/\mathfrak{p}_i : \mathbb{Z}/p_k]$ (Thm. 4.8.5, [Coh93]). Trial division of r by each η_i will determine the e_i's, using the exponents v_k in the prime factorization of R to determine when all prime ideals above each p_k are covered. The representation of r as a product of primes in O_K is then $u \prod_i \eta_i^{e_i}$, where u is a unit in O_K.

Step ??: Determining the existence of a solution Step **??** in the algorithm determines whether a solution to the relative norm equation exists. The existence criterion is captured in the following Lemma.

Lemma 8.5. *Given $r \in O_K$, where $r = u \prod \eta_i^{e_i}$ with η_i prime in O_K and u a unit in O_K, the relative norm equation $m_2 m_2^* = r, m_2 \in O_L$ is solvable if and only if e_i is even, for all relatively inert η_i [Kli+15b].*

Clearly, Step **??** ensures that Algorithm **??** correctly returns *No solution* if no solution exists for input r.

Step ??: Finding a unit w The existence of w, a unit in O_L, such that $ww^* = u$ is guaranteed by Definition **??**. Let us describe how to compute w in Step **??**. We can take advantage of the fact that we are in the unit group of O_L with the theorem below.

Theorem 8.6 (Dirichlet's Unit Theorem, 1846). *Let K be a number field with r_1 real homomorphisms and $2r_2$ pairs of conjugate homomorphisms. Let $r = r_1 + r_2 - 1$. Each order*

$\mathcal{O}$ of K contains multiplicatively independent units $u_1, \ldots, u_r$ of infinite order such that every unit in $\mathcal{O}$ can be written explicitly in the form

$$\omega^k u_1^{k_1} \cdots u_r^{k_r},$$

where ω is a root of unity in $\mathcal{O}$.

By Theorem **??**, w can be written as $\omega^k u_1^{k_1} \ldots u_{d-1}^{k_{d-1}}$ for some $k, k_1, \ldots, k_{d-1} \in \mathbb{Z}$. It follows that $u = ww^* = (\omega\omega^*)^k (u_1 u_1^*)^{k_1} \ldots (u_{d-1} u_{d-1}^*)^{k_{d-1}}$. Since the unit group generators are known, by Definition **??**, the following lemma asserts that we can generate the entire group of totally positive units of O_K.

Lemma 8.7. *Let d be the degree of K. Let $u_1, \ldots, u_{d-1}$ be infinite order units of O_L, the ring of integers of L. Then the multiplicative group generated by $u_1 u_1^*, \ldots, u_{d-1} u_{d-1}^*$ is equal to the group of totally positive units of O_K.*

Proof. Clearly, $u_i u_i^*$ are totally positive units of O_K.

Let u be some totally positive unit of O_K not equal to $u_i u_i^*$ for all i. By Definition **??**, there exists a unit $w \in O_L$ such that $u = ww^*$. Then, by Dirichlet we have $w = \omega^k u_1^{k_1} \ldots u_d^{k_{d-1}}$, with $k_i \in \mathbb{Z}$ and ω a root of unity. Clearly, u is a product of integer powers of $u_1 u_1^*, \ldots, u_{d-1} u_{d-1}^*$. □

This representation of u as a product of unit group generators motivates the reduction of finding w to an instance of finding an integer vector in the lattice induced by the unit group $O_L^\times$. Let the lattice be denoted $\mathcal{L}_S$, generated by basis vectors

$$(\log \sigma_1(u_j u_j^*), \ldots, \log \sigma_d(u_j u_j^*)), \quad j = 1, \ldots, d-1.$$

Let v be the vector $(\log \sigma_1(u), \ldots, \log \sigma_d(u))^T$.

We can find an integer vector $(x_1, \ldots x_{d-1})$ such that

$$u = (u_1 u_1^*)^{x_1} \cdots (u_{d-1} u_{d-1}^*)^{x_{d-1}}$$

by solving

$$A(x_1, \ldots, x_{d-1})^T = v,$$

where A is the $d \times (d-1)$ matrix whose rows correspond to the basis vectors of $\mathcal{L}_S$. Setting $w = u_1^{x_1} \cdots u_{d-1}^{x_{d-1}}$ completes Step **??**.

Step ??: Computing a solution m to the relative norm equation problem Setting

$$m = w \prod_{\substack{j:\, \eta_i \\ \text{inert}}} \eta_i^{e_i/2} \prod_{\substack{i:\, \eta_i \text{ split/} \\ \text{ramified}}} (\xi_i)^{e_i}$$

yields

$$mm^* = ww^* \prod_{\substack{i:\, \eta_i \\ \text{inert}}} \eta_i^{e_i} \prod_{\substack{i:\, \eta_i \text{ split/} \\ \text{ramified}}} (\xi_i \xi_i^*)^{e_i} = u \prod \eta_i^{e_i} = r, \tag{63}$$

as required.

Equation (**??**) shows that the output of Algorithm **??** is a solution to Problem **??**. Since each subroutine of the algorithm runs in polynomial time, Algorithm **??** runs in polynomial time. This proves Proposition **??**.

8.3 Subroutines of Algorithm ??

The subroutine, Algorithm **??**, called at Step **??** of Algorithm **??** describes a process for lifting primes p_k to prime ideals in O_L and finding corresponding primes in O_K.

Step ??: Factorizing primes into prime ideals By Theorem **??** and Theorem 14.14 of [VG13] there exists a polynomial time algorithm to factor each p_k into ideals $\mathfrak{p}_i$. The following theorem provides a reduction of factoring rational primes p into prime ideals to factoring a polynomial $\bmod p$.

Theorem 8.8 (Cohen, Thm.4.8.13 [Coh93]). *Let $L = \mathbb{Q}(\theta)$, where θ is an algebraic integer with minimal polynomial $T(X)$. Let $f = [O_L : \mathbb{Z}[\theta]]$ and let p be a prime not dividing f. Suppose*

$$T(X) = \sum T_i(X)^{e_i} \mod p.$$

Then, the prime decomposition of pO_L is given by

$$pO_L = \prod \mathfrak{p}_i^{e_i},$$

where $\mathfrak{p}_i = pO_L + T_i(\theta)O_L$.

When L is a cyclotomic field, $L = \mathbb{Q}(\zeta_n)$ for some n where ζ_n is a primitive n^{th} root of unity and $O_L = \mathbb{Z}[\zeta_n]$ [IR90]. Hence, $f = [O_L : \mathbb{Z}[\zeta_n]] = 1$ and there is no prime p such that $p \mid f$. So $\mathfrak{p}_i = p_k O_L + \alpha_i O_L$, for each prime in the prime factorization of R, where $\alpha_i \in O_L$. Factoring $T(X)$, the minimal polynomial of ζ_n, over the finite field $\mathbb{F}_p$ can be done in polynomial time in the degree of $T(X)$ and $\log(p)$ (Thm. 14.14, [VG13]). This completes Step **??** of the algorithm.

Step ??: Computing ideal generators Since O_L is a principal ideal domain, computing the generator ξ_i of a prime ideal, as in Step **??**, is an instance of the Principal Ideal Problem. Recall that O_L is norm-Euclidean, so the generator of $p_k O_L + \alpha_i O_L$ is computed using the Euclidean algorithm. Set $\xi_i = \mathrm{GCD}(p_k, \alpha_i)$ where $\mathrm{GCD}(a, b) \in O_L$ is the greatest common divisor computed by the Euclidean algorithm, using the absolute norm. Then, since L is Galois, the generators of all prime ideals above p_k can be recovered using Galois automorphisms of L, as the Galois group acts transitively on prime ideals $\mathfrak{p}_i$.

Step ??: Finding η, prime in O_K For the computation at Step **??**, recall that the unit group $O_K^\times$ of O_K is a finite index subgroup of the unit group of $O_L^\times$. Our aim is to find a prime factorization of $p \in O_K$, up to multiplication by a unit. To that end, the following lemma is used to find primes η_i in O_K corresponding to certain prime ideal generators ξ_i.

Lemma 8.9. *Let $\xi \in O_L$ be the generator of a prime ideal. If there exists v a unit from the finite quotient $O_L^\times / O_K^\times$ such that $v\xi \in O_K$ then $v\xi$ is relatively inert in O_L.*

Proof. Let v be such a unit from the finite quotient $O_L^\times / O_K^\times$ and suppose $v\xi$ not relatively inert in O_L. Then there exist $a, b \in O_L$ such that $v\xi = ab$. Then $\xi = v^{-1}(v\xi) = v^{-1}ab$, a contradiction. □

Each generator ξ_i is multiplied by a representative v of each element in the quotient $O_L^\times / O_K^\times$. If $v\xi_i \in O_K$, Lemma **??** asserts that $\eta_i := v\xi_i$ is prime in O_K. By Property (3) of Definition **??**, iterating through each element in the quotient to find a valid v is efficient. If this process fails, η_i is set to $\xi_i \xi_i^*$. Then η_i is prime in O_K and relatively split or ramified in O_L.

8.4 A shortcut property for solving the norm equation

Recall that in the general solution outline of Section **??**, the norm equation problem was simplified to the following problem.

Problem 8.10. *Given, $\hat{z}$ in $M_{\mathcal{O}}$, find $z' \in \hat{z} + \xi M_{\mathcal{O}}$ such that*

$$|z'|^2 = r \in O_K,$$

where $r = \xi\xi^* \ell^N - \hat{m_1}\hat{m_1}^*$.

We consider fields with class number equal to 1, and demonstrate a 'shortcut' for solving this problem. The following lemma identifies a property of fields K, L and ideals I sufficient to guarantee this simplification.

Lemma 8.11. *Let I be an integral ideal of O_L fixed by conjugation, so $x \in I \implies x^* \in I$. Let U be the group of torsion units of O_L modulo I. If*

$$\forall q \in O_L/I, \quad \exists u \in U \text{ such that } q^* = uq$$

then

$$\forall z \in O_L \text{ such that } |z|^2 = r \in O_K, \quad \exists u' \text{ such that } |u'z|^2 = r \text{ and } u'z - \hat{z} \in I.$$

Proof. Suppose z' is a solution to the norm equation with quotient constraint,

$$|z'|^2 = r, \quad z' \in \hat{z} + I, \hat{z} \in O_L. \tag{64}$$

Then z' is also a solution to the general norm equation

$$|z'|^2 = r, \quad z' \in O_L \tag{65}$$

and hence can be written as $z' = uz_0^2 z_1^{e_1}(z_1^*)^{n_1-e_1} \cdots z_m^{e_m}(z_m^*)^{n_m-e_m}$ for integers e_i, n_i, where u is a torsion unit of O_L, $z_0 O_L$ is a product of relatively inert prime ideals, and the z_i are such that $z_i O_L$ is a prime O_L ideal and $z_i z_i^* O_K$ is a prime O_K ideal. We can similarly write z as $wz_0^2 z_1^{c_1}(z_1^*)^{n_1-c_1} \cdots z_m^{c_m}(z_m^*)^{n_m-c_m}$, for integers n_i, c_i, where w is a torsion unit of O_L.

Now consider a ring homomorphism γ defined by $\gamma(z) = z + I$. By assumption on O_L/I, there exist $x_i \in U$ such that $x_i\gamma(z_i)^* = \gamma(z_i)$. In other words, there exists a torsion unit x_i' such that $z_i^* + I = x_i' z_i + I$, using that I is fixed by conjugation. Observe that $\gamma(z') = \gamma(\hat{z})$ since z' is a solution to Equation (**??**). However, we also have

$$\begin{aligned} \gamma(z') &= \gamma(u) \cdot \gamma(z_0)\gamma(z_1)^{n_1}\gamma((x_1')^{n_1-e_1}) \ldots \gamma(z_m)^{n_m}\gamma((x_m')^{n_m-e_m}) \\ \gamma(z) &= \gamma(w) \cdot \gamma(z_0)\gamma(z_1)^{n_1}\gamma((x_1')^{n_1-c_1}) \ldots \gamma(z_1)^{n_m}\gamma((x_m')^{n_m-c_m}) \end{aligned} \tag{66}$$

Based on the above we set $u' = uw^{-1}(x_1')^{c_1-e_1} \ldots (x_m')^{c_m-e_m}$ and see that $u'z$ is such that $|u'z|^2 = r$ and $\gamma(u'z) = \gamma(z') = \gamma(\hat{z})$, as required.

□

In essence, for any solution z to Equation (**??**), there exists a torsion unit such that $u'z$ is a solution to Equation (**??**). We call this property the 'Shortcut Property'. There exist ideals in which the shortcut property holds for K, L corresponding to the Clifford+T and Clifford+$\sqrt{\mathrm{T}}$ bases.

Let I be an integral ideal of O_L fixed by conjugation such that $I \subseteq \xi M_{\mathcal{O}} \subseteq O_L$. Then, $\xi M_{\mathcal{O}}$ is equal to the finite disjoint union $\xi M_{\mathcal{O}} = \bigsqcup_k (z_k + I)$. Then, Lemma **??** shows that a solution to Problem **??** can be found by solving the general norm equation $|z|^2 = r$, $z \in O_L$, then checking whether $u'z - (\hat{z} + z_k) \in I$ for some z_k and unit u. This requires only finitely many checks. Finally, a solution $u'z$ yields a candidate for m_2 by setting $m_2 = u'z/\xi$.

References

[Aru+19] Frank Arute et al. “Quantum supremacy using a programmable superconducting processor”. In: *Nature* 574.7779 (Oct. 2019), pp. 505–510. ISSN: 1476-4687. DOI: 10.1038/s41586-019-1666-5. URL: https://doi.org/10.1038/s41586-019-1666-5.

[Ban95] Wojciech Banaszczyk. “Inequalities for convex bodies and polar reciprocal lattices inr n”. In: *Discrete & Computational Geometry* 13.2 (1995), pp. 217–231.

[Bar+95] Adriano Barenco et al. “Elementary gates for quantum computation”. In: *Physical Review A* 52.5 (Nov. 1995), pp. 3457–3467. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.52.3457. arXiv: 9503016 [quant-ph].

[BBG15a] Andreas Blass, Alex Bocharov, and Yuri Gurevich. “Optimal Ancilla-free Pauli+V Circuits for Axial Rotations”. In: *Journal of Mathematical Physics* 56.12 (Nov. 2015). URL: https://www.microsoft.com/en-us/research/publication/optimal-ancilla-free-pauliv-circuits-for-axial-rotations/.

[BBG15b] Andreas Blass, Alex Bocharov, and Yuri Gurevich. “Optimal ancilla-free Pauli+V circuits for axial rotations”. In: *Journal of Mathematical Physics* 56.12 (Dec. 2015), p. 122201. ISSN: 0022-2488. DOI: 10.1063/1.4936990. arXiv: 1412.1033.

[Bev+20] Michael Beverland et al. “Lower bounds on the non-Clifford resources for quantum computations”. In: *Quantum Science and Technology* 5.3 (June 2020), p. 035009. DOI: 10.1088/2058-9565/ab8963. URL: https://doi.org/10.1088/2058-9565/ab8963.

[BG11] Jean Bourgain and Alex Gamburd. “A Spectral Gap Theorem in $SU(d)$”. In: *arXiv preprint arXiv:1108.6264* (2011).

[BGS13a] Alex Bocharov, Yuri Gurevich, and Krysta M Svore. “Efficient decomposition of single-qubit gates into V basis circuits”. In: *Physical Review A* 88.1 (2013), p. 012313.

[BGS13b] Alex Bocharov, Yuri Gurevich, and Krysta M. Svore. “Efficient Decomposition of Single-Qubit Gates into V Basis Circuits”. In: *Physical Review A* 88.1 (July 2013), pp. 1–13. DOI: 10.1103/PhysRevA.88.012313. arXiv: 1303.1411.

[BK05] Sergey Bravyi and Alexei Kitaev. “Universal quantum computation with ideal Clifford gates and noisy ancillas”. In: *Phys. Rev. A* 71 (2 Feb. 2005), p. 022316. DOI: 10.1103/PhysRevA.71.022316. URL: https://link.aps.org/doi/10.1103/PhysRevA.71.022316.

[BK13] Sergey Bravyi and Robert König. “Classification of Topologically Protected Gates for Local Stabilizer Codes”. In: *Phys. Rev. Lett.* 110 (17 Apr. 2013), p. 170503. DOI: 10.1103/PhysRevLett.110.170503. URL: https://link.aps.org/doi/10.1103/PhysRevLett.110.170503.

[BKS21] Michael E. Beverland, Aleksander Kubica, and Krysta M. Svore. “Cost of Universality: A Comparative Study of the Overhead of State Distillation and Code Switching with Color Codes”. In: *PRX Quantum* 2 (2 June 2021), p. 020341. DOI: 10.1103/PRXQuantum.2.020341. URL: https://link.aps.org/doi/10.1103/PRXQuantum.2.020341.

[BRS14] Alex Bocharov, Martin Roetteler, and Krysta M. Svore. "Efficient Synthesis of Universal Repeat-Until-Success Circuits". In: (Apr. 2014), p. 16. arXiv: 1404.5320. URL: http://arxiv.org/abs/1404.5320.

[BRS15a] Alex Bocharov, Martin Roetteler, and Krysta M. Svore. "Efficient synthesis of probabilistic quantum circuits with fallback". In: *Physical Review A* 91.5 (May 2015), p. 052317. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.91.052317. arXiv: 1409.3552.

[BRS15b] Alex Bocharov, Martin Roetteler, and Krysta M. Svore. "Efficient synthesis of probabilistic quantum circuits with fallback". In: *Physical Review A* 91.5 (May 2015), p. 052317. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.91.052317. arXiv: 1409.3552.

[Bur+21] Vera von Burg et al. "Quantum computing enhanced computational catalysis". In: *Phys. Rev. Research* 3 (3 July 2021), p. 033055. DOI: 10.1103/PhysRevResearch.3.033055. URL: https://link.aps.org/doi/10.1103/PhysRevResearch.3.033055.

[Cam17] Earl Campbell. "Shorter gate sequences for quantum computing by mixing unitaries". In: *Physical Review A* 95.4 (Dec. 2017). ISSN: 24699934. DOI: 10.1103/PhysRevA.95.042306. arXiv: 1612.02689. URL: http://arxiv.org/abs/1612.02689.

[Chi+21] Andrew M. Childs et al. "Theory of Trotter Error with Commutator Scaling". In: *Phys. Rev. X* 11 (1 Feb. 2021), p. 011020. DOI: 10.1103/PhysRevX.11.011020. URL: https://link.aps.org/doi/10.1103/PhysRevX.11.011020.

[CLG09] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. "Cryptographic hash functions from expander graphs". In: *Journal of Cryptology* 22.1 (2009), pp. 93–113.

[Coh12] Henri Cohen. *Advanced topics in computational number theory*. Vol. 193. Springer Science & Business Media, 2012.

[Coh93] Henri Cohen. "A course in computational algebraic number theory". In: *Graduate texts in Math.* 138 (1993).

[CP18] Eduardo Carvalho Pinto and Christophe Petit. "Better path-finding algorithms in LPS Ramanujan graphs". In: *Journal of Mathematical Cryptology* 12.4 (2018), pp. 191–202.

[EK09] Bryan Eastin and Emanuel Knill. "Restrictions on Transversal Encoded Quantum Gate Sets". In: *Phys. Rev. Lett.* 102 (11 Mar. 2009), p. 110502. DOI: 10.1103/PhysRevLett.102.110502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.102.110502.

[For+15a] Simon Forest et al. "Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets". In: *Journal of Mathematical Physics* 56.8 (2015), p. 082201.

[For+15b] Simon Forest et al. "Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets". In: *Journal of Mathematical Physics* 56.8 (Aug. 2015), p. 082201. ISSN: 0022-2488. DOI: 10.1063/1.4927100.

[GC99] Daniel Gottesman and Isaac L. Chuang. "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". In: *Nature* 402.6760 (Nov. 1999), pp. 390–393. ISSN: 1476-4687. DOI: 10.1038/46503. URL: https://doi.org/10.1038/46503.

[GF19] Craig Gidney and Austin G. Fowler. "Efficient magic state factories with a catalyzed $|CCZ>$ to $2|T>$ transformation". In: *Quantum* 3 (Apr. 2019), p. 135. ISSN: 2521-327X. DOI: 10.22331/q-2019-04-30-135. URL: https://doi.org/10.22331/q-2019-04-30-135.

[Gid18] Craig Gidney. "Halving the cost of quantum addition". In: *Quantum* 2 (June 2018), p. 74. ISSN: 2521-327X. DOI: 10.22331/q-2018-06-18-74. URL: https://doi.org/10.22331/q-2018-06-18-74.

[Gos+14] David Gosset et al. "An Algorithm for the T-Count". In: *Quantum Info. Comput.* 14.15–16 (Nov. 2014), pp. 1261–1276. ISSN: 1533-7146.

[Has17] Matthew B. Hastings. "Turning gate synthesis errors into incoherent errors". In: *Quantum Information and Computation* 17.5-6 (Dec. 2017), pp. 488–494. ISSN: 15337146. arXiv: 1612.01011. URL: http://arxiv.org/abs/1612.01011.

[HRC02] Aram W Harrow, Benjamin Recht, and Isaac L Chuang. "Efficient discrete approximations of quantum gates". In: *Journal of Mathematical Physics* 43.9 (2002), pp. 4445–4451.

[IR90] Kenneth Ireland and Michael Rosen. "A Classical Introduction to Modern Number Theory. 1990". In: *Grad. Texts in Math* (1990).

[Ite+16] Raban Iten et al. "Quantum circuits for isometries". In: *Phys. Rev. A* 93 (3 Mar. 2016), p. 032318. DOI: 10.1103/PhysRevA.93.032318. URL: https://link.aps.org/doi/10.1103/PhysRevA.93.032318.

[Ite+21] Raban Iten et al. *Introduction to UniversalQCompiler*. 2021. arXiv: 1904.01072 [quant-ph].

[JKP09] Nathaniel Johnston, David W. Kribs, and Vern I. Paulsen. "Computing Stabilized Norms for Quantum Operations via the Theory of Completely Bounded Maps". In: *Quantum Info. Comput.* 9.1 (Jan. 2009), pp. 16–35. ISSN: 1533-7146.

[Khi48] Aleksandr Yakovlevich Khinchin. "A quantitative formulation of the approximation theory of Kronecker". In: *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 12.2 (1948), pp. 113–122.

[Kli+15a] V Kliuchnikov et al. "A Framework for Approximating Qubit Unitaries". In: *ArXiv e-prints* (Oct. 2015). arXiv: 1510.03888 [quant-ph].

[Kli+15b] Vadym Kliuchnikov et al. "A framework for approximating qubit unitaries". In: *arXiv preprint arXiv:1510.03888* (2015).

[KLM07] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introduction to Quantum Computing*. USA: Oxford University Press, Inc., 2007. ISBN: 0198570007.

[KMM13a] V Kliuchnikov, D Maslov, and M Mosca. "Asymptotically Optimal Approximation of Single Qubit Unitaries by Clifford and T Circuits Using a Constant Number of Ancillary Qubits". In: *Physical Review Letters* 110.19 (May 2013), p. 190502. DOI: 10.1103/PhysRevLett.110.190502. arXiv: 1212.0822 [quant-ph].

[KMM13b] Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. "Fast and Efficient Exact Synthesis of Single-Qubit Unitaries Generated by Clifford and T Gates". In: *Quantum Info. Comput.* 13.7–8 (July 2013), pp. 607–630. ISSN: 1533-7146.

[KY15] Vadym Kliuchnikov and Jon Yard. “A framework for exact synthesis”. In: *arXiv preprint arXiv:1504.04350* (2015).

[LC17] Guang Hao Low and Isaac L. Chuang. “Optimal Hamiltonian Simulation by Quantum Signal Processing”. In: *Phys. Rev. Lett.* 118 (1 Jan. 2017), p. 010501. DOI: 10.1103/PhysRevLett.118.010501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.118.010501.

[Lem95] Franz Lemmermeyer. “The Euclidean algorithm in algebraic number fields”. In: *Expositiones Mathematicae* 13 (1995), pp. 385–416.

[Len83] Hendrik W Lenstra Jr. “Integer programming with a fixed number of variables”. In: *Mathematics of operations research* 8.4 (1983), pp. 538–548.

[Lit19] Daniel Litinski. “A Game of Surface Codes: Large-Scale Quantum Computing with Lattice Surgery”. In: *Quantum* 3 (Mar. 2019), p. 128. ISSN: 2521-327X. DOI: 10.22331/q-2019-03-05-128. URL: https://doi.org/10.22331/q-2019-03-05-128.

[LPS88] A Lubotzky, R Phillips, and P Sarnak. “Ramanujan graphs. Combinatorica 8 261–277”. In: *Mathematical Reviews (MathSciNet): MR963118 Digital Object Identifier: doi* 10 (1988).

[MGE12] Easwar Magesan, Jay M. Gambetta, and Joseph Emerson. “Characterizing quantum gates via randomized benchmarking”. In: *Phys. Rev. A* 85 (4 Apr. 2012), p. 042311. DOI: 10.1103/PhysRevA.85.042311. URL: https://link.aps.org/doi/10.1103/PhysRevA.85.042311.

[MIC21] Emanuel Malvetti, Raban Iten, and Roger Colbeck. “Quantum Circuits for Sparse Isometries”. In: *Quantum* 5 (Mar. 2021), p. 412. ISSN: 2521-327X. DOI: 10.22331/q-2021-03-15-412. URL: https://doi.org/10.22331/q-2021-03-15-412.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NRS06] Gabriele Nebe, Eric M. Rains, and Neil J.A. Sloane. “Real and Complex Clifford Groups”. In: *Self-Dual Codes and Invariant Theory*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 171–192. ISBN: 978-3-540-30731-0. DOI: 10.1007/3-540-30731-1˙6. URL: https://doi.org/10.1007/3-540-30731-1_6.

[NSM20] Yunseong Nam, Yuan Su, and Dmitri Maslov. “Approximate quantum Fourier transform with O(n log(n)) T gates”. In: *npj Quantum Information* 6.1 (Mar. 2020), p. 26. ISSN: 2056-6387. DOI: 10.1038/s41534-020-0257-5. URL: https://doi.org/10.1038/s41534-020-0257-5.

[PLQ08] Christophe Petit, Kristin Lauter, and Jean-Jacques Quisquater. “Full cryptanalysis of LPS and Morgenstern hash functions”. In: *International Conference on Security and Cryptography for Networks*. Springer. 2008, pp. 263–277.

[PS13] Adam Paetznick and Krysta M Svore. “Repeat-Until-Success: Non-deterministic decomposition of single-qubit unitaries”. In: *arXiv preprint arXiv:1311.1074* (2013).

[PS14] Adam Paetznick and Krysta M. Svore. "Repeat-until-success: Non-deterministic decomposition of single-qubit unitaries". In: *Quantum Information and Computation* 14.15-16 (Nov. 2014), pp. 1277–1301. ISSN: 15337146. arXiv: 1311.1074. URL: http://arxiv.org/abs/1311.1074.

[PS18] Ori Parzanchevski and Peter Sarnak. "Super-Golden-Gates for PU(2)". In: *Advances in Mathematics* 327 (2018). Special volume honoring David Kazhdan, pp. 869–901. ISSN: 0001-8708. DOI: https://doi.org/10.1016/j.aim.2017.06.022. URL: https://www.sciencedirect.com/science/article/pii/S0001870817301640.

[Ros15] Neil J. Ross. "Optimal Ancilla-Free Clifford+V Approximation of Z-Rotations". In: *Quantum Info. Comput.* 15.11–12 (Sept. 2015), pp. 932–950. ISSN: 1533-7146.

[RS15] Neil J. Ross and Peter Selinger. "Optimal ancilla-free Clifford+T approximation of z-rotations". In: *Quantum Information & Computation* 15.11-12 (2015), pp. 932–950. arXiv: 1403.2975.

[Sar] Peter Sarnak. "Letter to Aaronson and Pollington on the Solvay-Kitaev Theorem and Golden Gates, 2015". In: *URL: http://publications. ias. edu/sarnak/paper/2637* ().

[Sar17] Naser T Sardari. "Complexity of strong approximation on the sphere". In: *arXiv preprint arXiv:1703.02709* (2017).

[Sel15] Peter Selinger. "Efficient Clifford+T approximation of single-qubit operators". In: *Quantum Information \& Computation* 15.1-2 (Dec. 2015), pp. 159–180. arXiv: 1212.6253.

[Sti20] Zachary Stier. private communication. 2020.

[TZ08] Jean-Pierre Tillich and Gilles Zémor. "Collisions for the LPS expander graph hash function". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2008, pp. 254–269.

[VG13] Joachim Von Zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge university press, 2013.

[Voi05] John Michael Voight. *Quadratic forms and quaternion algebras: Algorithms and arithmetic*. University of California, Berkeley, 2005.

[Was97] Lawrence C Washington. *Introduction to cyclotomic fields*. Vol. 83. Springer Science & Business Media, 1997.

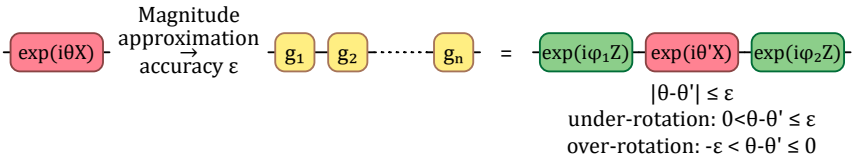
[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. DOI: 10.1017/9781316848142.

[WB20] Paul Webster and Stephen D. Bartlett. "Fault-tolerant quantum gates with defects in topological stabilizer codes". In: *Phys. Rev. A* 102 (2 Aug. 2020), p. 022403. DOI: 10.1103/PhysRevA.102.022403. URL: https://link.aps.org/doi/10.1103/PhysRevA.102.022403.

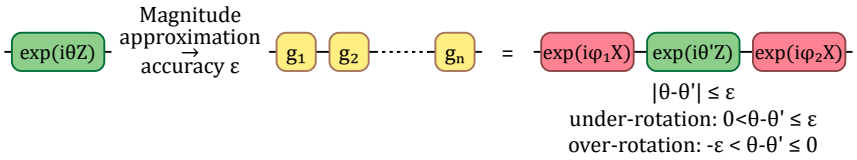
A Applications of the magnitude approximation problem

We show that magnitude approximation problem can provide resource savings not only when approximating general SU(2) unitaries, as discussed in **??** and **??**, but also for qubit

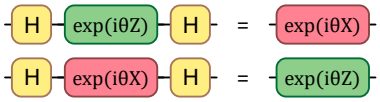
state preparation and approximating general SU(4) unitaries. We believe that idea of approximating X rotations up to Z rotations will be fruitful beyond provided examples.



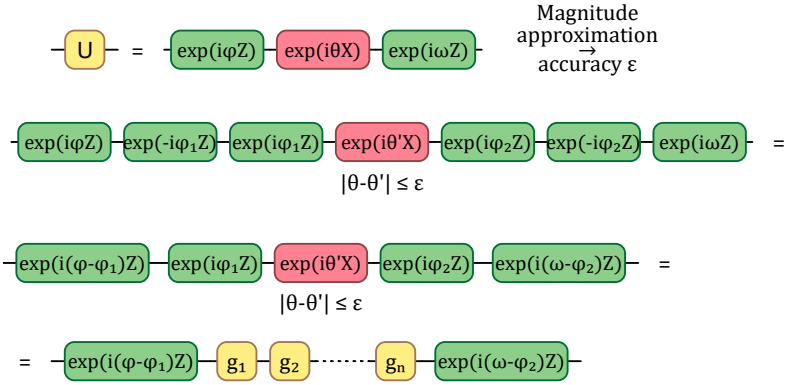
The main idea is that when approximating X rotation within a quantum circuit, extra Z exponents can be absorbed into surrounding gates. Similarly, if we are approximating Z rotations, extra X exponents can be absorbed into surrounding gates.



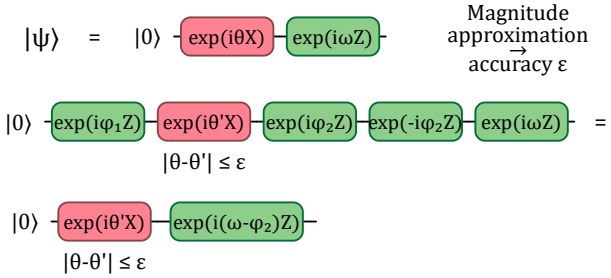
It is easy to exchange X and Z in our circuits by using Hadamard gates and following circuit identities:



For the above to hold we require that the gate set is fixed by Hadamard conjugation, that is for any gate g from the gate set, HgH is also in the gate set. Luckily Clifford+T, Clifford+$\sqrt{T}$ and V basis all have this property. The use of the magnitude approximation for approximating SU(2) unitaries discussed in **??** is summarized using circuit diagrams as follows:

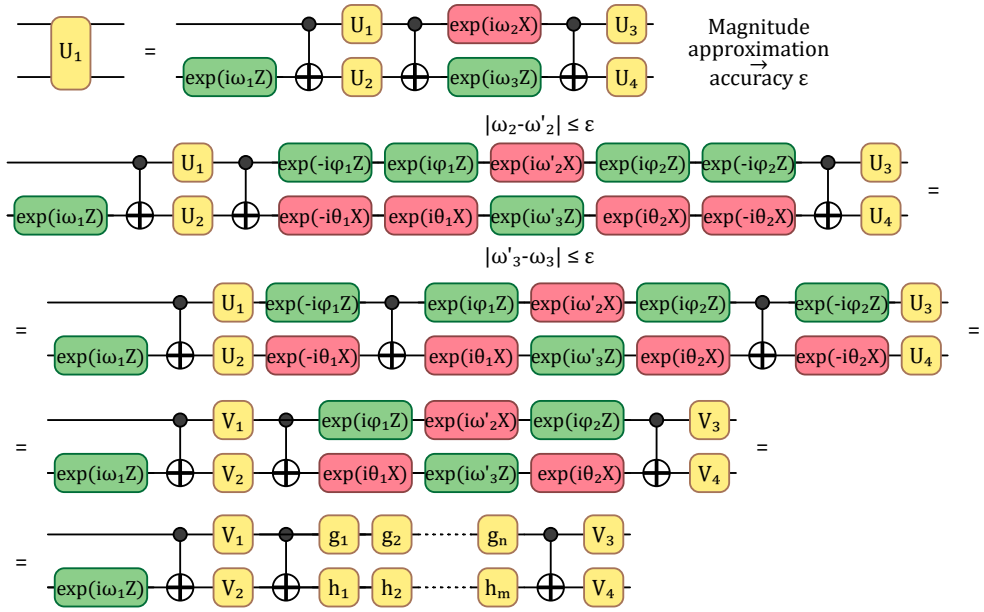


Approximating SU(2) requires solving one magnitude approximation and two diagonal approximation problems. Similarly we improve the preparation of an arbitrary one qubit state.



Above we use the fact that $|0\rangle$ is an eigenstate of any Z rotation. Approximating qubit state requires solving one magnitude approximation and one diagonal approximation problem.

Finally, we show that magnitude approximation can be used to find shorter approximations of two qubit unitaries. We use a rotation and CNOT optimal circuit from arxiv:quant-ph/0308033.



Above we used the following circuit identities:

which follow from representing CNOT matrix as:

$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = ((I+Z)\otimes I + (I-Z)\otimes X)/2$$

We then apply the result for approximating arbitrary qubit unitaries to V_1, V_2, V_3, V_4. Approximating SU(4) requires solving six magnitude approximation and nine diagonal approximation problems.

Mixing of under-rotated and over-rotated magnitude approximations applies in all of the above cases similarly to the general SU(2) case considered in **??**. Our improvements to approximating general SU(2), SU(4) unitaries and to qubit state preparation are summarized in **??**, along with comparison to the previous state of the art.

B Properties of the diamond norm

We use the diamond norm as the accuracy metric for all approximation problem definitions. Let us recall why we can replace various parts of a quantum algorithm with their approximations and still get useful results. The diamond norm is the key mathematical tool for understanding this. The result of running any quantum algorithm is a sample from a probability distribution. Let us call this distribution the answer distribution. We then process the answer distribution to get the final answer. This processing of the answer distribution is robust, that is if we are given a sample from a distribution that is within total variational distance ε from the answer distribution we can still recover the final answer. The value ε is different for different quantum algorithms. Every quantum algorithm corresponds to a quantum channel. Suppose that the diamond norm distance between the channels corresponding to the ideal quantum algorithm and its approximation is ε. Then,

the total variational distance between the ideal algorithm's answer distribution and the answer distribution produced by the approximation is also ε. The proof of this fact follows from the definition of the diamond norm that is discussed below.

The diamond norm also has two key properties that let us estimate the distance between two algorithms, given the diamond norm distances between their parts. The first property is the chain rule for the composition of channels, that is for channels Φ_1, Φ_2, Ψ_1, Ψ_2 we have

$$\|\Phi_1\Psi_1 - \Phi_2\Phi_2\|_\diamond \leq \|\Phi_1 - \Phi_2\|_\diamond + \|\Psi_1 - \Psi_2\|_\diamond$$

That is if we replaced N parts of a quantum algorithm with their ε approximations, the distance between the quantum algorithm and its approximation is at most $N \cdot \varepsilon$. The second property is stability with respect to the tensor product. When we write a quantum algorithm as a composition of channels $\Phi_1 \dots \Phi_N$ each acting on n-qubits, it is frequently the case that each Φ_k acts non-trivially on one qubit, that is

$$\Phi_k = \Phi'_k \otimes \mathcal{I} \text{ where } \mathcal{I} \text{ is the identity channel on } n-1 \text{ qubits.}$$

When we replace Φ'_k with its approximation Ψ'_k we can argue that $\Psi'_k \otimes \mathcal{I}$ is close to Φ_k by using the stability with respect to the tensor product:

$$\|\Phi'_k \otimes \mathcal{I} - \Psi'_k \otimes \mathcal{I}\|_\diamond = \|(\Phi'_k - \Psi'_k) \otimes \mathcal{I}\|_\diamond = \|\Phi'_k - \Psi'_k\|_\diamond$$

For an explanation of this and many other useful properties of the diamond norm we refer the reader to Chapter 3.3.2 of [Wat18]. For completeness we provide the basic definition and other important properties of the diamond norm below.

Let $\mathbb{C}^{d\times d}$ be the linear space over $\mathbb{C}$ of d by d matrices with entries in $\mathbb{C}$. For an arbitrary element of $\mathbb{C}^{d\times d}$ the Schatten one norm (also known as trace norm) is defined as $\|A\|_1 = \mathrm{Tr}\sqrt{A^\dagger A}$. For an arbitrary linear transformation Φ from $\mathbb{C}^{d\times d}$ into $\mathbb{C}^{d\times d}$, the *induced* one norm is defined as

$$\|\Phi\|_1 = \max\Big\{\|\Phi(X)\|_1 : X \in \mathbb{C}^{d\times d}, \|X\|_1 \leq 1\Big\}. \tag{67}$$

The diamond norm (also known as the completely-bounded trace norm) is a "stable" version of the induced one norm

$$\|\Phi\|_\diamond = \|\Phi \otimes \mathcal{I}_d\|_1, \tag{68}$$

where $\mathcal{I}_d$ is the identity map from $\mathbb{C}^{d\times d}$ into $\mathbb{C}^{d\times d}$. We call diamond norm stable, because in general $\|\Phi\|_1 \leq \|\Phi \otimes \mathcal{I}_k\|_1$. There are examples where the inequality is strict. However, for any $k \geq d$ we have equality $\|\Phi \otimes \mathcal{I}_k\|_1 = \|\Phi \otimes \mathcal{I}_d\|_1$.

Direct calculation of the diamond norm is tedious, in general. However, there are two cases useful for this paper when there is a simple way to calculate the diamond distance. The first case is the diamond distance between two channels $\mathcal{U}$ and $\mathcal{V}$ induced by unitaries U and V. Below is a re-statement of Theorem 26 in [JKP09]:

Theorem B.1 (Diamond distance between unitary channels). *For any two unitary operators U, V, the diamond norm of the difference of the unitary channels $\mathcal{U}$, $\mathcal{V}$ induced by U, V is equal to the diameter of the smallest disc (not necessarily centered at the origin) containing all the eigenvalues of $U^\dagger V$.*

We use above result when approximating unitaries by unitaries. The second case is the diamond distance between two Pauli channels. Below we restate the result Section V.A in [MGE12] and definition of a Pauli channel:

Theorem B.2 (Diamond norm distance between Pauli channels). *Suppose $\mathcal{E}_1$, $\mathcal{E}_2$ are n-qubit Pauli channels, that is*

$$\mathcal{E}_1(\rho) = \sum_{P\in\{I,X,Y,Z\}^{\otimes n}} q_P P\rho P^\dagger,\ \mathcal{E}_2(\rho) = \sum_{P\in\{I,X,Y,Z\}^{\otimes n}} r_P P\rho P^\dagger,$$

then $\|\mathcal{E}_1 - \mathcal{E}_2\|_\diamond = \sum_{P\in\{I,X,Y,Z\}^{\otimes n}} |q_P - r_P|$.

We use above result when approximating unitaries by probabilistic mixtures of unitaries. To take advantage of the above property we frequently use the unitary invariance of the diamond norm.

Proposition B.3 (Unitary invariance of the diamond norm). *Let Φ be channel and $\mathcal{U}$,$\mathcal{U}^\dagger$ be unitary channels induced by unitaries U,$U^\dagger$, then the following holds:*

$$\|\Phi - \mathcal{U}\|_\diamond = \left\|\mathcal{U}^\dagger\Phi - \mathcal{I}\right\|_\diamond = \left\|\Phi\mathcal{U}^\dagger - \mathcal{I}\right\|_\diamond$$

Proof. The first equality follows from the unitary left and right invariance of the Schatten one norm (also know as trace norm). That is for any matrix A we have $\|AU\|_1 = \|UA\|_1 = \|A\|_1$. For any density matrix ρ we have

$$\left\|(\Phi\otimes\mathcal{I})(\rho) - (U\otimes I)\rho(U^\dagger\otimes I)\right\|_1 = \left\|(U^\dagger\otimes I)(\Phi\otimes\mathcal{I})(\rho)(U\otimes I) - \rho\right\|_1,$$

which show the first equality by the definition of the diamond norm. The second equality follows from the fact that taking minimum over all matrices in **??** with trace norm at most one is the same as taking minimum over all matrices $(U^\dagger\otimes I)X(U\otimes I)$ with trace norm at most one. □

When approximating unitary U with probabilistic mixtures of unitaries described by a channel Φ, we typically find that $\mathcal{U}^\dagger\Phi$ is a Pauli channel. For qubit unitaries the following corollaries of **??** are useful:

Corollary B.4 (Diamond distance between qubit diagonal unitaries). *For any real numbers ϕ_1, ϕ_2, the diamond norm distance between channels $\mathcal{Z}_{\phi_1}$, $\mathcal{Z}_{\phi_2}$ induced by unitaries $e^{i\phi_1 Z}$, $e^{i\phi_2 Z}$ is*

$$\|\mathcal{Z}_{\phi_1} - \mathcal{Z}_{\phi_2}\|_\diamond = 2|\sin(\phi_1 - \phi_2)| \leq 2|\phi_1 - \phi_2|.$$

Proof. Use **??** and note that eigenvalues of $e^{i\phi_1 Z}e^{-i\phi_2 Z}$ are $e^{\pm i\delta}$ where $\delta = \phi_1 - \phi_2$. The diameter of the disc enclosing both eigenvalues is $|e^{i\delta} - e^{-i\delta}| = 2|\sin(\delta)|$. Finally we use inequality $|\sin(\delta)| \leq |\delta|$. □

There is a closed form expression for diamond norm distance when approximating diagonal qubit unitary by any qubit unitary:

Corollary B.5 (Diamond distance between qubit diagonal and general qubit unitaries). *For any real numbers ϕ and special qubit unitary $U = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}$, the diamond norm distance between channels $\mathcal{Z}_\phi$, $\mathcal{U}$ induced by unitaries $e^{i\phi Z}$, U is*

$$\|\mathcal{Z}_\phi - \mathcal{U}\|_\diamond = 2\sqrt{1 - \left(\mathrm{Re}(ue^{-i\phi})\right)^2} \leq 2\sqrt{2 - 2|\mathrm{Re}(ue^{-i\phi})|}$$

Proof. Use **??** and let $e^{\pm i\delta}$ be eigenvalues of $Ue^{-i\phi Z}$. The diameter of the disc enclosing both eigenvalues is $|e^{i\delta} - e^{-i\delta}| = 2|\sin(\delta)|$. Recall that $e^{i\delta} + e^{-i\delta} = \mathrm{Tr}(Ue^{-i\phi Z}) = 2\mathrm{Re}(ue^{-i\phi})$. That is $2\cos(\delta) = 2\mathrm{Re}(ue^{-i\phi})$. Now we use

$$|\sin(\delta)| = \sqrt{1 - \cos^2(\delta)} = \sqrt{1 - (\mathrm{Re}(ue^{-i\phi}))^2}.$$

To show the remaining inequality, write $\varepsilon = 1 - |\mathrm{Re}(ue^{-i\phi})|$. Note that ε is always positive and:

$$\sqrt{1 - (\mathrm{Re}(ue^{-i\phi}))^2} = \sqrt{1 - (1-\varepsilon)^2} = \sqrt{2\varepsilon - \varepsilon^2} \leq \sqrt{2\varepsilon}$$

Note that the inequality is tight when ε goes to zero. □

Finally we note that for qubit unitaries the spectral norm is related to the diamond norm distance between the corresponding channels.

Corollary B.6 (Diamond distance between qubit unitaries). *For an U, V from* SU(2) *the diamond distance between the unitary channels $\mathcal{U}$, $\mathcal{V}$ induced by U, V*

$$\|\mathcal{U} - \mathcal{V}\|_\diamond \leq 2\min(\|U - V\|, \|U + V\|)$$

Proof. There exist unitary V_0 such that $V = V_0 e^{i\phi Z} V_0^\dagger$. By using unitary invariance of the diamond norm and spectral norm, it is sufficient to show inequality for $U' = V_0^\dagger U V_0 = \begin{pmatrix} u & -v^* \\ v & u^* \end{pmatrix}$ and diagonal unitary $e^{i\phi Z}$. Let $e^{\pm i\delta}$ be eigenvalues of $U'e^{-i\phi Z}$, then the spectral distance between U' and $e^{i\phi Z}$ is equal to $\max\{|e^{\pm i\delta} - 1|\} = \sqrt{2 - 2\cos(\delta)}$. Similar to the argument in **??**, $\cos(\delta) = \mathrm{Re}(ue^{-i\phi})$ and therefore $\left\|U' \pm e^{i\phi Z}\right\| = \sqrt{2 \pm 2\mathrm{Re}(ue^{-i\phi})}$. Finally we use **??** and note that

$$\sqrt{2 - 2|\mathrm{Re}(ue^{-i\phi})|} = 2\min(\|U - V\|, \|U + V\|).$$

□

Note that bound in the above corollary is tight when $\|U \pm V\|$ goes to zero.

C Exact synthesis

This section covers the details of exact synthesis algorithms for the three example gate sets considered in Section **??**: V basis, Clifford+T and Clifford+$\sqrt{T}$. Given a gate set G and a matrix U from a certain set $\mathcal{U}$ uniquely determined by G, the goal of exact synthesis is to produce a sequence $g_1, \ldots, g_n$ of gates from G such that U is equal to the product of those gates, $U = g_1 \ldots g_n$. The set $\mathcal{U}$ is closed under left and right multiplication by elements of g.

The algorithm is similar for each gate set. Roughly, given a matrix U

1. select a gate g from the gate set such that $g^\dagger U$ has a lower cost than U,
2. set $U \leftarrow g^\dagger M$
3. repeat until cost of U is zero.

The gate sequence is recovered by collecting the gate g selected at each iteration. Intuitively, the algorithm works by picking off each gate of the product $g_1 \ldots g_n$ one at a time. Multiplication by $g^\dagger$ cancels the left most gate in M.

Importantly, it is possible to efficiently select a gate g so that the cost decreases monotonically. When the cost is zero, this measns the remaining gate is a Clifford gate.

Algorithms for exact synthesis has been proposed previously by [BGS13a] for the V basis and by [KMM13b; For+15a] for Clifford+T and Clifford+$\sqrt{T}$. We present the algorithms here for completeness. We provide a modified version of the algorithm with several optimizations for computational performance.

We begin with the simplest case, the V basis, and then address the progressively more complicated Clifford+T and Clifford+$\sqrt{T}$ gate sets.

C.1 V basis

Recall from Section **??** the six V basis matrices $V_{\pm X}$, $V_{\pm Y}$, $V_{\pm Z}$ and order

$$\mathcal{O} := \mathbb{Z} \cdot I + \mathbb{Z} \cdot iX + \mathbb{Z} \cdot iY + \mathbb{Z} \cdot iZ. \tag{69}$$

This order contains the V basis matrices each scaled by $\sqrt{5}$. For notational convenience we use $V_x = \sqrt{5}V_{+X}$, $V_y = \sqrt{5}V_{+Y}$ and $V_z = \sqrt{5}V_{+Z}$ to refer to the scaled V basis matrices. Note that $V_{-P} = V_{+P}^\dagger$ for $P \in \{X, Y, Z\}$ and $V_P V_P^\dagger = \mathrm{Det}(V_P)I = 5I$.

Define M_V as the function that, according to (**??**), maps integers a, b, c, d to a matrix in the natural way:

$$M_V(a, b, c, d) := aI + ibX + icY + idZ. \tag{70}$$

Any matrix $M_V(a, b, c, d)$ with determinant 5^n can be decomposed (exactly) into a length-n sequence of (scaled) V gates [BGS13a; Kli+15b]. Note that $\mathrm{Det}(M_V(a, b, c, d)) = 1$ if and only if $M_V(a, b, c, d)$ is a Pauli matrix.

Theorem C.1 (V basis exact decomposition). *Let $a, b, c, d \in \mathbb{Z}$ such that $\mathrm{Det}(M_V(a, b, c, d)) = 5^n$ for integer $n \geq 1$, and such that at least one of a, b, c, d is not divisible by 5. Then there exists a sequence $V_1, V_2, \ldots, V_n$, $V_k \in \{V_x, V_y, V_z, V_x^\dagger, V_y^\dagger, V_z^\dagger\}$ and Pauli matrix V_0 such that*

$$M_V(a, b, c, d) = V_0 \prod_{k=1}^{n} V_k. \tag{71}$$

The requirement that one of a, b, c, d is not divisible by 5 avoids artificially scaled inputs (e.g., $5I$). Scalars can be removed by simply dividing out the factors of 5. The proof follows by induction on the following Lemma.

Lemma C.2 (V basis factorization). *Let $a, b, c, d \in \mathbb{Z}$ such that $\mathrm{Det}(M_V(a, b, c, d)) = 5^n$ for integer $n \geq 1$, and such that at least one of a, b, c, d is not divisible by 5. Then there exists $V \in \{V_x, V_y, V_z, V_x^\dagger, V_y^\dagger, V_z^\dagger\}$ and $a', b', c', d' \in \mathbb{Z}$ such that*

$$M_V(a, b, c, d) = V M_V(a', b', c', d'), \tag{72}$$

and $\mathrm{Det}(M_V(a', b', c', d')) = 5^{n-1}$.

In other words, the matrix $M_V(a, b, c, d)$ can be factored into two parts: a V matrix and another matrix of the form M_V. Multiplication on the left by $V^\dagger$ yields

$$V^\dagger M_V(a, b, c, d) = \mathrm{Det}(V) M_V(a', b', c', d') = M_V(5a', 5b', 5c', 5d'). \tag{73}$$

and therefore

$$\mathrm{Det}(M_V(a', b', c', d')) = \mathrm{Det}(V^\dagger M_V(a', b', c', d')/5) = \mathrm{Det}(M_V(a, b, c, d))/5 = 5^{n-1}. \tag{74}$$

If we define the entrywise modulus

$$M_V(a, b, c, d) \bmod 5 := M_V(a \bmod 5, b \bmod 5, c \bmod 5, d \bmod 5), \tag{75}$$

then

$$V^\dagger M_V(a,b,c,d) \bmod 5 = V^\dagger (M_V(a,b,c,d) \bmod 5) \bmod 5, \tag{76}$$

by linearity. Equation **??** then implies that

$$V^\dagger (M_V(a,b,c,d) \bmod 5) \bmod 5 = M_V(0,0,0,0). \tag{77}$$

Solutions for V therefore depend only on values of a, b, c, d modulo 5. The proof proceeds by exhaustive numeric calculation over all tuples $a, b, c, d \mod 5$, $(a, b, c, d) \neq (0, 0, 0, 0)$, such that $\mathrm{Det}(M_V(a, b, c, d)) = 0 \mod 5$.

Exhausting over all tuples $a, b, c, d \mod 5$ produces a 12-bit indexed table that can be used to lookup an appropriate V for any $M_V(a, b, c, d)$ with determinant 5^n. This lookup can be used to construct an efficient algorithm for exact synthesis.

Input: Elements a, b, c, d from $\mathbb{Z}$ such that $\mathrm{Det}(M_V(a, b, c, d)) = 5^n$ for integer $n \geq 0$
Output: Sequence of matrices in $\{V_x, V_y, V_z, V_x^\dagger, V_y^\dagger, V_z^\dagger\}$ and a Pauli gate
gates $\leftarrow$ empty list;
while $\mathrm{Det}(M_V(a, b, c, d)) = 0 \mod 5$ **do**
  $V \leftarrow \mathrm{Lookup}_V(a \bmod 5, b \bmod 5, c \bmod 5, d \bmod 5)$;
  $M_V(a, b, c, d) \leftarrow V^\dagger M_V(a, b, c, d)/\mathrm{Det}(V)$;
  prepend V to *gates*;
end
return *gates,* $M_V(a, b, c, d)$

Algorithm 4: V basis exact synthesis.

The algorithm "picks off" each V gate sequentially. At each step, the leading factor of V is removed from $M_V(a, b, c, d)$ by multiplying on the left by $V^\dagger$. The resulting tuple a'', b'', c'', d'' is then divided by 5 yielding a new $M_V(a', b', c', d')$ with determinant 5^{n-1}. The output is the sequence of picked-off V gates, in reverse order.

C.2 Clifford + T

Recall from Section **??** the T matrices $T_P := \frac{1}{\sqrt{2+\sqrt{2}}}\left(I + \frac{I - iP}{\sqrt{2}}\right)$ for $P \in \{X, Y, Z\}$ and corresponding quaternion order

$$\mathcal{O} = \mathbb{Z}[\sqrt{2}] \cdot I + \mathbb{Z}[\sqrt{2}] \cdot \frac{I + iX}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}] \cdot \frac{I + iY}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}] \cdot \frac{I + iX + iY + iZ}{2}. \tag{78}$$

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \tag{79}$$

This order contains the T matrices each scaled by $\sqrt{2 + \sqrt{2}}$. For notational convenience we use $T_x = \left(\sqrt{2 + \sqrt{2}}\right) T_X$, $T_y = \left(\sqrt{2 + \sqrt{2}}\right) T_Y$, and $T_z = \left(\sqrt{2 + \sqrt{2}}\right) T_Z$ to refer to the scaled T matrices. Note that $T_p T_p^\dagger = \mathrm{Det}(T_p) I = (2 + \sqrt{2}) I$ for $p = x, y, z$.

Define M_T as a function that, according to (**??**), maps elements a, b, c, d of $\mathbb{Z}[\sqrt{2}]$ to a matrix:

$$M_T(a, b, c, d) := a \cdot I + b \cdot \frac{I + iX}{\sqrt{2}} + c \cdot \frac{I + iY}{\sqrt{2}} + d \cdot \frac{I + iX + iY + iZ}{2}. \tag{80}$$

Any matrix $M_T(a, b, c, d)$ with determinant $(2+\sqrt{2})^n$ can be decomposed into a length-n sequence of T gates [Kli+15b]. We omit the formal theorem because the situation is analogous to that of Theorem **??**. Note that $\mathrm{Det}(M_T(a, b, c, d)) = 1$ if and only if $M_T(a, b, c, d)$ is a Clifford unitary. For reference, we provide a standard T factorization.

Lemma C.3 (Clifford+T factorization). *Let* $a, b, c, d \in \mathbb{Z}[\sqrt{2}]$ *such that* $\mathrm{Det}(M_T(a,b,c,d)) = (2+\sqrt{2})^n$ *for integer* $n \geq 1$, *and at least one of* a, b, c, d *is not divisible by* $2+\sqrt{2}$. *Then there exists* $g \in \{T_x, T_y, T_z\}$ *and* $a', b', c', d' \in \mathbb{Z}[\sqrt{2}]$ *such that*

$$M_T(a,b,c,d) = gM_T(a',b',c',d'). \tag{81}$$

and $\mathrm{Det}(M_T(a',b',c',d')) = (2+\sqrt{2})^{n-1}$.

The proof of this Lemma is analogous to that of Lemma **??**, except that we exhaust over tuples a, b, c, d modulo $2+\sqrt{2}$ instead of tuples modulo 5. More precisely, we consider elements of $\mathbb{Z}[\sqrt{2}]$ modulo prime ideal $(2+\sqrt{2})\mathbb{Z}[\sqrt{2}] = \sqrt{2}\mathbb{Z}[\sqrt{2}]$. Considering values modulo $2+\sqrt{2}$ is the same as considering values modulo $\sqrt{2}$. Every element of $\mathbb{Z}[\sqrt{2}]$ is of the from $\sqrt{2}z$ or $\sqrt{2}z+1$ for some z from $\mathbb{Z}[\sqrt{2}]$, that is there are two possible values modulo $\sqrt{2}\mathbb{Z}[\sqrt{2}]$.

The Clifford+T exact synthesis algorithm is shown below. The table $\mathrm{Lookup}_T(a,b,c,d)$

Input: Elements a, b, c, d from $\mathbb{Z}[\sqrt{2}]$ such that $\mathrm{Det}(M(a,b,c,d)) = \ell^n$ for $\ell = 2+\sqrt{2}, n \in \mathbb{Z}, n \geq 0$
Output: Sequence of matrices in $\{T_x, T_y, T_z\}$ and a Clifford unitary.
gates $\leftarrow$ empty list;
while $\mathrm{Det}(M_T(a,b,c,d)) = 0 \mathrm{mod} \ell$ **do**
  $g \leftarrow \mathrm{Lookup}_T(a \bmod \ell, b \bmod \ell, c \bmod \ell, d \bmod \ell)$;
  $M_T(a,b,c,d) \leftarrow g^\dagger M_T(a,b,c,d)/\mathrm{Det}(g)$;
  prepend g to *gates*;
end
return *gates*, $M_T(a,b,c,d)$

Algorithm 5: Clifford+T exact synthesis.

is pre-calculated by enumerating over all tuples a, b, c, d modulo $2+\sqrt{2}$, in analogy to the V basis case. There are only 2^4 different options to consider in this case. Once factorizaton is complete, the remaning matrix that determinant one and therefore is a Clifford unitary.

C.3 Clifford + $\sqrt{T}$

Recall from Section **??** the $\sqrt{T}^k$ matrices

$$\sqrt{T}_Z^k = \frac{1}{\sqrt{2+2\cos\frac{\pi k}{8}}} \begin{pmatrix} 1+e^{-i\pi k/8} & 0 \\ 0 & 1+e^{i\pi k/8} \end{pmatrix} = \frac{I\cdot(1+\cos\frac{\pi k}{8}) - iZ\cdot\sin\frac{\pi k}{8}}{\sqrt{2+2\cos\frac{\pi k}{8}}}$$

For $\sqrt{T}_X^k, \sqrt{T}_Y^k$ we replace Z by X, Y in the equation above.

The corresponding quaternion order is

$$\mathcal{O} = \mathbb{Z}[2\cos\frac{\pi}{8}]\cdot I + \mathbb{Z}[2\cos\frac{\pi}{8}]\cdot\frac{I+iX}{\sqrt{2}} + \mathbb{Z}[2\cos\frac{\pi}{8}]\cdot\frac{I+iY}{\sqrt{2}} + \mathbb{Z}[2\cos\frac{\pi}{8}]\cdot\frac{I+iX+iY+iZ}{2}. \tag{82}$$

$$\mathbb{Z}[2\cos\frac{\pi}{8}] = \{a + b\cdot 2\cos\frac{\pi}{8} + c\sqrt{2} + d\cdot 2\cos\frac{3\pi}{8} : a,b,c,d \in \mathbb{Z}\} \tag{83}$$

This order contains the $\sqrt{T}_P, T_P, \sqrt{T}_P^3$ matrices when rescaled appropriately. We define such rescaled versions below:

$$\sqrt{T}_p = \ell(I\cdot(1+\cos\frac{\pi}{8}) - iP\cdot\cos\frac{3\pi}{8}),\ \ell = (2+2\cos\frac{\pi}{8})$$

$$\sqrt{T}_p^3 = u_1\ell(I\cdot(1+\cos\frac{3\pi}{8}) - iP\cdot\cos\frac{\pi}{8}), u_1 = 1-2\cos\frac{3\pi}{8}-\sqrt{2}$$

$$T_p = u_2(I\cdot(1+\cos\frac{\pi}{4}) - iP\cdot\cos\frac{\pi}{4}), u_2 = 1+2\cos\frac{\pi}{8}-2\cos\frac{3\pi}{8}$$

With the above rescaling we have

$$\sqrt{T}_p(\sqrt{T}_p)^\dagger = \mathrm{Det}(\sqrt{T}_p^3)\cdot I = \ell^3\cdot I$$

$$\sqrt{T}_p^3(\sqrt{T}_p^3)^\dagger = \mathrm{Det}(\sqrt{T}_p^3)\cdot I = \ell^3\cdot I$$

$$T_p(T_p)^\dagger = \mathrm{Det}(T_p)\cdot I = \ell^2\cdot I$$

Define $M_{\sqrt{T}}$ as a function that, according to (**??**), maps elements a,b,c,d of $\mathbb{Z}[2\cos\frac{\pi}{8}]$ to a matrix:

$$M_{\sqrt{T}}(a,b,c,d) := a\cdot I + b\cdot\frac{I+iX}{\sqrt{2}} + c\cdot\frac{I+iY}{\sqrt{2}} + d\cdot\frac{I+iX+iY+IZ}{2}. \tag{84}$$

Any matrix $M_{\sqrt{T}}(a,b,c,d)$ with determinant $\ell^n = (2+2\cos(\pi/8))^n$ can be decomposed into a sequence of $\sqrt{T}$ gates [For+15b; Kli+15b]. Unlike the V and T gate sets, the length of the sequence cannot be deduced exactly from the integer power n.

We again omit a formal decomposition theorem, which would be analogous to Theorem **??**. The remainder of this section describes $\sqrt{T}$ factorization algorithm.

Lemma C.4 (Clifford + $\sqrt{T}$ factorization). *Let $a,b,c,d\in\mathbb{Z}[2\cos\frac{\pi}{8}]$ such that $\mathrm{Det}(M_{\sqrt{T}}(a,b,c,d)) = \ell^n$ for integer $n\geq 3$, and at least one of a,b,c,d is not divisible by ℓ. Then there exists $g\in\{T_p^{k/2} : p\in\{x,y,z\}, k\in\{1,2,3\}\}$ and $a',b',c',d'\in\mathbb{Z}[2\cos\frac{\pi}{8}]$ such that*

$$g^\dagger M_{\sqrt{T}}(a,b,c,d) = \mathrm{Det}(g)M_{\sqrt{T}}(a',b',c',d'). \tag{85}$$

and $\mathrm{Det}(M_{\sqrt{T}}(a',b',c',d')) = \ell^{n-k}$ where $\mathrm{Det}(g) = \ell^k$

One can check via brute-force search that the only matrices with determinants $1,\ell,\ell^2$ are Clifford gates and a T_p times a Clifford gate correspondingly.

The asymmetry between determinants for T_p and $T_p^{1/2}$ and $T_p^{3/2}$ means that the gate sequence length cannot be calculated from n alone. Given a sequence with N_1 elements $T_p^{1/2}$, N_2 elements T_p and N_3 elements $T_p^{3/2}$ the total power n must be $3N_1+2N_2+3N_1$.

Like the Clifford+T case, the table $\mathrm{Lookup}_{\sqrt{T}}(a,b,c,d)$ is pre-calculated by enumerating over all tuples a,b,c,d modulo ℓ^3. Note, that every element of $\mathbb{Z}[\cos\frac{\pi}{8}]$ can be written as $a_0+a_1\ell+a_2\ell^2+z\ell^3$ for $a_k\in\{0,1\}$ and z from $\mathbb{Z}[\cos\frac{\pi}{8}]$. For this reason, there are only $2^{3\cdot4} = 4096$ options to consider when building the lookup table. Using lookup table reduces the number of matrix multiplications needed in the exact synthesis algorithm by factor of nine.

D Additional solutions for unitary and fallback mixing

Additional solutions for unitary mixing

In **??** we discussed a mixing strategy in which the approximation error ε was evenly divided between an "under rotation"

$$U_1 = \begin{pmatrix} r_1 e^{i(\theta+\delta_1)} & v_1^* \\ v_1 & r_1 e^{-i(\theta+\delta_1)} \end{pmatrix} \tag{86}$$

Input: Elements a, b, c, d from $\mathbb{Z}[2\cos\frac{\pi}{8}]$ such that $\mathrm{Det}(M_{\sqrt{T}}(a,b,c,d)) = \ell^n$ for $\ell = 2 + 2\cos\frac{\pi}{8}, n \in \mathbb{Z}, n \geq 0$

Output: Sequence of matrices in $\{T_x^{1/2}, T_y^{1/2}, T_z^{1/2}, T_x, T_y, T_z, T_x^{3/2}, T_y^{3/2}, T_z^{3/2}\}$ and a Clifford unitary

gates $\leftarrow$ empty list;
while $\mathrm{Det}(M_{\sqrt{T}}(a,b,c,d)) \bmod \ell^3 = 0$ **do**
  $g \leftarrow \mathrm{Lookup}_{\sqrt{T}}(a \bmod \ell^3, b \bmod \ell^3, c \bmod \ell^3, d \bmod \ell^3)$;
  $M_{\sqrt{T}}(a,b,c,d) \leftarrow g^\dagger M_{\sqrt{T}}(a,b,c,d)/\mathrm{Det}(g)$;
  prepend g to *gates*;
end
Rescale $M_{\sqrt{T}}(a,b,c,d)$ so it has determinant $(2+\sqrt{2})^n$ for $n = 0, 1$;
Apply Clifford+T synthesis to $M_{\sqrt{T}}(a,b,c,d)$;
return *gates,* $M_{\sqrt{T}}(a,b,c,d)$

Algorithm 6: Clifford + $\sqrt{T}$ exact synthesis.

and "over rotation"

$$U_2 = \begin{pmatrix} r_2 e^{i(\theta+\delta_2)} & v_2^* \\ v_2 & r_1 e^{-i(\theta+\delta_2)} \end{pmatrix}. \tag{87}$$

In this section, we discuss a strategy that might lead to lower expected and worst case gate cost.

The inefficiency in partitioning ε ahead of time is that it precludes solutions in which the approximation accuracy of U_1 and U_2 are significantly different. If, for example, U_1 is a close approximation to $e^{i\theta Z}$ then we would like to consider low-cost solutions for U_2 that are correspondingly loose.

Recall, that according to **??** we randomly choose $\{S, Z\}$ twirls of U_1, U_2 with probability $p, 1-p$ where

$$p = \frac{r_2^2 \sin(2\delta_2)}{r_2^2 \sin(2\delta_2) - r_1^2 \sin(2\delta_1)}.$$

and then the diamond norm distance is given by

$$||p\mathcal{T}_{U_1} + (1-p)\mathcal{T}_{U_2} - \mathcal{Z}_\theta||_\diamond = 2\left(p(1 - r_1^2\cos^2(\delta_1)) + (1-p)(1 - r_2^2\cos^2(\delta_2))\right) \leq \varepsilon$$

Suppose that we have already found a very cheap under-rotation and r_1, δ_1 are fixed. For example, when target angle θ is close to zero but

$$\mathcal{D}_\diamond(e^{i\theta Z}, I) = 2|\sin(\theta)| > \varepsilon$$

the identity gate is a very cheap under-rotated approximation, however it is not sufficiently close to $e^{i\theta Z}$ such that identity gate is a solution to the diagonal approximation problem. Next we derive the 2D region of all possible values of $r_2 e^{i(\theta+\delta_2)}$, such that the diamond norm distance is bounded by ε. We focus on the rotated region for values $r_2 e^{i\delta_2}$

Let us assume that $\delta_1 > -\pi/2$, $\delta_2 < \pi/2$ and introduce the following notation:

$$x_1 = r_1\cos(\delta_1),\ y_1 = -r_1\sin(\delta_1), x = r_2\cos(\delta_2), y = r_2\sin(\delta_2)$$

By definition x_1, y_1 are non-negative and the following constraints on x, y hold:

$$x > 0,\ y \geq 0,\ x^2 + y^2 \leq 1$$

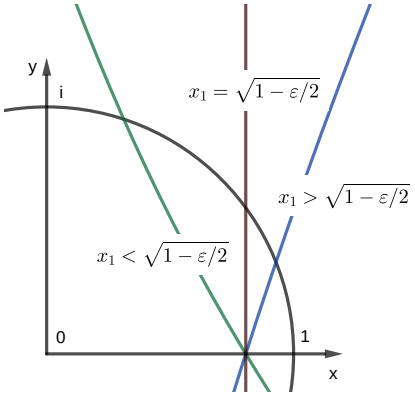


Figure 19: Curves bounding 2D region for the top-left entry u of over-rotated approximating unitary, when under-rotated approximating unitary is fixed. All curves must be rotated by angle θ around the origin $(0,0)$ for target rotation angle θ; $x_1 = r_1\cos(\delta_1)$, where $r_1 e^{i(\delta_1+\theta)}$ is top-left entry of the under-rotated approximating unitary. The curves intersection point has coordinates $(\sqrt{1-\varepsilon/2}, 0)$.

Using this notation probabilities $p, 1-p$ become:

$$p = xy/(xy + x_1y_1),\ 1-p = x_1y_1/(xy + x_1y_1)$$

And the diamond norm condition becomes

$$xy \cdot (1-x_1^2) + x_1y_1 \cdot (1-x^2) \le \varepsilon(xy + x_1y_1)/2$$

Next we collect coefficients in front of x^2 on the right and in front of xy on the left:

$$xy \cdot (1-\varepsilon/2-x_1^2) \le x^2 \cdot (x_1y_1) + (x_1y_1)(\varepsilon/2-1)$$

Because x is positive we get:

$$y \cdot (1-\varepsilon/2-x_1^2) \le x \cdot (x_1y_1) + \frac{1}{x} \cdot (x_1y_1)(\varepsilon/2-1). \tag{88}$$

Note that when $x_1 = \sqrt{1-\varepsilon/2}$, above conditions becomes $x \ge \sqrt{1-\varepsilon/2}$. This is exactly the case of evenly distributed errors between under and over rotations. When $x_1 > \sqrt{1-\varepsilon/2}$ the under-rotation is looser than evenly-distributed and over-rotation needs to be more accurate. When $x_1 < \sqrt{1-\varepsilon/2}$ under-rotation is more accurate than evenly-distributed and over-rotation can be looser. In the latter two cases the 2D region of possible values of the top-left entry is bounded by line $y = 0$, circle $x^2 + y^2$ and the hyperbola given by (**??**). The hyperbola crosses line $y = 0$ at $x = \sqrt{1-\varepsilon/2}$. In all cases we can use our general approach to find sequences with top-left entry in the 2D region. See Figure **??**.

Additional solutions for fallback mixing

Similar analysis applies to **??**. We again consider under-rotated approximation fixed and use notation from the previous subsection. Recall, that according to **??** we mix under-rotated and over-rotated approximations with the same probabilities as in unitary mixing case. However, the expression for the diamond norm distance is slightly different:

$$\left\| pr_1^2\left(\mathcal{Z}_{\theta+\delta_1} - \mathcal{Z}_\theta\right) + (1-p)r_2^2\left(\mathcal{Z}_{\theta+\delta_2} - \mathcal{Z}_\theta\right)\right\|_\diamond = 2\left(pr_1^2\sin^2(\delta_1) + (1-p)r_2^2\sin^2(\delta_2)\right) \le \varepsilon$$

Using the notation from the previous subsection we get

$$xy \cdot y_1^2 + y^2 \cdot x_1 y_1 \le \varepsilon(xy + x_1 y_1)/2$$

Collecting coefficients near xy on the left and coefficients near y^2 on the right we get:

$$xy \cdot (y_1^2 - \varepsilon/2) \le -y^2 \cdot x_1 y_1 + \varepsilon x_1 y_1/2$$

Using the fact that y is positive and dividing both sides by y we get inequality:

$$x \cdot (y_1^2 - \varepsilon/2) \le -y \cdot x_1 y_1 + \frac{1}{y} \cdot \varepsilon x_1 y_1/2. \tag{89}$$

Similarly to the previous subsection, the 2D region for complex values $r_2 e^{i\delta_2}$ is bounded by a unit circle, line $x = 0$ and the hyperbola (**??**).

The condition $y_1 = \sqrt{\varepsilon/2}$ corresponds to equally distributing errors. In this case we have $y \le \sqrt{\varepsilon/2}$. Note that this condition is different from the slightly weaker condition that we use in **??**. One can modify proofs in **??** to use condition $y \le \sqrt{\varepsilon/2}$ instead.

E Diamond difference of a twirled mixture

In this section we prove **??** and **??** which provide expressions for the accuracy of twirled mixtures. We begin by finding a convenient form for the SZ twirl of a qubit unitary. The following Proposition states that the twirl

$$\mathcal{T}_U(\rho) = \frac{1}{4} \sum_{\sigma \in \{I,Z,S,S^\dagger\}} \left(\sigma U \sigma^\dagger\right) \rho \left(\sigma U^\dagger \sigma^\dagger\right) \tag{90}$$

of U is a Pauli channel, except for two terms: ρZ and $Z\rho$.

Proposition E.1 (SZ twirling of a qubit unitary). *Given a qubit unitary*

$$U = \begin{pmatrix} re^{i\theta} & -v^* \\ v & re^{-i\theta} \end{pmatrix}, \tag{91}$$

the twirl of U over $\{S, Z\}$ can be expressed as

$$\mathcal{T}_U(\rho) = \mathcal{P}_{r,\theta}(\rho) - \frac{ir^2 \sin(2\theta)}{2}(\rho Z - Z\rho) \tag{92}$$

where Pauli channel $\mathcal{P}_{r,\theta}$ is defined by

$$\mathcal{P}_{r,\theta}(\rho) = r^2 \cos^2(\theta)\rho + \frac{1 - r^2}{2}(X\rho X + Y\rho Y) + r^2 \sin^2(\theta) Z\rho Z. \tag{93}$$

Proof (sketch). Recall that any qubit unitary can be written as:

$$U = t \cdot I + x \cdot iX + y \cdot iY + z \cdot iZ \tag{94}$$

where

$$\begin{aligned} t &= \mathrm{Re}(re^{i\theta}) = r\cos(\theta), \\ x &= \mathrm{Im}(v), \\ y &= -\mathrm{Re}(v), \\ z &= \mathrm{Im}(re^{i\theta}) = r\sin(\theta). \end{aligned} \tag{95}$$

Using $SXS^\dagger = Y$, $SYS^\dagger = -X$ and $SZS^\dagger = Z$ we have

$$ZUZ = t \cdot I - x \cdot iX - y \cdot iY + z \cdot iZ \tag{96}$$

$$SUS^\dagger = t \cdot I - y \cdot iX + x \cdot iY + z \cdot iZ \tag{97}$$

$$S^\dagger US = t \cdot I + y \cdot iX - x \cdot iY + z \cdot iZ \tag{98}$$

Any qubit channel can be written in term of its process matrix χ as:

$$\Phi(\rho) = \sum_{P,Q \in \{I,X,Y,Z\}} \chi_{P,Q} P \rho Q. \tag{99}$$

The proof then proceeds by deriving the process matrix with respect to t, x, y, z for each of the four terms of **??** and taking the sum. The resulting sum contains some $x^2 + y^2$ terms which can be rewritten as

$$x^2 + y^2 = 1 - t^2 - z^2 = 1 - r^2 \tag{100}$$

in order to remove the dependence on v. □

We now proceed with proving Lemma **??**, that the mixture $p\mathcal{T}_{U_1} + (1-p)\mathcal{T}_{U_2}$ yields a Pauli channel error. The main idea is to show that mixing U_1, U_2 eliminates the terms ρZ and $Z\rho$ from **??**.

Proof of **??**. By substituting $\mathcal{Z}_{-\theta}(\rho) = e^{-iZ\theta}\rho e^{i\theta Z}$ for ρ in **??**, proving **??** is equivalent to proving

$$p\mathcal{T}_{U_1}(\mathcal{Z}_{-\theta}(\rho)) + (1-p)\mathcal{T}_{U_2}(\mathcal{Z}_{-\theta}(\rho)) = \mathcal{E}(\rho). \tag{101}$$

Define rotated versions of U_1 and U_2,

$$V_1 := U_1 e^{-i\theta Z}, V_2 := U_2 e^{-i\theta Z}. \tag{102}$$

Then the twirl of V_1 is equivalent to $e^{-i\theta}$ followed by the twirl of U_1,

$$\begin{aligned} \mathcal{T}_{V_1}(\rho) &= \frac{1}{4} \sum_{W \in \{I,Z,S,S^\dagger\}} W V_1 \rho V_1^\dagger W^\dagger \\ &= \frac{1}{4} \sum_{W \in \{I,Z,S,S^\dagger\}} W U_1 (e^{-i\theta Z}\rho e^{i\theta Z}) U_1^\dagger W^\dagger \\ &= \mathcal{T}_{U_1}(\mathcal{Z}_{-\theta}(\rho)). \end{aligned} \tag{103}$$

Similarly for V_2,

$$\mathcal{T}_{V_2}(\rho) = \mathcal{T}_{U_2}(\mathcal{Z}_{-\theta}(\rho)). \tag{104}$$

We therefore seek to show that

$$p\mathcal{T}_{V_1}(\rho) + (1-p)\mathcal{T}_{V_2}(\rho) = \mathcal{E}(\rho) = p\mathcal{P}_{r_1,\delta_1} + (1-p)\mathcal{P}_{r_2,\delta_2}. \tag{105}$$

First, expand V_1

$$V_1 = U_1 e^{-i\theta Z} = \begin{pmatrix} r_1 e^{i\delta_1} & -e^{i\theta} v_1^* \\ e^{-i\theta} v_1 & r_1 e^{-i\delta_1} \end{pmatrix} \tag{106}$$

Next substitute into (**??**) to obtain

$$\mathcal{T}_{V_1}(\rho) = \mathcal{P}_{r_1,\delta_1}(\rho) - \frac{i r_1^2 \sin(2\delta_1)}{2}(\rho Z - Z\rho). \tag{107}$$

A similar result is obtained for $\mathcal{T}_{V_2}$,

$$\mathcal{T}_{V_2}(\rho) = \mathcal{P}_{r_2,\delta_2}(\rho) - \frac{ir_2^2\sin(2\delta_2)}{2}(\rho Z - Z\rho). \tag{108}$$

In order to obtain (**??**) the ρZ and $Z\rho$ terms of $p\mathcal{T}_{V_1} + (1-p)\mathcal{T}_{V_2}$ must cancel. Define $\alpha_k = r_k^2\sin(2\delta_k)$. Then indeed

$$\begin{aligned} p\frac{ir_1^2\sin(2\delta_1)}{2} + (1-p)\frac{ir_2^2\sin(2\delta_2)}{2} &= \frac{\alpha_2}{\alpha_2-\alpha_1}\cdot\frac{i\alpha_1}{2} + \left(1-\frac{\alpha_2}{\alpha_2-\alpha_1}\right)\frac{i\alpha_2}{2} \\ &= \frac{\alpha_2}{\alpha_2-\alpha_1}\cdot\frac{i\alpha_1}{2} - \frac{\alpha_1}{\alpha_2-\alpha_1}\cdot\frac{i\alpha_2}{2} \\ &= \frac{i\alpha_2\alpha_1}{2(\alpha_2-\alpha_1)} - \frac{i\alpha_1\alpha_2}{2(\alpha_2-\alpha_1)} \\ &= 0. \end{aligned} \tag{109}$$

Finally, note that $0 < p < 1$ since $r_1^2\sin(2\delta_1) < 0 < r_2^2\sin(2\delta_2)$ due to constraints on δ_1, δ_2. □

We are now ready to prove Theorem **??** that

$$||p\mathcal{T}_{U_1} + (1-p)\mathcal{T}_{U_2} - \mathcal{Z}_\theta||_\diamond = 2\left(1 - pr_1^2\cos^2(\delta_1) - (1-p)r_2^2\cos^2(\delta_2)\right). \tag{110}$$

Proof of Theorem **??**. First note that

$$e^{-i\theta}U_1 = \begin{pmatrix} r_1e^{i\delta_1} & e^{i\theta}v_1^* \\ e^{-i\theta}v_1 & r_1e^{-i\delta_1} \end{pmatrix}, \tag{111}$$

$$e^{-i\theta}U_2 = \begin{pmatrix} r_2e^{i\delta_2} & e^{i\theta}v_1^* \\ e^{-i\theta}v_1 & r_2e^{-i\delta_2} \end{pmatrix}. \tag{112}$$

By Lemma **??** we have

$$p\mathcal{T}_{e^{-i\theta}U_1}(\rho) + (1-p)\mathcal{T}_{e^{-i\theta}U_2}(\rho) = \mathcal{E}(\mathcal{Z}_0(\rho)) = \mathcal{E}(\rho). \tag{113}$$

Also note that $\mathcal{Z}_\theta(\mathcal{T}_U(\rho)) = \mathcal{T}_{e^{i\theta Z}U}(\rho)$ since $e^{i\theta Z}$ commutes with S and Z. Therefore by unitary invariance of the diamond norm

$$\begin{aligned} ||p\mathcal{T}_{U_1} + (1-p)\mathcal{T}_{U_2} - e^{i\theta Z}||_\diamond &= ||p\mathcal{Z}_{-\theta}(\mathcal{T}_{U_1}) + (1-p)\mathcal{Z}_{-\theta}(\mathcal{T}_{U_2}) - I||_\diamond \\ &= ||p\mathcal{T}_{e^{-i\theta}U_1} + (1-p)\mathcal{T}_{e^{-i\theta}U_2} - I||_\diamond \\ &= ||\mathcal{E} - I||_\diamond. \end{aligned} \tag{114}$$

The quantity $\mathcal{E} - I$ is a Pauli channel. The diamond norm of a Pauli channel is given by the sum of the absolute values of the terms in the process matrix (see **??**). We have

$$\begin{aligned} ||\mathcal{E} - I||_\diamond = &|pr_1^2\cos^2(\delta_1) + (1-p)r_2^2\cos^2(\delta_2) - 1| \\ &+ 2|p(1-r_1^2)/2 + (1-p)(1-r_2^2)/2| \\ &+ |pr_1^2\sin^2(\delta_1) + (1-p)r_2^2\sin^2(\delta_2)|. \end{aligned} \tag{115}$$

The right hand side can then be simplified to $2(1 - pr_1^2\cos^2(\delta_1) - (1-p)r_2^2\cos^2(\delta_2))$. □

F Diamond distance of a fallback mixture

In this section we prove the bound of Theorem **??** on the diamond difference between a mixture of fallback protocols and a target diagonal unitary. The main idea is to coerce the mixture of projective rotations into the form required by Theorem **??**. The bound then follows by simple substitution.

Proof of Theorem **??**. The mixture of the two fallback channels F_1 and F_2 is given by

$$pF_1(\rho) + p'F_2(\rho) = pq_1\mathcal{Z}_{\theta_1}(\rho) + pq_1'\mathcal{B}_1(\rho) + p'q_2\mathcal{Z}_{\theta_2}(\rho) + p'q_2'\mathcal{B}_2(\rho), \tag{116}$$

where we have used $p' = 1 - p$ and similarly for q_1', q_2'. Using the triangle inequality we obtain

$$\begin{aligned} ||pF_1 + p'F_2 - \mathcal{Z}_\theta||_\diamond \leq\, & ||pq_1\mathcal{Z}_{\theta_1} + p'q_2\mathcal{Z}_{\theta_2} - (pq_1 + p'q_2)\mathcal{Z}_\theta||_\diamond \\ & + pq_1'||\mathcal{B}_1 - \mathcal{Z}_\theta||_\diamond \\ & + p'q_2'||\mathcal{B}_{\theta_2'} - \mathcal{Z}_\theta||_\diamond. \end{aligned} \tag{117}$$

The second and third terms match those of **??**. We now examine the first term

$$||pq_1\mathcal{Z}_{\theta_1} + p'q_2\mathcal{Z}_{\theta_2} - (pq_1 + p'q_2)\mathcal{Z}_\theta||_\diamond = (pq_1 + p'q_2)||s\mathcal{Z}_{\theta_1} + (1-s)\mathcal{Z}_{\theta_2} - \mathcal{Z}_\theta||_\diamond \tag{118}$$

where

$$s = pq_1/(pq_1 + p'q_2) = \frac{\sin(2\delta_2)}{\sin(2\delta_2) - \sin(2\delta_1)}. \tag{119}$$

Now, since $\mathcal{Z}_\theta = \mathcal{T}_{e^{i\theta Z}}$ and by Theorem **??** we have

$$\begin{aligned} ||s\mathcal{Z}_{\theta+\delta_1} + (1-s)\mathcal{Z}_{\theta+\delta_2} - \mathcal{Z}_\theta||_\diamond &= ||s\mathcal{T}_{R(\theta+\delta_1)} + (1-s)\mathcal{T}_{R(\theta+\delta_2)} - \mathcal{Z}_\theta||_\diamond \\ &= 2(1 - s\cos^2(\delta_1) - (1-s)(\cos^2(\delta_2)) \\ &= 2(s\sin^2(\delta_1) - (1-s)(\sin^2(\delta_2)). \end{aligned} \tag{120}$$

Finally, substituting back into **??** we obtain

$$\begin{aligned} ||pq_1\mathcal{Z}_{\theta_1} + p'q_2\mathcal{Z}_{\theta_2} - (pq_1 + p'q_2)\mathcal{Z}_\theta||_\diamond &= (pq_1 + p'q_2)\cdot 2(s\sin^2(\delta_1) - (1-s)(\sin^2(\delta_2)) \\ &= 2\left(pq_1\sin^2(\delta_1) + (1-p)q_2\sin^2(\delta_2)\right). \end{aligned} \tag{121}$$

□