Optimal ancilla-free Clifford+V approximation of z-rotations

Neil J. Ross
Department of Mathematics and Statistics
Dalhousie University

Abstract

We describe a new efficient algorithm to approximate z-rotations by ancilla-free Clifford+V circuits, up to a given precision ε. Our algorithm is optimal in the presence of an oracle for integer factoring: it outputs the shortest Clifford+V circuit solving the given problem instance. In the absence of such an oracle, our algorithm is still near-optimal, producing circuits of V-count $m + O(\log(\log(1/\varepsilon)))$, where m is the V-count of the third-to-optimal solution. A restricted version of the algorithm approximates z-rotations in the Pauli+V gate set. Our method is based on previous work by the author and Selinger on the optimal ancilla-free approximation of z-rotations using Clifford+T gates and on previous work by Bocharov, Gurevich, and Svore on the asymptotically optimal ancilla-free approximation of z-rotations using Clifford+V gates.

1 Introduction

1.1 The synthesis problems

The *unitary group of order 2*, denoted $U(2)$, is the group of 2×2 complex unitary matrices. We also refer to the elements of this group as operators, or *gates*. The *special unitary group of order 2*, denoted by $SU(2)$, is the subset of $U(2)$ consisting of unitary matrices of determinant 1. We will be concerned with the notion of distance that arises from the operator norm, that is, for U and U' in $U(2)$:

$$\|U - U'\| = \sup\{|Uv - U'v| \ ; \ |v| = 1\}.$$

We refer to subsets of $U(2)$ as *gate bases* and to a finite word W over a gate base B as a *circuit over B*. By a slight abuse of notation, we write W to denote both a circuit over B and the unitary obtained by multiplying the basis elements composing W.

We are interested in decomposing, or *synthesizing*, unitary matrices into circuits over a given gate base. For a gate base B and unitary matrix U, the decomposition of U over B can be done *exactly*, if there exists a circuit W over B such that $W = U$, or *approximately up to some $\varepsilon > 0$*, if there exists a circuit W over B such that $\|U - W\| \leqslant \varepsilon$. We thus get the following two problems.

- *Exact synthesis problem for B:* given a unitary U, determine whether there exists a circuit W over B such that $W = U$ and, in case such a circuit exists, construct one.
- *Approximate synthesis problem for B:* given a unitary U and a precision $\varepsilon \geqslant 0$, determine whether there exists a circuit W over B such that $\|W - U\| \leqslant \varepsilon$ and, in case such a circuit exists, construct one.

In what follows, we focus on finite gate bases. If B is such a gate base, then the set of circuits over B is countable. Since $U(2)$ is uncountable, this implies that the exact synthesis problem for B will sometimes be solved negatively: there are unitary matrices that cannot be exactly synthesized over B. However, if the set of circuits over B is dense in $U(2)$, then the approximate synthesis problem for B can always be solved positively.

Because the state of a qubit is defined up to scaling by a unit scalar, the synthesis of a unitary U is sometimes done *up to a phase*. This means that instead of finding a circuit W such that $\|U - W\| \leqslant \varepsilon$, one looks for a circuit W and a unit scalar λ such that $\|U - \lambda W\| \leqslant \varepsilon$. This defines a third synthesis problem.

- *Approximate synthesis problem for B up to a phase:* given a unitary U and a precision $\varepsilon \geqslant 0$, determine whether there exists a circuit W over B and a unit scalar λ such that $\|U - \lambda W\| \leqslant \varepsilon$ and, in case such a circuit exists, construct one.

Since a global phase has no observable effect in quantum mechanics, it is often sufficient to define a decomposition method for special unitary matrices. Indeed, suppose that B is a gate base such that the set of circuits over B is dense in $SU(2)$. If we have an algorithm to approximately synthesize elements of $SU(2)$ into circuits over B, then we can synthesize arbitrary unitary matrices over B up to a phase, since the determinant of a unitary matrix always has norm 1.

A decomposition method solving any of the above three problems is evaluated with respect to its *time complexity* (what is its run-time?) and to its *circuit complexity* (how many gates are contained in the produced circuit?).

1.2 Synthesis of z-rotations using V-gates

We are interested in the following V-*gates*

$$V_X = \frac{1}{\sqrt{5}}(I + 2iX) = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \quad V_Y = \frac{1}{\sqrt{5}}(I + 2iY) = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}, \text{ and}$$

$$V_Z = \frac{1}{\sqrt{5}}(I + 2iZ) = \frac{1}{\sqrt{5}}\begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix},$$

and their adjoints

$$V_X^\dagger = \frac{1}{\sqrt{5}}(I - 2iX) = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & -2i \\ -2i & 1 \end{pmatrix}, \quad V_Y^\dagger = \frac{1}{\sqrt{5}}(I - 2iY) = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}, \text{ and}$$

$$V_Z^\dagger = \frac{1}{\sqrt{5}}(I - 2iZ) = \frac{1}{\sqrt{5}}\begin{pmatrix} 1-2i & 0 \\ 0 & 1+2i \end{pmatrix}.$$

It was shown in [7] and [8] that the group generated by the V-gates is dense in $SU(2)$. It was later shown in [6] that for any operator $U \in SU(2)$ and any precision ε, there exists an approximation for U over $V = \{V_X, V_Y, V_Z, V_X^\dagger, V_Y^\dagger, V_Z^\dagger\}$ that requires only $O(\log(1/\varepsilon))$ gates. However, no approximate synthesis algorithm was provided. In [2], Bocharov, Gurevich, and Svore defined a probabilistic algorithm for the approximate synthesis of unitaries over the Pauli+V gate set, which consists of the V-gates together with the Pauli gates X, Y, and Z. Because the Pauli gates form a subgroup of the Clifford gates, the algorithm of [2] is also a synthesis algorithm for the Clifford+V gate set, which consists of the V-gates together with the Clifford gates, whose generators are:

$$\omega = e^{i\pi/4}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \text{and} \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

In the context of the Clifford+V gate set, the complexity of a circuit is measured by counting the number of V-gates appearing in it, its V-*count*. This is due to the fact that the Clifford operators can always be moved to the end of a circuit using equations such as $\omega V_X = V_X \omega$, $SV_X = V_Y S$, $HV_X = V_Z H$, and so on.

The algorithm of [2] is efficient in the sense that it runs in probabilistic polynomial time. Moreover, it yields circuits of V-count bounded above by $12\log_5(2/\varepsilon)$ for arbitrary unitaries.

The method of [2] was adapted from the one developed in [11] for the Clifford+T gate set. It relies on the definition of an algorithm for the Clifford+V decomposition of z-*rotations*, i.e., matrices of the form

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

For these gates, the algorithm of [2] achieves circuits of V-count bounded above by $4\log_5(2/\varepsilon)$. Such an algorithm can then be used for the synthesis of an arbitrary element U of $SU(2)$ by first writing U as a product of three z-rotations using Euler angles

$$U = R_z(\theta_1) X R_z(\theta_2) X R_z(\theta_3)$$

and then applying the algorithm to each of the $R_z(\theta_i)$.

1.3 Results

In the present paper, we define an efficient and optimal algorithm for the approximate synthesis of z-rotations over the Clifford+V gate set. Our algorithm is defined by adapting techniques developed in [10] for the Clifford+T gate set. We stress that the algorithm is *literally optimal*, i.e., for any given pair (θ, ε) of an angle and a precision, the algorithm finds the shortest possible ancilla-free Clifford+V circuit W such that $\|W - R_z(\theta)\| \leqslant \varepsilon$. As in [10], the optimality of the algorithm depends on the presence of a factoring oracle. Because of Shor's algorithm [12], a quantum computer can serve as such an oracle. For this reason, the algorithm is actually an efficient and optimal *quantum* synthesis algorithm. However, the *classical* algorithm obtained in the absence of a factoring oracle is efficient and nearly optimal: in this case the algorithm produces circuits of V-count $m + O(\log(\log(1/\varepsilon)))$, where m is the V-count of the third-to-optimal solution. These properties of the classical algorithm are established under a mild number-theoretic assumption.

We also describe a restricted version of the algorithm which synthesizes z-rotations over the Pauli+V gate set. This restricted algorithm is also efficient and optimal, if a factoring oracle is available, and efficient, but only near-optimal, otherwise.

1.4 Related work

Independently of the present paper, in [1], Blass, Bocharov, and Gurevich defined an algorithm for the approximate synthesis of z-rotations in the Pauli+V basis. Their method is in principle similar to ours, but they use a different technique to solve the *grid problems* of Section 4.1.

2 Preliminaries

We write $\mathbb{N}$ for the semiring of non-negative integers, $\mathbb{Z}$ for the ring of integers and $\mathbb{C}$ for the field of complex numbers. The conjugate of a complex number is given by $(a+ib)^\dagger = a - ib$. The Gaussian integers $\mathbb{Z}[i]$ are the complex numbers whose real and imaginary parts are both integral, i.e., the complex numbers $a+ib$ with $a, b \in \mathbb{Z}$. The units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$. Finally, the group of Pauli operators is generated by the following matrices:

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

The Pauli group is a subgroup of the Clifford group. We write Pauli+S for the subgroup of the Clifford group generated by the Pauli gates and the S gate.

3 Clifford+V Exact Synthesis of Unitaries

In this section, we describe an algorithm to solve the problem of exact synthesis in the Clifford+V gate set. This material is adapted from [2], where an algorithm for exact synthesis in the Pauli+V gate set was described using the theory of quaternions. We also use some techniques developed in [4] for exact synthesis in the Clifford+T gate set.

Problem 1. Given a unitary operator $U \in U(2)$, determine whether there exists a Clifford+V circuit W such that $U = W$ and, in case such a circuit exists, construct one whose V-count is minimal.

To solve Problem 1, we consider unitary matrices of the form

$$U = \frac{1}{\sqrt{5}^k}\frac{1}{\sqrt{2}^\ell}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad \text{where } k, \ell \in \mathbb{N},\ \alpha, \beta, \gamma, \delta \in \mathbb{Z}[i], \text{ and } 0 \leqslant \ell \leqslant 2. \tag{1}$$

The integers k and ℓ in (1) are called the $\sqrt{5}$-*denominator exponent* and the $\sqrt{2}$-*denominator exponent* of U respectively. The least k (resp. ℓ) such that U can be written as above is the *least* $\sqrt{5}$-*denominator exponent* (resp. *least* $\sqrt{2}$-*denominator exponent*) of U. These notions extend naturally to vectors and scalars of the form

$$\frac{1}{\sqrt{5}^k}\frac{1}{\sqrt{2}^\ell}\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} \quad \text{and} \quad \frac{1}{\sqrt{5}^k}\frac{1}{\sqrt{2}^\ell}\ \alpha, \tag{2}$$

where $k, \ell \in \mathbb{N}$, $\alpha, \gamma \in \mathbb{Z}[i]$ and $0 \leqslant \ell \leqslant 2$. In what follows, we refer to the pair (k, ℓ) as the *denominator exponent* of a matrix, vector, or scalar. It is then understood that the first component of the pair is the $\sqrt{5}$-exponent, while the second is the $\sqrt{2}$-exponent. Note that the least denominator exponent of a matrix, vector, or scalar is the pair (k, ℓ), where k and ℓ are the least $\sqrt{5}$- and $\sqrt{2}$-exponents respectively.

We will show that a unitary operator U can be expressed as a Clifford+V circuit if and only if it is of the form (1) and its determinant is a power of i. We start by showing the left-to-right implication.

Lemma 2. *If U is a Clifford+V operator, then $U = ABC$ where A is a product of V-gates, B is a Pauli+S operator, and C is one of I, H, HS, ω, $H\omega$, and $HS\omega$.*

Proof. Clifford gates and V-gates can be commuted in the sense that for every pair C, V of a Clifford gate and a V-gate, there exists a pair C', V' such that $CV = V'C'$. This implies that a Clifford+V operator U can always be written as $U = AA'$, where A is a product of V-gates and A' is a Clifford operator. Furthermore, the Pauli+S group has index 6 as a subgroup of the Clifford group and its cosets are: Pauli+S, Pauli+$S \cdot H$, Pauli+$S \cdot HS$, Pauli+$S \cdot \omega$, Pauli+$S \cdot H\omega$, and Pauli+$S \cdot HS\omega$. It thus follows that a Clifford operator A' can always be written as $A' = BC$ with B a Pauli+S operator and C one of I, H, HS, ω, $H\omega$, and $HS\omega$. □

To show, conversely, that every matrix of the form (1) whose determinant is a power of i can be represented by a Clifford+V circuit, we proceed as in [4]. We show that every unit vector of the form (2) can be reduced to $e_1 = \binom{1}{0}$ by applying a sequence of carefully chosen Clifford+V gates. Then, we show how applying this method to the fist column of a unitary matrix U of the form (1) yields a Clifford+V circuit for U.

Lemma 3. *If u is a unit vector of the form (2) with least $\sqrt{5}$-denominator exponent k and W is a Clifford circuit, then Wu has least $\sqrt{5}$-denominator exponent k.*

Proof. It suffices to show that the generators of the Clifford group preserve the least $\sqrt{5}$-denominator exponent of u. The general result then follows by induction. To this end, write u as in (2), with $\alpha = a + ib$ and $\gamma = c + id$:

$$u = \frac{1}{\sqrt{5}^k} \frac{1}{\sqrt{2}^\ell} \begin{pmatrix} a+ib \\ c+id \end{pmatrix}.$$

Now apply H, ω, and S to u:

$$Hu = \frac{1}{\sqrt{5}^k} \frac{1}{\sqrt{2}^{\ell+1}} \begin{pmatrix} (a+c)+i(b+d) \\ (a-c)+i(b-d) \end{pmatrix}, \quad \omega u = \frac{1}{\sqrt{5}^k} \frac{1}{\sqrt{2}^{\ell+1}} \begin{pmatrix} (a-b)+i(a+b) \\ (c-d)+i(c+d) \end{pmatrix},$$

$$Su = \frac{1}{\sqrt{5}^k} \frac{1}{\sqrt{2}^\ell} \begin{pmatrix} a+ib \\ -d+ic \end{pmatrix}.$$

By minimality of k, one of a, b, c, d is not divisible by 5. The least $\sqrt{5}$-denominator of Su is therefore k. Moreover, for any two integers x and y, $x + y \equiv x - y \equiv 0 \pmod 5$ implies $x \equiv y \equiv 0 \pmod 5$. Thus the least $\sqrt{5}$-denominator exponent of Hu and ωu is also k. □

Lemma 4. *If u is a unit vector of the form (2) with least denominator exponent (k, ℓ), then there exists a Clifford circuit W such that Wu has least denominator exponent $(k, 0)$.*

Proof. By Lemma 3, we need not worry about k and only have to focus on reducing ℓ. Write u as in (2), with $0 \leqslant \ell \leqslant 2$, $\alpha = a + ib$, and $\gamma = c + id$. Since u has unit norm, we have $a^2 + b^2 + c^2 + d^2 = 5^k 2^\ell$. We prove the lemma by case distinction on ℓ. If $\ell = 0$, there is nothing to prove. The remaining cases are treated as follows.

- $\ell = 1$. In this case $a^2 + b^2 + c^2 + d^2 = 5^k \cdot 2 \equiv 0 \pmod 2$. Therefore only an even number amongst a, b, c, d can be odd. Using a Pauli+S operator, we can without loss of generality assume that $a \equiv c \pmod 2$ and $b \equiv d \pmod 2$ or that $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$. It then follows that either Hu or ωu has denominator exponent $(k, 0)$ since

$$Hu = \frac{1}{\sqrt{5}^k} \frac{1}{2} \begin{pmatrix} (a+c)+i(b+d) \\ (a-c)+i(b-d) \end{pmatrix} \quad \text{and} \quad \omega u = \frac{1}{\sqrt{5}^k} \frac{1}{2} \begin{pmatrix} (a-b)+i(a+b) \\ (c-d)+i(c+d) \end{pmatrix}.$$

- $\ell = 2$. In this case $a^2 + b^2 + c^2 + d^2 = 5^k \cdot 4 \equiv 0 \pmod 4$. This implies that a, b, c and d must have the same parity and thus, by minimality of ℓ, must all be odd. Using a Pauli+S operator, we can without loss of generality assume that $a \equiv b \equiv c \equiv d \equiv 1 \pmod 4$. It then follows that $H\omega u$ has denominator exponent $(k, 0)$ since

$$H\omega u = \frac{1}{\sqrt{5}^k} \frac{1}{4} \begin{pmatrix} (a-b+c-d)+i(a+b+c+d) \\ (a-b-c+d)+i(a+b-c-d) \end{pmatrix}.$$

□

Remark 5. Let V be one of the V-gates, u be a vector of the form (2), and k and k' be the least $\sqrt{5}$-denominator exponents of u and Vu respectively. Then $k' \leqslant k + 1$. Moreover, If it were the case that $k' < k - 1$, then the least $\sqrt{5}$-denominator exponent of $V^\dagger V u = u$ would be strictly less k which is absurd. Thus $k - 1 \leqslant k' \leqslant k + 1$.

Lemma 6. *If u is a unit vector of the form (2) with least denominator exponent $(k, 0)$, then there exists a Pauli+V circuit W of V-count k such that $Wu = e_1$, the first standard basis vector.*

Proof. Write u as in (2) with $\ell = 0$, $\alpha = a + ib$, and $\gamma = c + id$. Since u has unit norm, we have $a^2 + b^2 + c^2 + d^2 = 5^k 2^0 = 5^k$. We prove the lemma by induction on k.

- $k = 0$. In this case $a^2 + b^2 + c^2 + d^2 = 1$. It follows that exactly one of a, b, c, d is ± 1 while all the others are 0. Then u can be reduced to e_1 by acting on it using a Pauli operator.
- $k > 0$. In this case $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod 5$. We will show that there exists a Pauli+V operator U of V-count 1 such that the least denominator exponent of Uu is $k - 1$. It then follows by the induction hypothesis that there exists U' of V-count $k - 1$ such that $U'Uu = e_1$, which then completes the proof.

  Consider the residues modulo 5 of a, b, c, and d. Since $0, 1$, and 4 are the only squares modulo 5, then, up to a reordering of the tuple (a, b, c, d), we must have:

$$(a, b, c, d) \equiv \begin{cases} (0, 0, 0, 0) \\ (\pm 2, \pm 1, 0, 0) \\ (\pm 2, \pm 2, \pm 1, \pm 1). \end{cases}$$

  However, by minimality of k, we know that $a \equiv b \equiv c \equiv d \equiv 0$ is impossible, so the other two cases are the only possible ones. We treat them in turn.

  First, assume that one of a, b, c, d is congruent to ± 2, one is congruent to ± 1, and the remaining two are congruent to 0. By acting on u with a Pauli operator, we can moreover assume without loss of generality that $a \equiv 2$. Now if $b \equiv 1$, consider $V_Z u$:

$$V_Z u = \frac{1}{\sqrt{5}^{k+1}} \begin{pmatrix} (a - 2b) + i(2a + b) \\ (c + 2d) + i(d - 2c) \end{pmatrix}.$$

  Since $a \equiv 2$, $b \equiv 1$, and $c \equiv d \equiv 0$, we get $(a - 2b) \equiv (2a + b) \equiv (c + 2d) \equiv (d - 2c) \equiv 0 \pmod 5$. The least denominator exponent of $V_Z u$ is therefore $k - 1$. If on the other hand $b \equiv -1$ then

$$V_Z{}^\dagger u = \frac{1}{\sqrt{5}^{k+1}} \begin{pmatrix} (a + 2b) + i(b - 2a) \\ (c - 2d) + i(d + 2c) \end{pmatrix}$$

  and reasoning analogously shows that the least denominator exponent of $V_Z{}^\dagger u$ is $k - 1$. A similar argument can be made in the remaining cases, i.e., when $c \equiv \pm 1$ or $d \equiv \pm 1$. For brevity, we list the desired operators in the table below. The left column describes the residues of a, b, c, and d modulo 5 and the right column gives the operator U such that Uu has least denominator exponent $k - 1$.

(a, b, c, d)	U
$(2, 1, 0, 0)$	V_Z
$(2, 0, 1, 0)$	$V_Y{}^\dagger$
$(2, 0, 0, 1)$	V_X
$(2, -1, 0, 0)$	$V_Z^\dagger$
$(2, 0, -1, 0)$	V_Y
$(2, 0, 0, -1)$	$V_X{}^\dagger$

  Now assume that two of a, b, c, d are congruent to ± 2 while the remaining two are congruent to ± 1. We can use Pauli operators to guarantee that $a \equiv 2$ and $c \geqslant 0$. As above, we list the desired operators in a table for conciseness. It can be checked that in each case the given operator is such that the least denominator exponent of Uu is $k - 1$.

(a,b,c,d)	U
$(2,2,1,1)$	${V_Y}^\dagger$
$(2,1,2,1)$	V_X
$(2,1,1,2)$	V_Z
$(2,1,2,-1)$	V_Z
$(2,-1,2,1)$	${V_Z}^\dagger$
$(2,2,1,-1)$	${V_X}^\dagger$
$(2,-2,1,1)$	V_X
$(2,1,1,-2)$	${V_Y}^\dagger$
$(2,-1,1,2)$	${V_Y}^\dagger$
$(2,-1,1,-2)$	${V_Z}^\dagger$
$(2,-1,2,-1)$	${V_X}^\dagger$
$(2,-2,1,-1)$	${V_Y}^\dagger$

□

We can now solve Problem 1.

Proposition 7. *A unitary operator $U \in U(2)$ is exactly representable by a Clifford+V circuit if and only if U is of the form (1) and $\det(U) = i^n$ for some integer n. Moreover, there exists an efficient algorithm that computes a Clifford+V circuit for U with V-count equal to the least $\sqrt{5}$-denominator exponent of U, which is minimal.*

Proof. The left-to-right implication follows from Lemma 2 and the observation that all the generators of the Clifford+V group have determinant i^n for some integer n. For the right-to-left implication, it suffices to show that there exists a Clifford+V circuit W of V-count k such that $WU = I$, since we then have $U = W^\dagger$. To construct W, apply Lemma 4 and Lemma 6 to the first column u_1 of U. This yields a circuit W' such that the first column of $W'U$ is e_1. Since $W'U$ is unitary, it follows that its second column u_2 is a unit vector orthogonal to e_1. Therefore $u_2 = \lambda e_2$ where λ is a unit of the Gaussian integers. Since the determinant of W' is i^m for some integer m, the determinant of $W'U$ is i^{n+m}, so that $\lambda = i^{n+m}$. Thus one of the following equalities must hold

$$W'U = I,\ ZW'U = I,\ SW'U = I \text{ or } ZSW'U = I.$$

To prove the second claim, suppose that the least $\sqrt{5}$-denominator exponent of U is k. Then W can be efficiently computed because the algorithm described in the proofs of Lemma 4 and Lemma 6 requires $O(k)$ arithmetic operations. Moreover, W has V-count k by Lemma 6, which is minimal since any Clifford+V circuit of V-count up to $k-1$ has least $\sqrt{5}$-denominator exponent at most $k-1$. □

We conclude this section by noting that restricting ℓ to be equal to 0 in (1) and the determinant of U to be ± 1 yields a solution to the problem of exact synthesis in the Pauli+V gate set.

Proposition 8. *A unitary operator $U \in U(2)$ is exactly representable by a Pauli+V circuit if and only if U is of the form (1) with $\ell = 0$ and $\det(U) = \pm 1$. Moreover, there exists an efficient algorithm that computes a Pauli+V circuit for U with V-count equal to the least $\sqrt{5}$-denominator exponent of U, which is minimal.*

Proof. Analogous to the proof of Proposition 7, using the algorithm of Lemma 6. □

4 Clifford+V Approximate Synthesis of z-Rotations

In this section, we describe an algorithm to solve the problem of approximate synthesis of z-rotations over the Clifford+V gate set.

Problem 9. Given an angle θ and a precision $\varepsilon > 0$, construct a Clifford+V circuit U whose V-count is as small as possible and such that $\|U - R_z(\theta)\| \leqslant \varepsilon$.

Our algorithm is adapted from the one developed in [10] for the Clifford+T gate set. As in [10], we reduce Problem 9 to a pair of independent problems. From Proposition 7, we know that a unitary matrix U can be efficiently decomposed as a Clifford+V circuit if and only if

$$U = \frac{1}{\sqrt{5}^k}\frac{1}{\sqrt{2}^\ell}\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}, \quad \text{with } k,\ell \in \mathbb{N},\ \alpha,\beta,\gamma,\delta \in \mathbb{Z}[i],\ 0 \leqslant \ell \leqslant 2, \text{ and } \det(U) = i^n. \tag{3}$$

To solve Problem 9, we therefore need to find $k, \ell \in \mathbb{N}$ and $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[i]$ satisfying these conditions and such that the resulting matrix U approximates $R_z(\theta)$ up to ε. The following lemma shows that we can restrict our attention to matrices of determinant 1.

Lemma 10. *If $\varepsilon < |1 - e^{i\pi/4}|$, then all solutions to Problem 9 have the form*

$$U = \frac{1}{\sqrt{5}^k} \frac{1}{\sqrt{2}^\ell} \begin{pmatrix} \alpha & -\beta^\dagger \\ \beta & \alpha^\dagger \end{pmatrix}, \tag{4}$$

with $k, \ell \in \mathbb{N}$, $\alpha, \beta \in \mathbb{Z}[i]$, and $0 \leqslant \ell \leqslant 2$. If $\varepsilon \geqslant |1 - e^{i\pi/4}|$, then there exists a solution of V-count 0 (i.e., a Clifford operator), and it is also of the form (4).

Proof. Every complex 2×2 unitary operator U can be written as

$$U = \begin{pmatrix} a & -b^\dagger e^{i\phi} \\ b & a^\dagger e^{i\phi} \end{pmatrix},$$

for $a, b \in \mathbb{C}$ and $\phi \in [-\pi, \pi]$. This, together with the characterization of Clifford+V operators given by Proposition 7, implies that a complex 2×2 unitary operator U can be exactly synthesized over the Clifford+V basis if and only if

$$U = \frac{1}{\sqrt{2}^k} \frac{1}{\sqrt{2}^\ell} \begin{pmatrix} \alpha & -\beta^\dagger i^n \\ \beta & \alpha^\dagger i^n \end{pmatrix},$$

with $k, \ell, n \in \mathbb{N}$, $\alpha, \beta \in \mathbb{Z}[i]$, and $0 \leqslant \ell \leqslant 2$.

Now assume that $\varepsilon < |1 - e^{i\pi/4}|$ and $\|U - R_z(\theta)\| \leqslant \varepsilon$. Let $e^{i\phi_1}$ and $e^{i\phi_2}$ be the eigenvalues of $UR_z(\theta)^{-1}$, with $\phi_1, \phi_2 \in [-\pi, \pi]$. Then

$$|1 - e^{i\pi/4}| > \varepsilon \geqslant \|U - R_z(\theta)\| = \|I - UR_z(\theta)^{-1}\| = \max\{|1 - e^{i\phi_1}|, |1 - e^{i\phi_2}|\},$$

so that $|1 - e^{i\phi_j}| < |1 - e^{i\pi/4}|$. Therefore $-\pi/4 < \phi_j < \pi/4$, for $j \in \{1, 2\}$, which implies that $-\pi/2 < \phi_1 + \phi_2 < \pi/2$. Hence $|1 - e^{i(\phi_1+\phi_2)}| < |1 - e^{i\pi/2}| = \sqrt{2}$. But $e^{i(\phi_1+\phi_2)} = \det(UR_z(\theta)^{-1}) = i^n$. Thus $|1 - i^n| < \sqrt{2}$ which proves that $i^n = 1$.

For the last statement, note that if $\theta/2 \in [-\pi/4, \pi/4]$, then $\|I - R_z(\theta)\| = |1 - e^{i\theta/2}| \leqslant |1 - e^{i\pi/4}|$. Similarly, if $\theta/2$ belongs to one of $[\pi/4, 3\pi/4]$, $[3\pi/4, 5\pi/4]$, or $[5\pi/4, 7\pi/4]$, then one of $\|\omega^2 - R_z(\theta)\|$, $\|-I - R_z(\theta)\|$, or $\|-\omega^2 - R_z(\theta)\|$ is less than $|1 - e^{i\pi/4}|$. In each case, $R_z(\theta)$ is approximated to within ε by a Clifford operator. □

As a result of Lemma 10, we know that to solve Problem 9, it suffices to find $k, \ell \in \mathbb{N}$, with $0 \leqslant \ell \leqslant 2$, and $\alpha, \beta \in \mathbb{Z}[i]$ such that $\alpha^\dagger\alpha + \beta^\dagger\beta = 5^k 2^\ell$ and the resulting matrix U of the form (4) approximates $R_z(\theta)$ up to ε. The key observation here is that, given ε and θ, we can express the requirement $\|U - R_z(\theta)\| \leqslant \varepsilon$ as a constraint on the top left entry $\alpha/(\sqrt{5}^k\sqrt{2}^\ell)$ of U. Indeed, let $z = e^{-i\theta/2}$, $\alpha' = \alpha/(\sqrt{5}^k\sqrt{2}^\ell)$, and $\beta' = \beta/(\sqrt{5}^k\sqrt{2}^\ell)$. Since ${\alpha'}^\dagger\alpha' + {\beta'}^\dagger\beta' = 1$ and $z^\dagger z = 1$, we have

$$\begin{aligned} \|U - R_z(\theta)\|^2 &= |\alpha' - z|^2 + |\beta'|^2 \\ &= (\alpha' - z)^\dagger(\alpha' - z) + {\beta'}^\dagger\beta' \\ &= {\alpha'}^\dagger\alpha' + {\beta'}^\dagger\beta' - z^\dagger\alpha' - {\alpha'}^\dagger z + z^\dagger z \\ &= 2 - 2\,\mathrm{Re}(z^\dagger\alpha'). \end{aligned}$$

Thus $\|R_z(\theta) - U\| \leqslant \varepsilon$ if and only if $2 - 2\,\mathrm{Re}(z^\dagger\alpha') \leqslant \varepsilon^2$, or equivalently, $\mathrm{Re}(z^\dagger\alpha') \geqslant 1 - \frac{\varepsilon^2}{2}$. If we identify the complex numbers $z = x + yi$ and $\alpha' = a + bi$ with 2-dimensional real vectors $\vec{z} = (x, y)^T$ and $\vec{\alpha}' = (a, b)^T$, then $\mathrm{Re}(z^\dagger\alpha')$ is just their inner product $\vec{z} \cdot \vec{\alpha}'$, and therefore $\|U - R_z(\theta)\| \leqslant \varepsilon$ is equivalent to

$$\vec{z} \cdot \vec{\alpha}' \geqslant 1 - \frac{\varepsilon^2}{2}. \tag{5}$$

Moreover, ${\alpha'}^\dagger\alpha' + {\beta'}^\dagger\beta' = 1$ implies that ${\alpha'}^\dagger\alpha' = 1 - {\beta'}^\dagger\beta' \leqslant 1$ and therefore that $\vec{\alpha}'$ is an element of the closed unit disk $\overline{\mathcal{D}}$. These two remarks jointly define a subset of the unit disk

$$\mathcal{R}_\varepsilon = \{\vec{\alpha}' \in \overline{\mathcal{D}}\ ;\ \vec{z} \cdot \vec{\alpha}' \geqslant 1 - \frac{\varepsilon^2}{2}\}, \tag{6}$$

which we call the ε-*region* for θ, such that if $\alpha' \in \mathcal{R}_\varepsilon$, then $\|U - R_z(\theta)\| \leqslant \varepsilon$. In the presence of $\alpha' = \alpha/(\sqrt{5}^k\sqrt{2}^\ell) \in \mathcal{R}_\varepsilon$, all that remains is to find the other entry of U by solving the Diophantine equation

$$\alpha^\dagger\alpha + \beta^\dagger\beta = 5^k 2^\ell$$

for some unknown $\beta \in \mathbb{Z}[i]$.

Now recall that we wish to solve Problem 9 optimally, so that we need to find an approximating matrix U whose V-count is as low as possible. We know from Proposition 7 that the V-count of U is equal to its least $\sqrt{5}$-denominator exponent. Therefore if we can enumerate the points of $\mathcal{R}_\varepsilon$ of the form $\alpha/(\sqrt{5}^k\sqrt{2}^\ell)$ for $\alpha \in \mathbb{Z}[i]$ and $0 \leqslant \ell \leqslant 2$ in order of increasing k, then we can try to solve the Diophantine equation for each such point. The first candidate for which the Diophantine equation has a solution will then yield an optimal solution to Problem 9.

Problem 9 is therefore equivalent to the following problem.

Problem 11. Given an angle θ and a precision $\varepsilon > 0$, find $k, \ell \in \mathbb{N}$ with $0 \leqslant \ell \leqslant 2$ and $\alpha, \beta \in \mathbb{Z}[i]$ such that:

(i) $\alpha/(\sqrt{5}^k\sqrt{2}^\ell) \in \mathcal{R}_\varepsilon$,

(ii) $\alpha^\dagger\alpha + \beta^\dagger\beta = 5^k 2^\ell$,

(iii) and k is as small as possible.

In the above problem, the first two goals can be treated separately.

Problem 12 (Scaled grid problem)**.** Given a bounded convex subset A of $\mathbb{R}^2$ with non-empty interior, enumerate all points $\alpha/(\sqrt{5}^k\sqrt{2}^\ell) \in A$, where $\alpha \in \mathbb{Z}[i]$, $k, \ell \in \mathbb{N}$, and $0 \leqslant \ell \leqslant 2$, in order of increasing (k, ℓ).

Each point $\alpha/(\sqrt{5}^k\sqrt{2}^\ell) \in A$ is called a *solution* to the scaled grid problem for A of denominator exponent (k, ℓ).

Problem 13 (Diophantine equation)**.** Given $\alpha \in \mathbb{Z}[i]$ and $k, \ell \in \mathbb{N}$, find $\beta \in \mathbb{Z}[i]$ such that $\alpha^\dagger\alpha + \beta^\dagger\beta = 5^k 2^\ell$ if such a β exists.

We now discuss methods to solve both of these problems. We provide an algorithm for Problem 9 and analyze its properties in Section 4.3 and Section 4.4 respectively.

4.1 Grid problems

In this subsection, we define an efficient algorithm to solve Problem 12. In what follows we refer to the set $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ as the *grid* and to elements of $\mathbb{Z}^2$ as *grid points*. The instances of the scaled grid problem where the set A is an upright rectangle, i.e., of the form $[x_1, x_2] \times [y_1, y_2]$, are easy to solve. If A is not an upright rectangle, the problem can still be solved efficiently, provided that A can be made "upright enough".

Definition 14 (Uprightness)**.** Let A be a bounded convex subset of $\mathbb{R}^2$. The bounding box of A, denoted $\mathrm{BBox}(A)$, is the smallest set of the form $[x_1, x_2] \times [y_1, y_2]$ that contains A. The *uprightness of* A, denoted up(A), is defined to be the ratio of the area of A to the area of its bounding box:

$$\mathrm{up}(A) = \frac{\mathrm{area}(A)}{\mathrm{area}(\mathrm{BBox}(A))}.$$

We say that A is M-upright if $\mathrm{up}(A) \geqslant M$.

We will be especially interested in the case where the set A is an ellipse. Our interest in ellipses is motivated by the fact that a bounded convex subset A of the plane with non-empty interior can always be enclosed in an ellipse whose area differs from that of A by at most a constant factor. To increase the uprightness of a given subset A of the plane, we will then act on its "enclosing ellipse" using linear operators that map the grid to itself.

Definition 15 (Ellipse)**.** Let D be a positive definite real 2×2-matrix with non-zero determinant, and let $p \in \mathbb{R}^2$ be a point. The *ellipse defined by* D *and centered at* p is the set

$$E = \{u \in \mathbb{R}^2 \ ; \ (u-p)^\dagger D(u-p) \leqslant 1\}.$$

Proposition 16. *Let* A *be a bounded convex subset of* $\mathbb{R}^2$ *with non-empty interior. Then there exists an ellipse* E *such that* $A \subseteq E$*, and such that*

$$\mathrm{area}(E) \leqslant \frac{4\pi}{3\sqrt{3}}\,\mathrm{area}(A).$$

Proof. See theorems 5.17 and 5.18 of [10]. □

The uprightness of an ellipse can be expressed in terms of the entries of its defining matrix. Indeed, let D be the positive definite matrix defining some ellipse E and assume that the entries of D are as follows:

$$D = \begin{pmatrix} a & b \\ b & d \end{pmatrix}.$$

We can compute the area of E and the area of its bounding box using D:

$$\text{area}(E) = \pi/\sqrt{\det(D)} \quad \text{and} \quad \text{area}(\text{BBox}(E)) = 4\sqrt{ad}/\det(D).$$

Thus by Definition 14 we get:

$$\text{up}(E) = \frac{\text{area}(E)}{\text{area}(\text{BBox}(E))} = \frac{\pi}{4}\sqrt{\frac{\det(D)}{ad}}. \tag{7}$$

The uprightness of E is invariant under translation and scalar multiplication.

Definition 17 (Grid operator)**.** A *grid operator* is an integer matrix, or equivalently, a linear operator, that maps $\mathbb{Z}^2$ to itself. A grid operator G is called *special* if it has determinant ± 1, in which case G^{-1} is also a grid operator.

Remark 18. If A is a subset of $\mathbb{R}^2$ and G is a grid operator, then $G(A)$, the direct image of A, is defined as usual by $G(A) = \{G(v)\ ;\ v \in A\}$. If G is a grid operator and E is an ellipse centered at the origin and defined by D, then $G(E)$ is an ellipse defined by $(G^{-1})^\dagger D G^{-1}$.

Proposition 19. *Let E be an ellipse defined by D and centered at p. There exists a grid operator G such that $G(E)$ is $1/2$-upright. Moreover, if E is M-upright, then G can be efficiently computed in $O(\log(1/M))$ arithmetic operations.*

Proof. If E is an ellipse defined by a matrix D, we write $\texttt{Skew}(E)$ for the product of the anti-diagonal entries of D. Let A and B be the following special grid operators:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

and consider an arbitrary ellipse E. Since uprightness is invariant under translation and scaling, we may without loss of generality assume that E is centered at the origin and that D has determinant 1. Suppose moreover that the entries of D are as follows:

$$\begin{pmatrix} a & b \\ b & d \end{pmatrix}$$

We first show that there exists a grid operator G such that $\texttt{Skew}(G(E)) \leqslant 1$. Indeed, assume that $\texttt{Skew}(E) = b^2 \geqslant 1$. In case $a \leqslant d$, choose n such that $|na + b| \leqslant a/2$. Then we have:

$$A^{n\dagger} D A^n = \begin{pmatrix} \cdots & na+b \\ na+b & \cdots \end{pmatrix}.$$

Therefore, using Remark 18 with $G_1 = (A^n)^{-1}$, we have:

$$\texttt{Skew}(G_1(E)) = (na+b)^2 \leqslant \frac{a^2}{4} \leqslant \frac{ad}{4} = \frac{1+b^2}{4} = \frac{1+\texttt{Skew}(E)}{4} \leqslant \frac{2\ \texttt{Skew}(E)}{4} = \frac{1}{2}\texttt{Skew}(E).$$

Similarly, in case $d < a$, then choose n such that $|nd + b| \leqslant d/2$. A similar calculation shows that in this case, with $G_1 = (B^n)^{-1}$, we get $\texttt{Skew}(G_1(E)) \leqslant \frac{1}{2}\texttt{Skew}(E)$. In both cases, the skew of E is reduced by a factor of 2 or more. Applying this process repeatedly yields a sequence of operators $G_1, \ldots, G_m$ and letting $G = G_m \cdot \ldots \cdot G_1$ we find that $\texttt{Skew}(G(E)) \leqslant 1$.

Now let D' be the matrix defining $G(E)$, with entries as follows:

$$D' = \begin{pmatrix} \alpha & \beta \\ \beta & \delta \end{pmatrix}.$$

Then $\texttt{Skew}(G(E)) \leqslant 1$ implies that $\beta^2 \leqslant 1$. Moreover, since A and B are special grid operators we have $\det(D') = \alpha\delta - \beta^2 = 1$. Using the expression (7) for the uprightness of $G(E)$ we get the desired result:

$$\text{up}(G(E)) = \frac{\pi}{4}\sqrt{\frac{\det(D')}{\alpha\delta}} = \frac{\pi}{4\sqrt{\alpha\delta}} = \frac{\pi}{4\sqrt{\beta^2+1}} \geqslant \frac{\pi}{4\sqrt{2}} \geqslant \frac{1}{2}.$$

Finally, to bound the number of arithmetic operations, note that each application of G_j reduces the skew by at least a factor of 2. Therefore, the number n of grid operators required satisfies $n \leqslant \log_2(\texttt{Skew}(E))$. Now note that since D has determinant 1, we have:

$$M \leqslant \text{up}(E) = \frac{\pi}{4}\frac{1}{\sqrt{ad}} = \frac{\pi}{4\sqrt{b^2+1}}.$$

Therefore $\texttt{Skew}(E) = b^2 \leqslant (\pi^2/16M^2) - 1$, so that the computation of G requires $O(\log(1/M))$ arithmetic operations. □

We can now describe our algorithm to solve Problem 12. The algorithm inputs a bounded convex set A and we start by outlining the way in which the set A is given.

Remark 20. In the case of the present paper, a bounded convex set A is *given* if the following assumptions are satisfied.

(i) We are given an enclosing ellipse for A, whose area exceeds the area of A by no more than a constant factor (such an ellipse exists by Proposition 16).

(ii) We can efficiently decide, given $\alpha \in \mathbb{Z}[i]$ and $k, \ell \in \mathbb{N}$, whether or not $\alpha/\sqrt{5}^k\sqrt{2}^\ell$ belongs to A.

(iii) We can efficiently compute the intersection of any straight line in $\mathbb{Z}[i, 1/\sqrt{5}, 1/\sqrt{2}]$ and A.

Proposition 21. *There is an algorithm which, given a bounded convex subset A of $\mathbb{R}^2$ with non-empty interior, enumerates all solutions of the grid problem for A in order of increasing (k, ℓ). Moreover, if A is M-upright, then the algorithm requires $O(\log(1/M))$ arithmetic operations overall, plus a constant number of arithmetic operations per solution produced.*

Proof. Given A as in Remark 20, with an enclosing ellipse A' whose area only exceeds that of A by a fixed constant factor N, use Proposition 19 to find a grid operator G such that $G(A')$ is 1/2-upright. Then, enumerate the grid points of $\text{BBox}(G(A'))$ in order of increasing (k, ℓ). This can be done efficiently since $\text{BBox}(G(A'))$ is an upright rectangle. For each grid point u found, check whether it belongs to $G(A)$. This is the case if and only if $G^{-1}(u)$ is a solution to the grid problem for A with denominator exponent (k, ℓ). □

4.2 Diophantine equations

There is a well-known algorithm to solve Problem 13, i.e., to solve the equation:

$$\alpha^\dagger\alpha + \beta^\dagger\beta = 5^k 2^\ell, \tag{8}$$

for $\beta \in \mathbb{Z}[i]$, givenwhere $\alpha \in \mathbb{Z}[i]$ and $k, \ell \in \mathbb{N}$. First note that if we write $n = 5^k 2^\ell - \alpha^\dagger\alpha$ and $\beta = b + ic$, where $n, b, c \in \mathbb{Z}$, then Eq. (8) is equivalent to

$$n = b^2 + c^2. \tag{9}$$

The solutions to Eq. (9) were characterized by Euler:

Proposition 22 (Euler [3]). *Let n be a positive integer with prime factorization $p_1^{k_1} \ldots p_m^{k_m}$, where $p_1, \ldots, p_m$ are distinct positive primes. Then n can be written as the sum of two squares if and only if for all i either k_i is even or $p_i \equiv 1, 2 \pmod 4$.*

Proof. See Theorem 366 of [5]. □

Moreover, in case the equation $n = b^2 + c^2$ has a solution, there is an efficient probabilistic algorithm for finding b and c, given a prime factorization for n, see [9].

4.3 The approximate synthesis algorithm

We can now describe our algorithm to solve Problem 9.

Algorithm 23. Given θ and ε, let $A = \mathcal{R}_\varepsilon$ be the ε-region as defined in Eq. (6).

(i) Use Proposition 21 to enumerate the infinite sequence of solutions $\alpha/(\sqrt{5}^k\sqrt{2}^\ell)$ to the scaled grid problem for A in order of increasing least denominator exponent (k, ℓ).

(ii) For each such solution $\alpha/(\sqrt{5}^k\sqrt{2}^\ell)$ of least denominator exponent (k,ℓ):

(a) Let $n = 5^k 2^\ell - \alpha^\dagger\alpha$.

(b) Attempt to find a prime factorization of n. If $n \neq 0$ but no prime factorization is found, skip step (ii.c) and continue with the next α.

(c) Use the algorithm of Section 4.2 to solve the equation $\beta^\dagger\beta = n$. If a solution β exists, go to step (iii); otherwise, continue with the next α.

(iii) Define U as in Eq. (4) and use the exact synthesis algorithm of Proposition 7 to find a Clifford+V circuit for U. Output this circuit and stop.

Remark 24. By restricting ℓ to be equal to 0 throughout the algorithm and using Proposition 8 in step (iii), we obtain a method for the approximate synthesis of z-rotations in the Pauli+V basis.

4.4 Analysis of the algorithm

We now discuss the properties of Algorithm 23. The restricted algorithm of Remark 24 can be seen to enjoy the same properties.

4.4.1 Correctness

Proposition 25. *If Algorithm 23 terminates, then it yields a valid solution to the approximate synthesis problem, i.e., it yields a Clifford+V circuit approximating $R_z(\theta)$ up to ε.*

Proof. By construction, following the reduction of Problem 9 to Problem 11. □

4.4.2 Optimality in the presence of a factoring oracle

Proposition 26. *In the presence of an oracle for integer factoring, the circuit returned by Algorithm 23 has the smallest V-count of any single-qubit Clifford+V circuit approximating $R_z(\theta)$ up to ε.*

Proof. By construction, step (i) of the algorithm enumerates all solutions α to the scaled grid problem for $\mathcal{R}_\varepsilon$ in order of increasing least $\sqrt{5}$-denominator exponent k. Step (ii.a) always succeeds and, in the presence of the factoring oracle, so does step (ii.b). When step (ii.c) succeeds, the algorithm has found a solution of Problem 11 for a minimal k. □

4.4.3 Near-optimality in the absence of a factoring oracle

The proof that our algorithm is nearly optimal in the absence of a factoring oracle relies on the following number-theoretic hypothesis. We do not have a proof of this hypothesis, but it appears to be valid in practice.

Hypothesis 27. For each number n produced in step (ii.a) of Algorithm 23, write $n = 2^j m$, where m is odd. Then m is asymptotically as likely to be a prime congruent to 1 modulo 4 as a randomly chosen odd number of comparable size. Moreover, each m can be modelled as an independent random variable.

Lemma 28. *Let A be a bounded convex subset of $\mathbb{R}^2$, $k \geqslant 0$, and assume that the scaled grid problem for A has at least two distinct solutions with $\sqrt{5}$-denominator exponent k. Then for all $j \geqslant 0$, the scaled grid problem for A has at least 5^j+1 solutions with $\sqrt{5}$-denominator exponent $k+2j$.*

Proof. Let $\alpha \neq \beta$ be solutions of the scaled grid problem for A with $\sqrt{5}$-denominator exponent k. For each $\ell = 0, 1, \ldots, 5^j$, let $\phi = \frac{\ell}{5^j}$, and consider $\alpha_j = \phi\alpha + (1-\phi)\beta$. Then α_j has $\sqrt{5}$-denominator exponent $k+2j$. Also, α_j is a convex combination of α and β. Since A is convex, it follows that α_j is a solution of the scaled grid problem for A, yielding 5^j+1 distinct solutions with $\sqrt{5}$-denominator exponent $k+2j$. □

Lemma 29. *Fix an arbitrary constant $b > 0$. Then for $a \geqslant 1$,*

$$\sum_{x=1}^{\infty} \left(1 - \frac{1}{a + b\ln x}\right)^x = O(a).$$

Proof. The lemma is proved in Appendix E of [10]. □

Definition 30. Let U' and U'' be the following two solutions of the approximate synthesis problem

$$U' = \begin{pmatrix} \alpha' & -\beta'^{\dagger} \\ \beta' & \alpha'^{\dagger} \end{pmatrix} \quad \text{and} \quad U'' = \begin{pmatrix} \alpha'' & -\beta''^{\dagger} \\ \beta'' & \alpha''^{\dagger} \end{pmatrix}. \tag{10}$$

U' and U'' are said to be *equivalent solutions* if $\alpha' = \alpha''$.

Proposition 31. *Let k be the V-count of the solution of the approximate synthesis problem found by Algorithm 23 in the absence of a factoring oracle. Then*

(i) The approximate synthesis problem has at most $O(\log(1/\varepsilon))$ non-equivalent solutions with V-count less than k.

(ii) The expected value of k is $k''' + O(\log(\log(1/\varepsilon)))$, where k', k'', and k''' are the V-counts of the optimal, second-to-optimal, and third-to-optimal solutions of the approximate synthesis problem (up to equivalence).

Proof. If $\varepsilon \geqslant |1 - e^{i\pi/4}|$, then by Lemma 10 there is a solution of V-count 0 and the algorithm easily finds it. In this case there is nothing to show, so assume without loss of generality that $\varepsilon < |1 - e^{i\pi/4}|$. Then by Lemma 10, all solutions are of the form (4).

(i) Consider the list $\alpha_1, \alpha_2, \dots$ of candidates generated in step (i) of the algorithm. Let $k_1, k_2, \dots$ be their least $\sqrt{5}$-denominator exponent and let $n_1, n_2, \dots$ be the corresponding integers calculated in step (ii.a). Note that $n_j \leqslant 4 \cdot 5^{k_j}$ for all j. Write $n_j = 2^{z_j} m_j$ where m_j is odd. By Hypothesis 27, the probability that m_j is a prime congruent to 1 modulo 4 is asymptotically no smaller than that of a randomly chosen odd integer less than $4 \cdot 5^{k_j}$, which, by the well-known prime number theorem, is

$$p_j := \frac{1}{\ln(4 \cdot 5^{k_j})} = \frac{1}{k_j \ln 5 + \ln 4}. \tag{11}$$

By the pigeon-hole principle, two of k_1, k_2, and k_3 must be congruent modulo 2. Assume without loss of generality that $k_2 \equiv k_3 \pmod 2$. Then α_2 and α_3 are two distinct solutions to the scaled grid problem for $\mathcal{R}_\varepsilon$ with (not necessarily least) denominator exponent k_3. It follows by Lemma 28 that there are at least $5^r + 1$ distinct candidates of denominator exponent $k_3 + 2r$, for all $r \geqslant 0$. In other words, for all j, if $j \leqslant 5^r + 1$, we have $k_j \leqslant k_3 + 2r$. In particular, this holds for $r = \lfloor 1 + \log_5 j \rfloor$, and therefore,

$$k_j \leqslant k_3 + 2(1 + \log_5 j). \tag{12}$$

Combining (12) with (11), we have

$$p_j \geqslant \frac{1}{(k_3 + 2(1 + \log_5 j)) \ln 5 + \ln 4} = \frac{1}{(k_3 + 2) \ln 5 + 2 \ln j + \ln 4} \tag{13}$$

Let j_0 be the smallest index such that m_{j_0} is a prime congruent to 1 modulo 4. By Hypothesis 27, we can treat each m_j as an independent random variable. Therefore,

$$\begin{aligned} P(j_0 > j) &= P(n_1, \dots, n_j \text{ are not prime}) \\ &\leqslant (1 - p_1)(1 - p_2) \cdots (1 - p_j) \\ &\leqslant (1 - p_j)^j \\ &\leqslant \left(1 - \frac{1}{(k_3 + 2) \ln 5 + 2 \ln j + \ln 4}\right)^j. \end{aligned}$$

The expected value of j_0 is

$$E(j_0) = \sum_{j=0}^{\infty} P(j_0 > j) \leqslant 1 + \sum_{j=1}^{\infty} \left(1 - \frac{1}{(k_3 + 2) \ln 5 + 2 \ln j + \ln 4}\right)^j = O(k_3), \tag{14}$$

where we have used Lemma 29 to estimate the sum.

Next, we will estimate k_3. First note that if the ε region contains a circle of radius greater than $1/\sqrt{5}^k$, then it contains at least 3 solutions to the scaled grid problem for $\mathcal{R}_\varepsilon$ with denominator exponent k. The width of the ε-region $\mathcal{R}_\varepsilon$ is $\varepsilon^2/2$ at the widest point, and we can inscribe a disk of radius $r = \varepsilon^2/4$ in it. Hence the scaled grid problem for $\mathcal{R}_\varepsilon$, as in step (i) of the algorithm, has at least three solutions with denominator exponent k, provided that

$$r = \frac{\varepsilon^2}{4} \geqslant \frac{1}{\sqrt{5}^k},$$

or equivalently, provided that

$$k \geqslant 2\log_5(2) + 2\log_5(1/\varepsilon).$$

It follows that

$$k_3 = O(\log(1/\varepsilon)), \tag{15}$$

and therefore, using (14), also

$$E(j_0) = O(\log(1/\varepsilon)). \tag{16}$$

To finish the proof of part (i), recall that j_0 was defined to be the smallest index such that m_{j_0} is a prime congruent to 1 modulo 4. The primality of m_{j_0} ensures that step (ii.b) of the algorithm succeeds for the candidate α_{j_0}. Furthermore, because $m_{j_0} \equiv 1 \pmod 4$, the equation $\beta^\dagger\beta = n$ has a solution by Proposition 22. Hence the remaining steps of the algorithm also succeed for α_{j_0}.

Now let s be the number of non-equivalent solutions of the approximate synthesis problem of V-count strictly less than k. As noted above, any such solution U is of the form (4). Then the least denominator exponent of α is strictly smaller than k_{j_0}, so that $\alpha = \alpha_j$ for some $j < j_0$. In this way, each of the s non-equivalent solutions is mapped to a different index $j < j_0$. It follows that $s < j_0$, and hence that $E(s) \leqslant E(j_0) = O(\log(1/\varepsilon))$, as was to be shown.

(ii) Let U' be an optimal solution of the approximate synthesis problem, let U'' be optimal among the solutions that are not equivalent to U' and let U''' be optimal among the solutions that are not equivalent to either U' or U''. Assume that U', U'', and U''' are written as in (10) with top-left entry α', α'', and α''' respectively. Now let k', k'', and k''' be the least denominator exponents of α', α'', and α''', respectively. Let k_3 and j_0 be as in the proof of part (i). Note that, by definition, $k_3 \leqslant k'''$. Let k be the least denominator exponent of the solution of the approximate synthesis problem found by the algorithm. Then $k \leqslant k_{j_0}$. Using (12), we have

$$k \leqslant k_{j_0} \leqslant k_3 + 2(1 + \log_5 j_0) \leqslant k''' + 2(1 + \log_5 j_0).$$

This calculation applies to any one run of the algorithm. Taking expected values over many randomized runs, we therefore have

$$E(k) \leqslant k''' + 2 + 2E(\log_5 j_0) \leqslant k''' + 2 + 2\log_5 E(j_0). \tag{17}$$

Note that we have used the law $E(\log j_0) \leqslant \log(E(j_0))$, which holds because log is a concave function. Combining (17) with (16), we therefore have the desired result:

$$E(k) = k''' + O(\log(\log(1/\varepsilon))).$$

□

4.4.4 Time complexity

Proposition 32. *Algorithm 23 runs in expected time* $O(\text{polylog}(1/\varepsilon))$. *This is true whether or not a factorization oracle is used.*

Proof. This proposition is proved like the corresponding one in [10]. □

5 Conclusion

We have introduced an algorithm for the approximate synthesis of z-rotations into Clifford+V circuits. Our algorithm is optimal if an oracle for the factorization of integers is available. In the absence of such an oracle, our algorithm is still nearly optimal, yielding circuits of V-count $m + O(\log(\log(1/\varepsilon)))$, where m is the V-count of the third-to-optimal solution. We have also described an algorithm for the approximate synthesis of z-rotations into Pauli+V circuits. To the author's knowledge, these algorithms are the first optimal synthesis algorithms for extensions of the V-gates.

Acknowledgements

The author would like to thank Peter Selinger and Kira Scheibelhut for their helpful comments.

References

[1] A. Blass, A. Bocharov, and Y. Gurevich. Optimal ancilla-free Pauli+V circuits for axial rotations. Available from `arXiv:1412.1033`, Dec. 2014.

[2] A. Bocharov, Y. Gurevich, and K. M. Svore. Efficient decomposition of single-qubit gates into V basis circuits. *Phys. Rev. A*, 88:012313 (13 pages), 2013. Also available from `arXiv:1303.1411`.

[3] L. Euler. De numeris, qui sunt aggregata duorum quadratorum. *Novi Commentarii Academiae Scientiarum Imperialis Petropolitanae*, 4:3–40, 1758.

[4] B. Giles and P. Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Physical Review A*, 87:032332, 2013. Preprint available from `arXiv:1212.0506`.

[5] G. Hardy and E. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 6th edition, 2008.

[6] A. Harrow, B. Recht, and I. Chuang. Efficient discrete approximations of quantum gates. *Journal of Mathematical Physics*, 43, 2002. Also available from `arXiv:quant-ph/0111031`.

[7] A. Lubotzky, R. Phillips, and P. Sarnak. Hecke operators and distributing points on the sphere I. *Communications on Pure and Applied Mathematics*, 39:S149–S186, 1986.

[8] A. Lubotzky, R. Phillips, and P. Sarnak. Hecke operators and distributing points on S^2 II. *Communications on Pure and Applied Mathematics*, 40:401–420, 1987.

[9] M. O. Rabin and J. O. Shallit. Randomized algorithms in number theory. *Communications on Pure and Applied Mathematics*, 39:S239–S256, 1986.

[10] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. Available from `arXiv:1403.2975`, Mar. 2014.

[11] P. Selinger. Efficient Clifford+T approximation of single-qubit operators. *Quantum Information and Computation*, 15(1–2):159–180, 2015. Preprint available from `arXiv:1212.6253`.

[12] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. Also available from `arXiv:quant-ph/9508027`.