Efficient Topological Compilation for Weakly-Integral Anyon Model

Alex Bocharov*, Xingshan Cui†, Vadym Kliuchnikov*, and Zhenghan Wang*

* Quantum Architectures and Computation Group, Microsoft Research, Redmond, WA (USA)
† University of California, Santa Barbara, CA (USA)
• Station Q, Microsoft Research, Santa Barbara, CA (USA)

In a recent series of two research papers Cui, Wang and Hong proposed a class of anyonic models for universal quantum computation based on weakly-integral anyons. While universal set of gates cannot be obtained in this context by anyon braiding alone, designing a certain type of sector charge measurement provides universality.

From the mathematical standpoint the underlying unitary bases arising in various versions of the weakly-integral anyonic models are defined over a certain ring of Eisenstein rationals, that has useful number-theoretic properties. In this paper we develop a compilation algorithm to approximate arbitrary \( n \)-qutrit unitaries with asymptotically efficient circuits over the metaplectic anyon model, the most recent instance of the weakly-integral anyonic class. One flavor of our algorithm produces efficient circuits with upper complexity bound asymptotically in \( O(3^{2n} \log 1/\varepsilon) \) and entanglement cost that is exponential in \( n \). Another flavor of the algorithm produces efficient circuits with upper complexity bound in \( O(n 3^{2n} \log 1/\varepsilon) \) and no additional entanglement cost.

I. INTRODUCTION

Fault tolerance is becoming a key issue that will define success or failure of the future programmable quantum computers. Until relatively recently it was commonly accepted that quantum devices are to require vast amount of error correction to function reliably at desired fidelity level.

It is conjectured that certain quasiparticle species called non-abelian anyons provide a framework for coherent encoding of quantum information that will require little or no error correction. In particular Majorana non-abelian statistics (c.f. [1]) and Fibonacci non-abelian statistics (c.f. [2, 3]) have shown a great deal of promise for topologically-protected universal quantum computation.

Experimental progress on Majorana systems that support non-abelian objects such as Ising anyons and Majorana zero modes has been steady and encouraging [1]. But even if we succeed in controlling the Majorana systems, a missing topological \( \frac{\pi}{8} \)-gate for universality is a serious road-block for universal quantum computing. Theoretically, the ideal solution would be to control a Fibonacci system such as the fractional quantum Hall liquids at filling fraction \( \nu = \frac{12}{5} \), c.f. [4] or engineering a Fibonacci realization [5]. But this seems to be as hard engineering a \( \frac{\pi}{8} \)-gate in Majorana systems.

Braiding non-abelian objects such as anyons and zero-energy modes is the standard gate operation for topological quantum computation. But any physically realistic quantum operations are good for quantum information processing. Besides braiding in topological model or quantum circuit in the standard quantum circuit model, measurement is natural primitive for quantum computation. While measurements in the standard quantum circuit model in standard basis can always postponed to the end of computation, this cannot be done in topological quantum computation. Therefore, we could gain extra power for topological quantum computation by supplementing braiding with measurements. One physically realistic way to do measurements in topological quantum computation is to measure the total charge of a group of anyons. The measurement of the total charge can be done by either projective measurement or interferometric measurement. As is observed in [6], interferometric measurement is potentially more powerful than projective measurement—any projective measurement of the total charge can be simulated by interferometric measurement.

In [7], we pursue a qutrit generalization of the standard quantum circuit model. Some anyon systems are very natural for the implementation of qutrits, e.g. anyons with quantum dimension \( \sqrt{3} \). One such anyon system is \( SU(2)_4 \)—the first of the sequence of metaplectic anyons. While braiding alone for \( SU(2)_4 \) is not universal is just like the Majorana system, Majorana and metaplectic diverge when measurement is added. It is conjectured that any projective measurement of the total charge of a group of Ising anyons can also be simulated efficiently by classical computation, just as their braidings. We proved that for \( SU(2)_4 \), braiding supplemented by projective measurement of the total charge of a pair of metaplectic anyons is universal for qutrit quantum computation (see [7]).

Our motivation for metaplectic anyons is the potential realization of metaplectic anyons and metaplectic zero modes in physical systems. While Fibonacci is powerful for quantum computation, its realization and control seems to be hard. Majoranas are closer to be controlled well, their computational power is impacted by the high complexity and cost of a universal basis. Metaplectic model seems to strike the right balance between controllability and universality. Recently there is numerical evidence that \( SU(2)_4 \) might be realized in the \( \nu = \frac{8}{5} \) fractional quantum Hall liquid (see [8]). There are also theoretical set-ups to realize \( \mathbb{Z}_4 \)-parafermion zero modes in real materials (see [9]). Therefore, \( SU(2)_4 \) is a promising viable path to universal topological quantum compu-
In this paper we build upon the metaplectic model definition ([7]) and develop algorithms for effective synthesis of efficient multi-qutrit circuits over the model. Given a unitary target gate \(U\) and an arbitrary small target precision \(\varepsilon > 0\) a circuit approximating \(U\) to precision \(\varepsilon\) is considered \textit{efficient} if the number of primitive gates in that circuit is asymptotically proportional to \(\log \frac{1}{\varepsilon}\). An algorithm for synthesis of such efficient circuit is considered \textit{effective} it it can be completed on a classical computer in expected runtime that is polynomial in \(\log \frac{1}{\varepsilon}\).

We develop two flavors of an effective general synthesis algorithm.

The first flavor makes a distinction between the parameter approximation cost and entanglement cost in an efficient circuit and produces such circuits with upper complexity bound in \(O(32^n (\log_3 \frac{1}{\varepsilon} + n + \log(\log(1/\varepsilon)))) + O((9 (2 + \sqrt{3}))^n)\). The second flavor makes no such distinction and produces efficient circuits with upper complexity bound in \(O(n 3^2 n \log_3 \frac{1}{\varepsilon} + n + \log(\log(1/\varepsilon))))\). While the first flavor of our algorithm is clearly asymptotically superior when \(n\) is fixed and \(\varepsilon \to 0\), there is a practical tradeoff threshold between the two flavors when \(\varepsilon\) is fixed and \(n\) is growing. Leading terms of our upper bounds for both complexities are expressed in terms of specific leading coefficients, not merely in the big \(O\) terms.

The underlying mathematical apparatus for the algorithm is number-theoretic in nature and involves a credible number-theoretic conjecture that still remains to be proven.

For any range of practically interesting precisions the circuits produced by our algorithms are significantly more efficient (both in the asymptotical and practical sense) than any hypothetical circuits obtainable by Dawson-Neilsen flavor of Solovay-Kitaev algorithm (c.f. [10]).

We believe that our algorithm designs are more broadly applicable to other classes of weakly-integral anyons involving the quantum dimension of \(\sqrt{3}\), not just the metaplectic anyon model we have been focusing on here.

The paper is organized as follows:

in section II we give a formal definition of the primitive gate set and circuit complexity for the metaplectic model,

in section III we work out a description of the exactly representable single-qutrit states and single-qutrit unitaries over the model,

in section IV we lay the foundation of subsequent approximate synthesis by developing a method for approximation of two-level single-qutrit states,

in section V we generalize this approximation method to arbitrary two-level states,

section VI provides the last building block for the synthesis algorithm - the axial reflection.

In section VII we develop subalgorithms for approximate synthesis of two-level, diagonal and single-qutrit unitaries,

and in section VIII the general synthesis algorithm is introduced and the complexity bounds are derived.

II. TECHNICALITIES

Introduce \(\omega = e^{2\pi i/3}\).

The field of Eisenstein rationals \(\mathbb{Q}(\omega)\) is a quadratic extension of \(\mathbb{Q}\). \(\mathbb{Z}[\omega]\) is its integer ring. It has the group of units isomorphic to \(\mathbb{Z}_6\) generated by \(-\omega^2 = 1 + \omega\).

We introduce basic operations of the metaplectic anyon model and interpret them using matrices over the field of Eisenstein rationals.

Let \(|0\rangle, |1\rangle, |2\rangle\) be the computational basis of a standard qutrit.

1) The modified Hadamard gate \(H\) is defined as \(H|j\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^{2} \omega^{jk} |k\rangle\) and is described by the matrix

\[
\begin{pmatrix}
1 & 1 & 1 \\
1 & \omega & \omega^2 \\
1 & \omega^2 & \omega
\end{pmatrix}
\]

2) The increment gate \(\text{INC}\) is defined as \(\text{INC}|j\rangle = |j+1\rangle\mod 3\).

3) Operators \(Q_j = j = 0, 1, 2\) are represented by the matrices

\[
Q_0 = \begin{pmatrix}
\omega & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix},
Q_1 = \begin{pmatrix}
1 & 0 & 0 \\
0 & \omega & 0 \\
0 & 0 & 1
\end{pmatrix},
Q_2 = \begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & \omega
\end{pmatrix}
\]

4) The following two-qutrit gate is a generalization of the CNOT entangler: \(\text{SUM}|j,k\rangle = |j, (j+k)\mod 3\rangle\). It is described by the following matrix \(\text{SUM} = \frac{1}{\sqrt{3}} \left( \begin{array}{cccccc}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 \\
\end{array} \right)\)

The SUM may be considered a weakly-controlled increment gate.

5) The SWAP gate: \(\text{SWAP}|j,k\rangle = |k,j\rangle\).

6) The Flip gate defined as \(\text{Flip} = |0\rangle\langle 0| + |1\rangle\langle 1| - |2\rangle\langle 2|\) It is important to note that Flip is the elementary axial \textit{reflection} operator with respect to the basis vector \(|2\rangle\).

For that reason we will often use the \(R_{(2)}\) notation for the Flip.

As shown in [7], the \(H, \text{INC}, Q_0, \text{SUM}, \text{SWAP}\) gates can be implemented by anyon braiding alone but they generate a finite subgroup of \(SU(3^n)\) that coincides with the generalized Clifford subgroup.

Adding the Flip gate to the basis makes the basis universal for multi-qutrit quantum computation.
For both efficiency and convenience we will use a broader equivalent basis $B$ that also contains the $P_2$ gate $P_2 = \text{Flip} Q^2_2$ and its classical adjoints $P_0 = \text{INC} P_2 \text{INC}^\dagger$, $P_1 = \text{INC}^\dagger P_2 \text{INC}$.

The analysis and synthesis solutions proposed here are based on the following

Assumption. The cost of performing the classical single qutrit gates, the $H$ gate, the SUM or the SWAP gate is trivial (significantly lower) compared to the cost of performing a Flip gate.

Therefore we will be using the $R$-count as the measure of the cost of a quantum circuit of the basis $B$.

**Definition 1.** The $R$-count of a unitary circuit over the quantum basis $B$ is the minimal number of occurrences of the Flip gate in the circuit.

Remark: the $R$ in this definition underscores the important fact that the Flip gate is an elementary reflection operator. We could have called the measure "Flip-count" but it sounded too colloquial.

Note that $P_2^d = I$ and therefore there are exactly 15 distinct non-identity gates of the form $P^d_j, d = 0, \ldots, 5$. A $P^d_j$ gate requires a single Flip gate iff $d$ is odd. Thus there are nine gates $P^d_j, d = 1, 3, 5$ each with $R$-count of 1.

In the analysis and synthesis below it is also beneficial to track the $H$-count of a circuit:

**Definition 2.** The $H$-count of a unitary circuit over the quantum basis $B$ is the number of occurrences of the Hadamard gate $H$ in the circuit.

### III. EXACT REPRESENTATION OF SINGLE-QUTRIT UNITARIES OVER THE METAPLECTIC BASIS $B$

**Lemma 3.** If $|\psi\rangle$ is a unitary state the coefficients of which in computational basis are Eisenstein integers, then

1) One and only one coefficient is non-zero;

2) This non-zero coefficient is an Eisenstein integer unit;

3) $|\psi\rangle$ can be reduced to one of the computational basis states using at most one $P$ gate.

**Proof.** If $\psi_0, \ldots, \psi_N$ are the coefficients, then

$$\sum_{j=0}^N |\psi_j|^2 = 1.$$ 

Since for any $j$, $|\psi_j|^2$ is a non-negative integer, all the coefficients except one, some $\psi_j$, must be zeros, while $|\psi_j|^2 = 1$ and hence $\psi_j$ is a unit in $Z[\omega]$. Therefore $\psi_j = (-\omega^2)^d$ and $(-\omega^2)^{-d} \mod 6 \psi_j = 1$. Hence it is easy to find a $P$ gate of the form $G = I \otimes \ldots \otimes P^d_j \mod 6 \ldots \otimes I$ such that $G|\psi\rangle$ is a standard basis vector.

Let us introduce the finite ring $Z_3[\omega] = Z[\omega]/(3Z[\omega])$. This is a ring with exactly nine elements

$$\{0, 1, 2, \omega, 2 \omega, 1 + \omega, 1 + 2 \omega, 2 + \omega, 2 + 2 \omega\}.$$ 

Let $\rho : Z[\omega] \rightarrow Z_3[\omega]$ be the natural epimorphism. By construction, its kernel consists of elements that are divisible by 3.

Both the complex conjugation $* : Z[\omega] \rightarrow Z[\omega]$ and the norm map $|*|^2 : Z[\omega] \rightarrow \mathbb{Z}$ can be consistently factored down to the morphism $\tilde{*} : Z_3[\omega] \rightarrow Z_3[\omega]$ and the reduced norm map $|\tilde{*}|^2 : Z_3[\omega] \rightarrow Z_3$ (since both $\rho \tilde{*}$ and $|\tilde{*}|^2$ annihilate the kernel of $\rho$).

For the benefit of several future constructions we need to analyze the action of the group of Eisenstein units $EU = \{-\omega^2\}$ on $Z_3[\omega]$.

**Observation 4.** $Z_3[\omega]$ is split into three orbits under the action of the group $EU$ as follows:

1) The one-element orbit $O_0$ of 0; Note that $|0|^2 = 0$

2) The six-element orbit $O_1$ of 1; Note that for any $z \in O_1$, $|z|^2 = 1 \mod 3$.

3) The two-element orbit $O_2$ of $1 + 2 \omega$; Note that for any $z \in O_2$, $|z|^2 = 0 \mod 3$.

This split is established by direct computations.

**Observation 5.** Any gate in the group generated by $\{P_0, P_1, P_2\}$ can be effectively represented as a product of the global phase in $\{ \pm 1 \}$ and a circuit of the $R$-count of at most 1.

**Proof.** Clearly $\text{diag}(-1, -1, -1)$ is identity up to the global phase of $(-1)$ and has the $R$-count of 0. Similarly each of the gates $f_{01} = \text{diag}(-1, -1, 1), f_{02} = \text{diag}(-1, 1, -1), f_{12} = \text{diag}(1, -1, -1)$ is a Flip gate up to the global phase of $(-1)$ and has the $R$-count of 1. Now, any gate in the group generated by $\{P_0, P_1, P_2\}$ is of the form $\text{diag}((-\omega^2)^d_0, (-\omega^2)^d_1, (-\omega^2)^d_2) = \text{diag}(-1)^d_0, (-1)^d_1, (-1)^d_2) \times \text{diag}(\omega^2 d_0, \omega^2 d_1, \omega^2 d_2)$. The second factor in this product has the $R$-count of 0 by convention and the first factor is either $\pm I$ or one of the Flip gates or one of the $f_{01}, f_{02}, f_{12}$ gates and has the $R$-count of at most 1.

We start the single-qutrit synthesis case with an Eisenstein state reduction lemma as follows:

**Lemma 6** (Short column lemma). Let $|\psi\rangle$ be a unitary single-qutrit state of the form $|\psi\rangle = 1/\sqrt{-3}^L (u|0\rangle + v|1\rangle + w|2\rangle)$ where $u, v, w \in Z[\omega], L \in Z$. There exists an effectively computable circuit $c$ over the basis $B$ with $R$-count at most $L + 1$, $H$-count at most $L$ and global phase factor of at most 1 such that $c|\psi\rangle$ is a standard basis vector.

**Proof.** We will be proving the lemma by induction on $L$. For $L = 0$ the claim follows from the lemma 3.

Consider a state with denominator exponent $L > 0$.

Note that $\sqrt{-3} = 1 + 2 \omega$ and thus it is an Eisenstein integer. It follows, of course that $3 = (1 + 2 \omega)^2$ and thus 3 is divisible by both $1 + 2 \omega$ and $(1 + 2 \omega)^2$ in $Z[\omega]$.

The state $|\psi\rangle$ is immediately reducible to a state of the form $1/\sqrt{-3}^{L-1}(u' |0\rangle + v' |1\rangle + w' |2\rangle)$ if each of $u, v, w$ is divisible by $1 + 2 \omega$ and it is immediately reducible to
a state of the form $1/\sqrt{3}l^{2k-2}(u''|0\rangle+v''|1\rangle+w''|2\rangle)$ if each of $u, v, w$ is divisible by 3 in $\mathbb{Z}[\omega]$.

From the unitariness condition on $|\psi\rangle$ we have $|u|^2 + |v|^2 + |w|^2 = 3L$. Given $L > 0$, then $3L \mod 3 = 0$ and thus $(|u|^2 \mod 3) + (|v|^2 \mod 3) + (|w|^2 \mod 3) = 0$. By direct computation we check, however, that for any $z \in \mathbb{Z}[\omega], z^2 \mod 3$ is either 0 or 1. By simple exclusion argument for $(|u|^2 \mod 3) + (|v|^2 \mod 3) + (|w|^2 \mod 3) = 0$ to hold, either all the summands must be 0 or all the summands must be 1.

Let us distinguish the two cases.

Case 0: $(|u|^2 \mod 3) = (|v|^2 \mod 3) = (|w|^2 \mod 3) = 0$

As per the above observation 4 the residues $\rho(u), \rho(v), \rho(w)$ belong to the union of orbits $O_0$ and $O_2$.

In the edge case when all three belong to the orbit $O_0$, each of the $u, v, w$ is divisible by 3. As per earlier remark, $|\psi\rangle$ is reducible to the case of denominator exponent $L - 2$ and we do not need to apply any gates for this reduction.

More generally within the case 0 each of the residues $\rho(u), \rho(v), \rho(w)$ is divisible by $\rho(1 + 2\omega)$. However if $\rho(z)$ is divisible by $\rho(1 + 2\omega)$ then $z$ is divisible by $1 + 2\omega$ in the $\mathbb{Z}[\omega]$. Indeed, the divisibility of the residue implies that $z = (1 + 2\omega)z'' + 3z''', z'', z''' \in \mathbb{Z}[\omega]$, but, as we noted, 3 is divisible by $1 + 2\omega$ in the $\mathbb{Z}[\omega]$. Thus the general subcase allows reduction to the denominator exponent $L - 1$ without application of any gates.

Case 1: $(|u|^2 \mod 3) = (|v|^2 \mod 3) = (|w|^2 \mod 3) = 1$.

We are going to find a short circuit $c_L$ of R-count at most 2 such that $c_L|\psi\rangle$ is reduced to a case with denominator exponent at most $L - 1$. (This would complete the induction step.)

Let us observe first, that when $\rho(u) = \rho(v) = \rho(w) = r \in \mathbb{Z}_3[\omega]$ then $H|\psi\rangle$ is so reduced. Indeed, by direct computation, $H|\psi\rangle = 1/\sqrt{3}L_{-1}[u + v + w, u + \omega v + \omega^2 w, u + \omega^2 v + w + \omega w]$. We have $\rho(u + v + w) = 3 r = 0$, $\rho((u + v + w) + \omega w) = (1 + \omega^2 + \omega^2) r = 0$, $\rho((u + \omega^2 v + w) + (1 + \omega^2 + \omega^2) w) = 0$. Thus all the components of the $\{u + v + w, u + \omega v + \omega^2 w, u + \omega^2 v + w + \omega w\}$ are divisible by 3 and the claim follows from the earlier remark.

More generally $\rho(u), \rho(v), \rho(w)$ may be all different, but they must belong to the same orbit $O_1$ of the unit group $EU$. This means, in particular we can effectively find integers $d_u, d_w$ such that $\rho(u) = \rho((-\omega^2)^d_u v) = \rho((-\omega^2)^{d_w} w) = r \in \mathbb{Z}_3[\omega]$. Hence the short circuit $c_L = H P_1^{d_u} P_2^{d_w}$ prepares the state for reduction as claimed. As per the observation 5, $P_1^{d_u} P_2^{d_w}$ in this circuit is equivalent to a circuit of R-count at most 1 up to the possible global phase of $\pm 1$.

In all cases the short circuit $c_L$ has the H-count of at most 1.

This completes the induction step.

\[ |K\rangle \text{ is reduced to basis state at } R\text{-count of 2 as follows: } Q_0^P H P_0 H P_0 |K\rangle = |0\rangle. \]

Indeed, $(2 + i\sqrt{3}) = 2 + 3$ and the rightmost $P_0$ rotates $|K\rangle$ into $((-2 + 3(\omega + 1))|0\rangle + |1\rangle + |2\rangle)/3$, then under $H$ this collapses into $(1 + \omega)|0\rangle + \omega|1\rangle + \omega^2|2\rangle)/\sqrt{3}$.

The subsequent $H P_0$ term collapses this into $\omega|0\rangle$ and finally $Q_0^P$ yields $|0\rangle$.

Below we present the method suggested by the lemma 6 in algorithmic format.

\begin{algorithm}
\caption{Reduction of a short unitary column}
\begin{algorithmic}[1]
\Require $L \in \mathbb{Z}, u, v, w \in \mathbb{Z}[\omega]$
1: $\ket{\psi} \gets $ (empty)
2: while $L > 0$ do
3: \{$\nu u, \nu v, \nu w$\} $\mod 3$
4: \text{if } \nu u = \nu v = \nu v = 1 \text{ then}
5: \text{Find } d_u, d_w \in \{-2, -1, 0, 1, 2, 3\} \text{ such that}
6: \nu \equiv (-\omega^2)^{d_u} v, (-\omega^2)^{d_w} w \mod 3$
7: \{$u, v, w$\} $\leftarrow$ \{$u, (-\omega^2)^{d_u} v, (-\omega^2)^{d_w} w$\}
8: \{u, v, w\} $\leftarrow$
9: \{u + v + w, u + \omega v + \omega^2 w, u + \omega^2 v + \omega w\}$
10: \ret $\leftarrow$ $H P_1^{d_u} P_2^{d_w}$
11: \end if
12: \{u, v, w\} $\leftarrow$ \{u, v, w\}/(1 + 2\omega)
13: \text{L $\leftarrow$ L - 1}
14: \end while
15: \text{Implied } L = 0; \text{ Only one of } u, v, w \text{ is non-zero.}
16: \text{Find classical g.s. t. } g(u(0) + v(1) + w(2)) = u(0)$
17: \text{Find } d \in \{-2, -1, 0, 1, 2, 3\} \text{ such that } (-\omega^2)^d = u'$
18: \return $P_0^d$ \text{ \ret}
\end{algorithmic}
\end{algorithm}

We will need the following simple but important special case of lemma 6:

\begin{lemma}
Let $|\psi\rangle$ be a unitary single-qutrit state of the form $|\psi\rangle = 1/\sqrt{3}L_{-1}[v + w, u + w]$, where $v, w \in \mathbb{Z}[\omega], L \in \mathbb{Z}$. Then $|\psi\rangle$ is effectively and immediately reducible to a standard basis vector at the cost of at most one P gate.
\end{lemma}

\begin{proof}
We reuse remarks in the proof of lemma 6 to note that, whenever $L > 0$ then $|\nu|^2 \mod 3 = |w|^2 \mod 3 = 0$. This also implies that each of the $v, w$ is divisible by $1 + 2\omega = \sqrt{-3}$ in $\mathbb{Z}[\omega]$. Therefore, the state reduces algebraically to a unitary state of the form $|v'| |1\rangle + |w'| |2\rangle$ where $v', w' \in \mathbb{Z}[\omega]$ and the lemma follows for the lemma 3.
\end{proof}

\begin{theorem}[Single-qutrit exact synthesis theorem]
Consider a $3 \times 3$ unitary matrix of the form $U = 1/\sqrt{-3}M$ where $M$ is a $3 \times 3$ matrix over $\mathbb{Z}[\omega]$. Then $U$ is represented exactly by a circuit over $R$-count at most $L + 3$ and H-count at most $L$.
\end{theorem}

In order to prove the theorem, we handle the following special case first:

\begin{lemma}
Consider a $2 \times 2$ unitary matrix of the form $V = 1/\sqrt{-3}M$ where $M$ is a $2 \times 2$ matrix over Eisenstein integers. The $3 \times 3$ matrix $U = \begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix}$ can be
effectively reduced to identity by application of at most two \( P \) gates and at most one classical gate.

Proof. (Of the lemma.) Let \( 1/\sqrt{-3}^L [u, v, w]^T \) be the second column of the matrix \( U \). As per lemma 8 the column can be reduced to a standard basis vector using at most one \( P \) gate. Applying an appropriate classical gates if necessary we can force it to be 1 and thus \( U \) gets reduced to \( \text{diag}(1, 1, \varphi) \) where \( \varphi \in \mathbb{Z}[\omega] \) is a phase factor and thus an Eisenstein unit. Hence \( \varphi = (-\omega^2)^d, d \in \mathbb{Z} \) and \( D_2 \equiv 0 \mod 6 \) completes the reduction of the matrix to identity.

Proof. (Of the theorem.)
As per lemma 6 we can effectively find a unitary circuit \( c_1 \) of \( R \)-count at most \( L + 1 \) and \( H \)-count at most \( L \) that reduces the first column of \( U \) to a basis vector and, in fact \( \text{w.l.o.g. to 0} \).

Consider the matrix \( c_1 U \). Due to unitariness, it must be of the form \( \begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix} \) with \( V = 1/\sqrt{-3}^L M_1 \) where \( M_1 \) is a certain \( 2 \times 2 \) matrix over \( \mathbb{Z}[\omega] \).

As per lemma 10 this matrix can be effectively reduced to identity at the cost of at most two \( P \) gates.

Therefore we have effectively found a circuit \( c_2 \) with \( R \)-count at most \( L + 3 \) and \( H \)-count at most \( L \) such that \( c_2 U = I \) and thus \( U = c_2^{-1} \).

IV. SINGLE-QUTRIT STATE APPROXIMATION

A. Norm equation in Eisenstein integers

The ring of the Eisenstein integers \( \mathbb{Z}[\omega] \) is arguably the simplest cyclotomic ring ([11]).

In what follows we would need certain properties of the equation

\[
|z|^2 = n, \quad n \in \mathbb{Z}, \quad z \in \mathbb{Z}[\omega] \quad \quad (1)
\]

The two basic facts to deal with are: (a) the equation (1) is solvable with respect to \( z \) only for some of the right hand side values; (b) the complexity of solving the equation for \( z \) is no less than the complexity of factoring the integer \( n \).

The first thing to note is that \( |z|^2 \) is multiplicative in \( z \). Therefore if \( |z_1|^2 = n_1 \) and \( |z_2|^2 = n_2 \) then \( |z_1 z_2|^2 = n_1 n_2 \). Hence disregarding the integer factorization we only need to know the effective solvability of the equation when \( n \) is a power of a prime number. Moreover, since for \( p \in \mathbb{Z}, \quad |p|^2 = p^2 \), i.e. the equation is always solvable when \( n \) is a complete square, we only need the effective solvability when \( n \) is a prime number.

According to [11], if \( n \) is a positive prime number, the equation (1) is solvable if and only if \( n = 1 \mod 3 \).

Moreover, if \( n \) is a prime with \( n = 1 \mod 3 \) it is easy to obtain all the solutions of (1) at a runtime cost that is probabilistically polynomial in \( \log(n) \).

Here is the two step procedure to be used:

1) Compute \( m \in \mathbb{Z} \) such that \( m^2 = -3 \mod n \), using, for example, Tonelli-Shanks algorithm [12].
2) Compute \( z = GCD_Z(m + 2 \omega + 1, n) \)
3) Now \( \{(-\omega^2)^d z, (-\omega^2)^d z', d = 0, \ldots 5\} \) are the solutions of (1).

As a matter of principle we could limit ourself only to norm equations with integer prime right hand sides and thus sidestep the need for integer factorization.

If we pick an integer \( n \) at random from some interval \((B/2, B)\), then the probability that \( n \) is an integer prime with \( n = 1 \mod 3 \) is going to be in \( \Omega(1/\log(B)) \) (c.f. [13]).

While it is sufficient for establishing asymptotic properties of the algorithms we are about to design, for improved practical performance it is beneficial to be able to deal with easily solvable equations of the form (1), that is the ones where the integer \( n \) on the right hand side can be factored at some acceptable cost. A subset of solutions of the equation in this case is described by the following

Theorem 11. Let \( n \) be an integer, factored to the form \( n = m^2 p_1 \cdots p_\ell \), where \( m \in \mathbb{Z} \) and \( p_1 \cdots p_\ell \) are distinct positive integer primes.

Then
1) The equation (1) is solvable if and only if \( p_j = 1 \mod 3, j = 1, \ldots, \ell \).
2) If \( \{z_1, \ldots, z_\ell\} \) is a sequence of particular solutions of the equations \( |z_j|^2 = p_j, j = 1, \ldots, \ell \) then all of the following are solutions of the equation (1):

\[
z = m \text{Conj}^{d_1}[z_1] \cdots \text{Conj}^{d_\ell}[z_\ell], d \in \{0, 1\}^\ell \quad (2)
\]

where \( \text{Conj} \) is the complex conjugation operator.

Recall that an integer is smooth if it does not have prime factors above certain size [14]. Let us call an integer semi-smooth if it is a product of a smooth integer and at most one larger prime number.

In view of the theorem and the above effective procedure for solving a norm equation with a prime right hand side, solving a norm equation with semi-smooth right hand side is easy and can be effectively performed at the runtime cost that is polynomial in \( \log(n) \).

The distribution of smooth integers is described by the de Bruijn function [14]. Even though the density of semi-smooth numbers \( n \) for which the equation (1) is solvable in interval \((B/2, B)\), may still be in \( \Omega(1/\log(B)) \) asymptotically, in practice such integers are much more dense than the primes with \( n = 1 \mod 3 \).

Intuitively, in a random stream of norm equations easily solvable norm equations are not uncommon, and for large enough \( B > 0 \) we need to sample some \( O(\log(B)) \)}
integers \( n \in (B/2, B) \) to find, with sufficiently high probability, one that is semi-smooth and such that the equation (1) is solvable.

Approximation methods developed in the next subsection depend on the following more specific

**Conjecture 12.** Let \( k \) be an arbitrarily large positive integer and let \( u, v \in \mathbb{Z}[\omega] \) be randomly picked Eisenstein integers such that

\[
\Theta(3^k/2) \leq |u|^2 + |v|^2 \leq 3^k.
\]

Then for \( n = 3^k - |u|^2 - |v|^2 \) the equation (1) is easily solvable with probability that has uniform lower bound in \( \Omega(1/k) \).

**B. Approximation of single-qutrit states**

We start with the following

**Lemma 13.** Let \( |\psi\rangle \) be a unitary state of the form \( x|0\rangle + y|1\rangle \), \( x, y \in \mathbb{C}, |x|^2 + |y|^2 = 1 \) and let \( \varepsilon \) be small enough positive value. the unitary state \( |\psi\rangle \) can be approximated to precision \( \varepsilon \) by a unitary state for the form \((u|0\rangle + w|1\rangle + v|2\rangle)/\sqrt{3}^k\), \( u, v, w \in \mathbb{Z}[\omega], k \in \mathbb{Z} \) such that \( k \leq 4 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon))) \). The expected classical runtime required to do the approximation effectively is polynomial in \( \log(1/\varepsilon) \).

Before proving the lemma, let us make the following

**Proposition 14.** For a given complex number \( z \) with \( |z| \leq 1 \) and small enough \( \varepsilon > 0 \) there exists an integer \( k \leq 2 \log_3(1/\varepsilon) + 5 \) and an Eisenstein integer \( u \in \mathbb{Z}[\omega] \) such that \( |u/\sqrt{3}^k - z| < \varepsilon \) and \( |u/\sqrt{3}^k| \leq |z| \).

Set \( k_0 = \lceil 2 \log_3(1/\varepsilon) + 2 \log_3(2) + 2 \rceil \) and let \( \ell \) be a non-negative integer that can be arbitrarily large. For \( k = k_0 + \ell \) there are \( \Omega(3^\ell) \) distinct choices of Eisenstein integer \( u \) such that \( |u/\sqrt{3}^k - z| < \varepsilon \)

**Proof.** Note that \( |u/\sqrt{3}^k - z| = |u/\sqrt{3}^k - z)k| \), and we can simplify the statement a bit by relabeling \( z)k \) as \( z \).

We start by taking a geometric view on the feasibility of both claims in this proposition.

On the complex plain Eisenstein integers are found at the nodes of a hexagonal lattice spanned, for example, by 1 and \( 1 + \omega = +1/2 + i\sqrt{3}/2 \). These two lattice basis vectors are at the angle \( \pi/3 \) (and thus the entire lattice is a tiling of the plane with equilateral triangles of side length 1, see Figure 1). A circle of radius \( R \) centered at the origin contains at least \( 3R(R + 1) \) nodes of this lattice. As per general properties of integral lattices, a convex domain with large enough area \( A \) is to contain \( O(A) \) lattice nodes and, in this case, at least \( 3/\pi A \) nodes.

Desired Eisenstein integer \( u \) must be within \( \varepsilon \sqrt{3}^k \) from \( z \sqrt{3}^k \) and satisfy the side condition

\[
|u| \leq |z| \sqrt{3}^k \tag{3}
\]

Geometrically this means that \( u \) must belong to the intersection of the two circles \( B(k, \varepsilon) = \{|u| \leq |z| \sqrt{3}^k\} \cap |u - z \sqrt{3}^k| < \varepsilon \sqrt{3}^k \).

\( B(k, \varepsilon) \) is a convex domain and, when \( \varepsilon \) is sufficiently smaller than \( |z| \) it contains a sector of the smaller circle with the area of at least \( 1/2 (1 - \varepsilon/|z|) \varepsilon^2 3^k \). Thus (assuming \( \varepsilon < 2/3 |z| \)) if \( k \) is larger than \( k = \log_3(2/\varepsilon^2) + 1 \) then the area of \( B(k, \varepsilon) \) is greater than 1 and \( B(k) \) has a good chance of containing at least one node of the Eisenstein lattice. It may not contain one for a specific geometric configuration, but one notes that for \( k = k_0 + \ell \) the area of \( B(k, \varepsilon) \) grows exponentially in \( \ell \) so there exists a small constant \( \ell_0 \) such that for \( k_0 = \lfloor k \rfloor + \ell_0 \) the \( B(k_0, \varepsilon) \) contains an Eisenstein lattice node. It is geometrically obvious that from that point on for integer \( \ell > 0 \) the number of Eisenstein lattice points in \( B(k_0 + \ell, \varepsilon) \) grows as \( O(3^\ell) \).

We now propose a procedure for effectively finding such points in \( B(k, \varepsilon) \).

The task is reduced to the case when \( \pi/12 \leq \text{arg} \ z \leq 5 \pi/12 \). Indeed, the multiplication by the Eisenstein unit \(-\omega^2 = 1 + \omega \) is interpreted as a central rotation of the complex plane by the angle \( \pi/3 \) and an automorphism of the Eisenstein integer lattice. A complex number \( z \neq 0 \) lying in any of the six sectors \( \pi/12 + \pi/3 m \leq \text{arg} \ z \leq 5 \pi/12 + \pi/3 m \), \( m = 0, \ldots, 5 \) can be moved into the sector \( \pi/12 \leq \text{arg} \ z \leq 5 \pi/12 \) by applying zero or more of such rotations. An Eisenstein integer properly approximating
the rotated target can be rotated back into an Eisenstein integer approximating the original target.

We now assume that $k \geq \log_3(2/\varepsilon) + 2 = 2 \log_3(1/\varepsilon) + 2 \log_3(2) + 2$ (this is a convenient even if somewhat excessive assumption).

This implies that $\varepsilon \sqrt{3}^{-1} \geq 2 \sqrt{3}$ and $\varepsilon \sqrt{3}^k \geq 6$.

Considering $\pi/12 \leq \arg z \leq 5\pi/12$, the circle (3) contains the vertical segment $[z \sqrt{3}^k - i \varepsilon \sqrt{3}^k (2 \sin(\pi/12)), z \sqrt{3}^k]$ of length at least $1/2 \varepsilon \sqrt{3}^k$. Assuming, again, $\varepsilon < |z|$ the $B(k, \varepsilon/4)$ contains the vertical segment $V = [z \sqrt{3}^k - i \sqrt{3}^k \varepsilon/4, z \sqrt{3}^k]$.

We are now ready to build the desired Eisenstein integer $u = a + \delta b = (a - b/2) + i (b \sqrt{3}/2), a, b \in \mathbb{Z}$. We are going to choose $b$ such that $b \sqrt{3}/2$ is at a distance at most $(\varepsilon/4) \sqrt{3}^k$ from $\text{Im}(z) \sqrt{3}^k$. As per our choice of $k$ this implies that it is necessary and sufficient for the integer $b$ to belong to a segment of length $\varepsilon \sqrt{3}^{-1}/2 > \sqrt{3} > 1$.

Therefore at least one such integer exists and can be effectively picked.

Next one must find an integer $a$ such that $a = a - (\delta/2) + i (b \sqrt{3}/2) \in B(k, \varepsilon)$. As per the geometric condition $\arg z \leq 5\pi/12$, the circle (3) contains horizontal segment $H = [z \sqrt{3}^k - |z| \sqrt{3}^k \sin(\pi/12), z \sqrt{3}^k]$ of length at least $1/4 |z| \sqrt{3}^k$ and under $\varepsilon < |z|$ the $B(k, \varepsilon)$ contains horizontal segment $H' = [z \sqrt{3}^k - \varepsilon \sqrt{3}^k/4, z \sqrt{3}^k]$. By elementary geometric considerations $B(k, \varepsilon)$ also contains the horizontal segment $H'' = [z \sqrt{3}^k - i b \sqrt{3}/2 - 3/16 \varepsilon \sqrt{3}^k, z \sqrt{3}^k - i b \sqrt{3}/2]$ of length at least $3/16 \varepsilon \sqrt{3}^k$.

For our choice of $k$, $3/16 \varepsilon \sqrt{3}^k \geq 3/16 \times 6 > 1$. It is necessary and sufficient for the desired integer $a$ to belong to the segment $|\text{Re}(z) \sqrt{3}^k + b/2 - 3/16 \varepsilon \sqrt{3}^k, \text{Re}(z) \sqrt{3}^k + b/2|$ of length greater than 1 as we have just seen so the desired $a$ exists and can be effectively picked.

The geometry of this approximation procedure is shown schematically on Figure 2.

Set $k_0 = [2 \log_3(1/\varepsilon) + 2 \log_3(2) + 2]$. Let $\ell$ be some positive integer. Since the geometry of the problem for $k = k_0 + \ell$ is simply the geometry of the problem at $k = k_0$ scaled out by the factor of $\sqrt{3}$ then the segments we used above to pick the values of $b$ and $a$ are scaled out by a factor of $\Omega(\sqrt{3})$ and thus allow at least $\Omega(\sqrt{3})$ distinct choices of $b$ and at least $\Omega(\sqrt{3})$ distinct choices of $a$ for each choice of $b$. Therefore there are $\Omega(3^\ell)$ distinct Eisenstein integer $u$ yielding as many distinct approximations of $z$ as claimed.

\begin{proof}
For convenience we assume that $\varepsilon < 1$.

Let us do some preliminary analysis first.

We start by observing that for a unitary state $|\varphi\rangle$ to be within $\varepsilon$ of $|\psi\rangle$, it would suffice that

\begin{equation}
2 \text{Re}(|\langle \varphi | \psi \rangle|) > 2 - \varepsilon^2
\end{equation}

Consider some small $\delta > 0$ and a tri-level unitary state $|\varphi\rangle = u'|0\rangle + v'|1\rangle + w'|2\rangle$ and assume that $|u' - x| < \delta$, $|v' - y| < \delta$.

By direct computation

\begin{align*}
2 \text{Re}(u' x^*) &> |u'|^2 + |x|^2 - \delta^2 \\
2 \text{Re}(v' y^*) &> |v'|^2 + |y|^2 - \delta^2
\end{align*}

Hence $2 \text{Re}(\langle \varphi | \psi \rangle) > 2 - (|u'|^2 - |v'|^2) - 2 \delta^2$.

Expanding triangle inequalities $|u'| \geq |x| - |x' - u'|$, $|v'| \geq |y| - |y' - v'|$, we get $|u'|^2 + |v'|^2 \geq 1 - 2(|x| - x' + |y| - y' + |x - u'| + |y - v'|) + |x - u'|^2 + |y - v'|^2 \geq 1 - 4 \delta^2$.

Assuming w.l.o.g that $\delta^2 < \delta/2$ we conclude that $2 \text{Re}(\langle \varphi | \psi \rangle) > 2 - 5 \delta$.

Set $\delta = \varepsilon^2/5$ in order to satisfy the inequality (4) and start with $k_0 = [2 \log_3(1/\varepsilon) + 2 \log_3(2) + 2] \leq 4 \log_3(1/\varepsilon) + \log_3(5) + 5$.

We will look for a sufficient $k = k_0 + \ell$ where $\ell$ iterates sequentially through non-negative integers.

As per the Proposition 14 there exist several suitable Eisenstein integers $u, v$ such that $u/\sqrt{-3}$ is an $\delta$-approximation of $x$ and $v/\sqrt{-3}$ is a $\delta$-approximation of $y$. In fact as $\ell$ grows, there are $\Omega(9^\ell)$ distinct subunitary states $u/\sqrt{-3}^k |0\rangle + v/\sqrt{-3}^k |1\rangle$ that are $\delta$-close to $|\psi\rangle$.

To effectively prove the lemma it suffices to find one such state that can be completed to a unitary state $|\varphi\rangle = u/\sqrt{-3}^k |0\rangle + v/\sqrt{-3}^k |1\rangle + w/\sqrt{-3}^k |2\rangle$ for some $\ell$ that is not too large.

The sufficient inequality (4) does not explicitly involve $w$ and is satisfied for $\delta = \varepsilon^2/5$ as shown above.

By unitariness of the desired $|\varphi\rangle$, the $w \in \mathbb{Z}[\omega]$ must satisfy the equation
\[ |w|^2 = 3^k - |u|^2 - |v|^2 \] (5)

which is an instance of the norm equation (1). As we have seen in the subsection IV A, any particular instance of the norm equation is not necessarily solvable. However we are going to randomize the choice of \(u\) and \(v\) so that the Conjecture 12 becomes applicable.

To this end, let \(\ell\) be an integer iterating from 0 to some sufficiently large \(L\) and \(k = k_0 + \ell\) iterate with it. For each subsequent value of \(\ell\) we will inspect all the available \(u, v\) that generate \(\delta\)-approximations \(u/\sqrt{3^k}, v/\sqrt{3^k}\) of \(x, y\). As we have pointed out the number of such distinct \(u, v\) grows exponentially with \(\ell\). Assuming Conjecture 12 we only need to inspect as many as \(O(3^k - |u|^2 - |v|^2)) = O(k) = O(k_0 + \ell)\) of such distinct \(u, v\) to find one for which the equation \((5)\) is easily solvable with sufficiently high probability.

It is easy to see that there exists such \(\ell = O(\log(k_0))\) for which an easily solvable norm equation \((5)\) is obtained with near certainty. Therefore a desired unitary state 

\[
(u\ket{0} + v\ket{1} + w\ket{2})/\sqrt{3^k}
\]

will be obtained for some \(k = k_0 + O(\log(k_0)) \leq 4 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))\)

Finally we note that we only needed to inspect \(O(1)\) candidate pairs \(u, v\) for completion. Each inspection involved a decision whether the corresponding norm equation was easily solvable which incurred expected runtime cost that was polynomial in \(O(\log(3^k)) = O(k) = O(\log(1/\varepsilon))\), Therefore the overall expected runtime cost of the algorithm is also polynomial in \(O(\log(1/\varepsilon))\).

Below we present the method suggested by this lemma in pseudo-code format

**Algorithm 2** Approximation of a short state

**Require:** \(x, y \in \mathbb{C}; |x|^2 + |y|^2 = 1; \varepsilon > 0\)

1: \(\delta \leftarrow \varepsilon^2/5\)
2: \(k_0 \leftarrow \lfloor \log_3(1/\varepsilon) + \log_3(5) + 5 \rfloor\)
3: \(w \leftarrow \text{None}; k \leftarrow k_0 - 1\)
4: while \(w = \text{None}\) do
5: \(k \leftarrow k + 1\)
6: \(\text{enum} \leftarrow \text{enumerator for all } u, v \in \mathbb{Z}[\omega]\)
7: \(\text{s.t. } (u \ket{0} + v \ket{1})/\sqrt{3^k} \text{ is } \delta\text{-close to } x \ket{0} + y \ket{1}\)
8: while \(w = \text{None} \land \text{enum.Next} \) do
9: \((u, v) \leftarrow \text{enum.Current}\)
10: if Equation \(|z|^2 = 3^k - |u|^2 - |v|^2\) is easily solvable for \(z\) then
11: \(w \leftarrow z\)
12: end if
13: end while
14: end while
15: return \((u, v, w, k)\)

V. TWO-LEVEL STATE APPROXIMATION

In this section we develop an algorithm for effective approximation of an arbitrary \(n\)-qutrit unitary state with at most two non-zero components over the metaplectic basis.

For technical reasons we need the following two lemmas that are useful in their own right:

**Lemma 15.** Let \(\ket{b_1}\) and \(\ket{b_2}\) be two standard \(n\)-qutrit basis states. There exists an effectively and exactly representable classical permutation \(\pi\) such that \(\ket{b_2} = \pi \ket{b_1}\)

**Proof.** In the case of \(n = 1\) the \(\mathbb{Z}_3\) group generated by INC acts transitively on the standard basis \(\{\ket{0}, \ket{1}, \ket{2}\}\).

Consider \(\ket{b_i} = (b_{i1}, \ldots, b_{in})\), \(n \geq 1\), \(i = 1, 2\). Let \(\pi_j \in \{\text{INC, INC}^2\}\) be such that \(\pi_j(b_{1j}) = (b_{2j})\), \(j = 1, \ldots, n\).

Then \(\pi = \otimes_{j=1}^n \pi_j\) is the desired permutation.

**Lemma 16.** 1) For any two standard \(n\)-qutrit basis vectors \((\ket{j})\) and \((\ket{k})\) there exists a classical gate \(g\) that is exactly and effectively representable over \(\mathbb{B}\), such that for \(|j’\rangle = g(|j\rangle)\) and \(|k’\rangle = g(|k\rangle)\) \(|j’ - k’| < 3\).

2) Such a gate \(g\) can be effectively represented with at most \(2(n - 1)\) instances of the SUM and SWAP gates.

In other words, digital representations of \(j’\) and \(k’\) base 3 are the same except possibly for the least-significant base-3 digit.

**Proof.** At \(n = 1\) there is nothing to prove.

It is important to prove it for \(n = 2\). Since the subgroup of of local classical gates acts transitively on the standard basis, we can assume w.l.o.g. that \(j = 0\). Let \(k = 3k_1 + k_0\), where \(k_0, k_1 \in \{0, 1, 2\}\). If \(k_1 = 0\) there is nothing to prove. If \(k_0 = 0\) in suffices to set \(g = \text{SWAP}\). It remains to prove the claim for \(k \in \{4, 5, 7, 8\}\), but we have, explicitly:

| SWAP(00) = SUM(00) = 00 | SWAP SUM^2(11) = 01 |
| SWAP SUM(12) = 01 | SWAP SUM(21) = 02 |
| SWAP SUM^2(22) = 02 | |

Suppose \(n > 2\) and the lemma has been proven for multi-qutrit vectors in fewer than \(n\) qutrits.

By induction hypothesis, one can effectively find \((n-1)\)-qutrit classical gate \(g_{n-1}\) over \(\mathbb{B}\) such that \((g_{n-1} \otimes I) |j_1, \ldots, j_{n-1}, j_n\rangle = |j_1, \ldots, j_{n-1}, j_n'\rangle\) and \((g_{n-1} \otimes I) |k_1, \ldots, k_{n-1}, k_n\rangle = |k_1, \ldots, k_{n-1}, k_n'\rangle\) may differ only at the \((n-1)\)-st and \(n\)-th position.

Select a two-qutrit classical gate \(g_2\), as shown above, such that \(g_2|j_{n-1}', k_{n-1}'\rangle\) and \(g_2|k_{n-1}', j_{n-1}'\rangle\) differ only in the last position. Then, by setting \(g = (I^\otimes(n-2) \otimes g_2)(g_{n-1} \otimes I)\) we complete the induction step.
Corollary 17. 1) A two-level n-qutrit state $a_1 |b_1⟩ + a_2 |b_2⟩$ (where $|b_1⟩, |b_2⟩$ are elements of the standard basis) can be effectively classically reduced to one of the form $a_1 |c_1⟩ ... c_{n-1}, d⟩ + a_2 |c_1⟩ ... c_{n-1}, e⟩$, $c_1, ... , c_{n-1}, d, e ∈ [0, 1, 2]$.

2) Such reduction uses at most $2(n-1)$ instances of the SUM and SWAP gates.

Corollary 18. Given a two-level n-qutrit state $|ψ⟩ = x |b_1⟩ + z |b_2⟩$ and a small enough $ε > 0$, the state $|ψ⟩$ can be approximated to precision $ε$ by a state of the form $c |0⟩$ where $c$ is an effectively synthesizable circuit over $B$ containing at most $2(n-1)$ instances of SWAP and SUM gates and with $R$-count at most $4 \log_3(1/ε) + O(\log(\log(1/ε)))$.

Proof. We start by reducing $|ψ⟩$ to the form $x |a_1⟩ ... a_{n-1}, d⟩ + z |a_1⟩ ... a_{n-1}, f⟩$, $a_1, ... , a_{n-1}, d, f ∈ [0, 1, 2]$ using a classical circuit $b$ described in Corollary 17. Let $e ∈ [0, 1, 2]$ be the “missing” digit such that $(d, e, f)$ is a permutation of $(0, 1, 2)$.

Using Lemma 13 we can effectively approximates the single-qutrit state $x |d⟩ + z |f⟩$ by an Eisenstein state of the form $|φ⟩ = (u |d⟩ + v |f⟩)/\sqrt{3}$, $u, v ∈ \mathbb{Z}[\omega], k ∈ \mathbb{Z}$ to precision $ε$ with $k ≤ 4 \log_3(1/ε) + O(\log(\log(1/ε)))$.

Using Lemma 6 we can effectively synthesize a single-qutrit circuit $c_1$ over $B$ with $R$-count at most $k+1$ such that $c_1 |0⟩ = |φ⟩$.

Let $c_n = (f ⊗ (n-1) ⊗ c_1)$.

Clearly $b^1 c_n |a_1⟩ ... a_{n-1}, 0⟩$ is an $ε$-approximation of $|ψ⟩$. But $|a_1⟩ ... a_{n-1}, 0⟩$ can be prepared exactly from $|0⟩$ using at most $n-1$ local INC gates, which finalizes the desired circuit.

VI. IMPLEMENTATION OF AXIAL REFLECTION OPERATORS

Let $|b⟩$ be a standard n-qutrit basis state. Then an axial reflection operator $R_{|b⟩}$ is defined as $R_{|b⟩} = I ⊗ n - 2 |b⟩ ⟨b|$

Clearly, $R_{|b⟩}$ is represented by a diagonal matrix that has a $-1$ on the diagonal in the position corresponding to $|b⟩$ and $+1$ in all other positions.

In particular in the trivial case of $n = 1$ the basic Flip gate is the same as $R_{|2⟩}$. Also $R_{|0⟩} = INC Flip INC^2$ and $R_{|1⟩} = INC^2 Flip INC$.

It turns out that, in the general case as well, any two axial reflection operators are equivalent by conjugation with an effectively and exactly representable classical permutation. This follows from Lemma 15.

Since we consider the cost of classical permutations to be negligible compared to the cost of the Flip $R_{|2⟩}$ gate we hold that in the context of fixed $n$ all the n-qutrit axial reflection operators have essentially the same cost. In particular, we hold that the $R$-count of each of the single-qutrit operators $R_{|0⟩}, R_{|1⟩}, R_{|2⟩}$ is 1.

We are going to show in this section that all the n-qutrit axial reflection operators can be effectively and exactly represented.

In view of the above if suffices to represent just one such operator for each $n$. We start with somewhat special case of $n = 2$.

Observation 19. The circuit $(I ⊗ R_{|0⟩}) SUM(I ⊗ R_{|1⟩}) SUM(R_{|2⟩} ⊗ R_{|2⟩}) SUM$ is an exact representation of $(-1)R_{|20⟩}$

This is established by direct matrix computation.

We are going to generalize this solution to arbitrary $n ≥ 2$ and note that the occurrence of the global phase $(-1)$ is exceptional and happens only at $n = 2$.

Lemma 20. Given $n > 2$, denote by $2$ in the context of this lemma a string of $n-2$ occurrences of 2.

Then the circuit $e_{202} = (I ⊗ R_{|2⟩}) SUM_{1,2} (I ⊗ I ⊗ R_{|2⟩}) I ⊗ R_{|12⟩) SUM_{1,2} SWAP_{1,2} (I ⊗ R_{|22⟩}) SWAP_{1,2} (I ⊗ R_{|22⟩}) SUM_{1,2}$ is an exact representation of the operator $R_{|202⟩}$.

Proof. Let $|b⟩$ be an element of the standard n-qutrit basis. The circuit consists of diagonal operators and three occurrences of $SUM_{1,2}$. Let $|b_1 b_2 b⟩$ be the ternary representation of $|b⟩$ where $b$ stands for the substring of the $n-2$ least significant ternary digits of $b$. It is almost immediate that the circuit $e_{202}$ represents a diagonal unitary. Indeed, when the input is $|b_1 b_2 b⟩$ we can only get $±b_1 b_2 b⟩$, $±b_1 INC b_2 b⟩$ or $±b_1 INC^2 b_2 b⟩$, up to swap, after applying each subsequent operator of the circuit, and clearly we can only get $φ_{b_1 b_2 b}, φ = ±1$ after the entire circuit is applied.

The lemma claims that $φ = -1$ if and only if $b = 202$.

Consider the cases when $b_1 = 0$ or $b_2 = 1$. It is easy to see that, whatever is the value of $b_2$, one and only one of the operators $(I ⊗ R_{|0⟩})$, $(I ⊗ R_{|1⟩})$, $(I ⊗ R_{|2⟩})$ activates $R_{|2⟩}$ on $|b⟩$ and this activation always cancels out with $(I ⊗ I ⊗ R_{|2⟩})$ (since $R^2 = identity$ for any reflection $R$). So the result is identity.

If $b_1 = 2, b_2 ≠ 0$ the five rightmost operations of the circuit produce $|2⟩ ⊗ (INC^2 |b_2⟩) ⊗ (R_{|2⟩} |b⟩)$, an action that is subsequently canceled out by $I ⊗ I ⊗ R_{|2⟩}$. It is also easy to see that for $b_2 = 1$ or $b_2 = 2$ the remaining two reflections $R_{|0⟩}$ and $R_{|2⟩}$ amount to non-operations. Therefore the net result is identity.

We are left with the important case of $b_1 = 2, b_2 = 0$. By definition, $SUM_{1,2} |20⟩ = |22⟩$ and then the subsequence $SWAP_{1,2} (I ⊗ R_{|22⟩}) SWAP_{1,2} (I ⊗ R_{|22⟩})$ activates operator $R_{|2⟩}$ on $|b⟩$ twice, and of course these two activations cancel each other.

We proceed with $SUM_{1,2} |22⟩ = |21⟩$ and $I ⊗ R_{|12⟩}$ activates the $R_{|2⟩}$ on $|b⟩$ which is immediately cancelled out by the $I ⊗ I ⊗ R_{|2⟩}$. Finally $SUM_{1,2} |21⟩ = |20⟩$, and $I ⊗ R_{|0⟩}$ activates $R_{|2⟩}$ on $|b⟩$ as desired. This applies the factor of $-1$ if and only if $b = 2$, and that’s what is claimed.
Using this lemma we implement the operator $R_{[202]}$ exactly by linear recursion.

As we noted earlier, all the axial reflection operators in $n$ qutrits have the same $R$-count.

Denote this $R$-count by $rc(n)$.

**Observation 21.** $rc(n) = O((2 + \sqrt{5})^n)$ when $n \to \infty$.

**Proof.** We have $rc(1) = 1, rc(2) = 2$ (see Observation 19).

The recurrence $rc(n) = 4rc(n-1) + rc(n-2)$, $rp(1) = 1, rc(2) = 4$ can be solved in closed form as $rc(n) = ((2 + \sqrt{5})^n - (2 - \sqrt{5})^n)/(2\sqrt{5})$. Because $|2 - \sqrt{5}| < 1$ the $-(2 - \sqrt{5})^n$ term is asymptotically insignificant.

Thus the cost of the above exact implementation of the $n$-qutrit axial reflection operator is exponential in $n$. This defines several tradeoffs explored in the following sections.

**VII. APPROXIMATE SYNTHESIS OF SPECIAL TWO-LEVEL, DIAGONAL AND SINGLE-QUTRIT UNITARIES**

Let $|j\rangle$ and $|k\rangle$ be two distinct elements of the standard $n$-qutrit basis. Then a special two-level unitary with signature $[v; j, k]$ is a unitary operator of the form

$$I^\otimes n + (u - 1)|j\rangle\langle j| + v|j\rangle\langle k| - v^*|k\rangle\langle j| + (u^* - 1)|k\rangle\langle k|$$

where $|u|^2 + |v|^2 = 1$.

In other words, the matrix of a two-level unitary is different from the identity matrix in at most four locations and the determinant of a special two-level unitary is equal to 1.

**Lemma 22.** A special two-level unitary operator is effectively represented as a product of two reflection operators, each factor being a reflection with respect to a two-level $n$-qutrit vector.

**Proof.** We start with the well known fact that any $U \in SU(2)$ is effectively represented as a product of two reflections. For completeness we review the recipe for this factorization.

Let $\varphi$ be a real angle and consider the vector $v_{\varphi} = \cos(\varphi/2)|0\rangle + \sin(\varphi/2)|1\rangle$. By direct computation $e^{i\varphi Y} = R_{00} R_{v\varphi}$, where $Y$ is the Pauli matrix $i(|1\rangle\langle 0| - |0\rangle\langle 1|)$.

Any special unitary $U \in SU(2)$ can be effectively diagonalized to a diagonal special unitary of the form $e^{i\varphi Z}$ where $Z$ is the Pauli matrix $|0\rangle\langle 0| - |1\rangle\langle 1|$ (cf. [15]).

But $e^{i\varphi Z} = (s h)^i e^{i\varphi Y} (s h)$, where $s$ is the phase gate $|0\rangle\langle 0| + i|1\rangle\langle 1|$ and $h$ is the two-level Hadamard gate $(X + Z)/\sqrt{2}$.

In summary, $U \in SU(2)$ can be represented as $V e^{i\varphi Y} V^\dagger$ with some effectively computed unitary $V$ and the latter is equal to $R_{V|0\rangle} R_{V|v\rangle}$.

Consider now a multidimensional special two-level unitary $G = I^\otimes n + (u - 1)|j\rangle\langle j| + v|j\rangle\langle k| - v^*|k\rangle\langle j| + (u^* - 1)|k\rangle\langle k|$ and let $R_{G|0\rangle} R_{G|v\rangle}$ be the decomposition of the $SU(2)$ unitary $U = u|0\rangle\langle 0| + v|0\rangle\langle 1| - v^*|1\rangle\langle 0| + (u^* - 1)|1\rangle\langle 1|$ as outlined above. By way of notation, let $V |0\rangle = x_0 |0\rangle + z_0 |1\rangle$ and let $V v_\varphi = x_1 |0\rangle + z_1 |1\rangle$.

Consider two-level $n$-qutrit states $v_m = x_m |j\rangle + z_m |k\rangle, m = 0, 1$.

Clearly, $G = R_{v_0} R_{v_1}$.

**Corollary 23.** Let $\varepsilon > 0$ be small enough precision level. A special two-level unitary operator is effectively approximated to precision $\varepsilon$ by a circuit over $B$ containing two axial reflection operators and local gates with cumulative $R$-count at most $16 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$.

**Proof.** As per the above lemma, the subject operator is effectively represented as $R_{v_0} R_{v_1}$ where $v_0, v_1$ are two-level states.

As per corollary 18 each $v_m, m = 0, 1$ can be approximated to precision $\varepsilon/4\sqrt{2}$ by $c_m |0\rangle$ where $c_m$ is effectively synthesized circuit over $B$ of $R$-count at most $4 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$.

As per [16] the reflection $R_{v_m}$ is then approximated to $\varepsilon/2$ by $c_m^\dagger R_{00} c_m$ which is a circuit with one axial reflection and $R$-count at most $8 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$.

Therefore the subject operator is approximated to precision $\varepsilon$ by $c_0^\dagger R_{00} c_0 c_1^\dagger R_{00} c_1$ that contains two axial reflections and has $R$-count at most $16 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$ (in general case we do not expect any cancellations in the $c_0 c_1^\dagger$ that could reduce the $R$-count).

Let $N$ stand for $3^n$ in subsequent $n$-qutrit contexts.

**Corollary 24.** Let $D$ be an arbitrary $n$-qutrit diagonal unitary in general position and let $\varepsilon > 0$ be small enough precision level. $D$ can be effectively approximated, up to a global phase, to precision $\varepsilon$ by a circuit over $B$ containing $2(N-1)$ axial reflection operators and local gates with cumulative $R$-count at most

$$16(N - 1)(\log_3(1/\varepsilon) + n + O(\log(\log(1/\varepsilon))))$$

**Proof.** Removing a global phase we are left with $D' = \text{diag}(e^{i\theta_0}, e^{i\theta_1}, \ldots, e^{i\theta_{N-1}})$ where $\theta_j \in \mathbb{R}, j = 1, \ldots, N-1$ and $\sum_{j=0}^{N-1} \theta_j = 0$.

$D'$ can be easily decomposed into a product of $(N-1)$ special two-level diagonal unitaries: $D' = \prod_{j=1}^{N-1} D_j$, $D_j = I^\otimes n + (e^{i\Theta_j} - 1)|j\rangle\langle j| + (e^{-i\Theta_j} - 1)|j\rangle\langle j|$ where $\Theta_j = \sum_{k=1}^{j-1} \theta_k$.

It now suffices to approximate each $D_j$ to precision $\varepsilon/(N-1)$ using corollary 23 and tally the gate counts.
Algorithm 3 Implementation of a diagonal unitary

Require: \( \text{diag}(e^{i\theta_0}, e^{i\theta_1}, \ldots, e^{i\theta_{N-1}}) \)

1: \( \text{ret} \leftarrow \text{empty} \)
2: \( \bar{\theta} \leftarrow \frac{1}{N} \sum_{j=1}^{N-1} \theta_j \)
3: for \( j = 1, N - 1 \) do
4: \( \Theta \leftarrow \sum_{k=0}^{j-1} (\theta_k - \bar{\theta}) \)
5: \( D_j \leftarrow I^{\otimes n} + (e^{i\Theta} - 1)j)(j - 1) + (e^{i\Theta} - 1)j)(j) \)
6: \( \{ R_{j,1}, R_{j,2} \} \leftarrow \text{two-reflection-decomposition}(D_j) \) using corr. 23
7: \( \text{ret} \leftarrow \text{ret} R_{j,1}, R_{j,2} \)
8: end for
9: return \( \text{ret} \)

It is worthwhile to remember that our existing ancilla-free implementation of an \( n \)-qutrit axial reflection is exact but produces a circuit with \( R \)-count that is exponential in \( n \). This might be practically challenging for larger values of \( n \) when coarser values of the desired precision \( \epsilon \) are sufficient. In subsequent sections we point out an alternative, ancilla-assisted solution to this challenge.

Application of the above synthesis in case of \( n = 1 \) leads to a somewhat suboptimal circuit. A better solution for single-qutrit case is offered by the following

Lemma 25. \((\text{Approximation of a single-qutrit unitary.})\)

Any \( U \in U(3) \) is effectively approximated, up to a global phase to precision \( \epsilon \) by a circuit over \( \mathbb{B} \) with \( R \)-count in \( 48 \log_3(1/\epsilon) + O(\log(\log(1/\epsilon))) \)

Proof. Removing \( \det(U)^{1/3} \) as a global phase if needed we get \( U = \det(U)^{1/3}U' \) where \( U' \in SU(3) \).

It is well known (c.f. 4.5.1. in [15]) that \( U' \) can be effectively decomposed into three special two-level unitaries. Each of the two-level unitaries can be effectively approximated using corollary 23 into a circuit with two single-qutrit reflections and a collection gates with cumulative \( R \)-count in \( 16 \log_3(1/\epsilon) + O(\log(\log(1/\epsilon))) \). Note that the single-qutrit reflections each has a \( R \)-count of one and we just let this incremental count get absorbed into the \( O(\log(\log(1/\epsilon))) \) term.

\[ \text{VIII. APPROXIMATE SYNTHESIS OF ARBITRARY MULTI-QUTRIT UNITARIES} \]

We start this section with a somewhat special case of strictly controlled single-qutrit unitary.

\[ \text{A. Multicontrolled single-qutrit units, reflection style} \]

For \( V \in U(3) \) introduce \( C^n(V) \in U(3^{n+1}) \) where

\[ C^n(V) |j_1, \ldots, j_n, j_{n+1} \rangle = \begin{cases} |j_1, \ldots, j_n \rangle \otimes V |j_{n+1} \rangle, & j_1 = \cdots = j_n = 2 \\ |j_1, \ldots, j_n, j_{n+1} \rangle, & \text{otherwise.} \end{cases} \]

The \( C^4(\text{INC}) \) gate,

\[ C^4(\text{INC}) |j, k \rangle = |j, (k + \delta_{j,2}) \text{ mod } 3 \] is going to be of a particular interest in this context.

For technical reasons we need to cover the following special case:

Observation 26. \((\text{Controlled phase, reflection style.})\)

1) A diagonal unitary with only one non-zero phase, \( C^n(e^{i\theta}), \theta \in \mathbb{R}, \theta \neq 0 \) can be effectively emulated approximately to precision \( \epsilon \) by ancilla-assisted \((n+1)\)-qutrit circuit with \( R \)-count of at most \( 32 \log_3(1/\epsilon) + O(\log(\log(1/\epsilon))) \) plus the cost of two \((n+1)\)-qutrit axial reflections.

2) A strictly controlled single-qutrit phase factor \( C^n(e^{i\theta}I) \) can be effectively emulated approximately to precision \( \epsilon \) by ancilla-assisted \((n+2)\)-qutrit circuit with \( R \)-count of at most \( 16 \log_3(1/\epsilon) + O(\log(\log(1/\epsilon))) \) plus the cost of two \((n+1)\)-qutrit axial reflections.

Proof. 1) Add \((n+1)\)st qutrit as an ancilla prepared at state \( |0 \rangle \) and consider the following \((n+1)\)-qutrit diagonal unitary \( U = C^n(\text{diag}(e^{i\theta}, e^{-i\theta}, 1)) \). Clearly \( U \) emulates the \( C^n(e^{i\theta}) \) and it is also a special two-level unitary. As per the corollary 23 \( U \) can be effectively approximated by a circuit with \( R \)-count of at most \( 16 \log_3(1/\epsilon) + O(\log(\log(1/\epsilon))) \) plus the cost of two \((n+1)\)-qutrit axial reflections.

2) Follows from 1) and \( C^n(e^{i\theta}I) = C^n(e^{i\theta}) \otimes I. \)

Lemma 27. \((\text{Controlled single-qutrit unitary, reflection style.})\)

1) Given a \( V \in SU(3) \) integer \( n > 0 \) and a small enough \( \epsilon > 0 \), the \( C^n(V) \) can be effectively approximated to precision \( \epsilon \) by \((n+1)\)-qutrit circuit with \( R \)-count of at most \( 48 \log_3(1/\epsilon) + O(\log(\log(1/\epsilon))) \) plus the cost of six \((n+1)\)-qutrit axial reflections.

2) Given a \( V \in U(3) \) integer \( n > 0 \) and a small enough \( \epsilon > 0 \), the \( C^n(V) \) can be effectively approximated approximately to precision \( \epsilon \) by ancilla-assisted \((n+2)\)-qutrit circuit with \( R \)-count of at most \( 64 \log_3(1/\epsilon) + O(\log(\log(1/\epsilon))) \) plus the cost of eight \((n+1)\)-qutrit axial reflections.

Proof. This proof is a variation of the proof of the lemma 25.

A \( V \in U(3) \) can be effectively represented as a product of a global phase and three two-level special unitaries:

\[ V = e^{i\theta} V_1 V_2 V_3, \]

\( \theta = 0 \) iff \( V \in SU(3) \).

Each of the \( C^n(V_j), j = 1, 2, 3 \) is a special two-level unitary which can be effectively approximated to \( \epsilon/4 \) by a circuit with \( R \)-count of at most \( 16 \log_3(1/\epsilon) + O(\log(\log(1/\epsilon))) \) plus the cost of two \((n+1)\)-qutrit axial reflections.

If \( \theta \neq 0 \) we will need to deal additionally with the \( C^n(e^{i\theta}) \) factor which leads to the claim 2).
We note that the part of the implementation cost of $C^m(V)$ due to the cost of the axial reflections is in $O((2+\sqrt{3})^n)$ unless we find way of improving on the results of section VI. This could be a practical challenge when $n$ is large and $\varepsilon$ is coarse.

Therefore in the next subsection we explore a practical alternative that sometimes yields more efficient circuits.

B. Multicontrolled single-qutrit units, ancilla-assisted circuits.

Bullock et al. [17] offer a certain ancilla-assisted circuit that emulates $C^n(V)$ using only two-qudit (in our case - two-qutrit) gates.

The circuit requires $n-1$ ancillary qutrits, $4(n-1)$ instances of the $C^1(\text{INC})$ gate (see equation (6)) and one single $C^1(V)$ gate.

Here the width of required axial reflections does not exceed two and we are using only $O(n)$ of such reflections.

At this point we do not believe that the classical $C^1(\text{INC})$ gate can be represented exactly over $B$.

Therefore we must resort to approximating $C^1(\text{INC})$ to desired precision. Although the baseline solution might be based on decomposing the $C^1(\text{INC})$ into two special two-level unitaries, we can do twice better as per the following

**Lemma 28.** $C^1(\text{INC})$ (as defined by (6)) can be approximated to precision $\varepsilon$ by a pure unitary circuit over $B$ that contains at most $16 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$ occurrences of local Flip gates, at most $16 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$ occurrences of $H$ gate and two two-qutrit axial reflections.

**Proof.** We observe that $C^1(\text{INC})$ is the composition of two reflection operators: $\text{INC} = R_0 \otimes v_2 \ R_2 \otimes v_0$ where $v_0 = (|1\rangle - |2\rangle)/\sqrt{2}$, $v_2 = (|0\rangle - |1\rangle)/\sqrt{2}$.

As per Lemmas 13 and 6 each of the states $v_j$ is effectively approximated to precision $\varepsilon/2$ as $c_j |0\rangle$ where $c_j$ is a single-qutrit unitary circuit over $B$ with at most $4 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$ occurrences of $P$ gates and at most $4 \log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$ occurrences of the $H$ gate.

Therefore $C^1(\text{INC}) \approx (I \otimes c_2)R_{20}(I \otimes c_0)R_{20}(I \otimes c_1)$ to precision $\varepsilon$ with the upper bound on gate counts as claimed.

**Corollary 29.** Given a $V \in U(3^n)$, integer $n > 0$ and a small enough $\varepsilon > 0$, the $C^n(V)$ can be effectively emulated approximately to precision $\varepsilon$ by ancilla-assisted 2-n-qutrit circuit with $R$-count of at most $64 \ n \ (\log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon))))$.

**Proof.** We are emulating $4(n-1)$ instances of the $C^1(\text{INC})$ gate by using circuits from lemma 28 to the total $R$-count bounded by $64(n-1)(\log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon))))$ and a circuit for the $C^1(V)$ gate with the $R$-count bounded by $64(\log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon))))$ as per lemma 27.

The cost of required two-qutrit axial reflection is trivial in this case and we allow it to be absorbed by the $O(\log(\log(1/\varepsilon)))$ term.

Assuming ancillary qutrits are inexpensive one might compare the core entanglement cost bound of approximately $64(n-1)(\log_3(1/\varepsilon)$ suggested by the corollary 29 to the entanglement cost of approximately $1.8 (2+\sqrt{3})^n$ suggested by the lemma 27. Assuming the worst case scenario where the cost is close to the upper bounds, simple numeric simulation shows that we do not want to use the reflection-style implementation for $n > 6$ and we always want to use it for $n \leq 2$.

The intermediate tradeoff points are given in the following table:

| Qutrits | Ancilla-assisted favored when |
|---------|-----------------------------|
| $n = 3$  | $\varepsilon > 10^{-2}$     |
| $n = 4$  | $\varepsilon > 10^{-4}$     |
| $n = 5$  | $\varepsilon > 10^{-10}$    |
| $n = 6$  | $\varepsilon > 10^{-33}$    |

Since any two-level $n$-qutrit unitary is classically equivalent to a $C^{n-1}(V)$ we now have an ancilla-assisted alternative to the corollary 23 in form of the following

**Observation 30.** Let $n > 1$ be an integer and $\varepsilon > 0$ be small enough precision level. A special two-level unitary $n$-qutrit operator is effectively emulated to precision $\varepsilon$ by an ancilla-assisted circuit over $B$ in $2n-1$ qutrits with cumulative $R$-count at most $16(4n-7)(\log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon))))$.

**Proof.** Let $U \in U(3^n)$ be such operator. We can effectively find a classical circuit which reduces the operator to such two-level unitary $n$-qutrit operator $U'$ that acts non-trivially only on the standard basis vectors $|3^n-2\rangle$ and $|3^n-1\rangle$. Such $U'$ is $C^{n-1}(V)$ for the obvious special two-level single-qutrit unitary operator $V$. Using the ancilla-assisted decomposition described above, $C^{n-1}(V)$ can be emulated by a $2n-1$-qutrit circuit with $n-2$ ancillas composed of $4(n-2)$ instances of the $C^1(\text{INC})$ gate and one $C^1(V)$ gate. It remains to observe that $C^1(V)$ is a special two-level two-qutrit unitary that can be implemented by a circuit with the $R$-count at most $16(\log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon))))$ and containing two two-qutrit axial reflections. The latter reflections require a total of 8 instances of the $\text{Flip}$ gate and we allow this cost to be absorbed into the $O(\log(\log(1/\varepsilon)))$ term.

As per lemma 28 each of the $C^1(\text{INC})$ gates can also be implemented with $R$-count at most $16(\log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon))))$, and the observation follows herewith.
C. General $n$-qutrit unitaries

Let, again $N = 3^n$ for convenience.

In [18] Jesus Urias offers an effective $U(2)$ parametrization if the $U(N)$ group, whereby any $U \in U(N)$ is factored into a product of at most $N(N-1)/2$ special Householder reflections and possibly one diagonal unitary.

The reflections used in that decomposition are two-level reflections that in their two non-trivial dimensions take up the form

$$
\begin{pmatrix}
\sin(\varphi) & e^{i\theta} \cos(\varphi) \\
e^{-i\theta} \cos(\varphi) & -\sin(\varphi)
\end{pmatrix}
$$

This immediately leads to the following

**Theorem 31.** (General unitary decomposition, reflection style.) Given a $U \in U(N)$ in general position and small enough $\varepsilon > 0$ the $U$ can be effectively approximated up to a global phase to precision $\varepsilon$ by ancilla-free circuit over $B$ with $R$ count of at most $4(N + 4)(N - 1)(\log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon))))$ and at most $(N + 4)(N - 1)$ axial reflections (in $n$ qutrits).

**Proof.** This immediately follows from [18] and corollaries 23, 24.

Recalling that the exact circuits for axial reflections are currently somewhat expensive, one might consider the following

**Theorem 32.** (General unitary decomposition, ancilla assisted.) Given a $U \in U(N)$ in general position and small enough $\varepsilon > 0$ the $U$ can be effectively emulated up to a global phase to precision $\varepsilon$ by a circuit over $B$ in $2n - 1$ qutrits with $R$ count of at most $8(N + 2)(N - 1)(4n - 7)(\log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon))))$.

**Proof.** We perform initial decomposition as in [18] and use observation 30 to tally ancillas and $R$-count for the $N(N-1)/2$ special two-level unitaries in the decomposition. We also re-review corollary 24 and note that observation 30 applies to each of at most $(N-1)$ two-level unitaries required for implementation of the diagonal part of the decomposition.

We summarize the above two theorems in the following pseudo-code (algorithm 4):

```
\begin{algorithm}
\caption{Approximate decomposition of multi-qutrit unitaries}
\begin{algorithmic}
\Require $U \in U(3^n), \varepsilon > 0$, ancillaFlag
1: $U = D \prod_{k=1}^{K} U_k$ as per [18] \{Diagonal $D$ and two-level $U_k$\}
2: if ancillaFlag then
3: \quad ret \leftarrow ancilla assisted decomposition($D, \varepsilon$)
4: else
5: \quad ret \leftarrow decomposition($D, \varepsilon$) as per Corol. 24
6: end if
7: for $k = 1..K$ do
8: \quad if ancillaFlag then
9: \quad \quad $c \leftarrow$ decomposition($U_k, \varepsilon$) as per Observ. 30
10: \quad else
11: \quad \quad $c \leftarrow$ decomposition($U_k, \varepsilon$) as per Corol. 23
12: \quad end if
13: \quad ret \leftarrow ret $c$
14: end for
15: \Return ret
\end{algorithmic}
\end{algorithm}
```

It is notable that that the two flavors of the algorithm can be run in parallel on a multicore classical computer and the determination as to which flavor of the resulting circuit is better can be set as a post-determination. This approach is shown schematically in Figure 3.

**Algorithm 4** Approximate decomposition of multi-qutrit unitaries

**Figure 3:** Parallelizable control flow for the two flavors of the main algorithm.

**IX. CONCLUSION AND FUTURE WORKS**

We have developed two flavors of synthesis algorithm for compiling efficient approximation circuits over the metaplectic basis $B$ for arbitrary multi-qutrit unitaries.

The first flavor of the algorithm is ancilla-free and it
reduces the approximation of a target $n$-qutrit unitary to a circuit consisting of local gates, optimal number of the SUM and SWAP gates and $O(3^2n)$ instances of axial reflection gates. Each of the latter reflection gates can be represented exactly over the metaplectic basis at the cost of $O(2 + \sqrt{5})^n$ local single-qutrit axial reflections. This flavor of the algorithm is asymptotically optimal in the target precision $\varepsilon$ and is a good candidate for being practically optimal in $\varepsilon$, but it is unlikely to be optimal in terms of the entanglement cost which is an additive term in $O((2 + \sqrt{5})^n)$.

The second flavor of the algorithm requires $n$ ancillary qutrits to approximate a unitary on $n - 2$ primary qutrits. It uses approximate entanglers in order to side step the complexity of exact multiqutrit reflections. The resulting circuit contains local gates and two-qutrit entanglers only, but the overall $R$-count of the circuit gets inflated by a factor in $O(n)$ compared to the circuit approximated by the first flavor of the algorithm. This solution is not asymptotically optimal with respect to $\varepsilon$ but in practice it is more efficient for a certain domain in the $(n, \varepsilon)$ space (see table 1).

At this point we do not have theoretical lower bounds for the resource count of approximating circuits in the worst case or typical case. Establishing such bounds is the most important direction of the future work.

A. Other recent work

A different anyonic model that resulted from the collaboration of Microsoft Station Q with UCSB has been described very recently in [19]. It strives to map anyonic gates to the familiar multi-qubit scheme. The problem of effective and efficient circuit synthesis for this model is, predictably, quite open as of this writing.

ACKNOWLEDGMENTS

The Authors wish to thank Martin Roetteler for useful discussions.

[1] S. D. Sarma, M. Freedman, and C. Nayak, “Majorana zero modes and topological quantum computation,” (2015), 1501.02813.
[2] M. Freedman, M. Larsen, and Z. Wang, Comm. Math. Phys. 227(3), 605 (2002).
[3] M. Freedman, M. Larsen, and Z. Wang, Comm. Math. Phys. 228, 177 (2002).
[4] N. Read and E. Rezay, Phys. Rev. B59, 8084 (1999).
[5] R. S. K. Mong and et al., Phys. Rev. X 4, 011036 (2014).
[6] M. H. Freedman and C. I. Levallant, “Interferometry versus projective measurement of anyons,” (2015), 1501.01339.
[7] S. X. Cui and Z. Wang, J. Math. Phys. 56, 032202 (2015), doi/10.1063/1.491494.
[8] M. R. Peterson and et al., “Abelian and non-abelian states in nu=2/3 bilayer fractional quantum hall systems,” (2015), 1502.02671.
[9] K. S. D. J. Clarke, J. Alicea, Nature Commun. 4, 1348 (2013).
[10] C. Dawson and M. Nielsen, Quantum Information and Computation 6, 81 (2006).
[11] L. Washington, Introduction to Cyclotomic Fields (Springer, New York, 1997).
[12] D. Shanks, Proceedings of the Second Manitoba Conference on Numerical Mathematics, 51 (1973).
[13] M. Hazewinkel, Distribution of prime numbers in Encyclopedia of Mathematics (Springer, 2001).
[14] A. Granville, Smooth numbers: Computational number theory and beyond (Proc. of MSRI workshop, 2008).
[15] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, UK, 2000).
[16] V. Kluchnikov, “Synthesis of unitaries with clifford+t circuits,” (2013), 1306.3200.
[17] G. K. B. Stephen S. Bullock, Diann P. O’Leary, Physical Review Letters 94, 230502 (2005).
[18] J. Uriais, Journal of Mathematical Physics 51(7), 072204 (2010).
[19] C. Levaillant, B. Bauer, and P. B. M. Freedman, Z. Wang, “Fusion and measurement operations for su(2)/4 anyons,” (2015), 1504.02098.
[20] L. L. Scott, The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979) 37, 319 (1980).
[21] M. W. Liebeck, C. E. Praeger, and J. Saxl, Journal of the Australian Mathematical Society (Series A) 44, 389 (1988).

Appendix A: Two-qutrit classical gates generated by SUM and SWAP

It is currently not known what two-qutrit gates can be represented exactly over the $B$. In particular it is not known whether the important classical $C^1$(INC) gate (6) is so representable.

Let $S_B$ be the permutation group on 9 elements. There is a natural unitary representation of $S_B$ on $\mathbb{C}^9$ where a permutation $\pi$ is mapped to the unitary that extends the permutation $\pi$ applied to the standard basis vectors $\{00, \ldots, 22\}$. The image of this faithful representation coincides, by definition, with the group of all the classical two-qutrit gates. By a slight abuse of notation we also use $S_B$ to denote the image.

The following proposition addresses the maximality of the subgroup of 2-qutrit classical gates obtained from braiding.

**Proposition 33.** The group, $G$, generated by SUM, SWAP, and all the 1-qutrit classical gates is
a maximal subgroup of $S_9$.

Proof. Of course, one can always do a brute force computer search to verify this statement. Here we provide an elegant alternative proof. Let $AGL(2, \mathbb{F}_3) = GL(2, \mathbb{F}_3) \rtimes \mathbb{F}_3^2$ be the affine linear group acting on the 2-dimensional vector space $\mathbb{F}_3^2$. Explicitly, given $\varphi = (A, c) \in AGL(2, \mathbb{F}_3)$, $v \in \mathbb{F}_3^2$, we have $\varphi(v) = Av + c$. Note that $\mathbb{F}_3^2$ has in total 9 vectors, whose coordinates under the standard basis are $\{(i, j) | i, j = 0, 1, 2\}$. We identify the coordinate $(i, j)$ with the 2-qutrit basis vector $|i, j\rangle$.

Since elements of $AGL(2, \mathbb{F}_3)$ permute the 9 coordinates, we then have a group morphism $\psi: AGL(2, \mathbb{F}_3) \rightarrow S_9 \subset U(3^2)$, such that $\psi(A, c)|i, j\rangle = A(i,j) + c$.

For instance, let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, since $A(i,j) = (i+j, j)$, then $\psi(A) = \text{SUM}$. Similarly, one can check the following correspondences.

$$
\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \rightarrow \quad \text{SWAP}
$$

$$
\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \quad \rightarrow \quad \text{SWAP}
$$

$$
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \rightarrow \quad \text{INC} \otimes \text{ID}
$$

$$
\begin{pmatrix} 0 & 1 \end{pmatrix} \quad \rightarrow \quad \text{ID} \otimes \text{INC}
$$

It’s easy to check that the matrices(vectors) on the LHS of the above correspondences generate the group $AGL(2, \mathbb{F}_3)$ and the gates on the RHS generate $G$. Also, it’s not hard to verify that the map $\psi$ is injective and thus $G \cong AGL(2, \mathbb{F}_3)$. Now by O’Nan-Scott Theorem [20][21], $AGL(2, \mathbb{F}_3)$ is a maximal subgroup of $S_9$.

Therefore $G$ is a maximal subgroup of $S_9 \subset U(3^2)$. □

An immediate consequence of this proposition is that, as soon as the $C^1(\text{INC})$ gate is exactly representable over $B$ then all the classical two-qutrit gates are also exactly representable.