Efficient topological compilation for a weakly integral anyonic model

Alex Bocharov,[1,*] Xingshan Cui,[2] Vadym Kliuchnikov,[1] and Zhenghan Wang[2,3]
[1]*Quantum Architectures and Computation Group, Microsoft Research, Redmond, Washington 98052, USA*
[2]*University of California, Santa Barbara, Santa Barbara, California 93106, USA*
[3]*Station Q, Microsoft Research, Santa Barbara, California 93106, USA*
(Received 29 June 2015; revised manuscript received 24 August 2015; published 8 January 2016)

A class of anyonic models for universal quantum computation based on weakly-integral anyons has been recently proposed. 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. In this paper we develop a compilation algorithm to approximate arbitrary n-qutrit unitaries with asymptotically efficient circuits over the metaplectic anyon model. 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.

DOI: 10.1103/PhysRevA.93.012313

I. INTRODUCTION

Fault tolerance is becoming a key issue that will define the success or failure of future programmable quantum computers. Certain quasiparticles, called non-Abelian anyons, provide a framework for coherent encoding of quantum information that will require little or no error correction. Our primary goal is to propose an algorithm for efficient circuit synthesis (compilation) in one such non-Abelian framework.

Braiding non-Abelian objects such as anyons and zero-energy modes is the standard gate operation for topological quantum computation [1,2]. But any physically realistic quantum operations are good for quantum information processing. Besides braiding, measurement is a natural primitive for quantum computation. While measurements in the quantum circuit model in the computational basis can always be postponed to the end, this cannot be done in topological quantum computation. Therefore, we could gain extra computational power by supplementing braiding with measurements. One physically realistic measurement in topological quantum computation is to measure the total charge of a group of anyons, which can be done by either projective measurement or interferometric measurement.

In [3], 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 $\mathrm{SU}(2)_4$: the first in the sequence of metaplectic anyons [4]. While braiding alone for $\mathrm{SU}(2)_4$ is not universal as is the case with the Majorana system, the metaplectic system is no longer like Majorana when measurement is added. We proved that for $\mathrm{SU}(2)_4$, braiding supplemented by projective measurement of the total charge of a pair of metapletic anyons is universal for qutrit quantum computation (see [3]).

Our motivation for weakly integral anyon framework is the potential realization of metaplectic anyons and zero modes in physical systems. Majoranas are closer to being well controlled, but their computational power is impacted by the high complexity and cost of a universal basis [5]. Metaplectic models strike the right balance between controllability and universality. There is some recent numerical evidence that $\mathrm{SU}(2)_4$ might be realized in a $\nu = \frac{8}{3}$ fractional quantum Hall liquid (see [6]). There is also recent research potentially leading to practical recipes for synthesizing and braiding parafermionic zero modes in fractional quantum Hall liquids paired with s-wave superconductors (see [7]). These are essentially recipes generalizing the synthesis of Majorana zero modes in the same general setup. In particular, it is theoretically feasible that a species of Z_4-parafermion zero modes exhibiting $\mathrm{SU}(2)_4$ statistics can be realized along these lines [7]. Therefore, $\mathrm{SU}(2)_4$ is a promising viable path to universal topological quantum computation.

In this paper we build upon the metaplectic model definition [3] and develop algorithms for effective synthesis of efficient n-qutrit circuits over the model. Given a unitary target gate U and an arbitrary low target precision, $\varepsilon > 0$, a circuit approximating U to precision ε is considered *efficient* if the number of primitive gates in that circuit is asymptotically proportional to $\log 1/\varepsilon$. An algorithm for synthesis of such an efficient circuit is considered *effective* if it can be completed on a classical computer in the expected run time, which is polynomial in $\log 1/\varepsilon$.

We develop two flavors of an effective general synthesis algorithm. The first flavor makes a distinction between the parameter approximation cost and the entanglement cost in an efficient circuit and produces such circuits with an upper complexity bound in $O(3^{2n}\{\log_3 1/\varepsilon + 2n + \log[\log(1/\varepsilon)]\}) + O([9\,(2+\sqrt{5})]^n)$. The second flavor makes no such distinction and produces efficient circuits with an upper complexity bound in $O(n\,3^{2n}\,\{\log_3 1/\varepsilon + 2\,n + \log[\log(1/\varepsilon)]\})$. While the first flavor of our algorithm is clearly asymptotically superior when n is fixed and $\varepsilon \to 0$, there is obviously a practical trade-off threshold between the two flavors when ε is fixed and n is growing. The leading terms of our upper bounds for both complexities are expressed in terms of specific leading coefficients, not merely in the large O terms.

The technique for the algorithm is number-theoretic in nature. For any range of practically interesting precisions the

*alexeib@microsoft.com

circuits produced by our algorithms are significantly more efficient (in both the asymptotical and the practical sense) than any hypothetical circuits obtainable with the Dawson-Neilsen version of the Solovay-Kitaev algorithm (cf. [8]). Our algorithm designs are more broadly applicable to other classes of weakly integral anyons involving the quantum dimension of $\sqrt{3}$.

The paper is organized as follows: in Sec. II we provide a very brief introduction to the fundamental properties of metaplectic anyons, basic encodings, and quantum gates; in Sec. III the core circuit synthesis tools are developed, which are meant to reduce Householder reflections to axial reflections, and axial reflections are then described as metaplectic circuits in Sec. IV. In Secs. V and VI two approaches to synthesizing approximation circuits for arbitrary unitaries are introduced and compared, then a top-level overview of the synthesis flow is given in Sec. VII. Section VIII concludes the paper with some open problems and future work directions.

II. FUSION, BRAIDING, AND BASIC GATES

For completeness and readability we start with a very brief introduction to the concepts of braiding and fusion, focusing narrowly on the mathematical and logical side of these concepts. For a broader exposure the reader is encouraged to look up the available tutorials on the subject such as [9], [2], and [10].

A. Background on fusion and braiding of non-Abelian anyons

Anyons are quasiparticles described by a certain topological quantum-field theory (TQFT), and axiomatically this theory allows for a finite number of anyon species that have distinct values $\{\alpha,\beta,\gamma,\ldots\}$ of topological charge. For example, one of the simplest theories leads to Fibonacci anyons and allows only two values of charge, 1 and τ, where τ is the charge of a nontrivial anyon and 1 is the charge of "no anyon" or a vacuum ([10]).

Given an ensemble of anyons $(a_1, a_2, \ldots, a_n)$ the structure of their collective state space H depends on the underlying theory. If we measure the collective topological charge of some subsequence of anyons in the ensemble, say $(a_i, \ldots, a_j)$, $1 \leqslant i < j \leqslant n$, the charge will probabilistically assume some value $c \in \{\alpha, \beta, \gamma, \ldots\}$. After this is done, the state space of the ensemble is reduced to some smaller subspace $H_{i,j,c} \subset H$. This is the phenomenon known as *fusion* and the resulting topological charge is often called the *fusion charge*.

Once we have measured the fusion charge of several subsequences, we may end up with a one-dimensional state space or, up to a global phase, with one specific state. This state can be characterized by the collection of measurement outcomes, and it is an established practice to represent this collection as a tree, called the *fusion tree*.

As a segueway into the next subsection consider the following.

Example 1. The theory of *metaplectic anyons* allows five values of topological charge: $\{1,Z,X,X',Y\}$. Consider a quartet of anyons of type X, i.e., an ensemble (a_1,a_2,a_3,a_4) where each anyon a_i has charge X. Let us measure the charge c_{12} of the pair (a_1,a_2), then the charge c_{34} of the pair (a_3,a_4), and then the charge c_{14} of the entire quartet. This sequence of measurements is represented by the tree shown in Fig. 1.

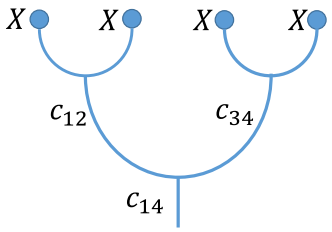

FIG. 1. A fusion tree for an anyonic quartet. The left pair of anyons has fusion charge c_{12}, the right pair has charge c_{34}, and the overall charge of the quartet is c_{14}.

Possible outcomes of fusion charge measurement are dictated by a set of *fusion rules*. A fusion rule has the following syntax:

$$a \otimes b = \sum_c N_{a\,b}^c\, c.$$

Here the left-hand side stands for the fusion of two systems with topological charges a and b. The $\sum_c$ on the right is a disjunction indexed by all possible outcomes (c) of fusing of the two systems. $N_{a\,b}^c$ is the multiplicity of the corresponding outcome c. Its meaning is: if a pair of anyons of types a and b happened to fuse to the charge c, then their collective state space have reduced to an $N_{a\,b}^c$-dimensional Hilbert space.

Example 2. [1] The following three rules are among the fusion rules of the metaplectic anyon theory:

$$\forall c \in \{1,Z,X,X',Y\}, \quad c \otimes 1 = 1 \otimes c = c, \tag{1}$$

$$X \otimes X = 1 + Y, \tag{2}$$

$$Y \otimes Y = 1 + Z + Y. \tag{3}$$

To simplify matters, we allow only multiplicities of 1 below. Suppose $(a_1,a_2,\ldots,a_n)$ is an ensemble of anyons and a sequence of topological charge measurements has been selected that defines a certain fusion tree structure. Then the number of distinct fusion trees that are allowed by the fusion rules is precisely the dimension of the Hilbert state space H of the ensemble, and there exists a basis in H whose elements are labeled by those distinct fusion trees. We describe a basis like this in the beginning of the next subsection.

While fusion bases are suitable for encoding quantum information, natively topologically protected gates on such encodings can be derived from braiding of non-Abelian anyons. Quite simply, braiding is either an exchange of two distinct anyons in an ensemble or the movement of a single anyon along a complete closed loop. In general, braiding causes a nontrivial unitary action on the state space. By the definition of "non-Abelian," these actions caused by different exchanges do not have to commute and the corresponding sets of unitary operators are not simultaneously diagonalizable. This creates the opportunity for building interesting and useful groups of unitary gates from braiding operations. Such groups are not always universal for quantum computation. Braiding happens to be universal in the case of Fibonacci anyons ([1]),

[1] The incomplete set of rules is sufficient for our purposes.

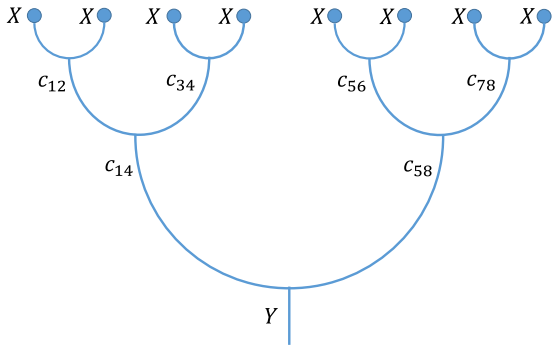

FIG. 2. A fusion tree for eight anyons. The overall charge is assumed to be Y. There are six fusion charges defining the specific fused state.

and in the case of metaplectic anyons below universality can be achieved with a little help from measurement.

B. Metaplectic basis and metaplectic circuits

The metaplectic anyon model is defined in [3] as an idealized multiqutrit model, where each qutrit is encoded using a specific quartet of $SU(2)_4$ anyons and thus an n-qutrit quantum register is encoded using $4n$ anyons. The model allows five values of topological charge $\{1,Z,X,X',Y\}$ and the relevant subset of fusion rules is listed in Example 2. We encode a standard qutrit using a quartet of anyons of type X prepared such that their joint topological charge is Y. The corresponding basis states can be labeled by fusion trees such as shown in Fig. 1 with the $c_{14} = Y$ constraint. It follows from the fusion rules that $(c_{12},c_{34}) \in \{(1,Y),(Y,1),(Y,Y)\}$.

One can do a similar analysis on the state space H of eight anyons of type X prepared such that their overall topological charge is Y. The possible charges that label a basis in H are shown in Fig. 2. Under the constraint $c_{14} = c_{58} = Y$ the system is reduced to a state in a nine-dimensional subspace $H' \subset H$ with an obvious *ad hoc* isomorphism of this subspace and $H_3 \otimes H_3$, where H_3 is the state space of the standard qutrit. We use H' to encode a standard two-qutrit register and call it the *computational subspace*. It is not difficult to compute the dimension of H. As per the fusion rules, (1)–(3), and by combinatorial enumeration, $\dim H = 21$. Thus H' is a proper subspace of codimension 12.

This analysis generalizes in a natural way to multiqutrit encodings with more than two qutrits. One should be cognizant that braiding of anyons from quartets encoding different qutrits (cf. Fig. 2) does not, in general, preserve the computational subspace, therefore we should only be deriving the multiqutrit gates from the subgroup of braids that do preserve H'.

The actual derivation of primitive gates is beyond the scope of this paper. Below we summarize the designs developed in [3]. Consider the one-qutrit fusion basis $\{|1,Y\rangle,|Y,1\rangle,|Y,Y\rangle\}$ introduced at the beginning of this subsection and relabel it $\{|0\rangle = -|Y,Y\rangle, |1\rangle = |1,Y\rangle, |2\rangle = |Y,1\rangle\}$ (the minus sign leads to nicer algebra). Introduce $\omega = e^{2\pi i/3}$ and $\gamma = e^{\pi i/12}$.

Braiding of the anyons constituting a qutrit amounts to a finite-image representation of the braid group B_4, where the generators of B_4 are represented by the following unitaries in the above basis:

$$\sigma_1 = \gamma\,\mathrm{diag}(1,\omega,1), \quad \sigma_3 = \gamma\,\mathrm{diag}(1,1,\omega),$$
$$\sigma_2 = \gamma^3 s_2, \quad s_2 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & \omega & \omega \\ \omega & 1 & \omega \\ \omega & \omega & 1 \end{pmatrix}. \tag{4}$$

We observe that, up to global phase, σ_1 is equivalent to $Q_1 = \mathrm{diag}(1,\omega,1)$, σ_3 is equivalent to $Q_2 = \mathrm{diag}(1,1,\omega)$, and σ_2 is equivalent to s_2.

For completeness we also need classical transpositions of the qutrit basis. By direct computation, $\tau_{0,1} = i\,(\sigma_3\,\sigma_2\,\sigma_3)^2$, $\tau_{0,2} = i\,(\sigma_1\,\sigma_2\,\sigma_1)^2$, where $\tau_{j,k}$ is the $|j\rangle \leftrightarrow |k\rangle$ transposition. Obviously $\tau_{0,1}$ and $\tau_{0,2}$ generate a faithful representation of the symmetric group S_3 on the qutrit, and in particular, in terms of notations in [3] we have $Q_0 = \tau_{0,1}\,\sigma_1\,\tau_{0,1}^\dagger = \tau_{0,2}\,\sigma_3\,\tau_{0,2}^\dagger$, $\mathrm{INC} = \tau_{0,2}\,\tau_{0,1}$, $\mathrm{INC}^\dagger = \tau_{0,1}\,\tau_{0,2}$, where INC is the increment gate defined by $\mathrm{INC}|j\rangle \mapsto |j+1 \mod 3\rangle$.

In the two-qutrit encoding explained above there is a certain braid explicitly composed of 92 anyon exchanges that preserves the computational subspace and, in the $|j\rangle \otimes |k\rangle$, $j,k = 0,1,2$ basis, implements the entangler

$$\mathrm{SUM}|j,k\rangle = |j,(j+k) \mod 3\rangle,$$

which is a natural qutrit generalization of the CNOT. It turns out that the gates designed above are not sufficient for the universal quantum computation, per [11]. They are known to generate a finite group that is projectively equivalent to the two-qutrit Clifford group. However, the *reflection gate*,[2]

$$R_{|2\rangle} = \mathrm{diag}(1,1,-1),$$

is outside the Clifford group and thus provides universality when added to the above gates.

The other two single-qutrit axial reflection operators are classically equivalent to $R_{|2\rangle}$: $R_{|0\rangle} = \tau_{0,2}\,R_{|2\rangle}\,\tau_{0,2}^\dagger$, $R_{|1\rangle} = \tau_{0,1}\,R_{|0\rangle}\,\tau_{0,1}^\dagger$. We collectively call these reflections the *R gates*. An R gate is implemented exactly via a certain *measurement-assisted repeat-until-success circuit with two ancillary qutrits*, as described in Lemma 5 in [3]. The circuit performs a probabilistic protocol that succeeds in three iterations on average (with the variance of the iterations to success equal to six). This is the most expensive protocol in our set so far,[3] and for the purposes of resource estimation, we take the following.

Assumption. The cost of performing any braiding-only (generalized Clifford) gate, including the SUM, is trivial compared to the cost of performing an R gate.

Therefore we use the *R count* as the measure of the cost of a quantum circuit.

Definition 3. A circuit composed of unitary gates introduced in this section is called a *metaplectic circuit*.

The R count of a metaplectic circuit is the minimal number of R gates in all equivalent representations of the circuit. All the generators of metaplectic circuits are defined by matrices that are populated by algebraic numbers, and it follows from

[2]Also called the Flip [12] gate elsewhere.

[3]However, this protocol is not nearly as expensive as a magic-state distillation.

[12] that the generator set is *efficiently universal*, meaning that for any target unitary operator G and small enough desired approximation precision ε, there exists a circuit of depth in $O(\log(1/\varepsilon))$ that approximates G to precision $<\varepsilon$. The main purpose of this paper is to develop an actual classically feasible algorithm for finding such efficient approximating circuits.

C. Useful additional gates

Here we expand the metaplectic basis defined in Sec. II B with additional useful gates.

1. P gates

$$P_j = I - (\omega^2+1)|j\rangle\langle j| = R_{|j\rangle}\, Q_j^2, \quad j = 0,1,2.$$

By design a P gate has an R count of 1. Any odd power of a P gate also has an R count of 1, while an even power of a P gate has an R count of 0. A useful observation regarding the cost of P-gate sequences is as follows.

Observation 4. 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, $\mathrm{diag}(-1,-1,-1)$ is identity up to the global phase of (-1) and has an R count of 0. Similarly, each of the gates $f_{01} = \mathrm{diag}(-1,-1,1)$, $f_{02} = \mathrm{diag}(-1,1,-1)$, and $f_{12} = \mathrm{diag}(1,-1,-1)$ is an R gate up to the global phase of (-1) and has an R count of 1.

Now, any gate in the group generated by $\{P_0, P_1, P_2\}$ is of the form $\mathrm{diag}((-\omega^2)^{d_0},(-\omega^2)^{d_1},(-\omega^2)^{d_2}) = \mathrm{diag}((-1)^{d_0},(-1)^{d_1},(-1)^{d_2}) \times \mathrm{diag}(\omega^{2d_0},\omega^{2d_1},\omega^{2d_2})$. The second factor in this product has an R count of 0 by convention and the first factor is either $\pm I$, or one of the R gates, or one of the f_{01}, f_{02}, f_{12} gates and has an R count of at most 1. ∎

2. The SWAP gate

While it is intuitively clear that the two-qutrit SWAP gate can be obtained by pure braiding, direct computation leads to the following.

Observation 5. $\mathrm{SWAP} = (\tau_{1,2} \otimes I)\mathrm{SUM}_{1,2}\mathrm{SUM}_{2,1}\mathrm{SUM}_{2,1}\mathrm{SUM}_{1,2}$.

Here $\tau_{1,2}$ is the single-qutrit transposition $|1\rangle \leftrightarrow |2\rangle$ (which can be expressed through already available transpositions as $\tau_{1,2} = \tau_{0,2}\tau_{0,1}\tau_{0,2}$). By the usual notation convention here and everywhere the $\mathrm{SUM}_{j,k}$ in the multiqutrit context is shorthand for the two-qutrit sum gate applied to the jth qutrit as the control and the kth qutrit as the target (tensored with the identity gates on all other qutrits).

3. Axial reflection

The following is key for our circuit synthesis.

Definition 6. Consider an integer $n \geqslant 1$ and let $|j\rangle, j = 0,\ldots,3^n-1$ be an element of the standard n-qutrit basis.

The operator $R_{|j\rangle} = I^{\otimes n} - 2\,|j\rangle\langle j|$ is called an n-qutrit *axial reflection* (operator). Clearly it is indeed a reflection with regard to the hyperplane orthogonal to $|j\rangle$.

III. EXACT SINGLE-QUTRIT AND APPROXIMATE TWO-LEVEL STATES

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

The two core tools needed for effective synthesis of metaplectic circuits are described in Lemmas 7 and 8 below.

Lemma 7 ("short-column" lemma). Consider a unitary single-qutrit state $|\psi\rangle = (u\,|0\rangle + v\,|1\rangle + w\,|2\rangle)/\sqrt{-3}^L$, where $u,v,w \in \mathbb{Z}[\omega]$, $L \in \mathbb{Z}$.

(1) There is an effectively synthesizable metaplectic circuit c with an R count of at most $L+1$ such that $c\,|\psi\rangle \in \{|0\rangle,|1\rangle,|2\rangle\}$.

(2) The classical cost of finding such a circuit is linear in L.

Before proving the lemma, we need to handle one special case and make one algebraic observation.

Lemma 8 (special case). 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 nonzero.

(2) This nonzero 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 ψ_{j_*}, must be 0's, while $|\psi_{j_*}|^2 = 1$ and hence ψ_{j_*} is a unit in $\mathbb{Z}[\omega]$. 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 $G = I \otimes \ldots P_j^{-d \mod 6} \ldots \otimes I$ such that $G|\psi\rangle$ is a standard basis vector. ∎

Let us introduce the finite ring $\mathbb{Z}_3[\omega] = \mathbb{Z}[\omega]/(3\,\mathbb{Z}[\omega])$. 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 $\rho : \mathbb{Z}[\omega] \to \mathbb{Z}_3[\omega]$ be the natural epimorphism. By construction, its kernel consists of elements that are divisible by 3. Both the complex conjugation $*:\mathbb{Z}[\omega]\to\mathbb{Z}[\omega]$ and the norm map $|*|^2 : \mathbb{Z}[\omega]\to\mathbb{Z}$ can be consistently factored down to the morphism $\tilde{*} : \mathbb{Z}_3[\omega] \to \mathbb{Z}_3[\omega]$ and the reduced norm map $|\tilde{*}|^2 : \mathbb{Z}_3[\omega] \to \mathbb{Z}_3$ (since both $\rho *$ and $|*|^2 \mod 3$ annihilate the kernel of ρ). For the benefit of several future constructions we need to analyze the action of the group of Eisenstein units $\mathrm{EU} = \{-\omega^2\}$ on $\mathbb{Z}_3[\omega]$.

Observation 9. $\mathbb{Z}_3[\omega]$ is split into three orbits under the action of the group EU as follows:

0. The one-element orbit O_0 of 0. Note that $|0|^2 = 0$.

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

2. 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.

Proof (of Lemma 7). We prove the lemma by induction on L. For $L = 0$ the claim follows from Lemma 8.

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 $\mathbb{Z}[\omega]$.

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 $1/\sqrt{-3}^{L-2}(u''\,|0\rangle + v''\,|1\rangle + w''\,|2\rangle)$ if each of u, v, w is divisible by 3 in $\mathbb{Z}[\omega]$. From the unitariness condition on $|\psi\rangle$ we have $|u|^2+|v|^2+|w|^2 = 3^L$. Given $L>0$, then $3^L \mod 3 = 0$ 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: $(|u|^2 \mod 3)=(|v|^2 \mod 3)=(|w|^2 \mod 3)=0$.

Per Observation 9 (above) the residues $\rho(u)$, $\rho(v)$, $\rho(w)$ belong to the union of orbits O_0 and O_2. In the edge case where all three belong to the orbit O_0, each of u, v, and w is divisible by 3. Per our 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 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 $\mathbb{Z}[\omega]$. Indeed, the divisibility of the residue implies that $z=(1+2\,\omega)\,z'+3\,z''$, $z',z''\in\mathbb{Z}[\omega]$, but as noted, 3 is divisible by $1+2\,\omega$ in $\mathbb{Z}[\omega]$. 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 1 such that $c_L\,|\psi\rangle$ is reduced to a case with denominator exponent at most $L-1$. (This would complete the induction step.)

Suppose first that $\rho(v)=\rho(w)=\omega^2\,\rho(u)\in\mathbb{Z}_3[\omega]$, which means that $v=\omega^2\,u+3\,v'$, $w=\omega^2 u+3w'$ for some $v',w'\in\mathbb{Z}[\omega]$, and it follows that $s_2\,|\psi\rangle = (-(u+\omega\,v'+\omega\,w')\,|0\rangle - (v'+\omega\,w')\,|1\rangle - (\omega\,v'+w')\,|2\rangle))/\sqrt{-3}^{L-1}$. Thus, in this particular special case the denominator exponent is reduced to $L-1$ by application of the single s_2 gate that has R count 0.

In general, since $(|\omega^2\,u|^2 \mod 3)=(|u|^2 \mod 3)=(|v|^2 \mod 3)=(|w|^2 \mod 3)=1$, then $\omega^2\,\rho(u)$, $h\rho(v)$, $\rho(w)$ must belong to the same orbit O_1 of the unit group EU. This means, in particular, that we can effectively find integers d_v, d_w such that $\omega^2\,\rho(u)=\rho((-\omega^2)^{d_v}\,v)=\rho((-\omega^2)^{d_w}\,w)=r\in\mathbb{Z}_3[\omega]$. Hence the short circuit $c_L=s_2\,P_1^{d_v}\,P_2^{d_w}$ reduces the state as shown. Per Observation 4, $P_1^{d_v}\,P_2^{d_w}$ in this circuit is equivalent to a circuit of R count at most 1 up to the possible global phase of ±1. This completes the induction step. ■

Example 10. Consider unitary column $|K\rangle = ((2+i\,\sqrt{3})\,|0\rangle + |1\rangle + |2\rangle)/3$.

$|K\rangle$ is reduced to the basis state at an R count of 2 as follows: $s_2\,R_{|0\rangle}\,Q_1^2\,Q_2^2\,s_2\,R_{|0\rangle}\,|K\rangle = |0\rangle$.

Note that

$$s_2\,R_{|0\rangle}\,Q_1^2\,Q_2^2\,s_2\,R_{|0\rangle} = -\omega\,\sigma_2\,R_{|0\rangle}\,\sigma_1^2\,\sigma_3^2\,\sigma_2\,R_{|0\rangle}.$$

In Algorithm 1 we present the method suggested by Lemma 7 in algorithmic format.

Algorithm 1 Reduction of a short unitary column.

Require: $L\in\mathbb{Z}$, $u,v,w\in\mathbb{Z}[\omega]$
1. $ret \leftarrow \langle\text{empty}\rangle$
2. **while** $L>0$ **do**
3. $\{vu,vv,vw\}=\{|u|^2,|v|^2,|w|^2\} \mod 3$
4. **if** $vu=vv=vw=1$ **then**
5. Find $d_v,d_w\in\{-2,-1,0,1,2,3\}$ such that
6. $\omega^2\,u\equiv(-\omega^2)^{d_v}\,v\equiv(-\omega^2)^{d_w}\,w \mod 3$
7. $\{u,v,w\}\leftarrow\{u,(-\omega^2)^{d_v}\,v,(-\omega^2)^{d_w}\,w\}$
8. $v'\leftarrow(v-\omega^2\,u)/3$; $w'\leftarrow(w-\omega^2\,u)/3$
9. $\{u,v,w\}\leftarrow$
10. $\{-(u+\omega\,v'+\omega\,w'),-(v'+\omega\,w'),-(\omega\,v'+w')\}$
11. $ret\leftarrow s_2\,P_1^{d_v}\,P_2^{d_w}\,ret$
12. **else**
13. $\{u,v,w\}\leftarrow\{u,v,w\}/(2\,\omega+1)$
14. **end if**
15. $L\leftarrow L-1$
16. **end while**
17. Implied $L=0$; Only one of u,v,w is nonzero.
18. Find classical g s. t. $g(u|0\rangle+v|1\rangle+w|2\rangle)=u'|0\rangle$
19. Find $d\in\{-2,-1,0,1,2,3\}$ such that $(-\omega^2)^d=u'$
20. **return** $P_0^{-d}\,g\,ret$

Lemma 11. Consider a "two-level" unitary single-qutrit state $|\varphi\rangle = x\,|0\rangle + y\,|1\rangle + z\,|2\rangle$ where $x\,y\,z=0$ and let ε be an arbitrarily small positive number.

(1) There is a family of effectively synthesizable states of the form $|\psi_\varepsilon\rangle=(u_\varepsilon\,|0\rangle+v_\varepsilon\,|1\rangle+w_\varepsilon\,|2\rangle)/\sqrt{-3}^{L_\varepsilon}$, $u_\varepsilon,v_\varepsilon,w_\varepsilon\in\mathbb{Z}[\omega]$, $L_\varepsilon\in\mathbb{Z}$, such that $|\psi_\varepsilon\rangle$ is an ε approximation of $|\varphi\rangle$ and $L_\varepsilon\leqslant 4\,\log_3(1/\varepsilon)+O(\log[\log(1/\varepsilon)])$.

(2) The expected average classical cost of finding each $|\psi_\varepsilon\rangle$ is polynomial in $\log(1/\varepsilon)$.

A proof of this lemma is given in Appendix B. The proof is very technical. It combines elementary geometry with rather profound number theory, which is based on a mild number-theoretical hypothesis (Conjecture 29).

It follows from the two lemmas that a two-level unitary state can be prepared with precision ε from a standard basis state using a metaplectic circuit of R count at most $4\,\log_3(1/\varepsilon)+O(\log[\log(1/\varepsilon)])$, and in fact this readily generalizes to multiple qutrits as follows.

Lemma 12 ("two-level approximation" lemma). Consider an integer $n\geqslant 1$ and let $|\varphi\rangle$ be a unitary n-qutrit state that has at most two nonzero components in the standard n-qutrit basis.

For arbitrarily small $\varepsilon>0$:

(1) There is an effectively synthesizable metaplectic circuit c with an R count of at most $4\,\log_3(1/\varepsilon)+O(\log[\log(1/\varepsilon)])$ such that $c\,|0\rangle$ is an ε approximation of $|\varphi\rangle$.

(2) The expected average classical cost of finding such a circuit is polynomial in $\log(1/\varepsilon)$.

Before proving the lemma we need two lesser technical facts, which are useful in their own right:

Lemma 13. Let $|b_1\rangle$ and $|b_2\rangle$ be two standard n-qutrit basis states. There exists an effectively and exactly representable classical permutation π such that $|b_2\rangle=\pi\,|b_1\rangle$

Proof. In the case of $n=1$ the $\mathbb{Z}_3$ group generated by INC acts transitively on the standard basis $\{|0\rangle,|1\rangle,|2\rangle\}$.

Consider $|b_k\rangle = |(b_k)_1, \ldots, (b_k)_n\rangle$, $n \geqslant 1$, $k = 1,2$. Let $\pi_j \in \{I, \mathrm{INC}, \mathrm{INC}^2\}$ be such that $\pi_j|(b_1)_j\rangle = |(b_2)_j\rangle$, $j = 1, \ldots, n$. Then $\pi = \otimes_{j=1}^{n} \pi_j$ is the desired permutation. ■

Lemma 14.

(1) For any two standard n-qutrit basis vectors $|j\rangle$ and $|k\rangle$ there exists a classical effectively representable metaplectic gate g, such that for $|j'\rangle = g|j\rangle$ and $|k'\rangle = g|k\rangle$ we have $|j' - k'| < 3$.

(2) Such a gate g can be effectively represented with at most $(n-1)$ instances of the SUM, $\mathrm{SUM}^\dagger$ or 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.

Given Lemma 13, for $n = 2$ the general pair of basis vectors can be reduced to the case where $|j\rangle = |00\rangle$. When $|k\rangle = |0,k_1\rangle$ no further transformations are needed; when $|k\rangle = |k_0,0\rangle$ a single SWAP suffices. The remaining cases are covered by $\mathrm{SUM}_{2,1}^\dagger|11\rangle = \mathrm{SUM}_{2,1}|21\rangle = |01\rangle$, $\mathrm{SUM}_{2,1}|12\rangle = \mathrm{SUM}_{2,1}^\dagger|22\rangle = |02\rangle$. Suppose $n > 2$ and the lemma has been proven for multiqutrit vectors in fewer than n qutrits.

Let $|j\rangle = |j_1 \ldots, j_{n-1}, j_n\rangle$, $|k\rangle = |k_1 \ldots, k_{n-1}, k_n\rangle$ be base-3 representations of the two vectors. By induction hypothesis, one can effectively find an $(n-1)$-qutrit classical metaplectic gate g_{n-1} such that $(g_{n-1} \otimes I)|j_1 \ldots, j_{n-1}, j_n\rangle = |\ldots, j'_{n-1}, j'_n\rangle$ and $(g_{n-1} \otimes I)|k_1 \ldots, k_{n-1}, k_n\rangle = |\ldots, k'_{n-1}, k'_n\rangle$ may differ only at the $(n-1)$st and nth positions.

Select a two-qutrit classical gate g_2, as shown above, such that $g_2|j'_{n-1}, j'_n\rangle$ and $g_2|k'_{n-1}, k'_n\rangle$ 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. ■

Proof (of Lemma 12). We start by reducing $|\varphi\rangle$ to the form $x\,|a_1 \ldots a_{n-1}, d\rangle + z\,|a_1 \ldots a_{n-1}, f\rangle$, $a_1, \ldots, a_{n-1}$, $d, f \in \{0,1,2\}$ using the classical circuit b described in Lemma 14. Let $e \in \{0,1,2\}$ be the "missing" digit such that $\{d, e, f\}$ is a permutation of $\{0,1,2\}$.

Using Lemma 11 we can effectively approximate the single-qutrit state $x\,|d\rangle + z\,|f\rangle$ with an Eisenstein state of the form $|\eta\rangle = (u\,|d\rangle + v\,|e\rangle + w\,|f\rangle)/\sqrt{-3}^k$, $u, v, w \in \mathbb{Z}[\omega]$, $k \in \mathbb{Z}$ to precision ε, with $k \leqslant 4\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$. Using Lemma 7 we can effectively synthesize a single-qutrit metaplectic circuit c_1 with R-count at most $k+1$ such that $c_1|0\rangle = |\eta\rangle$.

Let $c_n = (I^{\otimes(n-1)} \otimes c_1)$. Clearly $b^\dagger c_n\,|a_1 \ldots a_{n-1}, 0\rangle$ is an ε approximation of $|\varphi\rangle$. But $|a_1 \ldots a_{n-1}, 0\rangle$ can be prepared exactly from $|0\rangle$ using at most $n-1$ local INC gates, which finalizes the desired circuit. ■

Corollary 15. Consider an integer $n \geqslant 1$ and let $|\varphi\rangle$ be a unitary n-qutrit state that has at most two nonzero components in the standard n-qutrit basis and consider the corresponding Householder reflection operator $R_{|\varphi\rangle} = I^{\otimes n} - 2\,|\varphi\rangle\langle\varphi|$.

For arbitrarily small $\varepsilon > 0$:

(1) There is an effectively synthesizable metaplectic circuit c with an R count of at most $4\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$ such that $c\,R_{|\bar{0}\rangle}\,c^\dagger$ is an ε approximation of $R_{|\varphi\rangle}$ (where $|\bar{0}\rangle = |0\rangle^{\otimes n}$).

(2) The expected average classical cost of finding such a circuit is polynomial in $\log(1/\varepsilon)$.

Proof. Per [13], if the distance between state $|\varphi\rangle$ and state $|\psi\rangle$ is less than $\varepsilon/(2\sqrt{2})$, then the distance between $R_{|\varphi\rangle}$ and $R_{|\psi\rangle}$ is less than ε. Using Lemma 12 one can effectively find a metaplectic circuit c with an R count of $4\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$ such that $c\,|\bar{0}\rangle$ approximates $|\varphi\rangle$ to precision $\varepsilon/(2\sqrt{2})$ and the corollary follows. ■

This result applies in a straightforward manner to the one-parameter special diagonal unitary:

Corollary 16. Consider an integer $n \geqslant 1$ and an n-qutrit diagonal operator of the form $D = I^{\otimes n} + (e^{i\theta} - 1)\,|j\rangle\langle j| + (e^{-i\theta} - 1)\,|k\rangle\langle k|$, where $j, k \in \{0, \ldots, 3^n - 1\}$, $j \neq k$.

For arbitrarily small $\varepsilon > 0$ there is an effectively synthesizable circuit at distance $< \varepsilon$ from D composed of at most two axial n-qutrit reflection operators and local metaplectic gates with a total R count of

(1) at most $8\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$ when $n = 1$ and

(2) at most $16\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$ when $n > 1$.

Indeed, the diagonal unitary of this form is equal to $r_1\,r_2$, where $r_1 = I^{\otimes n} - |j\rangle\langle j| - |k\rangle\langle k| + |j\rangle\langle k| + |k\rangle\langle j|$, $r_2 = I^{\otimes n} - |j\rangle\langle j| - |k\rangle\langle k| + e^{-i\theta}\,|j\rangle\langle k| + e^{i\theta}\,|k\rangle\langle j|$, and both r_1 and r_2 are two-level reflection operators. We note that for $n = 1$ the r_1 is a Clifford gate and has a trivial cost.

Since multiqutrit axial reflections become more important below, we offer a decomposition method for them in the next section.

IV. IMPLEMENTATION OF AXIAL REFLECTION OPERATORS

Let $|b\rangle$ be a standard n-qutrit basis state. Then the *axial reflection operator* $R_{|b\rangle}$ is defined as

$$R_{|b\rangle} = I^{\otimes n} - 2\,|b\rangle\langle b|.$$

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

Per Lemma 13 any two axial reflection operators are equivalent by conjugation with an effectively and exactly representable classical permutation. Since we consider the cost of classical permutations to be negligible compared to the cost of R gates, we hold that for a fixed n all the n-qutrit axial reflection operators have essentially the same cost. We show in this section that all the n-qutrit axial reflection operators can be effectively and exactly represented.

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

Observation 17. The circuit

$$(I \otimes R_{|0\rangle})\,\mathrm{SUM}(I \otimes R_{|1\rangle})\,\mathrm{SUM}(R_{|2\rangle} \otimes R_{|2\rangle})\,\mathrm{SUM} \qquad (5)$$

is an exact representation of $(-1)R_{|20\rangle}$.

This is established by direct matrix computation. We generalize this solution to arbitrary $n \geqslant 2$ and note that the occurrence of the global phase (-1) is exceptional and happens only at $n = 2$.

Lemma 18. Given $n > 2$, denote by $\bar{2}$ in the context of this lemma a string of $n-2$ occurrences of 2.

Then the circuit

$$c_{20\bar{2}} = (I \otimes R_{|0\bar{2}\rangle})\,\mathrm{SUM}_{1,2}\,(I \otimes I \otimes R_{|\bar{2}\rangle})\,(I \otimes R_{|1\bar{2}\rangle}) \times \mathrm{SUM}_{1,2}\mathrm{SWAP}_{1,2}(I \otimes R_{|2\bar{2}\rangle})\mathrm{SWAP}_{1,2}\,(I \otimes R_{|2\bar{2}\rangle})\,\mathrm{SUM}_{1,2}$$

is an exact representation of the operator $R_{|20\bar{2}\rangle}$.

Proof. Let $|b\rangle$ be an element of the standard n-qutrit basis. The circuit consists of diagonal operators and three occurrences of $\mathrm{SUM}_{1,2}$. Let $|b_1 b_2 \bar{b}\rangle$ be the ternary representation of $|b\rangle$, where $\bar{b}$ stands for the substring of the $n-2$ least significant ternary digits of b. It is almost immediate that the circuit $c_{20\bar{2}}$ represents a diagonal unitary. Indeed, when the input is $|b_1 b_2 \bar{b}\rangle$ we can only get $\pm|b_1 b_2 \bar{b}\rangle$, $\pm|b_1\,\mathrm{INC}\,b_2\bar{b}\rangle$, or $\pm|b_1\,\mathrm{INC}^2 b_2\bar{b}\rangle$, up to swap, after applying each subsequent operator of the circuit, and clearly we can only get $\varphi|b_1 b_2\bar{b}\rangle$, $\varphi = \pm 1$ after the entire circuit is applied.

The lemma claims that $\varphi = -1$ if and only if $b = 20\bar{2}$. Consider the cases where $b_1 = 0$ or $b_1 = 1$. It is easy to see that, whatever is the value of b_2, one and only one of the operators $(I \otimes R_{|0\bar{2}\rangle})$, $(I \otimes R_{|1\bar{2}\rangle})$, $(I \otimes R_{|2\bar{2}\rangle})$ activates $R_{|\bar{2}\rangle}$ on $|\bar{b}\rangle$ and this activation always cancels out with $(I \otimes I \otimes R_{|\bar{2}\rangle})$ (since $R^2 =$ identity for any reflection R). So the result is identity.

If $b_1 = 2$, $b_2 \neq 0$, the five rightmost operations in the circuit produce $|2\rangle \otimes (\mathrm{INC}^2|b_2\rangle) \otimes (R_{|\bar{2}\rangle}|\bar{b}\rangle)$, an action that is subsequently canceled out by $I \otimes I \otimes R_{|\bar{2}\rangle}$. It is also easy to see that for $b_2 = 1$ or $b_2 = 2$ the remaining two reflections $R_{|0\bar{2}\rangle}$ and $R_{|1\bar{2}\rangle}$ amount to nonoperations. Therefore the net result is identity.

We are left with the important case of $b_1 = 2$, $b_2 = 0$. By definition, $\mathrm{SUM}_{12}|20\bar{b}\rangle = |22\bar{b}\rangle$ and then the subsequence $\mathrm{SWAP}_{1,2}\,(I \otimes R_{|2\bar{2}\rangle})\,\mathrm{SWAP}_{1,2}\,(I \otimes R_{|2\bar{2}\rangle})$ activates the operator $R_{|\bar{2}\rangle}$ on $|\bar{b}\rangle$ twice, and of course these two activations cancel each other. We proceed with $\mathrm{SUM}_{12}|22\bar{b}\rangle = |21\bar{b}\rangle$, and $I \otimes R_{|1\bar{2}\rangle}$ activates $R_{|\bar{2}\rangle}$ on $|\bar{b}\rangle$, which is immediately canceled out by $I \otimes I \otimes R_{|\bar{2}\rangle}$. Finally, $\mathrm{SUM}_{12}|21\bar{b}\rangle = |20\bar{b}\rangle$, and $I \otimes R_{|0\bar{2}\rangle}$ activates $R_{|\bar{2}\rangle}$ on $|\bar{b}\rangle$ as desired. This applies the factor of -1 if and only if $\bar{b} = \bar{2}$, and that is what is claimed. ■

Using this lemma we implement the operator $R_{|20\bar{2}\rangle}$ exactly by linear recursion. As noted earlier, all the axial reflection operators in n qutrits have the same R count. Denote this R count $\mathrm{rc}(n)$.

Observation 19. $\mathrm{rc}(n) = \Theta((2+\sqrt{5})^n)$ when $n \to \infty$.

Proof. We have $\mathrm{rc}(1) = 1$, $\mathrm{rc}(2) = 4$ (see Observation IV). The recurrence $\mathrm{rc}(n) = 4\,\mathrm{rc}(n-1) + \mathrm{rc}(n-2)$, $\mathrm{rp}(1) = 1$,$\mathrm{rc}(2) = 4$ can be solved in closed form as $\mathrm{rc}(n) = ((2+\sqrt{5})^n - (2-\sqrt{5})^n)/(2\sqrt{5})$. 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 trade-offs explored in the following sections.

V. ANCILLA-FREE REFLECTION-BASED UNIVERSALITY

Consider integer $n \geqslant 1$. For the duration of this section we set $N = 3^n$.

Lemma 20. Given a diagonal unitary $D \in U(N)$ and arbitrarily small $\varepsilon > 0$ there is an effectively synthesizable ε approximation of D composed of a global phase factor, at most $2(N-1)$ axial reflection operators, and metaplectic local gates with a total R count that is

(1) $16\,(\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)]))$ when $n = 1$ and

(2) less than $16\,(N-1)(\log_3(1/\varepsilon) + n + O(\log[\log(1/\varepsilon)]))$ when $n > 1$.

Indeed, a unitary diagonal D is decomposed into a product of a global phase factor and $(N-1)$ special two-level diagonals as in Corollary 16. Each of the latter diagonals needs to be approximated to precision $\varepsilon/(N-1)$ with $\log_3(1/(\varepsilon/(N-1))) < \log_3(1/\varepsilon) + n$.

In [14] Urias offers an effective $U(2)$ parametrization of 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. All reflections in that decomposition are two level. This immediately leads to the following.

Theorem 21 (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 ε by an ancilla-free metaplectic circuit with an R count of at most $4(N+4)(N-1)(\log_3(1/\varepsilon) + 2n + O(\log[\log(1/\varepsilon)]))$ and at most $(N+4)(N-1)/2$ axial reflections (in n qutrits).

Proof. It follows from [14] that $U \in U(N)$ is effectively decomposed into $N(N-1)/2$ special Householder reflections and possibly a diagonal unitary $D \in U(N)$ that may add up to $2(N-1)$ such reflections (see Lemma 20) to the decomposition to a total of $(N+4)(N-1)/2$ reflections. Each of these allows an effective $\varepsilon/((N+4)(N-1)/2)$ approximation by a metaplectic circuit with an R count of at most eight $(\log_3(1/\varepsilon) + 2n + O(\log(\log(1/\varepsilon))$ plus at most two axial reflections per Corollary 15, and the cost bound claimed in the theorem follows. ■

The best-known cost of exact metaplectic implementation of an n-qutrit axial reflection is $\Theta((2+\sqrt{5})^n)$ as per Observation 19. This may become prohibitive when n is large.

In the next section we show how to curb the R count at the cost of roughly doubling the width of the circuits.

VI. ANCILLA-ASSISTED APPROXIMATION OF ARBITRARY UNITARIES

An alternative way of implementing a two-level unitary operator is through a network of strongly controlled gates. 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 $C^1(\mathrm{INC})$ gate,

$$C^1(\mathrm{INC})|j,k\rangle = |j,(k+\delta_{j,2}) \mod 3\rangle, \tag{6}$$

is of particular interest in this context.

Bullock *et al.* [15] offer a certain ancilla-assisted circuit that emulates $C^n(V)$ using only two-qudit gates. The circuit requires $n-1$ ancillary qutrits, $4(n-1)$ instances of the $C^1(\mathrm{INC})$ gate [see Eq. (6)], and one single $C^1(V)$ gate.

We do not believe that the classical $C^1(\mathrm{INC})$ gate can be represented exactly, and we must resort to approximating $C^1(\mathrm{INC})$ to the desired precision.

Lemma 22. $C^1(\mathrm{INC})$ [as defined by (6)] can be approximated to precision ε by a metaplectic circuit with an R count

of at most 16 $\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$ and 2 two-qutrit axial reflections.

Proof. $C^1(\mathrm{INC})$ is the composition of two reflection operators, $C^1(\mathrm{INC}) = R_{|2\rangle\otimes v_2} R_{|2\rangle\otimes v_0}$, where $v_0 = (|1\rangle - |2\rangle)/\sqrt{2}$, $v_2 = (|0\rangle - |1\rangle)/\sqrt{2}$, and the lemma follows. ■

Corollary 23. Given $V \in U(3)$, integer $n > 0$, and a small enough $\varepsilon > 0$, $C^n(V)$ can be effectively emulated approximately to precision ε by an ancilla-assisted $2n$-qutrit circuit with an R count smaller than $64\,n\,(\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)]))$.

It is easy to see from Lemma 14 that any two-level n-qutrit unitary W is effectively classically equivalent to some $C^{n-1}(\tilde{W})$, where $\tilde{W}$ is a certain (two-level) single-qutrit derivative of W. This applies, in particular, to the two-level Householder reflections that constitute the factors in the explicit $U(2)$ factorization of $U(3^n)$ ([14]).

An upper bound for the cost of ancilla-assisted emulation of arbitrary n-qutrit unitary is summarized in the following.

Theorem 24 (general unitary decomposition, ancilla assisted). Given $U \in U(N)$ in a general position and small enough $\varepsilon > 0$ the U can be effectively emulated up to a global phase to precision ε by a metaplectic circuit with $(n-2)$ ancillas and an R count smaller than $32\,(N+4)(N-1)(n-1)(\log_3(1/\varepsilon) + 2n + O(\log[\log(1/\varepsilon)]))$.

Proof. We can still exactly and effectively decompose U into a global phase and at most $(N+4)(N-1)/2$ two-level Householder reflections (see the proof of Theorem 21).

But now we treat each two-level reflection as the classical equivalent of a $C^{n-1}(V)$, where V is a single-qutrit unitary. We emulate each reflection as such using Corollary 23, and the cost bound for the overall decomposition follows. ■

This synthesis procedure is summarized as pseudocode in Algorithm II.

Algorithm 2 Ancilla-assisted decomposition of a general unitary.

Require: $U \in U(3^n)$, $\varepsilon > 0$
1. $U = D \prod_{k=1}^{K} U_k$ as per [14] Diagonal D and two-level U_k
2. ret ← decomposition(D,ε) as per Corollary 23
3. **for** $k = 1..K$ **do**
4. $\quad c \leftarrow$ decomposition(U_k,ε) as per Corollary 23
5. $\quad$ ret ← ret c
6. **end for**
7. **return** *ret*

VII. OVERALL SYNTHESIS ALGORITHM FLOW

Assuming that ancillary qutrits are readily available, the decision point on choosing between the ancilla-free and the ancilla-assisted decomposition strategies is defined by the relative magnitudes of $(2+\sqrt{5})^n$ and $64\,n\,\log_3(1/\varepsilon)$. Comparison of the upper bounds suggests that in practice the ancilla-free solution becomes prohibitively costly when $n > 7$. Otherwise the decision threshold in ε is of the form $\varepsilon_n = \Omega(3^{-(2+\sqrt{5})^n/(64\,n)})$.

The two strategies can be run in parallel on a classical computer, with the best resulting circuit postselected. This approach is shown schematically in Fig. 3.

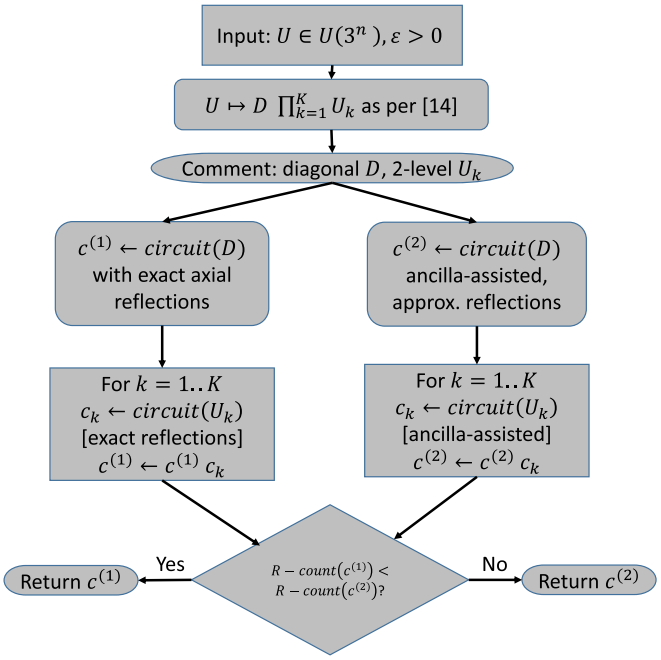

FIG. 3. Parallelizable control flow for the two flavors of the main algorithm.

VIII. SIMULATION, THEORETICAL LOWER BOUND, AND FUTURE WORK

The scaling of the cost of our metaplectic circuits is fully defined by the cost of approximating a two-level state. The R count of a circuit performing an ε approximation of the latter is, in turn, defined by the denominator exponent k of an approximating trilevel Eisenstein state $|\varphi_k\rangle = (u\,|j\rangle + v\,|\ell\rangle + w\,|m\rangle)/\sqrt{-3}^k$.

We currently have k upper-bounded by $4\,\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$. Our numerical simulation over a large set of randomly generated two-level targets demonstrates that an approximation algorithm based solely on Lemma 11 yields k extremely close to this upper bound in the overwhelming majority of cases.

A certain volume argument suggests that a uniform lower bound for k is $5/2\,\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$. Indeed for a given two-level target state $|\psi\rangle$ and its ε approximation $|\varphi_k\rangle$ the real vector $[\mathrm{Re}(u),\mathrm{Im}(u),\mathrm{Re}(v),\mathrm{Im}(v)]^T$ is found in a certain four-dimension meniscus of four-volume $\Theta(\varepsilon^5\,3^{2k})$. If we expect, uniformly, each of these menisci to contain $\Theta(\log(1/\varepsilon))$ such vectors, we need to have $\varepsilon^5\,3^{2k}$ in $\Theta(\log(1/\varepsilon))$ and the above lower bound on k follows.

There is clearly a gap between our guaranteed cost leading term $4\,\log_3(1/\varepsilon)$ and the cost' lower-bound leading term $5/2\,\log_3(1/\varepsilon)$ and we currently do not know (a) whether the lower bound is reachable at all using metaplectic circuits or (b) if it is reachable, whether this can be done using a classically tractable algorithm. More theoretical (and, possibly, simulation) work is needed to answer these questions. At stake here is the potential practical reduction of the metaplectic circuitry cost by 37.5%.

Another important open question is whether there is a set of exact metaplectic circuits for n-qutrit axial reflections with an R count that is subexponential (preferably, polynomial) in n.

IX. CONCLUSION

We have addressed the problem of performing efficient quantum computations in a framework where the quantum information is represented in multiqutrit encoding by ensembles of certain weakly integral anyons and the native quantum gates are represented by braids with the targeted use of projective measurement. We have developed two flavors of a classically feasible algorithm for the synthesis of efficient metaplectic circuits that approximate arbitrary n-qutrit unitaries to a desired precision ε. The first flavor of the algorithm produces circuits that are ancilla-free and asymptotically optimal in ε (but may have additive entanglement overhead that is exponential in n). The second flavor produces circuits requiring roughly n clean ancillae and has a depth overhead factor of approximately n but may be, nevertheless, more efficient in practice when n is large. The combined algorithm enables us to compile logical multiqutrit circuits with scalability properties comparable to the scalability of the recent crop of efficient logical circuits over multiqubit bases such as Clifford + T, Clifford +V, and Fibonacci.

In summary, we have demonstrated that circuit synthesis for a prospective ternary topological quantum computer based on weakly integral anyons can be done effectively and efficiently. This implicitly validates this prospective computer for quantum algorithm development.

Although we have achieved asymptotic optimality of the resulting circuits, there is some potential slack left in the practical bounds of leading coefficients for the circuit depths, as explained in Sec. VIII. Investigating this presumed slack is one of our future research topics.

ACKNOWLEDGMENT

The authors wish to thank Martin Roetteler for useful discussions.

APPENDIX A: EXACT REPRESENTATION OF SINGLE-QUTRIT UNITARIES OVER THE METAPLECTIC BASIS

Surprisingly, our synthesis algorithms did not require the usual theorem regarding the exact decomposition of exactly representable matrices. For completeness we state this result here (Theorem 26).

Lemma 25. Let $|\psi\rangle$ be a unitary single-qutrit state of the form $|\psi\rangle = 1/\sqrt{-3}^{L}(v\,|1\rangle + w\,|2\rangle)$, 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.

Proof. We reuse remarks in the proof of Lemma 7 to note that, whenever $L > 0$, then $|v|^2 \mod 3 = |w|^2 \mod 3 = 0$. 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 Lemma 8. ■

Theorem 26 (single-qutrit exact synthesis theorem). Consider a 3×3 unitary matrix of the form $U = 1/\sqrt{-3}^{L} M$, where M is a 3×3 matrix over $\mathbb{Z}[\omega]$. Then U is represented exactly by a metaplectic circuit of R count at most $L + 3$.

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

Lemma 27. Consider a 2×2 unitary matrix of the form $V = 1/\sqrt{-3}^{L} M$, where M is a 2×2 matrix over Eisenstein integers. The 3×3 matrix $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & V \end{smallmatrix}\right)$ 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 $1/\sqrt{-3}^{L}\,[0,u,v]^T$ be the second column in matrix U. Per Lemma 25 the column can be reduced to a standard basis vector using at most one P gate. Applying an appropriate classical gate if necessary we can force it to be $|1\rangle$ and thus U is reduced to $\mathrm{diag}(1,1,\varphi)$, 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 $P_2^{-d \mod 6}$ completes the reduction of the matrix to identity. ■

Proof (of the theorem). Per Lemma 7 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 in U to a basis vector and, in fact, without loss of generality, to $|0\rangle$.

Consider the matrix $c_1\,U$. Due to unitariness, it must be of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & V \end{smallmatrix}\right)$ with $V = 1/\sqrt{-3}^{L_1} M_1$, where M_1 is a certain 2×2 matrix over $\mathbb{Z}[\omega]$. Per Lemma 27 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 an R count of at most $L + 3$ and an H count of at most L such that $c_2\,U = I$ and thus $U = c_2^{-1}$. ■

APPENDIX B: SINGLE-QUTRIT-STATE APPROXIMATION

1. Norm equation in Eisenstein integers

The ring of Eisenstein integers $\mathbb{Z}[\omega]$ is arguably the simplest *cyclotomic* ring [16]. In what follows we need certain properties of the equation

$$|z|^2 = n, \quad n \in \mathbb{Z}, \quad z \in \mathbb{Z}[\omega]. \tag{B1}$$

The two basic facts to deal with are that (a) Eq. (B1) is solvable with respect to z only for some of the right-hand-side values, and (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 $p \in \mathbb{Z}$, $|p|^2 = p^2$, 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 [16], if n is a positive prime number, Eq. (B1) is solvable if and only if $n = 1 \mod 3$ or $n = 3$. In the case of $n = 3$ the six solutions of the equation are $(-\omega)^{2\,d}\,(2\,\omega + 1)$, $d = 0,\ldots,5$.

In the more general case where n is a prime with $n = 1 \mod 3$ it is easy to obtain all the solutions of (B1) at a run-time cost that is probabilistically polynomial in $\log(n)$. The two-step procedure used is as follows:

(1) Compute $m \in \mathbb{Z}$ such that $m^2 = -3 \mod n$, using, for example, the Tonelli-Shanks algorithm [17].

(2) Compute $z = GCD_{\mathbb{Z}[\omega]}(m + 2\,\omega + 1, n)$.

(3) Now $\{(-\omega^2)^d\, z, (-\omega^2)^d\, z^*, d = 0, \ldots, 5\}$ are the solutions of (B1).

As a matter of principle, we could limit ourselves 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 $\Omega(1/\log(B))$ (cf. [18]). While this 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 (B1), that is, 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 28. Let n be an integer, factored to the form $n = m^2\, p_1 \ldots p_\ell$, where $m \in \mathbb{Z}$ and $p_1 \ldots p_\ell$ are distinct positive integer primes.

Then

(1) Eq. (B1) 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 Eq. (B1):

$$z = m\mathrm{Conj}^{d_1}[z_1] \ldots \mathrm{Conj}^{d_\ell}[z_\ell], \quad d \in \{0,1\}^\ell, \tag{B2}$$

where Conj is the complex conjugation operator.

Recall that an integer is *smooth* if it does not have prime factors above a certain size [19]. Let us call an integer *semismooth* 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 a semismooth right-hand side n is easy and can be effectively performed at the run-time cost that is polynomial in $\log(n)$.

The distribution of smooth integers is described by the de Bruijn function [19]. Even though the density of semismooth numbers n for which Eq. (B1) 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 a sufficiently high probability, one that is semismooth and such that Eq. (B1) is solvable.

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

Conjecture 29. Let k be an arbitrarily large positive integer and let $u, v \in \mathbb{Z}[\omega]$ be randomly picked Eisenstein integers such that

$$\Theta(3^{k/2}) \leqslant |u|^2 + |v|^2 \leqslant 3^k.$$

Then for $n = 3^k - |u|^2 - |v|^2$ Eq. (B1) is easily solvable with a probability that has a uniform lower bound in $\Omega(1/k)$.

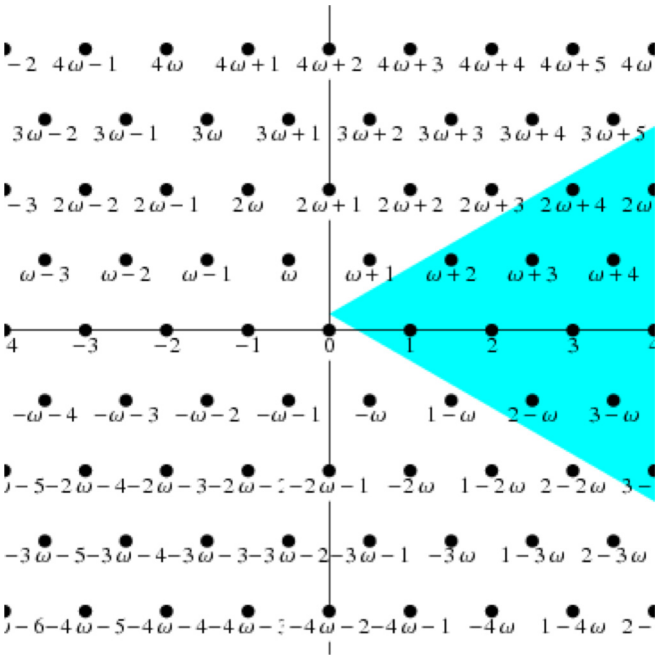

FIG. 4. Lattice of Eisenstein integers. (Downloaded from http://mathworld.wolfram.com/EisensteinInteger.html, a Wolfram Research Inc. web resource.)

2. Approximation of single-qutrit states

We start with the following.

Lemma 30. 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 ε be a small enough positive value. The unitary state $|\psi\rangle$ can be approximated to precision ε by a unitary state for the form $(u\,|0\rangle + v\,|1\rangle + w\,|2\rangle)/\sqrt{-3}^k$, $u, v, w \in \mathbb{Z}[\omega]$, $k \in \mathbb{Z}$ such that $k \leqslant 4\,\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$. The expected classical run time required to carry out the approximation effectively is polynomial in $\log(1/\varepsilon)$.

Before proving the lemma, let us state the following.

Proposition 31. For a given complex number z with $|z| \leqslant 1$ and small enough $\varepsilon > 0$ there exists an integer $k \leqslant 2\,\log_3(1/\varepsilon) + 5$ and an Eisensten integer $u \in \mathbb{Z}[\omega]$ such that $|u/\sqrt{-3}^k - z| < \varepsilon$ and $|u/\sqrt{-3}^k| \leqslant |z|$.

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

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

We start by taking a geometric view of the feasibility of both claims in this proposition. On the complex plane 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 Fig. 4). A circle of radius R centered at the origin contains at least $3\,R\,(R+1)$ nodes of this lattice. Per the general properties of integral lattices, a convex domain with a large enough area A is to contain $O(A)$ lattice nodes and, in this case, at least $3/\pi\ A$ nodes.

The desired Eisenstein integer u must be within $\varepsilon\sqrt{3}^k$ from $z\sqrt{3}^k$ and satisfy the side condition

$$|u| \leqslant |z|\sqrt{3}^k. \tag{B3}$$

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

$B(k,\varepsilon)$ is a convex domain, and when ε is sufficiently smaller than $|z|$ it contains a sector of the smaller circle with an area of at least $1/2\,(1-\varepsilon/|z|)\varepsilon^2\,3^k$. Thus (assuming $\varepsilon < 2/3\,|z|$) if k is larger than $\underline{k} = \log_3(2/\varepsilon^2) + 1$, 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 $k = \underline{k} + \ell$ the area of $B(k,\varepsilon)$ grows exponentially in ℓ so there exists a small constant ℓ_0 such that for $k_0 = \lceil \underline{k} \rceil + \ell_0$ 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 where $\pi/12 \leqslant \arg z \leqslant 5\,\pi/12$. Indeed, the multiplication by the Eisensten 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 $\pi/12 + \pi/3\,m \leqslant \arg z \leqslant 5\,\pi/12 + \pi/3m$, $m = 0,\ldots,5$, can be moved into the sector $\pi/12 \leqslant \arg z \leqslant 5\,\pi/12$ by applying zero or more 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 $k \geqslant \log_{\sqrt{3}}(2/\varepsilon) + 2 = 2\,\log_3(1/\varepsilon) + 2\,\log_3(2) + 2$ (this is a convenient if somewhat excessive assumption). This implies that $\varepsilon\sqrt{3}^{k-1} \geqslant 2\sqrt{3}$ and $\varepsilon\sqrt{3}^k \geqslant 6$.

Considering $\pi/12 \leqslant \arg z \leqslant 5\,\pi/12$, the circle, (B3), contains the vertical segment $[z\sqrt{3}^k - i\,|z|\sqrt{3}^k(2\,\sin(\pi/12)), z\sqrt{3}^k]$ of length at least $1/2\,|z|\sqrt{3}^k$. Assuming, again, that $\varepsilon < |z|$, $B(k,\varepsilon/4)$ 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 $u = a + b\,\omega = (a - b/2) + i\,(b\sqrt{3}/2)$, $a,b \in \mathbb{Z}$. We choose b such that $b\sqrt{3}/2$ is at a distance at most $(\varepsilon/4)\sqrt{3}^k$ from $\mathrm{Im}(z)\sqrt{3}^k$. Per our choice of k this implies that it is necessary and sufficient for the integer b to belong to a segment of length $\varepsilon\sqrt{3}^{k-1}/2 \geqslant \sqrt{3} > 1$. Therefore at least one such integer exists and can be effectively picked.

Next one must find an integer a such that $u = a - (b/2) + i\,(b\sqrt{3}/2) \in B(k,\varepsilon)$. Per the geometric condition $\arg z \leqslant 5\,\pi/12$, the circle, (B3), contains the 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 $\varepsilon < |z|$, $B(k,\varepsilon)$ contains the 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 $3/16\,\varepsilon\sqrt{3}^k$.

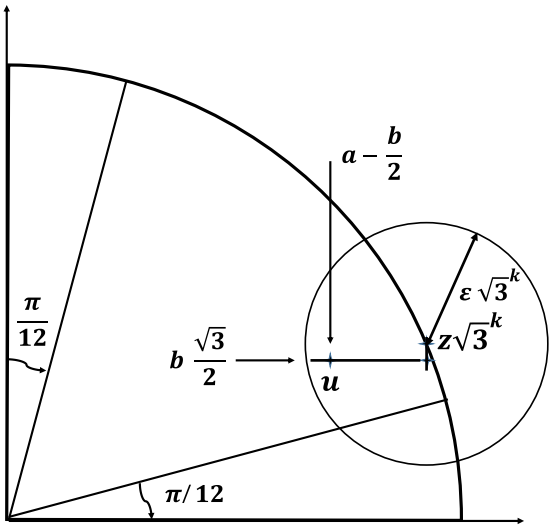

FIG. 5. Approximating a scaled complex number with an Eisenstein integer.

For our choice of k, $3/16\,\varepsilon\sqrt{3}^k \geqslant 3/16 \times 6 > 1$. It is necessary and sufficient for the desired integer a to belong to the segment $[\mathrm{Re}(z)\sqrt{3}^k + b/2 - 3/16\,\varepsilon\sqrt{3}^k, \mathrm{Re}(z)\sqrt{3}^k + b/2]$ 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 in Fig. 5. Set $k_0 = \lceil 2\,\log_3(1/\varepsilon) + 2\,\log_3(2) + 2 \rceil$. Let ℓ 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 $\sqrt{3}^\ell$, then the segments we used above to pick the values of b and a are scaled out by a factor of $\Omega(\sqrt{3}^\ell)$ and thus allow at least $\Omega(\sqrt{3}^\ell)$ distinct choices of b and at least $\Omega(\sqrt{3}^\ell)$ distinct choices of a for each choice of b. Therefore there are $\Omega(3^\ell)$ distinct choices of Eisenstein integer u, yielding as many distinct approximations of z as claimed. ■

Proof (of the lemma). 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 ε of $|\psi\rangle$, it would suffice that

$$2\,\mathrm{Re}(\langle\varphi|\psi\rangle) > 2 - \varepsilon^2. \tag{B4}$$

Consider some small $\delta > 0$ and a trilevel *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,

$$2\,\mathrm{Re}(u'\,x^*) > |u'|^2 + |x|^2 - \delta^2,$$
$$2\,\mathrm{Re}(v'\,y^*) > |v'|^2 + |y|^2 - \delta^2.$$

Hence $2\,\mathrm{Re}(\langle\varphi|\psi\rangle) > 2 - (1 - |u'|^2 - |v'|^2) - 2\,\delta^2$.

Expanding the triangle inequalities $|u'| \geqslant |x| - |x - u'|$, $|v'| \geqslant |y| - |y - v'|$, we get $|u'|^2 + |v'|^2 \geqslant 1 - 2(|x|\,|x - u'| + |y|\,|y - v'|) + |x - u'|^2 + |y - v'|^2 \geqslant 1 - 4\,\delta$. Assuming without loss of generality that $\delta^2 < \delta/2$ we conclude that $2\,\mathrm{Re}(\langle\varphi|\psi\rangle) > 2 - 5\,\delta$.

Set $\delta = \varepsilon^2/5$ in order to satisfy inequality (B4) and start with $k_0 = \lceil 2\,\log_3(1/\delta) + 2\,\log_3(2) + 2 \rceil \leqslant 4\,\log_3(1/\varepsilon) + \log_3(5) + 5$. We look for a sufficient $k = k_0 + \ell$ where ℓ iterates sequentially through non-negative integers.

Per Proposition31 there exist several suitable Eisenstein integers u, v such that $u/\sqrt{-3}^k$ is a δ approximation of x and $v/\sqrt{-3}^k$ is a δ approximation of y. In fact as ℓ grows, there are $\Omega(9^\ell)$ distinct subunitary states $u/\sqrt{-3}^k|0\rangle + v/\sqrt{-3}^k|1\rangle$ that are δ 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 ℓ and that is not too large. The sufficient inequality, (B4), does not explicitly involve w and is satisfied for $\delta = \varepsilon^2/5$ as shown above.

By unitariness of the desired $|\varphi\rangle$, $w \in \mathbb{Z}[\omega]$ must satisfy the equation

$$|w|^2 = 3^k - |u|^2 - |v|^2, \tag{B5}$$

which is an instance of the norm equation, (B1). As we have seen in subsection B 1, 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 Conjecture 29 becomes applicable.

To this end, let ℓ be an integer iterating from 0 to some sufficiently large L and let $k = k_0 + \ell$ iterate with it. For each subsequent value of ℓ we inspect all the available u,v that generate δ 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 ℓ. Assuming Conjecture 29 we only need to inspect as many as $O(\log(3^k - |u|^2 - |v|^2)) = O(k) = O(k_0 + \ell)$ such distinct u, v to find one for which (B5) is easily solvable with a sufficiently high probability.

It is easy to see that there exists such $\ell = O(\log(k_0))$ for which an easily solvable norm equation, (B5), is obtained with near certainty. Therefore a desired unitary state $(u|0\rangle + v|1\rangle + w|2\rangle)/\sqrt{-3}^k$ will be obtained for some $k = k_0 + O(\log(k_0)) \leqslant 4\log_3(1/\varepsilon) + O(\log[\log(1/\varepsilon)])$.

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

In Algorithm 3 we present the method suggested by this lemma in pseudocode format.

Algorithm 3 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. $k_0 \leftarrow \lfloor 4\log_3(1/\varepsilon) + \log_3(5) + 5\rfloor$
3. $w \leftarrow$ None; $k \leftarrow k_0 - 1$
4. **while** $w =$ None
5. $k \leftarrow k + 1$
6. enum $\leftarrow$ enumerator for all $u,v \in \mathbb{Z}[\omega]$
7. s.t. $(u|0\rangle + v|1\rangle)/\sqrt{-3}^k$ is δ close to $x|0\rangle + y|1\rangle$
8. **while** $w =$ None $\wedge$ enum.Next **do**
9. $(u,v) \leftarrow$ 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** $\{u,v,w,k\}$

APPENDIX C: TWO-QUTRIT CLASSICAL GATES GENERATED BY SUM AND SWAP

It is currently not known which two-qutrit gates can be represented exactly over the metaplectic basis. In particular, it is not known whether the important classical C^1(INC) gate, (4), is so representable.

Let S_9 be the permutation group on nine elements. There is a natural unitary representation of S_9 on $\mathbb{C}^{3^2}$ where a permutation π is mapped to the unitary that extends the permutation π applied to the standard basis vectors $\{|00\rangle,\ldots,|22\rangle\}$. The image of this faithful representation coincides, by definition, with the group of all the classical two-qutrit gates. With a slight abuse of notation we also use S_9 to denote the image.

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

Proposition 32. The group, G, generated by SUM,SWAP, and all the one-qutrit classical gates is a maximal subgroup of S_9.

Proof. Of-course, one can always conduct a brute-force computer search to verify this statement. Here we provide an elegant alternative proof. Let $\mathrm{AGL}(2,\mathbb{F}_3) = \mathrm{GL}(2,\mathbb{F}_3) \ltimes \mathbb{F}_3^2$ be the affine linear group acting on the two-dimensional vector space $\mathbb{F}_3^2$. Explicitly, given $\varphi = (A,c) \in \mathrm{AGL}(2,\mathbb{F}_3)$, $v \in \mathbb{F}_3^2$, we have $\varphi(v) = Av + c$. Note that $\mathbb{F}_3^2$ has, in total, nine vectors, whose coordinates under the standard basis are $\{(i,j)|i,j = 0,1,2\}$. We identify the coordinate (i,j) with the two-qutrit basis vector $|i,j\rangle$. Since elements of $\mathrm{AGL}(2,\mathbb{F}_3)$ permute the nine coordinates, we then have a group morphism $\psi : \mathrm{AGL}(2,\mathbb{F}_3) \longrightarrow S_9 \subset U(3^2)$, such that $\psi(A,c)|i,j\rangle = A.\binom{i}{j} + c$.

For instance, let $A = \left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$, since $A \cdot \binom{i}{j} = \binom{i}{i+j}$; then $\psi(A) =$ SUM. Similarly, one can check the following correspondences:

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \mapsto \text{SUM},$$

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \mapsto \text{SWAP},$$

$$\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix} \mapsto \mathrm{Id} \otimes S_{1,2}, \quad \text{where} \quad S_{1,2} = \begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix},$$

$$\begin{pmatrix}1\\ 0\end{pmatrix} \mapsto \mathrm{INC} \otimes \mathrm{Id},$$

$$\begin{pmatrix}0\\ 1\end{pmatrix} \mapsto \mathrm{Id} \otimes \mathrm{INC}.$$

It is easy to check that the matrices (vectors) on the left-hand side of the above correspondences generate the group $\mathrm{AGL}(2,\mathbb{F}_3)$ and the gates on the right-hand side generate G. Also, it is not hard to verify that the map ψ is injective and thus $G \simeq \mathrm{AGL}(2,\mathbb{F}_3)$. Now by O'Nan-Scott theorem [20,21], $\mathrm{AGL}(2,\mathbb{F}_3)$ 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(INC) gate is exactly representable, all of the classical two-qutrit gates are also exactly representable.

[1] M. H. Freedman, A. Kitaev, M. J. Larsen, and Z. Wang, Topological quantum computation, Bull. Amer. Math. Soc. **40**, 31 (2003).
[2] A. Kitaev, Fault-tolerant quantum computation by anyons, Ann. Phys. (NY) **303**, 2 (2003).
[3] S. X. Cui and Z. Wang, Universal quantum computation with metaplectic anyons, J. Math. Phys. **56**, 032202 (2015).
[4] M. Hastings, C. Nayak, and Z. Wang, Metaplectic anyons, Majorana zero modes, and their computational power, Phys. Rev. B **87**, 165421 (2013).
[5] S. Das Sarma, M. Freedman, and C. Nayak, Majorana zero modes and topological quantum computation, npj Quantum information **1**, 15001 (2015).
[6] M. R. Peterson *et al.*, Abelian and non-Abelian states in $\nu = 2/3$ bilayer fractional quantum Hall systems, Phys. Rev. B **92**, 035103 (2015).
[7] D. J. Clarke, J. Alicea, and K. Shtengel, Exotic non-Abelian anyons from conventional fractional quantum Hall states, Nature Commun. **4**, 1348 (2013).
[8] C. M. Dawson and M. A. Nielsen, The Solovay-Kitaev algorithm, Quantum Inf. Comput. **6**, 81 (2006).
[9] M. E. Beverland, O. Buerschaper, R. Koenig, F. Pastawski, J. Preskill, and S. Sijher, Protected gates for topological quantum field theories, arXiv:1409.3898.
[10] J. Preskill, Topological quantum computing for beginners, http://online.itp.ucsb.edu/online/exotic_c04/preskill/pdf/Preskill.pdf (2003).
[11] D. Gottesman, Fault-tolerant quantum computation with higher-dimensional systems, Chaos Solitons Fractals **10**, 1749 (1999).
[12] J. Bourgain and A. Gamburd, A Spectral Gap Theorem in SU(d), J. Eur. Math. Soc. **14**, 1455 (2012).
[13] V. Kliuchnikov, Synthesis of unitaries with Clifford + T circuits, arXiv:1306.3200.
[14] J. Urias, Householder factorizations of unitary matrices, J. Math. Phys. **51**, 072204 (2010).
[15] S. S. Bullock, D. P. O'Leary, and G. K. Brennen, Asymptotically Optimal Quantum Circuits for d-level Systems, Phys. Rev. Lett. **94**, 230502 (2005).
[16] L. Washington, *Introduction to Cyclotomic Fields* (Springer, New York, 1997).
[17] D. Shanks, Five number theoretic algorithms, in *Proceedings of the Second Manitoba Conference on Numerical Mathematics, October 5–7, 1972*, edited by R. S. D. Thomas and H. C. Williams (Utilitas Mathematica, Winnipeg, 1973).
[18] M. Hazewinkel, Distribution of prime numbers, in *Encyclopedia of Mathematics* (Springer, Berlin, 2001).
[19] A. Granville, *Smooth Numbers: Computational Number Theory and Beyond*, Math. Sci. Res. Inst. Publ., Vol. 44 (Cambridge Univ. Press, Cambridge, 2008), pp. 267–323.
[20] M. W. Liebeck, C. E. Praeger, and J. Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups, J. Austral. Math. Soc. (Ser. A) **44**, 389 (1988).
[21] L. L. Scott, Representations in characteristic p, Santa Cruz Conf. Finite Groups **37**, 319 (1980).