Synthesis and Arithmetic of Single Qutrit Circuits

Amolak Ratan Kalra[1,2,3], Michele Mosca[1,4,3], and Dinesh Valluri[1,4]

[1]Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada
[2]David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada
[3]Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada
[4]Dept. of Combinatorics & Optimization, University of Waterloo, Waterloo, Ontario, Canada

In this paper we study single qutrit circuits consisting of words over the Clifford+$\mathcal{D}$ cyclotomic gate set, where $\mathcal{D} = \mathrm{diag}(\pm\xi^a, \pm\xi^b, \pm\xi^c)$, ξ is a primitive 9-th root of unity and a, b, c are integers. We characterize classes of qutrit unit vectors z with entries in $\mathbb{Z}[\xi, \frac{1}{\chi}]$ based on the possibility of reducing their smallest denominator exponent (sde) with respect to $\chi := 1 - \xi$, by acting an appropriate gate in Clifford+$\mathcal{D}$. We do this by studying the notion of 'derivatives mod 3' of an arbitrary element of $\mathbb{Z}[\xi]$ and using it to study the smallest denominator exponent of HDz where H is the qutrit Hadamard gate and $D \in \mathcal{D}$. In addition, we reduce the problem of finding all unit vectors of a given sde to that of finding integral solutions of a positive definite quadratic form along with some additional constraints. As a consequence we prove that the Clifford+$\mathcal{D}$ gates naturally arise as gates with sde 0 and 3 in the group $U(3, \mathbb{Z}[\xi, \frac{1}{\chi}])$ of 3×3 unitaries with entries in $\mathbb{Z}[\xi, \frac{1}{\chi}]$. We illustrate the general applicability of these methods to obtain an exact synthesis algorithm for Clifford+R and recover the previous exact synthesis algorithm in [14]. The framework developed to formulate qutrit gate synthesis for Clifford+$\mathcal{D}$ extends to qudits of arbitrary prime power.

1 Introduction

Implementing a target unitary U using a finite sequence of gates over a universal gate set G is a fundamental problem in quantum computing. This problem arises naturally in the context of quantum compilation, where the goal is to map an abstract instruction set to a physical architecture. The abstract instruction set usually specifies a quantum algorithm or protocol and the physical architecture or hardware usually refers to a quantum circuit. A circuit synthesis algorithm takes as input a target unitary U, a universal gate set G and a precision parameter ϵ and outputs a sequence of gates from G that realizes/implements the unitary U up-to ϵ precision efficiently.

The general synthesis problem benefits greatly from the subroutine of exact synthesis which is: given a finite universal gate set G and an element g in the group generated by G find a sequence $g_1 ... g_k$ in G such that $g = g_1 ... g_k$. In the qubit case Kliuchnikov, Maslov and Mosca (KMM) [14] solved the exact synthesis problem. In particular they showed that single qubit unitaries U which are exactly implementable (decomposable) over the Clifford+T gate set are equivalent to the 2×2 unitaries over the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$. Great progress was made in designing efficient synthesis algorithms by using this exact synthesis result as a sub-routine, see [14, 15, 23].

Motivated by the results in these papers we aim to formulate and address the analogous problem of exact synthesis for qutrits over various families of universal gate sets. The motivation for studying quantum circuits based on qutrits and more generally qudits comes from recent experimental progress made on implementing and controlling higher dimensional quantum systems in the lab [1, 13, 16, 17, 22, 24]. From a theoretical perspective, magic state distillation protocols based on qudits have been shown to outperform their qubit counterparts, see [3, 19, 26]. Qudits have also been used to make the connection between quantum speed-up and contextuality more transparent [11, 18]. There are several other experimental and theoretical advantages for considering qudits over qubits with reference to circuit complexity and ease of experimental implementations, these are discussed in some detail in [25]. The question of circuit synthesis for qudits has partially been addressed previously using normal forms, see [7, 20, 21].

A direct generalization of the main result of [14] fails for qutrit circuit synthesis. In other words, the Clifford+T gates are insufficient to generate $U(3, R_{9,\chi})$, the analogous group of 3×3 unitary matrices whose entries are in $R_{9,\chi} := \mathbb{Z}[\xi, \frac{1}{\chi}]$, where $\xi = e^{\frac{2\pi i}{9}}$, a primitive 9-th root of unity and $\chi = 1 - \xi$. In this paper we rescue the situation for qutrits by proposing two gate sets that satisfy an algebraic characterization analogous to [14]. To this end, we study the qutrit analogue of [14] over the Clifford+$\mathcal{D}$ gate set where $\mathcal{D} = \text{diag}(\pm\xi^a, \pm\xi^b, \pm\xi^c)$, for integers a, b, c. The choice of these gates is not arbitrary, as we show in Section 4 that the $\mathcal{D}$ gates and the H gate arise as, in a sense, the only gates whose smallest denominator exponent (sde) is 0 and 3 respectively. This sets us up with the question of whether Clifford+$\mathcal{D}$ adequately generates $U(3, R_{9,\chi})$, i.e., given a matrix $M \in U(3, R_{9,\chi})$, can it be generated by gates from Clifford+$\mathcal{D}$. If so, does there exist a reasonably efficient algorithm to do so? In this paper we make progress towards answering this question by a study of the smallest denominator exponents of unit vectors with entries in $R_{9,\chi}$.

The following property holds for G = Clifford+T in $U(2, R_{8,\chi})$ and G = Clifford+R in $U(3, R_{3,\chi})$:

P: Given any unit vector $z \in R^3_{n,\chi}$ with sde $\geq c$ there exists an element $g \in G$ such that $sde(gz, \chi) < sde(z, \chi)$, where c is a constant less than or equal to 3 only depending on n.

Existence of property P for a given $G \subset U(p, R_\chi)$ allows us to find a sequence of letters $g_1, \ldots, g_k$ such that the $\text{sde}(g_1 \ldots g_k z) = c-1$. This reduces the problem of exact synthesis to a finite computation.

However, P need not hold for every p^l. For instance, whenever $p = 3, l = 2$ we prove in Theorem 5.12 that there exists a $\Delta \in \mathbb{Z}_3$ associated to the unit vector z in such a way that there exists a $g \in$ Clifford+$\mathcal{D}$ such that $sde(gz) < sde(z)$ iff $\Delta \neq -1$. Therefore, we identify an easily computable obstruction Δ for property P. While Δ is an obstruction, our method in fact helps us recover g explicitly when $\Delta \neq -1$.

The general strategy of employing property P, if it is true, makes sense for a general prime power $n = p^l$ and in fact most of the tools we develop, such as the notion of derivatives mod p, do extend to such generality. However, in the case where $p = 2$ or 3, by Lemma 5.1 the sdes of each entry of a given unitary in $U_p(R_\chi)$ are equal, a property which fails to be true when $p \geq 5$. This failure makes the sde profile for $p \geq 5$ more complicated to study. A key idea to prove our results is the reduction of property P for a particular instance of z to the existence of $\mathbb{Z}_p$- rational solutions of a system of polynomial equations over $\mathbb{Z}_p$. For $p \leq 3$ the equations are simple enough (at most quadratic) to be solved completely.

A brief summary of the contents are as follows. In Section 2, we review the background material on rings and universal gate sets required for the rest of the paper. In Section 3, we formulate the notion of 'derivatives mod p' of an element $f(\zeta)$ of $\mathbb{Z}[\zeta]$, where ζ is a primitive p^l-th root of unity. These are simply the elements $\frac{f^{(k)}(1)}{k!} \pmod p$ for $0 \leq k \leq \phi(p^l)$. We prove that this notion is well defined, i.e., if $f(x), g(x) \in \mathbb{Z}[x]$ such that $f(\zeta) = g(\zeta)$, then $f^k(1)/k! = g^k(1)/k! \pmod p$. This essentially follows from the fact that $f(x) = g(x) \pmod{\Phi_{p^l}(x)}$, which implies $f^{(k)}(1)/k! = g^{(k)}(1)/k!$ modulo an integral linear combination of $\Phi^{(k)}_{p^l}(1)/k!$ which divisible by p for all $0 \leq k \leq \phi(p^l)$ by Lemma 3.2. Here $\Phi_n(x)$ is the n-th cyclotomic polynomial, a monic irreducible polynomial over $\mathbb{Z}$. An intuitive way to see these derivatives is as Taylor coefficients of f at '$\zeta = 1$'. This can be made precise by considering the quotient map $\mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/(p)$ and looking at the image of $f(\zeta)$ in terms of $\chi = 1 - \zeta$. We prove a criterion which is repeatedly used: for $0 \leq k \leq \phi(p^l)$, χ^k divides $f(\zeta)$ iff $f(1) = \frac{f'(1)}{1!} = \ldots = \frac{f^{k-1}(1)}{(k-1)!} = 0 \pmod p$. This is in fact easy to see using the Taylor series picture presented above.

In Section 4, we find an algorithm to obtain all the unit vectors with a given sde. The unit vector condition over $R_{9,\chi} := \mathbb{Z}[\xi]_\chi$ with respect to the hermitian metric, namely $\sum |z_i|^2 = 1$, can be reduced to solutions of three non-homogeneous integral quadratic forms in 18 variables. One of the quadratic forms is positive definite therefore the set of its integral solutions is finite. This allows us to find all the unit vectors of a given sde by finding the integral solutions of the positive definite quadratic form and checking if the solution obtained satisfies the other two equations. This way of obtaining all the unit vectors of a particular sde is practical for small sde. Using this we can characterize the unitary matrices of sde $= 0$ as precisely the ones generated by the Pauli gates $+ \mathcal{D}$ gates, while the gates with sde $= 3$ are, up to permutation of their columns, the H gate, possibly multiplied by two gates from $\mathcal{D}$ on the left and right respectively. Therefore, we obtain the Clifford+$\mathcal{D}$ gates as natural objects in the arithmetic of the group $U(3, R_{9,\chi})$.

In Section 5, we study the difference $\mathrm{sde}(HDR^\epsilon z) - \mathrm{sde}(z)$, where D varies over the cyclotomic gate set $\mathcal{D}$ in the context of single qubit and single qutrit gates. This question of dropping sde of z can be tied to the question of divisibility of z by powers of $\chi := 1 - \zeta_{p^l}$. We reformulate this condition of divisibility by powers of χ in terms of derivatives vanishing mod p, using Theorem 3.7. This condition gives rise to a system of polynomial equations as explained in the proofs of Theorems 5.7 and 5.12. This is done for $p^l = 2^3$ to recover the main theorem of [14]. For, $p^l = 3$ we give an exact synthesis algorithm for Clifford+R and prove a result (as an easy consequence) analogous to the one in [14], i.e., Clifford+R = $U(3, R_\chi)$. This algorithm is closely connected to the approximate synthesis algorithm for Clifford+R explored in [2]. For $p^l = 3^2$ we obtain a criterion $\mathrm{sde}(HDR^\epsilon z) - \mathrm{sde}(z) = -1$ iff $\Delta \neq -1$, where $\Delta \in \mathbb{Z}_3$ is an element associated to the unit vector z.

Historical Note: After this paper appeared, the exact synthesis problem posed in this paper was completely solved for the group $U_3(\mathbb{Z}[\xi]_\chi)$, where ξ is a primitive 9-th root of unity and $\chi = 1 - \xi$ by Shai Evra and Ori Parzanchevski in [5]. In particular, they showed that Clifford+$\mathcal{D}$ is a set of generators for $U_3(\mathbb{Z}[\xi]_\chi)$ using the theory of buildings. This extends the qubit synthesis results of [14] to qutrits. In particular, the current work gives the frame work and proposes the candidate set of gates, namely Clifford+$\mathcal{D}$ gates in place of the Clifford+T gates for qubits. The question of multi-qutrit exact synthesis was later addressed later by two independent works [9, 12].

2 Preliminaries

In this introductory section, we recall basic definitions of various qubit and qutrit gate sets, and the various cyclotomic rings and their localizations and the notions of smallest denominator exponent and greatest dividing exponent used throughout the paper.

Definition 2.1. *The single qubit Clifford+T gate set is generated by the following matrices:*

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & \zeta_8 \end{bmatrix}$$

where $\zeta_8 = e^{\frac{2\pi i}{8}}$ is the primitive 8th root of unity.

We will also be interested in qutrit analogue of the single qubit Clifford+T group which is defined as follows:

Definition 2.2. *The single qutrit Clifford+T group is generated by the following matrices:*

$$H = -\frac{i}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} \qquad S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad T = \begin{bmatrix} \xi & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi^{-1} \end{bmatrix}$$

where $\xi = e^{\frac{2\pi i}{9}}$ which is the primitive 9th root of unity.

For qutrits, another universal gate set referred to as the Clifford+R gate set [8] is defined as follows:

Definition 2.3. *The single qutrit Clifford+R gate set is generated by:*

$$H = \frac{1}{\sqrt{-3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} \qquad S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

The R gate is sometimes referred to as the metaplectic gate. As shown in [8], the multi-qutrit Clifford+R gate set is a subset of multi-qutrit Clifford+T gate set. We define the Clifford+$\mathcal{D}$ gate set which can be thought of as the single qutrit analogue of the Clifford Cyclotomic gate set discussed in [6]:

Definition 2.4. *The single qutrit Clifford+$\mathcal{D}$ gate set is generated by the following gates:*

$$H = \frac{1}{\sqrt{-3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} \qquad D_{[a,b,c]} = \begin{bmatrix} \xi^a & 0 & 0 \\ 0 & \xi^b & 0 \\ 0 & 0 & \xi^c \end{bmatrix} \qquad R_{[a,b,c]} = \begin{bmatrix} (-1)^a & 0 & 0 \\ 0 & (-1)^b & 0 \\ 0 & 0 & (-1)^c \end{bmatrix}$$

where $\xi = e^{\frac{2\pi i}{9}}$. Here we denote all gates of the form $diag(\pm\xi^a, \pm\xi^b, \pm\xi^c)$ as $\mathcal{D}$. Often we drop the subscript $[a, b, c]$ from $D_{[a,b,c]}$ and simply write D. We denote $R := R_{[0,0,1]}$ as it is frequently used.

Note that a D gate is a diagonal operator in the Clifford Hierarchy [4]. More generally, one can define the qudit version of the Clifford+T gate set for odd prime dimensions as follows:

Definition 2.5. *The single qudit Clifford+T group is generated by the following:*

$$H = \frac{1}{\sqrt{p}} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} {\zeta_p}^{ij} |i\rangle \langle j| \quad S = \sum_{j=0}^{p-1} {\zeta_p}^{j(j+1)2^{-1}} |j\rangle \langle j| \quad T = \sum_{j=0}^{p-1} \zeta_p^{j^3 6^{-1}} |j\rangle \langle j|$$

Note that for qudits of odd prime dimension $p > 3$, the T gate requires only the powers of ζ_p and no higher roots of unity as explained in [10]. It is well known that these single qutrit gate sets are universal for quantum computation when supplemented with an appropriately chosen two qutrit entangling gate.
We now recall the definition of certain rings which are used later in the paper and are closely connected to exact synthesis. Note that the ring R "localized" at χ is denoted as R_χ:

Definition 2.6. *Let p be a prime, $l \geq 1$ an integer, denote $n = p^l$, and $R_n := \mathbb{Z}[\zeta_n]$ be the ring of cyclotomic integers, i.e., ζ_n is a primitive n-th root of unity and $R_{n,\chi} := \{\frac{a}{\chi^f} : a \in R_n\}$, where $\chi = 1 - \zeta_{p^n}$ i.e., it is the ring obtained by allowing powers of χ in the denominators. We denote by $U(p, R_{n,\chi})$ the group of $p \times p$ unitary matrices whose entries are in $R_{n,\chi}$. We will suppress the subscript n for both R_n and $R_{n,\chi}$ when it is clear from the context. We will also write ζ in place of ζ_n, when n is clear from the context.*

It is easy to see that $U(p, R_\chi)$ is a group since the inverse of a unitary is its conjugate transpose and that $\overline{\chi} = 1 - \zeta^{-1} = -\zeta^{-1}\chi$.

Remark 2.7.

1. *When $n = 2^3$, the ring R_χ is precisely $\mathbb{Z}[e^{\frac{2\pi i}{8}}, 1/\sqrt{2}] = \mathbb{Z}[i, 1/\sqrt{2}]$ the ring in [14]. When $n = 3$ the ring is the one considered in [2].*
2. *For arbitrary $n = p^l$, the gates Clifford+$\mathcal{D}$ (which includes the T gate) are contained in $U(p, R_\chi)$.*

More explicitly, we can describe the rings R_n and $R_{n,\chi}$ in the cases where $n = 3, 8$ and 9 as follows:

- $R_8 = \{\sum_{i=0}^{i=3} a_i \zeta_8^i \mid a_i \in \mathbb{Z},\ \zeta_8 = e^{\frac{2\pi i}{8}}\}$
- $R_{8,\chi} = \{\frac{a}{\chi^f} \mid a \in R_8,\ f \in \mathbb{Z}_{\geq 0}\}$
- $R_9 = \mathbb{Z}[\xi] := \{\sum_{i=0}^{5} a_i \xi^i \mid a_i \in \mathbb{Z},\ \xi = e^{\frac{2\pi i}{9}}\}$
- $R_{9,\chi} = \{\frac{a}{\chi^f} \mid a \in R_9,\ f \in \mathbb{Z}_{\geq 0}\}$
- $R_3 = \{a_0 + a_1\omega \mid a_i \in \mathbb{Z},\ \omega = e^{\frac{2\pi i}{3}}\}$
- $R_{3,\chi} = \{\frac{a}{\chi^f} \mid a \in R_3,\ f \in \mathbb{Z}_{\geq 0}\}$

In general, for qudits we will have the ring $R_\chi = \{\frac{a}{\chi^f} \mid a \in R,\ f \geq 0\}$ where $R = \mathbb{Z}[\zeta]$ and ζ is the primitive nth root of unity for some $n = p^l$.
We will now define two key notions which are in fact the main tool to study exact synthesis:

Definition 2.8. *The smallest denominator exponent (sde) of $z \in R_\chi$ with respect to χ is defined as the smallest non-negative integer f such that $\chi^f z \in R$.*

Definition 2.9. *The greatest dividing exponent (gde) of an element $f(\zeta) \in \mathbb{Z}[\zeta]$ with respect to χ is defined as the largest integer k such that χ^k divides $f(\zeta)$.*

The notions of sde and gde are closely related. If $u = \frac{a}{\chi^f}$, for $a \in \mathbb{Z}[\xi]$, then we have

$$sde(u) = \max\{0, f - gde(a)\}.$$

Example 2.10. *Let* $g = \frac{f(\xi)}{3}$, *where* $f(\xi) = 1 + \xi + \xi^2 \in \mathbb{Z}[\xi]$. *We see that* $f(\xi) = 1 + (1-\chi) + (1-\chi)^2 = 3 - \chi - 2\chi + \chi^2 = u\chi^6 - u\chi^7 + \chi^2 = \chi^2(1 + u\chi^4 - u\chi^5)$. *Therefore,* $gde(f(\xi), \chi) = 2$ *and* $sde(g, \chi) = 4$.

Example 2.11. *Let* $n = 3$, *i.e.,* $\omega = e^{\frac{2\pi i}{3}}$. *Since* ω *satisfies* $\omega^2 + \omega + 1 = 0$, *an arbitrary element of* $\mathbb{Z}[\omega]$ *can be written as* $\alpha = a + b\omega$, *where* $a, b \in \mathbb{Z}$. *Note that* $3 = \chi^2 u$, *for some unit* $u \in \mathbb{Z}[\omega]$. *Therefore,* χ *divides* α *iff* $a + b = 0 \pmod 3$.
If $a = 1 \pmod 3$ *and* $b = -1 \pmod 3$ *then* χ^2 *does not divide* α. *Indeed, if* χ^2 *divides* α *then both* a *and* b *are divisible by* 3. *Therefore,* $gde(\alpha, \chi) = 1$.

We briefly discuss a tool to compute the sde of an arbitrary element of $R_{n,\chi}$ for any $n = p^l$, to be fully described in the next section. Consider the map

$$P : \mathbb{Z}[\zeta] \xrightarrow{f(\zeta) \mapsto f(1)} \mathbb{Z}/p$$

The map is a well-defined ring homomorphism with $\ker(P) = \chi$. Indeed, if $f(\zeta) = g(\zeta)$, where $f, g \in \mathbb{Z}[x]$, then $f(x) \equiv g(x) \pmod{\Phi_n(x)}$. It is well known that $\Phi_n(1) = 0 \pmod p$ whenever n is a power of p. Therefore, $f(1) \equiv g(1) \pmod p$. Note that $f(1) = 0 \pmod p$ iff χ divides $f(\zeta)$. This essentially follows from the remainder theorem, i.e., $f(\zeta) = f(1) + \chi g(\zeta)$, for some $g(\zeta) \in \mathbb{Z}[\zeta]$ and the fact that $p = u\chi^{\phi(n)} = u\chi^{p^{l-1}(p-1)}$, for some unit u in $\mathbb{Z}[\zeta]$. Note that the map P already captures the divisibility of an element in $\mathbb{Z}[\zeta]$ by χ. In the next section, we introduce higher analogues of P which capture the divisibility of an element in $\mathbb{Z}[\zeta]$ by χ^k.

3 Derivatives mod p

In this section, we shall make sense of differentiation of elements of the ring of cyclotomic integers $\mathbb{Z}[\zeta]$, modulo a prime p, where ζ is a primitive $n = p^l$-th root of unity, for $l \geq 1$. The morphism $\mathbb{Z}[x] \to \mathbb{Z}[\zeta]$ defined by $f(x) \mapsto f(\zeta)$ is a ring homomorphism whose kernel is generated by $\Phi_n(x)$, the n-th cyclotomic polynomial. In other words, $f(\zeta) = g(\zeta)$ iff $f(x) \equiv g(x) \pmod{\Phi_n(x)}$. The polynomial $\Phi_n(x)$ is monic and irreducible in the ring $\mathbb{Z}[x]$ and has degree $\phi(n) = p^{l-1}(p-1)$, the Euler totient of n. More explicitly,

$$\Phi_n(x) = \prod_{k:\ gcd(k,n)=1} (x - \zeta^k)$$

It is well known that:

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

By applying the above identity for $n = p$ and p^2, we have $x^p - 1 = \Phi_1(x)\Phi_p(x)$, $x^{p^2} - 1 = \Phi_1(x)\Phi_p(x)\Phi_{p^2}(x)$ where $\Phi_1(x) = x - 1$. These imply $\Phi_p(x) = x^{p-1} + \ldots + 1$ and $\Phi_{p^2}(x) = (x^p)^{p-1} + (x^p)^{p-2} \ldots + x^p + 1$ respectively. In particular, when $p = 3$, $\Phi_3(x) = x^2 + x + 1$ and $\Phi_9(x) = x^6 + x^3 + 1$. Similarly $\Phi_8(x) = x^4 + 1$. More generally, we have

$$\Phi_{p^l}(x) = \frac{x^{p^l} - 1}{x^{p^{l-1}} - 1} = \sum_{j=0}^{p-1} x^{jp^{l-1}}$$

Remark 3.1. *By substituting $x = 1$ in the above identity we obtain*

$$p = \prod_{k:\ \gcd(k,n)=1} (1-\zeta^k) = (1-\zeta)^{\phi(n)} \prod_{k:\ \gcd(k,n)=1} \frac{1-\zeta^k}{1-\zeta}$$

For integers k such that $gcd(k,n) = 1$, $\frac{1-\zeta^k}{1-\zeta}$ is in fact a unit. Therefore, we may write $p = (1-\zeta)^{\phi(n)}u$ for some unit u in $\mathbb{Z}[\zeta]$.

The following lemma follows easily from the above identity. Although, we only need this lemma for $n = 3, 8, 9$ and $n = p$ for prime $p \geq 5$.

Lemma 3.2. *For $0 \leq k < \phi(p^l) = p^{l-1}(p-1)$,*

$$\frac{\Phi_{p^l}^{(k)}(1)}{k!} \equiv 0 \pmod{p}$$

Proof. If $y = x^{p^{l-1}} - 1$ then the above identity can be written as

$$\Phi_{p^l}(x) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{p-1} y^{p-2} + \ldots + \binom{p}{1}$$

Now the lemma follows from the fact that p divides $\binom{p}{j}$ for $1 \leq j \leq p-1$. □

Example 3.3. *We may verify the above lemma for $n = 9$ by explicit computation. Using $\Phi_9(x) = x^6 + x^3 + 1$, we may compute $\frac{\Phi_9^{(1)}(1)}{1!} = 6x^5 + 3x^2|_{x=1} = 9$, $\frac{\Phi_9^{(2)}(1)}{2!} = 30x^4 + 6x|_{x=1} = 36$, $\frac{\Phi_9^{(3)}(1)}{3!} = \frac{1}{3!}120x^3 + 6|_{x=1} = 21$, $\frac{\Phi_9^{(4)}(1)}{4!} = \frac{1}{4!}360x^2|_{x=1} = 360/24 = 15$, $\frac{\Phi_9^{(5)}(1)}{5!} = \frac{1}{5!}720x|_{x=1} = 6$, and $\frac{\Phi_9^{(6)}(1)}{6!} = 720/6! = 1$. Observe that $\frac{\Phi_9^{(k)}(1)}{k!} \equiv 0 \pmod 3$ for $0 \leq k \leq 5$.*

Proposition 3.4. *Let $f(x), g(x) \in \mathbb{Z}[x]$ such that $f(\zeta) = g(\zeta)$, where ζ is an n-th root of unity, $n = p^l, l \geq 1$. For every $0 \leq k < \phi(n) = p^{l-1}(p-1)$*

$$\frac{f^{(k)}(1)}{k!} = \frac{g^{(k)}(1)}{k!} \pmod{p}$$

Proof. As we noted before, $f(\zeta) = g(\zeta)$ if and only if $f(x) = g(x) \pmod{\Phi_n(x)}$, i,e., $f(x) = g(x) + h(x)\Phi_n(x)$ for some $h(x) \in \Phi_n(x)$. By differentiating on both sides k times and dividing by $k!$ we get

$$\frac{f^{(k)}(x)}{k!} = \frac{g^{(k)}(x)}{k!} + \sum_{r=0}^{k} \frac{h^{(r)}(x)}{r!} \frac{\Phi_n^{(k-r)}(x)}{(k-r)!}$$

By substituting $x = 1$, the proposition follows from Lemma 3.2. □

Definition 3.5. *Let $\zeta = \zeta_{p^l}$ be a primitive p^l-th root of unity and $f(\zeta) \in \mathbb{Z}[\zeta]$. For $0 \leq k \leq \phi(p^l)$ we define the k-th derivative modulo p as $\frac{f^{(k)}(1)}{k!} \pmod p$.*

The above proposition makes the notion of 'k-th derivative mod p' well-defined.
Let $q : \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/(p)$ be the usual quotient map mod p. For $f(x) \in \mathbb{Z}[x]$, suppose $f(x) = \sum a_i(1-x)^i$. We have $\frac{f^{(k)}(1)}{k!} = a_k$ for all k. In particular, when $x = \zeta$ and $\chi := 1 - \zeta$, $f(\zeta) = \sum a_i \chi^i$. Therefore, the 'derivatives mod p' are precisely the Taylor coefficients of $f(x)$ modulo p at $x = 1$.

Remark 3.6. *Note that since $\Phi_n(x)$, the minimal polynomial of ζ, is monic of degree $\phi(n)$, we may always assume that the degree of $f(x)$ is less than $\phi(n)$. Therefore, $\frac{f^{(k)}(1)}{k!} = 0 \pmod p$ for $k > \phi(n)$.*

The following theorem relates these derivatives with the gde of elements of $\mathbb{Z}[\zeta]$, therefore giving a straight forward and efficient algorithm to compute the gde of any arbitrary element of $\mathbb{Z}[\zeta]$.

Theorem 3.7. *Let $n = p^l$, $l \geq 1$ and $1 \leq k \leq \phi(n)$ for a prime p. Let $f(x)$ be an arbitrary polynomial with integer coefficients then*

$$\chi^k \text{ divides } f(\zeta) \text{ iff } f(1) = \tfrac{f^{(1)}(1)}{1!} = \ldots = \tfrac{f^{(k-1)}(1)}{(k-1)!} = 0 \mod p$$

Proof. We may write

$$f(\zeta) = f(1-\chi) = \sum_{i=0}^{d} a_i(-\chi)^i$$

We may assume $d < \phi(n)$ by Remark 3.6. Suppose χ^k divides $f(\zeta)$ for $k \geq 1$ then it is immediate that χ divides a_0. Since a_0 is an integer, the norm $N(\chi) = p$ divides a_0. However, $p = u\chi^{\phi(n)}$ for some unit u in $\mathbb{Z}[\zeta]$. In particular, this implies χ divides a_1 which again implies $N(\chi) = p$ divides a_1. Carrying on iteratively, we may obtain $a_0 = \ldots = a_{k-1} = 0 \pmod p$. Conversely, if $a_0 = \ldots = a_{k-1} = 0 \pmod 3$ then χ^k obviously divides $f(\xi)$ by the above Taylor expansion for f. This concludes the proof of the theorem. □

4 Unit vectors and unitary matrices with entries in $R_\chi = \{\frac{a}{\chi^f} : a \in \mathbb{Z}[\zeta]\}$

In this section, we characterize qutrit unit vectors of a given sde f as integer vectors $a := (a_0, \ldots, a_5), b := (b_0, \ldots, b_5), c := (c_0, \ldots, c_5) \in \mathbb{Z}^6$ satisfying certain integral quadratic forms. This yields us an algorithm to give a list of all unit vectors of sde f whose complexity is equivalent to the complexity of finding $a, b, c \in \mathbb{Z}^6$ such that

$$q(a) + q(b) + q(c) = N$$

where $N = O(3^{\frac{f}{3}})$ and $q(a) := \frac{1}{4}((2a_0 - a_3)^2 + 3a_3^2 + (2a_1 - a_4)^2 + 3a_4^2 + (2a_2 - a_5)^2 + 3a_5^2)$.

Let $R = \mathbb{Z}[\xi], \xi = e^{\frac{2\pi i}{9}}, \chi = 1 - \xi$ and $R_\chi := \{\frac{a}{\chi^f} : a \in R\}$. In this section, we study qutrit unit vectors with entries in R_χ, i.e., $z = (z_1, z_2, z_3) \in R_\chi^3$ such that $|z_1|^2 + |z_2|^2 + |z_3|^2 = 1$. Note that we may write $z = \frac{1}{\chi^f}(w_1, w_2, w_3)$, where $\chi \nmid w_i$, for some some i and an integer $f \geq 0$. The integer f is the smallest denominator exponent (sde) of z.

Recall that the map $P : \mathbb{Z}[\xi] \to \mathbb{Z}_3$, defined by $P(f(\xi)) = f(1) \pmod 3$ is well defined. The unit vector condition can be rewritten as

$$|w_1|^2 + |w_2|^2 + |w_3|^2 = |\chi|^{2f} \tag{1}$$

If $f \geq 1$, by applying the map P to this equation gives $\sum_{i=1}^{3} w_i(1)^2 = 0$. This implies that $w_i(1) = \pm 1$, for all i, in other words $\chi \nmid w_i$ for all i.

Let $\tau := \xi + \xi^{-1}$. Note that the subring $\mathbb{Z}[\tau] \subset \mathbb{Z}[\xi]$ is precisely the set of real elements of $\mathbb{Z}[\xi]$. The minimal polynomial of τ is $x^3 - 3x + 1$. Therefore $1, \tau, \tau^2$ form a basis of $\mathbb{Z}[\tau]$ over $\mathbb{Z}$. Since $|w_i|^2$ are real numbers, we may express them as an integral linear combination of

$1, \tau, \tau^2$. This allows us to reduce Equation 1 to a system of equations of integral quadratic forms by writing $|w_i|^2$ on the LHS and $|\chi|^2$ on the RHS with respect to the basis $1, \tau, \tau^2$. First, an element $f(\xi)$ of $\mathbb{Z}[\xi]$ can be written uniquely as $f(\xi) = \sum_{i=0}^{5} a_i \xi^i$, where $a_i \in \mathbb{Z}$. We have

$$|f(\xi)|^2 = \sum_{0 \le i,j \le 5} a_i a_j \xi^i \xi^{-j} \tag{2}$$

$$= \sum_{i=0}^{5} a_i^2 + \sum_{1 \le i < j \le 5} a_i a_j (\xi^{i-j} + \xi^{j-i}) \tag{3}$$

$$= \sum_{i=0}^{5} a_i^2 + \sum_{k=1}^{5} \Big(\sum_{i<j, |i-j|=k} a_i a_j \Big)(\xi^k + \xi^{-k}) \tag{4}$$

We denote $\alpha_k = \sum_{i \le j, |i-j|=k} a_i a_j$. Therefore, $|f(\xi)|^2 = \alpha_0 + \sum_{k=1}^{5} \alpha_k \tau_k$.
Recall that $\xi^9 = 1$ and the minimal polynomial of ξ is the cyclotomic polynomial $\Phi_9(x) = x^6 + x^3 + 1$. Denote $\tau_k = \xi^k + \xi^{-k}$, for $0 \le k \le 5$, and $\tau := \tau_1$. It is straightforward to write τ_k in terms of τ as follows

$$\tau_2 = \tau^2 - 2 \tag{5}$$

$$\tau_3 = \xi^3 + \xi^{-3} = -1 \tag{6}$$

$$\tau_4 = -\tau^2 - \tau + 2 \tag{7}$$

$$\tau_5 = \tau_4 = -\tau^2 - \tau + 2 \tag{8}$$

The expression for τ_4 is derived as $\tau^4 = \xi^4 + 4\xi^3\xi^{-1} + 6\xi^2\xi^{-2} + 4\xi^1\xi^{-3} + \xi^{-4} = \tau_4 + 4\tau_2 + 6 = 3\tau^2 - \tau \implies \tau_4 = 3\tau^2 - \tau - 4\tau_2 - 6 = 3\tau^2 - \tau - 4(\tau^2 - 2) - 6 = -\tau^2 - \tau + 2$. Therefore, we find

$$|f(\xi)|^2 = \alpha_0 + \alpha_1\tau + \alpha_2(\tau^2 - 2) + \alpha_3(-1) + \alpha_4(-\tau^2 - \tau + 2) + \alpha_5(-\tau^2 - \tau + 2) \tag{9}$$

$$= \underbrace{(\alpha_0 - 2\alpha_2 - \alpha_3 + 2\alpha_4 + 2\alpha_5)}_{q_0} + \underbrace{(\alpha_1 - \alpha_4 - \alpha_5)}_{q_1}\tau + \underbrace{(\alpha_2 - \alpha_4 - \alpha_5)}_{q_2}\tau^2 \tag{10}$$

We may view $q_i = q_i(a_0, \ldots, a_5)$ (also written as $q_i(a)$) as quadratic forms in the six variables $a = (a_0, \ldots, a_5)$. In particular, if $w_1(\xi) = \sum_{j=0}^{5} a_j \xi^j$, $w_2(\xi) = \sum_{j=0}^{5} b_j \xi^j$ and $w_3 = \sum_{j=0}^{5} c_j \xi^j$ then $|w_1|^2 = q_0(a) + q_1(a)\tau + q_2(a)\tau^2, |w_2|^2 = q_0(b) + q_1(b)\tau + q_2(b)\tau^2$ and $|w_3|^2 = q_0(c) + q_1(c)\tau + q_2(c)\tau^2$. Therefore, the unit vector condition implies

$$(q_0(a)+q_0(b)+q_0(c)) + (q_1(a)+q_1(b)+q_1(c))\tau + (q_2(a)+q_2(b)+q_2(c))\tau^2 = |\chi|^{2f} = A + B\tau + C\tau^2,$$

for some integers A, B and C. By the linear independence of $\{1, \tau, \tau^2\}$ in $\mathbb{Z}[\tau]$ over $\mathbb{Z}$, we have

$$q_0(a) + q_0(b) + q_0(c) = A$$
$$q_1(a) + q_1(b) + q_1(c) = B$$
$$q_2(a) + q_2(b) + q_2(c) = C$$

Note that given f, the integers A, B and C are easily computable by writing $|\chi|^2 = (1-\xi)(1-\xi^{-1}) = 2-\tau$, and therefore using the binomial theorem to expand $|\chi|^{2f} = (2-\tau)^f$. Since τ satisfies its minimal polynomial $\tau^3 - 3\tau + 1 = 0$, we can write any τ^k for $k \ge 3$ as an integral linear combination of $1, \tau$ and τ^2. In the following examples, we fully describe A, B and C using a minor simplification.

Example 4.1.

1. *For* $f = 0$, $(A, B, C) = (1, 0, 0)$.
2. *For* $f = 1$, $(A, B, C) = (2, -1, 0)$.
3. *For* $f = 2$, $|\chi|^{2f} = (2-\tau)^2 = 4 - 4\tau + \tau^2$, *therefore* $(A, B, C) = (4, -4, 1)$.
4. *For* $f = 3$, $\chi^{2f} = (2-\tau)^3 = 8 - 12\tau + 6\tau^2 - \tau^3 = 9 - 15\tau + 6\tau^2$. *Therefore,* $(A, B, C) = (9, -15, 6)$. *However, in this case we can simplify the above quadratic form equations by observing that* $3 = \chi^6 u$ *for some unit* u *in* $\mathbb{Z}[\xi]$. *Indeed, simply multiply* $|u|^2$ *on both sides of Equation 1, which gives us* 3 *on the RHS. Therefore, we may assume* $(A, B, C) = (3, 0, 0)$.
5. *In fact, by applying the reasoning in the above example we can simplify the RHS for any* $f \geq 3$. *Indeed, write* $|\chi|^{2f} = 3^r(2-\tau)^s$, *where* $r = \lfloor \frac{f}{3} \rfloor$ *and* $s = f \pmod 3$, *the remainder of* f *upon division by* 3, *therefore* $0 \leq s \leq 2$. *In other words, we may always assume* $(A, B, C) = 3^r(1, 0, 0)$ *(when* $s = 0$*) or* $3^r(2, -1, 0)$ *(when* $s = 1$*) or* $3^r(4, -4, 1)$ *(when* $s = 2$*).*

We record our observations so far as follows.

Lemma 4.2. *Assume* $f \geq 3$ *and let* $w_1(\xi) = \sum_{j=0}^5 a_j \xi^j$, $w_2(\xi) = \sum_{j=0}^5 b_j \xi^j$ *and* $w_3 = \sum_{j=0}^5 c_j \xi^j$. *If* $z = \frac{1}{\chi^f}(w_1, w_2, w_3)$ *is a unit vector then* $a, b, c \in \mathbb{Z}^6$ *satisfy*

$$\begin{aligned} q_0(a) + q_0(b) + q_0(c) &= A \\ q_1(a) + q_1(b) + q_1(c) &= B \\ q_2(a) + q_2(b) + q_2(c) &= C \end{aligned}$$

for some integers A, B *and* C *which are determined by* $A + B\tau + C\tau^2 = 3^r(2-\tau)^s$, *where* $r = \lfloor \frac{f}{3} \rfloor$ *and* $s = f \pmod 3$. *By the linear independence of* $1, \tau, \tau^2$ *over* $\mathbb{Z}$, *we can explicitly write down* A, B *and* C *for a given* f.

Theorem 4.3. *For* $p = 3$, *there exists finitely many (including zero) unit vectors with fixed sde* f. *The problem of listing all unit vectors with a given sde* f *reduces to finding all the integer solutions of a positive-definite quadratic form in* 18 *variables.*

Proof. First, observe that

$$\begin{aligned} q = q_0 + 2q_2 = \alpha_0 - \alpha_3 &= \sum_{i=0}^5 a_i^2 - a_0a_3 - a_1a_4 - a_2a_5 && (11) \\ &= (a_0^2 + a_3^2 - a_0a_3) + (a_1^2 + a_4^2 - a_1a_4) + (a_2^2 + a_5^2 - a_2a_5) && (12) \\ &= \frac{1}{4}((2a_0 - a_3)^2 + 3a_3^2 + (2a_1 - a_4)^2 + 3a_4^2 + (2a_2 - a_5)^2 + 3a_5^2) && (13) \end{aligned}$$

which is a positive definite quadratic form.
By the above lemma, for a unit vector $z = \frac{1}{\chi^f}(w_1, w_2, w_3)$ of sde f, the three 6-tuples $a, b, c \in \mathbb{Z}^6$ must satisfy

$$q(a) + q(b) + q(c) = A + 2C$$

□

Remark 4.4. *Suppose $a \in \mathbb{Z}^6$ such that $q(a) = 1$, then exactly one of the three integers $a_0^2+a_3^2-a_0a_3, a_1^2+a_4^2-a_1a_4$ or $a_2^2+a_5^2-a_2a_5$ is $= 1$ and the other two are $= 0$. Assuming $a_0^2 + a_3^2 - a_0a_3 = 1$, we have $a = (\pm1, 0, 0, 0, 0, 0)$ or $(0, 0, 0, \pm1, 0, 0)$ or $(1, 0, 0, 1, 0, 0)$ or $(-1, 0, 0, -1, 0, 0)$. In other words, the corresponding element in $\mathbb{Z}[\xi]$ is $w_1(\xi) = \pm\xi^3$ or $1+\xi^3$ or $-1-\xi^3$. Since ξ satisfies its minimal polynomial x^6+x^3+1, we have $\xi^6 = -(1+\xi^3)$. Therefore, $w_1(\xi) = \pm1$ or $\pm\xi^3$ or $\pm\xi^6$. Similarly when $a_1^2 + a_4^2 - a_1a_4 = 1$ (resp. when $a_2^2 + a_5^2 - a_2a_5 = 1$) we have $w_1(\xi) = \pm\xi$ or $\pm\xi^4$ or $\pm\xi^7$. (resp. $\pm\xi^2$ or $\pm\xi^5$ or $\pm\xi^8$). Therefore, all the possibilities for $w_1(\xi)$, namely $\pm\xi^a$, where $a \in \{0, \ldots, 8\}$ are in fact possible.*

Corollary 4.5. *Let $z = \frac{1}{\chi^f}(w_1, w_2, w_3) \in R_\chi^3$ be a unit vector such that $\chi \nmid w_i$ for all i, i.e, $sde(z, \chi) = f$.*

(1.) If $f = 0$ then $z = (\pm\xi^a, 0, 0)$ up to permutation of coordinates, for some $a \in \mathbb{Z}$.

(2.) If $f = 3$ then $z = \frac{1}{\chi^3}(\pm\xi^a, \pm\xi^b, \pm\xi^c)$.

Proof. When $f = 0$, we have $q(a) + q(b) + q(c) = 1 + 2(0) = 1$. Since q is positive definite and takes integral values, $q(a) = 1$ and $q(b) = q(c) = 0$ up to permutation of a, b and c. Then by Remark 4.4, the corollary follows.
When $f = 3$, we have $q(a) + q(b) + q(c) = 3 + 2(0) = 3$. Therefore $q(a) = q(b) = q(c) = 1$. It follows that $(w_1(\xi), w_2(\xi), w_3(\xi)) = (\pm\xi^a, \pm\xi^b, \pm\xi^c)$ for some integers a, b and c. □

Now we argue that the unitary matrices in $U(3, R_\chi)$ of sde 3 are precisely the ones of the form D_1HD_2, for some matrices $D_1, D_2 \in U(3, R_\chi)$ of sde 0. For this we first derive relations between two orthogonal unit vectors of sde 3.

Remark 4.6. *Two unit vectors $z_1 = \frac{1}{\chi^3}(\xi^{a_1}, \xi^{a_2}, \xi^{a_3})$ and $z_2 = \frac{1}{\chi^3}(\xi^{b_1}, \xi^{b_2}, \xi^{b_3})$ of sde 3, are orthogonal iff $\xi^{a_1-b_1}+\xi^{a_2-b_2}+\xi^{a_3-b_3} = 0$ iff $1+\xi^p+\xi^q = 0$, where $p = (a_2-b_2)-(a_1-b_1) = (a_2 - a_1) - (b_2 - b_1)$ and $q = (a_3 - b_3) - (a_1 - b_1) = (a_3 - a_1) - (b_3 - b_1)$. Note that by taking conjugate of this equation we get $\xi^p + \xi^q = \xi^{-p} + \xi^{-q}$ which implies $\xi^{p+q} = 1$ and therefore, $p + q = 0 \pmod 9$, so $(p, q) = (3, 6)$ or $(6, 3) \pmod 9$.*

From the above remark if z_1, z_2, z_3 are mutually orthogonal unit vectors of sde 3, then after an appropriate permutation we may write the matrix with z_i as columns as

$$[z_1, z_2, z_3] = \mathrm{diag}(\pm\xi^{\alpha_1}, \pm\xi^{\alpha_2}, \pm\xi^{\alpha_3}) * H * \mathrm{diag}(\pm\xi^{\beta_1}, \pm\xi^{\beta_2}, \pm\xi^{\beta_3}),$$

for some integers α_i, β_i.
This observation shows that the choice of gates Clifford+$\mathcal{D}$ is not arbitrary, as the H gate naturally arises as the unique gate of sde 3 modulo multiplication by matrices of sde 0 on both sides.

5 Main results

In the following lemma we observe that the sde of the entries of a given unit vector in $R_{8,\chi}^2$ or $R_{3,\chi}^3$ or $R_{9,\chi}^3$ are equal.

Lemma 5.1.

(i) Suppose $z = (z_1, z_2)^T$ is a unit vector whose entries are in $R_{8,\chi}$. Then $sde(z_1) = sde(z_2)$

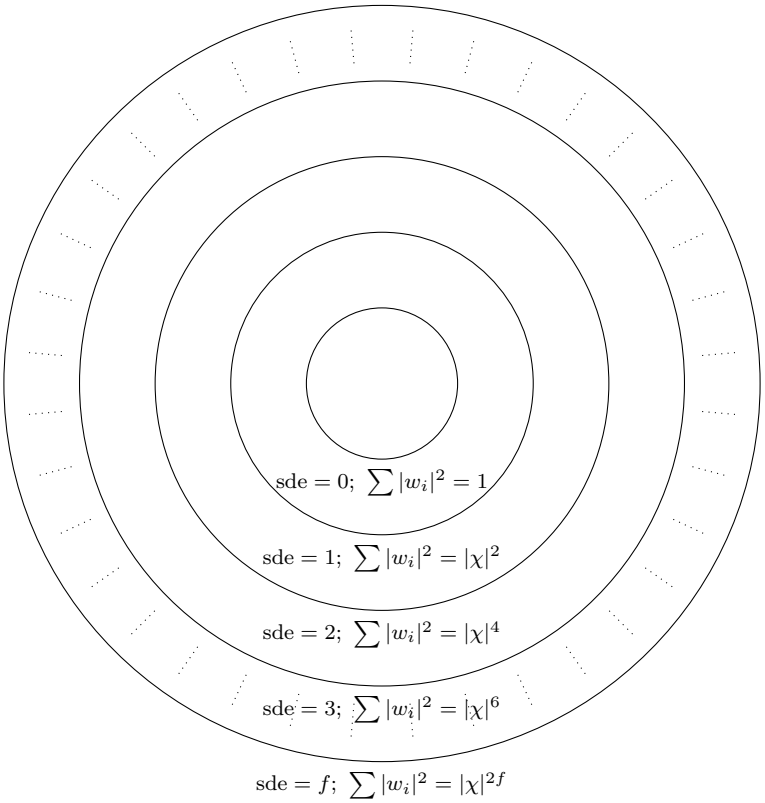

Figure 1: Unit vectors $R^p_{n,\chi}$ can be partitioned by their smallest denominator exponent. By multiplying a unit vector of a given sde by a unitary U in $U(p, R_{n,\chi})$ we may change its sde. Having control of this change by choosing an appropriate unitary U helps us in exact synthesis in $U(p, R_{n,\chi})$. In what follows we study the possibility of this phenomenon when $n = p^l = 3, 8, 9$.

(ii) Suppose $z = (z_1, z_2, z_3)$ is a unit vector whose entries are in $R_{3,\chi}$ or $R_{9,\chi}$. Then $sde(z_1) = sde(z_2) = sde(z_3)$

Proof. Write $z = \frac{1}{\chi^f}(w_1, w_2)^T$ in case 1 and $z = \frac{1}{\chi^f}(w_1, w_2, w_3)^T$ in case 2. By writing the unit vector condition for z and applying the maps $P : \mathbb{Z}[\omega] \to \mathbb{Z}_2$ and $P : \mathbb{Z}[\xi] \to \mathbb{Z}_3$ respectively, we get $w_1(1)^2 + w_2(1)^2 = 0 \pmod 2$ and $w_1(1)^2 + w_2(1)^2 + w_3(1)^2 = 0 \pmod 3$ respectively.
The solutions of $w_1(1)^2 + w_2(1)^2 = 0 \pmod 2$ or $w_1(1)^2 + w_2(1)^2 + w_3(1)^2 = 0 \pmod 3$ are such that $w_i(1) = 0$ for all i or $w_i(1) \neq 0$ for all i. □

Remark 5.2. *Moreover, we can argue that given a unitary matrix $U \in U(p, R_{n,\chi})$, when $n = p^l$ and $p \leq 3$ the sde of all the entries of U are equal. Indeed, note that each entry u_{ij} of U is shared by the i-th row u_i and the j-th column w_j of U. Since both u_i and w_j are unit vectors in $R_{n,\chi}$, so the claim follows by the above lemma. Therefore, the notions of sde of an element, a vector and a matrix coincide when $p = 2$ or 3.*

5.1 Qubit Clifford+T

In this section, we give an alternative proof of the main ideas in [14] using the 'derivatives mod p' trick introduced earlier. This also gives us an alternative approach for exact synthesis of a qubit gate U with entries in $\mathbb{Z}[i, \frac{1}{\sqrt{2}}]$. In particular, given a unitary U in $U(2, R_{8,\chi})$ of sde ≥ 3, we consider its first column z and find an integer k such that

$\mathrm{sde}(HT^k z) = \mathrm{sde}(z) - 1$. We do this by computing the derivative of the entry of $HT^k z$ after clearing the denominator $\sqrt{2}$ and by solving certain linear equations mod 2. This is precisely part of lemma 3 of [14]. By proceeding inductively we find integers $k_1, \ldots, k_r$ such that

$$\mathrm{sde}(HT^{k_1} \ldots HT^{k_r} u) = 2$$

We already know all the unit vectors of sde = 2 or lower (in fact, we can find them by the qubit analogue of section 4). Therefore, we recover U as a word in H, T and a sde = 2 matrix. The following remark highlights the simple yet important relation between χ and $\sqrt{2}$.

Remark 5.3. *In $\mathbb{Z}[\zeta_8]$, we have the identity*

$$2 = (1-\zeta_8)(1-\zeta_8^3)(1-\zeta_8^5)(1-\zeta_8^7) = u\chi^4$$

where $\chi = 1-\zeta_8$ and $u = \frac{(1-\zeta_8^3)}{(1-\zeta_8)}\frac{(1-\zeta_8^5)}{(1-\zeta_8)}\frac{(1-\zeta_8^7)}{(1-\zeta_8)}$. This can be obtained by the fact that $\Phi_8(x) = x^4+1 = (x-\zeta_8)(x-\zeta_8^3)(x-\zeta_8^5)(x-\zeta_8^7)$. Here u is a unit in $\mathbb{Z}[\zeta_8]$. We can further simplify this identity by observing that $\zeta_8^5 = \zeta_8^{-3}$ and $\zeta_8^7 = \zeta_8^{-1}$ which gives $2 = \zeta_8^4(1-\zeta_8)^2(1-\zeta_8^3)^2$, i.e., 2 is a perfect square $\mathbb{Z}[\zeta_8]$ which further implies that $\sqrt{2} = \zeta_8^2(1-\zeta_8)(1-\zeta_8^3) \in \mathbb{Z}[\zeta_8]$. This observation immediately gives us that $sde(z,\chi) = 2sde(z,\sqrt{2})$.

We now the prove the lemmas stated in [14] using our methods. Note that we write $\mathrm{sde}(z,\chi)$ as $\mathrm{sde}(z)$.

Lemma 5.4. *(Lemma 2 in [14]) Let $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ be a unit vector with entries in $\mathbb{Z}[\zeta_8]_\chi$ and let $sde(z,\chi) \geq 4$, Then for any integer k:*

$$-1 \leq sde\left(\frac{z_1 + \zeta_8^k z_2}{\sqrt{2}}\right) - sde(z_1) \leq 1 \tag{14}$$

Proof. Now recall that

$$HT^k z = \begin{pmatrix} \frac{z_1+\zeta_8^k z_2}{\sqrt{2}} \\ \frac{z_1-\zeta_8^k z_2}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}\chi^f}\begin{pmatrix} q_1 + \zeta_8^k q_2 \\ q_1 - \zeta_8^k q_2 \end{pmatrix}$$

Let $q := q_1 + \zeta_8^k q_2$ and $q' = q_1 - \zeta_8^k q_2$. Note that $\mathrm{gde}(q) = \mathrm{gde}(q')$ by Lemma 5.1. Let l be the largest integer such that χ^l divides $q = q_1 + \zeta_8^k q_2$, i.e., $l = \mathrm{gde}(q)$. Suppose $l \geq 5$, i.e., χ^5 divides q and q'. Since $q + q' = 2q_1$, we have χ^5 divides $2q_1$. Since $2 = \chi^4 u$ for some unit $u \in \mathbb{Z}[\zeta_8]$, we may conclude that χ divides q_1 which is a contradiction. Therefore, $l \leq 4$.

On the other hand, $q(1) = q_1(1) + q_2(1) = 0 \pmod 2$. Therefore, χ divides $q(1)$ and hence $l \geq 1$.

Since χ^2 divides $\sqrt{2}$, we have

$$\mathrm{sde}(HT^k z) = \mathrm{sde}(z) + 2 - l$$

Therefore,

$$\mathrm{sde}(HT^k z) - \mathrm{sde}(z) = 2 - l$$

Since $1 \leq l \leq 4$

$$-1 \leq \mathrm{sde}\left(\frac{z_1 + \zeta_8^k z_2}{\sqrt{2}}\right) - \mathrm{sde}(z_1) \leq 2$$

If $\text{sde}(z) \geq 3$ then we may in fact conclude that $\text{sde}\left(\frac{z_1+\zeta_8^k z_2}{\sqrt{2}}\right) - \text{sde}(z_1) \leq 1$ by a finer analysis of q and q'. However, we skip the proof. □

Let $z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \frac{1}{\chi^f}\begin{pmatrix} q_1 \\ q_2 \end{pmatrix}$ and $q(\zeta_8) = q_0 + \zeta_8^k q_1$ as above. Note that the first three derivatives of $q(\zeta_8)$ (starting from 0-th) at $\omega = 1$ are $q(1) = q_0(1) + q_1(1)$, $q'(1) = q_0'(1) + q_1'(1) + kq_1(1)$ and $\frac{q^{(2)}(1)}{2!} = \frac{q_1^{(2)}(1)}{2!} + \frac{q_2^{(2)}(1)}{2!} + kq_2'(1) + \binom{k}{2}q_2(1)$. If $k = 2t+e$, where $e = 0$ or 1 then we note that $\binom{k}{1} = e \pmod 2$ and $\binom{k}{2} = t \pmod 2$. This set-up immediately yields us the following theorem.

Theorem 5.5. *(Lemma 3 in [14]) Let $z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \frac{1}{\chi^f}\begin{pmatrix} q_1 \\ q_2 \end{pmatrix}$ be a unit vector in R_χ^2 such that $q_1, q_2 \in R$ and $\chi \nmid q_1, q_2$ then for each $s \in \{-1, 0, 1\}$ there always exists $k \in \{0, 1, 2, 3\}$ such that*

$$sde(HT^k z) - sde(z) = s$$

Proof. First, we notice that $q(1) = q_0(1) + q_1(1) = 0 \pmod 2$ by default. One can choose $e = -q_1'(1) - q_2'(1)$ so that $q'(1) = 0$ and choose $t = -(\frac{q_1^{(2)}(1)}{2!} + \frac{q_2^{(2)}(1)}{2!} + eq_2'(1))$ so that $\frac{q^{(2)}(1)}{2!} = 0$. In summary, we can choose an integer $0 \leq k \leq 3$ such that $q(1) = q'(1) = \frac{q^{(2)}(1)}{2!} = 0 \pmod 2$. By Theorem 3.7 for $n = 8$, χ^3 divides $q(\zeta_8)$, i.e, $\text{sde}(HT^k z) - \text{sde}(z) = 2 - l = -1$.
In a similar vein, we can choose k such that $f(1) = 0$ and $f'(1) \neq 0$ or $f(1) = f'(1) = 0$ and $f''(1) \neq 0$. □

5.2 Qutrit Clifford+R

Let $U \in U(3, R_\chi)$, where $R = \mathbb{Z}[\omega]$, where $\omega = e^{\frac{2\pi i}{3}}$, $\chi = 1-\omega$ and $z = \frac{1}{\chi^f}(p(\omega), q(\omega), r(\omega))^{\mathrm{T}}$ be the first column of U. Here p, q and r are polynomials with integer coefficients such that $\chi \nmid p(\omega), q(\omega)$ and $r(\omega)$. Here $f = sde(z, \chi)$ (denoted as $sde(z)$) by definition. Since ω has $x^2 + x + 1$ as the minimal polynomial over $\mathbb{Z}$, we may assume that p, q, r are polynomials of degree at most 1. In the following remark, we show that $3 = \chi^2 u$ for some unit u in $\mathbb{Z}[\omega]$. Therefore, $sde(H) = 1$.

Remark 5.6. *Recall that $\Phi_3(x) = x^2 + x + 1 = (x - \omega)(x - \omega^2)$, which gives us that $3 = (1 - \omega)(1 - \omega^2) = (1 - \omega)^2\frac{1-\omega^2}{1-\omega} = \chi^2 u$, where $u = \frac{1-\omega^2}{1-\omega}$ is a unit in $\mathbb{Z}[\omega]$. In fact, $\frac{1-\omega^2}{1-\omega} = 1+\omega = -\omega^2$. Therefore, $-3 = \omega^2(1-\omega)^2$ is a perfect square in $\mathbb{Z}[\omega]$, which implies $\sqrt{-3} = \omega(1 - \omega) = \omega\chi$.*

Theorem 5.7. *For every unit vector $z \in R_\chi^3$ of sde $f \geq 1$, there exists integers $0 \leq a_0, a_1, a_2 \leq 2, \epsilon \in \{0, 1\}$ and $\delta \in 0, 1, 2$ such that $sde(HDR^\epsilon X^\delta z, \chi) < sde(z, \chi)$, where $R = diag(1, 1, -1)$ and $D = diag(\omega^{a_0}, \omega^{a_1}, \omega^{a_2})$.*

Proof. We prove this theorem by providing an algorithm for choosing ϵ, δ and D. First note that $(p(1), q(1), r(1)) \pmod 3 = \pm(1, 1, 1)$ or $\pm(1, 1, -1)$ or $\pm(1, -1, 1)$ or $\pm(-1, 1, 1)$. The latter three cases can be reduced to $\pm(1, 1, -1)$ by applying the Pauli gates X or X^2. Indeed, the unit vector condition for z can be written as

$$|p(\omega)|^2 + |q(\omega)|^2 + |r(\omega)|^2 = |\chi|^{2f}$$

By taking the image of the map $P : R \to \mathbb{Z}_3$, we obtain the equation $p(1)^2+q(1)^2+r(1)^2 = 0$ in $\mathbb{Z}_3$. Note that $p(1), q(1)$ and $r(1) \neq 0 \pmod 3$ as χ does not divide any of them. Therefore, you get the possibilities listed above for $(p(1), q(1), r(1))$.
Choose $\epsilon = 1$ if $(p(1), q(1), r(1)) = \pm(1, 1, -1)$ and $\epsilon = 0$ otherwise. In other words, we may replace z with $R^\epsilon X^\delta z$ for appropriate $\epsilon \in \{0, 1\}, \delta \in \{0, 1, 2\}$ and assume that $(p(1), q(1), r(1)) = \pm(1, 1, 1)$.

Now, consider the polynomial $f(x) = x^{a_0}p(x) + x^{a_1}q(x) + x^{a_2}r(x)$. Note that $f(\omega)$ is precisely the first coordinate of $\chi^{f+1}HDR^\epsilon z$ up to multiplication by a unit in $\mathbb{Z}[\omega]$. Therefore, by Lemma 5.1, $\mathrm{sde}(HDU) = \mathrm{sde}(HDz) = \mathrm{sde}(\frac{f(\omega)}{\chi^{f+1}}) = f + 1 - k$, where k is the largest integer for which χ^k divides $f(\omega)$. So $\mathrm{sde}(HDz, \chi) - \mathrm{sde}(z, \chi) = 1 - k < 0$ iff $k \geq 2$, i.e., χ^2 divides $f(\omega)$.
Using the notion of derivatives mod 3 and Theorem 3.7, we have that χ^2 divides $f(\omega)$ iff

$$f(1) = p(1) + q(1) + r(1) = 0 \pmod 3$$

and

$$f'(1) = a_0p(1) + a_1q(1) + a_2r(1) + (p'(1) + q'(1) + r'(1)) = 0 \pmod 3.$$

The first condition is automatically satisfied as $(p(1), q(1), r(1)) = \pm(1, 1, 1)$. Since each of $p(1), q(1)$ and $r(1)$ are non-zero, there exists plenty of triples $(a_0, a_1, a_2) \in \mathbb{Z}_3^3$ for which the second equation is satisfied - simply choose arbitrary a_1 and a_2 then determine a_0. □

Corollary 5.8. *Clifford+R = $U_3(\mathbb{Z}[\omega]_\chi)$*

Proof. By the above theorem, for each $U \in U_3(\mathbb{Z}[\omega]_\chi)$ of sde at least 1, there exists a syllable of the form $HDR^\epsilon X^\delta$ such that $\mathrm{sde}(HDR^\epsilon X^\delta z) \leq \mathrm{sde}(z) - 1$. Therefore, by proceeding inductively there exists a sequences of pairs $(D_1, \epsilon_1, \delta_1), \ldots (D_k, \epsilon_k, \delta_k)$ such that

$$\mathrm{sde}(HD_1R^\epsilon X^{\delta_1}HD_2R^{\epsilon_2} \ldots HD_kR^{\epsilon_k}X^{\delta_k}U) = 0.$$

We know that the matrices of sde 0 in $U_3(\mathbb{Z}[\omega]_\chi)$ are precisely the matrices generated by $\mathrm{diag}(\pm\omega^{a_0}, \pm\omega^{a_1}, \pm\omega^{a_2})$, H^2 and the Pauli gates. □

Algorithm 1 Algorithm for Clifford+R exact synthesis.

Input: $U \in U(3, R_{3,\chi})$, let $z = U|0\rangle$
while $\mathrm{sde}(z) > 0$ **do**
  choose: (D, ϵ, δ), where $D = \mathrm{diag}(\omega^{a_0}, \omega^{a_1}, \omega^{a_2})$ and $\epsilon \in \{0, 1\}$ and $\delta \in \{0, 1, 2\}$
  such that $\mathrm{sde}(HDR^\epsilon X^\delta z) \leq \mathrm{sde}(z) - 1$
  update $z = HDR^\epsilon X^\delta z$

end while

Remark 5.9. *The while loop in Algorithm 1 is guaranteed to terminate since sde(z) decreases in each iteration as shown in Theorem 5.7.*

5.3 Qutrit Clifford+$\mathcal{D}$

Now we turn to the case $n = 3^2$, i.e., $p = 3$ and $l = 2$. We denote $\xi = e^{\frac{2\pi i}{9}}$, a primitive 9-th root of unity. Unlike for $n = 3$ and 8 dealt with in the previous sections, for $n = 9$ the property P fails to hold for a certain set of unit vectors. To be more precise, for each

unit vector $z \in R^3_{9,\chi}$ there exists a $\Delta \in \mathbb{Z}_3$ such that $\mathrm{sde}(HDR^\epsilon X^f z) - \mathrm{sde}(z) = -1$ if and only if $\Delta \neq -1$. Moreover, the Δ can be easily described in terms of the derivatives mod 3 of the entries of z.

We begin by deriving certain basic properties of derivatives (mod 3) of w_i imposed by the unit vector condition, where $z = \frac{1}{\chi^f}(w_1, w_2, w_3)$ and $\chi \nmid w_i$ for some i. Recall that by applying the map $P : w_i(\xi) \mapsto w_i(1) \pmod 3$ to the unit vector condition we may in fact conclude that $\chi \nmid w_i$ for all i. Moreover, for each w_i there is a unique vector $(w_i(1), \ldots, \frac{w_i^{(5)}(1)}{5!}) \in \mathbb{Z}_3^6$ associated to it as discussed Section 3. Recall that this vector is simply the image of w_i via the quotient map $\mathbb{Z}[\xi] \to \mathbb{Z}[\xi]/(3)$ written with respect to the basis $\{1, \bar{\chi}, \ldots, \bar{\chi}^5\}$. Here $\mathbb{Z}[\xi]/(3)$ is a 6 dimensional vector space over $\mathbb{Z}_3$ with $\{1, \bar{\chi}, \ldots, \bar{\chi}^5\}$ as a basis.

If the vector z has sde ≥ 1 the unit vector condition imposes more restrictions on $\frac{w_i^{(k)}(1)}{k!}$ also for $k \geq 1$. We can similarly apply the higher analogues of the map P, defined in section 3, namely the maps $P^{(k)} : R \to \mathbb{Z}_3$, defined by $P^{(k)}(f(\zeta)) = \frac{f^{(k)}(1)}{k!}$ to get the restrictions on higher derivatives of w_i. Note that $|w_i(\zeta)|^2 = w_i(\zeta)\overline{w_i(\zeta)} = w_i(\zeta)w_i(\zeta^{-1})$. The derivative of $w_i(x)w_i(x^{-1})$ is $w_i'(x)w_i(x^{-1}) + w_i(x)w_i'(x^{-1})\frac{-1}{x^2}$, which is 0 at $x = 1$. Therefore, we get a vacuous equation '$0 = 0$' by applying $P^{(1)}$ on both sides of Equation 1.

From now on, let us follow the notation $(p, q, r) := (w_1, w_2, w_3)$ whenever we work with qutrits to avoid cumbersome double indices. We further denote, $p_k := \frac{p^{(k)}(1)}{k!}$ (resp. for q_k and r_k) for $0 \leq k \leq 5$. With this notation we get the following equation by applying $P^{(2)}$ on both sides of Equation 1

$$2p_2p_0 + p_1^2 - \frac{p_0p_1}{2} + 2q_2q_0 + q_1^2 - \frac{q_0q_1}{2} + 2r_2r_0 + r_1^2 - \frac{r_0r_1}{2} = 0.$$

We record this expression for future use in the case where $(p_0, q_0, r_0) = (1, 1, 1)$. Note that all the p_k, q_k, r_k's are elements of $\mathbb{Z}_3$.

Lemma 5.10. *Let $\pi_i := p_i + q_i + r_i$ for $i = 1, 2$. If $(p_0, q_0, r_0) = (1, 1, 1)$ then*

$$-\pi_2 + \pi_1 + p_1^2 + q_1^2 + r_1^2 = 0$$

For the qutrit Hadamard gate H, recall that $\mathrm{sde}(H, \chi) = 3$ as the denominator of H is $\sqrt{-3} = u\chi^3$ for some unit $u \in \mathbb{Z}[\xi]$, where $\chi = 1 - \xi$. For a unitary matrix $U \in U(3, R_\chi)$, by lemma 5.1, the sde's of every coordinate of Uz are equal.

Therefore, $\mathrm{sde}(HDu) \leq \mathrm{sde}(u) - 1$ for some $D = \mathrm{diag}(\xi^{a_1}, \xi^{a_2}, \xi^{a_3})$ if and only if χ^4 divides $f(\xi) = \xi^{a_1}p(\xi) + \xi^{a_2}q(\xi) + \xi^{a_3}r(\xi)$, the first coordinate of $\chi^{3+f}HDz$ up to a unit in $\mathbb{Z}[\xi]$. Theorem 5.12 essentially gives a criterion for the existence of a_1, a_2 and a_3 such that χ^4 divides $f(\xi)$. For this to work we may have to permute the coordinates of z using the X gate and multiply a specific coordinate by -1 using the R gates. We begin with a proposition which reduces the problem to that of existence of a_1, a_2 and a_3 such that χ^3 divides $f(\xi)$.

Proposition 5.11. *Let $z \in R^3_\chi$ be a unit vector. If there exists a $D = \mathrm{diag}(\xi^a, \xi^b, \xi^c)$ such that $\mathrm{sde}(HDz, \chi) \leq \mathrm{sde}(z, \chi)$ then there exits a $D' = \mathrm{diag}(\xi^{a'}, \xi^{b'}, \xi^{c'})$ such that $\mathrm{sde}(HD'z, \chi) < \mathrm{sde}(z, \chi)$.*

Proof. Let $(a, b, c) = (3k_1 + \epsilon_1, 3k_2 + \epsilon_2, 3k_3 + \epsilon_3)$. Since $\mathrm{sde}(H) = 3$ the hypothesis is satisfied if and only if $f(1) = \frac{f^{(1)}(1)}{1!} = \frac{f^{(2)}(1)}{2!} = 0 \pmod 3$. But the first three derivatives depend only on ϵ_i.

Now, we may choose $(a', b', c') = (3k_1' + \epsilon_1, 3k_2' + \epsilon_2, 3k_3' + \epsilon_3)$ so that

$$\frac{f^{(3)}(1)}{3!} = k_1'p_0 + k_2'q_0 + k_3'r_0 + (\epsilon_1 - \epsilon_1^2)p_1 + (\epsilon_2 - \epsilon_2^2)q_1 + (\epsilon_3 - \epsilon_3^2)r_1 \tag{15}$$

$$+ \epsilon_1 p_2 + \epsilon_2 q_2 + \epsilon_3 r_3 + (p_3 + q_3 + r_3) = 0 \tag{16}$$

is satisfied. We can always do this as p_0, q_0 and r_0 are non-zero. □

Theorem 5.12. *Let $z \in R_\chi^3$ be a unit vector, where $R = \mathbb{Z}[\xi]$ and $\chi = 1 - \xi$. There exists a polynomial $g(x_1, x_2) = (x_1 - x_2)^2 + \alpha(x_1 - x_2) + \beta \in \mathbb{Z}_3[x_1, x_2]$ such that $sde(HDR^\epsilon z) \leq sde(z) - 1$ iff $g(x_1, x_2) = 0$ has a solution in $\mathbb{Z}_3^2$ iff $\Delta = \alpha^2 - \beta \neq -1$.*

Proof. As it was discussed in Section 5.2, for the unit vector $z = \frac{1}{\chi^f}(p, q, r)^{\mathrm{T}}$, either $(p(1), q(1), r(1)) = \pm(1, 1, 1)$ or $\pm(1, 1, -1)$ or $\pm(1, -1, 1)$ or $\pm(-1, 1, 1)$. The latter two cases can be reduced to $\pm(1, 1, -1)$ by applying the Pauli gates X or X^2. Now, for the first case choose $\epsilon = 0$ and for the latter, $\epsilon = 1$ i.e., ϵ is chosen in such a way that $R^\epsilon(p(1), q(1), r(1)) = \pm(1, 1, 1)$. In other words, we may replace z with $R^\epsilon X^f z$ for appropriate $\epsilon \in \{0, 1\}, f \in \{0, 1, 2\}$ and assume that $(p(1), q(1), r(1)) = \pm(1, 1, 1)$.
To choose D such that $\mathrm{sde}(HDz) \leq \mathrm{sde}(z) - 1$ is equivalent to choosing $0 \leq a_1, a_2, a_3 \leq 8$ such that χ^4 divides $f(\xi)$. By Theorem 3.7, χ^4 dividing $f(\xi)$ is equivalent to $f(1) = \frac{f^{(1)}(1)}{1!} = \frac{f^{(2)}(1)}{2!} = \frac{f^{(3)}(1)}{3!} = 0 \pmod 3$. Note that $f(1) = p(1) + q(1) + r(1) \pmod 3 = 0$ is automatically satisfied. Furthermore, by Proposition 5.11, if there exists a diagonal cyclotomic D such that $\mathrm{sde}(HDu) \leq \mathrm{sde}(z)$, there exists a D' such that $\mathrm{sde}(HD'z) \leq \mathrm{sde}(z) - 1$. Therefore, we are reduced to finding a_i's such that $\frac{f^{(1)}(1)}{1!} = \frac{f^{(2)}(1)}{2!} = 0 \pmod 3$, i.e.,

$$a_1p(1) + a_2q(1) + a_3r(1) + p'(1) + q'(1) + r'(1) = 0$$

and

$$\binom{a_1}{2}p(1) + \binom{a_2}{2}q(1) + \binom{a_3}{2}r(1) + a_1p'(1) + a_2q'(1) + a_3r'(1) + \frac{p^{(2)}(1)}{2!} + \frac{q^{(2)}(1)}{2!} + \frac{r^{(2)}(1)}{2!} = 0$$

They simplify as

$$\pi_1 + \sum_{i=1}^{3} a_i = 0$$

and

$$\sum_{i=1}^{3}(a_i - a_i^2) + a_1p'(1) + a_2q'(1) + a_3r'(1) + \pi_2 = 0$$

respectively, where $\pi_i = p_i + q_i + r_i$. By writing $a_3 = -\pi_1 - a_1 - a_2$ and substituting in the second equation, we get a polynomial $g(a_1, a_2) = -\pi_1 + \pi_2 - a_1^2 - a_2^2 - (-\pi_1 - a_1 - a_2)^2 + a_1p'(1) + a_2q'(1) + (-\pi_1 - a_1 - a_2)r'(1) = -\pi_1 + \pi_2 - \pi_1^2 - \pi_1r'(1) + (\pi_1 + p'(1) - r'(1))a_1 + (\pi_1 + q'(1) - r'(1))a_2 + (a_1^2 + a_2^2 + a_1a_2) = \gamma + \alpha(a_1 - a_2) + (a_1 - a_2)^2$, where

$$\alpha = q'(1) - p'(1)$$

and

$$\gamma = -\pi_1 + \pi_2 - \pi_1^2 - \pi_1r'(1)$$

Furthermore, $g(a_1, a_2) = 0$ has a solution in $\mathbb{Z}_3^2$ iff $\Delta = \alpha^2 - \gamma \neq -1$

□

Remark 5.13. *We explicitly describe the element* $\Delta := \alpha^2 - \gamma \in \mathbb{Z}_3$ *associated to the unit vector* z *in terms of the derivatives of the numerators of entries of* z *in their reduced form in* R_9, χ. *From the formulae for* Δ *in the proof, we have* $\Delta = \alpha^2 - \gamma = (q_1 - p_1)^2 - (-\pi_1 + \pi_2 - \pi_1^2 - \pi_1 r_1) = q_1^2 + p_1^2 + p_1 q_1 + \pi_1 - \pi_2 + p_1^2 + q_1^2 + r_1^2 + 2p_1 q_1 + 2q_1 r_1 + 2p_1 r_1 + p_1 r_1 + q_1 r_1 + r_1^2 = 2(p_1^2 + q_1^2 + r_1^2) + \pi_1 - \pi_2$.
But if $(p_0, q_0, r_0) = (1, 1, 1)$ *then by Lemma 5.10 we have,*

$$-\pi_2 + \pi_1 + p_1^2 + q_1^2 + r_1^2 = 0.$$

Therefore, $\Delta = p_1^2 + q_1^2 + r_1^2$.

6 Conclusion

In this paper we provide a general framework for qutrit synthesis over several families of universal gate sets. We used the notion of 'derivatives mod p' to reproduce and extend the results in [14] and [2]. This is achieved by relating the problem of synthesis to solving a system of polynomial equations mod p. We explored this for $p = 2$ and 3 in this paper. On the other hand, we can try applying the same technique to multiqutrit synthesis.
While the above method helped us derive the results in Section 5, it remains unknown whether $U(3, R_{9,\chi})$ is finitely generated where the maximum sde of a generating set is relatively small. In such a case, we can in fact search for such a generating set using the methods of Section 4. Consequently, this could help us achieve the exact analogue of [14] for qutrits.
Moreover, the techniques in this paper do not fully apply for $p \geq 5$, as Lemma 5.1 fails. Indeed, for $p = 5$ we see that $2^2 + 1^2 + 0^2 + 0^2 + 0^2 \equiv 0 \pmod 5$. This suggests that there could be unit vectors such that the sde of the entries are not equal to each other. Therefore, the analogous systems of polynomials over $\mathbb{Z}_p$ are far too many to analyze as in the previous section for $p = 2, 3$. We intend to explore this direction in the future.

7 Acknowledgements

ARK and DV would like to thank Neil Julien Ross, Peter Selinger, Jon Yard, Shiroman Prakash, Yash Totani, Vadym Kliuchnikov, Richard Cleve and David Gosset for sharing their understanding of various aspects of circuit synthesis and for suggesting relevant references at different times of the project. A majority of this work was done while DV was at IQC as a postdoc, he thanks David Jao for support.
ARK and MM thank NTT research for financial and technical support. Research at IQC is supported in part by the Government of Canada through Innovation, Science and Economic Development Canada (ISED).

References

[1] B. E. Anderson, H. Sosa-Martinez, C. A. Riofrío, Ivan H. Deutsch, and Poul S. Jessen. Accurate and robust unitary transformations of a high-dimensional quantum system. *Phys. Rev. Lett.*, 114:240401, Jun 2015. DOI: 10.1103/PhysRevLett.114.240401.

[2] Alex Bocharov, Xingshan Cui, Vadym Kliuchnikov, and Zhenghan Wang. Efficient topological compilation for a weakly integral anyonic model. *Physical Review A*, 93 (1), jan 2016. DOI: 10.1103/physreva.93.012313.

[3] Earl T. Campbell, Hussain Anwar, and Dan E. Browne. Magic-state distillation in all prime dimensions using quantum reed-muller codes. *Phys. Rev. X*, 2:041021, Dec 2012. DOI: 10.1103/PhysRevX.2.041021.

[4] Shawn X. Cui, Daniel Gottesman, and Anirudh Krishna. Diagonal gates in the clifford hierarchy. *Physical Review A*, 95(1), jan 2017. DOI: 10.1103/physreva.95.012329.

[5] Shai Evra and Ori Parzanchevski. Arithmeticity and covering rate of the 9-cyclotomic clifford+d gates in pu (3). *arXiv preprint arXiv:2401.16120*, 2024. DOI: https://doi.org/10.48550/arXiv.2401.16120.

[6] Simon Forest, David Gosset, Vadym Kliuchnikov, and David McKinnon. Exact synthesis of single-qubit unitaries over clifford-cyclotomic gate sets. *Journal of Mathematical Physics*, 56(8):082201, aug 2015. DOI: 10.1063/1.4927100.

[7] Andrew N. Glaudell, Neil J. Ross, and Jacob M. Taylor. Canonical forms for single-qutrit clifford+t operators. *Annals of Physics*, 406:54–70, 2019. ISSN 0003-4916. DOI: https://doi.org/10.1016/j.aop.2019.04.001.

[8] Andrew N. Glaudell, Neil J. Ross, John van de Wetering, and Lia Yeh. Qutrit metaplectic gates are a subset of clifford+t. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. DOI: 10.4230/LIPICS.TQC.2022.12.

[9] Andrew N. Glaudell, Neil J. Ross, John van de Wetering, and Lia Yeh. Exact synthesis of multiqutrit clifford-cyclotomic circuits. *Electronic Proceedings in Theoretical Computer Science*, 406:44–62, August 2024. ISSN 2075-2180. DOI: 10.4204/eptcs.406.2.

[10] Mark Howard and Jiri Vala. Qudit versions of the qubit $\pi/8$ gate. *Phys. Rev. A*, 86: 022316, Aug 2012. DOI: 10.1103/PhysRevA.86.022316.

[11] Mark Howard, Joel Wallman, Victor Veitch, and Joseph Emerson. Contextuality supplies the 'magic' for quantum computation. *Nature*, 510(7505):351–355, jun 2014. DOI: 10.1038/nature13460.

[12] Amolak Ratan Kalra, Manimugdha Saikia, Dinesh Valluri, Sam Winnick, and Jon Yard. Multi-qutrit exact synthesis. *arXiv preprint arXiv:2405.08147*, 2024. DOI: https://doi.org/10.48550/arXiv.2405.08147.

[13] A. B. Klimov, R. Guzmán, J. C. Retamal, and C. Saavedra. Qutrit quantum computer with trapped ions. *Phys. Rev. A*, 67:062313, Jun 2003. DOI: 10.1103/PhysRevA.67.062313.

[14] Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. Fast and efficient exact synthesis of single-qubit unitaries generated by clifford and t gates. *Quantum Info. Comput.*, 13(7–8):607–630, jul 2013. ISSN 1533-7146. DOI: https://doi.org/10.26421/QIC13.7-8-4.

[15] Vadym Kliuchnikov, Alex Bocharov, Martin Roetteler, and Jon Yard. A framework for approximating qubit unitaries. *arXiv preprint arXiv:1510.03888*, 2015. DOI: https://doi.org/10.48550/arXiv.1510.03888.

[16] Pei Jiang Low, Brendan White, and Crystal Senko. Control and readout of a 13-level trapped ion qudit. *arXiv preprint arXiv:2306.03340*, 2023. DOI: https://doi.org/10.48550/arXiv.2306.03340.

[17] Eufemio Moreno-Pineda, Clément Godfrin, Franck Balestro, Wolfgang Wernsdorfer, and Mario Ruben. Molecular spin qudits for quantum algorithms. *Chem. Soc. Rev.*, 47:501–513, 2018. DOI: 10.1039/C5CS00933B.

[18] Shiroman Prakash and Aashi Gupta. Contextual bound states for qudit magic state distillation. *Phys. Rev. A*, 101:010303, Jan 2020. DOI: 10.1103/PhysRevA.101.010303.

[19] Shiroman Prakash and Tanay Saha. Low overhead qutrit magic state distillation. 2024. DOI: https://doi.org/10.48550/arXiv.2403.06228.

[20] Shiroman Prakash, Akalank Jain, Bhakti Kapur, and Shubangi Seth. Normal form for single-qutrit clifford+t operators and synthesis of single-qutrit gates. *Phys. Rev. A*, 98:032304, Sep 2018. DOI: 10.1103/PhysRevA.98.032304.

[21] Shiroman Prakash, Amolak Ratan Kalra, and Akalank Jain. A normal form for single-qudit clifford+t operators. *Quantum Information Processing*, 20(10), October 2021. ISSN 1570-0755. DOI: 10.1007/s11128-021-03280-0.

[22] Martin Ringbauer, Michael Meth, Lukas Postler, Roman Stricker, Rainer Blatt, Philipp Schindler, and Thomas Monz. A universal qudit quantum processor with trapped ions. *Nature Physics*, 18(9):1053–1057, jul 2022. DOI: 10.1038/s41567-022-01658-0.

[23] Neil J Ross. Optimal ancilla-free clifford+ v approximation of z-rotations. *arXiv preprint arXiv:1409.4355*, 2014. DOI: https://doi.org/10.48550/arXiv.1409.4355.

[24] Mahadevan Subramanian and Adrian Lupascu. Efficient two-qutrit gates in superconducting circuits using parametric coupling. *Phys. Rev. A*, 108:062616, Dec 2023. DOI: 10.1103/PhysRevA.108.062616.

[25] Yuchen Wang, Zixuan Hu, Barry C. Sanders, and Sabre Kais. Qudits and high-dimensional quantum computing. *Frontiers in Physics*, 8, 2020. ISSN 2296-424X. DOI: 10.3389/fphy.2020.589504.

[26] Fern H. E. Watson, Earl T. Campbell, Hussain Anwar, and Dan E. Browne. Qudit color codes and gauge color codes in all spatial dimensions. *Phys. Rev. A*, 92:022312, Aug 2015. DOI: 10.1103/PhysRevA.92.022312.