Fermilab

Magic State Distillation using Asymptotically Good Codes on Qudits

Magic State Distillation using Asymptotically Good Codes on Qudits

Michael J. Cervia [1, *] Henry Lamm [2, 3, †] Diyi Liu [4, ‡] Edison M. Murairi [2, 3, §] and Shuchen Zhu [5, 6, ¶]

[1]*Department of Physics, University of Washington, Seattle, WA, 98195, USA*
[2]*Superconducting and Quantum Materials System Center (SQMS), Batavia, IL, 60510, USA.*
[3]*Fermi National Accelerator Laboratory, Batavia, IL 60510, USA*
[4]*Applied Mathematics and Computational Research Division,*
Lawrence Berkeley National Laboratory, Berkeley, CA 94720, USA
[5]*Department of Mathematics, Duke University, Durham, NC 27708, USA*
[6]*Duke Quantum Center, Duke University, Durham, NC 27701, USA*
(Dated: December 29, 2025)

Qudits offer the potential for low-overhead magic state distillation, although previous results for asymptotically good codes have required qudit dimension $q \gg 100$ or code length $\mathcal{N} \gg 100$. These parameters far exceed experimental demonstrations of qudit platforms, and thus motivate the search for better codes. Using a novel lifting procedure, we construct the first family of good triorthogonal codes on the $\mathbb{F}_{2^{2m}}$ alphabet with $m \geq 3$ that lies above the Tsfasman-Vladut-Zink bound. These codes yield a family of asymptotically good quantum codes with transversal CCZ gates, enabling constant space overhead magic state distillation with qudit dimension as small as $q = 64$. Further, we identify a promising code with parameters $[[42, 14, 6]]_{64}$. Finally, we show that a distilled $|CCZ\rangle_{2^{2m}}$ can be reduced to a $|CCZ\rangle_{2^n}$ state for arbitrary n with a constant-depth Clifford circuit of at most 9 computational basis measurements, 12 single-qudit and 9 two-qudit Clifford gates.

I. INTRODUCTION

Quantum computation with higher-dimensional systems, or qudits, has emerged as a compelling alternative to qubit-based architectures [1–3]. The enlarged Hilbert space per quantum register leads to higher effective connectivity by replacing entangling gates with single-qudit rotations [4–8]. This alternative permits lower gate fidelities for the same algorithmic fidelity [9–15], which in turn would yield higher error thresholds for the prospect of fault-tolerant computation. This promise has driven algorithmic research in qudits across multiple fields, including numerical optimization [16, 17], condensed matter [18–21], and particle physics [22–30].

Complementing these theoretical efforts, recent experiments on various physical platforms have demonstrated both the capability and near-term potential of large-dimension qudit quantum processors. In trapped-ion systems, researchers have realized qudits with dimensions $q = 7$ [31], $q = 8$ [32], and $q = 13$ [33]. Transmon systems have further realized $q = 8$ [34] and $q = 12$ [35], illustrating that the circuit quantum electrodynamics naturally extends to larger local dimensions. Molecular spins ($q = 8$ [36]), solid-state spin systems ($q = 10$ [37], $q = 16$ [38]) and cold-atom experiments (reaching $q = 25$ [39]) further demonstrate how diverse hardware can support many-level encoding with promising coherence and control properties. Notably, superconducting radio-frequency (SRF) cavities have demonstrated

extremely large single-mode Hilbert spaces ($q = 20$ with high fidelity [40] and up to $q = 100$ with lower fidelity [41]). Altogether, these experiments point toward architectures where large local dimensions are available.

Fault-tolerant computations on these architectures requires new quantum error correcting codes and protocols. Magic state distillation (MSD) is commonly proposed to enable universal computation by preparing high-fidelity resource states from several low-fidelity ones [42]. The resulting resource state is used to implement a non-Clifford gate to a desired accuracy. The number of noisy inputs required to achieve an infidelity ϵ scales as $\sim \log^{\gamma}(1/\epsilon)$, where the exponent γ is called the MSD overhead.

In Ref. [43], it was shown that a quantum code with a transversal non-Clifford gate may be used to distill the corresponding resource with overhead equal to

$$\gamma = \frac{\log(\mathcal{N}/\mathcal{K})}{\log \mathcal{D}}, \tag{1}$$

where $\mathcal{N}$, $\mathcal{K}$, and $\mathcal{D}$ are the code length, code dimension, and code distance of a quantum code $[[\mathcal{N}, \mathcal{K}, \mathcal{D}]]_q$ over q-dimensional qudit. The authors identified qubit codes achieving $\gamma = 1.585$ and conjectured a lower bound $\gamma \geq 1$. Their construction relied on classical triorthogonal codes.

Since then, several efforts have been made to construct quantum codes with transversal non-Clifford gates and lower overhead γ. Quantum Reed–Muller codes over prime dimensions allow implementation of some transversal non-Clifford gates and $\gamma < 1$ [44–46]. Another code with $\gamma \leq 0.678$ was found to be achievable for $q \geq 2^{58}$ [47]. Further, Calderbank-Shor-Steane (CSS) codes constructed from Reed-Solomon codes could obtain arbitrary small overhead ($\gamma \to 0$) as $q \to \infty$ [48]. Recently, it was demonstrated that constant space overhead and constant overhead are achievable with finite, albeit large, $q \geq 2^6$ and $q \geq 2^{10}$ respectively by constructing *asymp-*

* cervia@uw.edu
† hlamm@fnal.gov
‡ diyiliu@lbl.gov
§ emurairi@fnal.gov
¶ shuchen.zhu@duke.edu

totically good codes which are families of codes which as the code length increases the encoding rate and relative distance are bounded away from zero [49–51].

The existence of these codes naturally raises the question of how much more efficient can the codes be. This can partially be addressed by considering the efficiency of constituent classical codes $[n, k, d]_q$ which can be quantified by how large the encoding rate $R = \frac{k}{n}$ can be for relative distance $\delta = \frac{d}{n}$, usually with respect to two lower bounds. First is the Gilbert–Varshamov (GV) bound [52, 53] provides a non-constructive lower bound based on sphere-packing arguments. Remarkably, randomly-drawn linear code yields parameters that saturate the GV bound with high probability [54], and therefore more efficient codes should rely upon additional structure. When $q \geq 49$, the Tsfasman–Vladut–Zink (TVZ) bound [55] is tighter than the GV bound on an interval around $\delta \sim 0.4$ which grows larger with q. This latter bound is the one we will consider here since for all our codes $q \geq 64$. Codes meeting or exceeding the TVZ bound have large R for their δ, a feature desirable for optimizing quantum-code performance. While previous works [49, 50] did not demonstrate it, Garcia–Stichtenoth towers can yield families of asymptotically good codes that satisfy the TVZ bound [55]; we refer to such codes as TVZ codes. While no triorthogonal TVZ code has been previous identified, TVZ codes with iso-duality (a less-restrictive condition) exist [56].

In this work, we present a construction of triorthogonal TVZ codes over $q = r^2$, where $r \geq 8$ is a power of two. Our approach is based on a *lifting method*, which we prove preserves triorthogonality from a base code. Code lifting is a well-known technique to create new codes from old codes; see e.g. Refs. [56–61]. In the context of algebraic geometry (AG) codes, a similar lifting method was employed [56, 57] to establish the existence of iso-dual TVZ codes [56]. We adapt and extend the lifting procedure to maintain triorthogonality, and obtain triorthogonal TVZ codes. Thus, we find that despite the strong algebraic constraints of triorthogonality, codes exist with 'very good' parameters. We further show how these classical codes can be used to construct quantum codes with correspondingly improved MSD performance.

The rest of this article is organized as follows: Sec. II summarizes our results. In Sec. III, we review the notions of algebraic geometry, defining AG codes and their parameters, with particular focus on triorthogonal codes. In Sec. IV we provide our construction of triorthogonal TVZ codes, and in Sec. V we derive a corresponding family of good quantum codes, explicit examples of which we provide in Sec. VI. Furthermore, in Sec. VII, we show how to obtain $|CCZ\rangle$ magic states for any 2^n-qudit. Finally, we summarize and reflect upon future directions in Sec. VIII.

II. SUMMARY OF RESULTS

Our approach to developing quantum codes introduces a lifting method that generates larger triorthogonal codes

from smaller ones, while preserving the triorthogonality. Using our lifting method, we prove the existence of asymptotically good families of triorthogonal codes defined over the alphabet $\mathbb{F}_q$ with $q = 2^{2m}$ and $m \geq 3$, improving on the result of Refs. [50] and Ref. [49] where it was required $m \geq 4$ and $m \geq 5$, respectively. We further show that our codes can exceed the TVZ bound [55].

Using our triorthogonal codes, we have constructed a family of good quantum codes with transversal CCZ gate on qudit $q = 2^{2m}$ where $m \geq 3$, enabling magic state distillation with constant space $\gamma = 0$ overhead following e.g. the protocol in Ref. [50]. Further, we have identified a low-overhead $\gamma \approx 0.613$ code $[[42, 14, 6]]_{64}$. Finally, we show that we can obtain the $|CCZ\rangle_{2^n}$ state for any n with a constant-depth Clifford circuit given the ability to distill a $|CCZ\rangle_{2^{2m}}$ ($m \geq 3$). This result may be viewed as a generalization of a result in Ref. [49] where a 2^{10}-qudit magic state is converted to qubit $|CCZ\rangle$ states.

TABLE I. Asymptotically good triorthogonal classical codes.

	$q = r^2$	$\lim_{j \to \infty} \left(\frac{k_j}{n_j} + \frac{d_j}{n_j} \right)$
Wills et al. [49][a]	$\geq 2^{10}$	Not determined
Nguyen [50]	$\geq 2^8$	$\geq \frac{1}{2}$[b]
Present work	$\geq 2^6$	$\geq 1 - \frac{2r+3}{3r(r-1)}$[c]

[a] A different notion of triorthogonality from [49, Definition A.3].
[b] Deduced from [50, Theorem 3.6].
[c] Above the TVZ bound, i.e. $1 - 1/(r-1)$ for alphabet size $q = r^2$.

Theorem 1 (Informal version of the main results). *(1) Suppose the code $C_{j+1} := C_{\mathcal{L}}(D_{j+1}, G_{j+1})$ is the lifted code of $C_j := C_{\mathcal{L}}(D_j, G_j)$ in the sense of Def. 8. Then, if C_j is triorthogonal, so is C_{j+1}.*

(2) For every $r = 2^m$ with $m \geq 3$ and $q = r^2$, there exists a family of classical triorthogonal AG codes $\{C_j\}$ over alphabet size q with parameters $[n_j, k_j, d_j]$ such that

$$\lim_{j \to \infty} \left(\frac{k_j}{n_j} + \frac{d_j}{n_j} \right) \geq 1 - \frac{2r+3}{3r(r-1)} > 1 - \frac{1}{(r-1)}. \quad (2)$$

Note that the latter inequality of Eq. (2) is the TVZ bound for codes on $\mathbb{F}_{r^2}$. We summarize this result and compare with Refs. [49, 50] in Tab. I.

(3) These classical codes yield a family of good quantum codes over the alphabet $q = r^2$ for $r = 2^m \geq 8$ with parameters $[[\mathcal{N}_j, \mathcal{K}_j, \mathcal{D}_j]]_q$

$$\mathcal{N}_j = r^j(r^2 - r) - \mathcal{K}_j$$
$$\mathcal{K}_j = x_1 \, r^j \left((r+1) \left\lfloor \frac{r-2}{3} \right\rfloor - 2r \right) + x_2 \, v(r, j)$$
$$\mathcal{D}_j \geq (1 - x_1) \, r^j \left((r+1) \left\lfloor \frac{r-2}{3} \right\rfloor - 2r \right)$$
$$+ (1 - x_2) \, v(r, j) \quad (3)$$

where

$$v(r,j) := \begin{cases} 4r^{\frac{j+1}{2}} & \text{if } j \text{ is odd} \\ 2r^{\frac{j}{2}}(1+r) & \text{otherwise,} \end{cases}$$

the constants $x_1 \in (0,1)$ and $x_2 \in [0,1]$ are chosen such that $\mathcal{K}_j$ is an integer. We compare this result with Refs. [49–51] in Tab. II.

(4) Finally, given the ability to distill a state $|CCZ\rangle_{2^{2m}}$ (where $m \geq 3$), we can obtain the state $|CCZ\rangle_{2^n}$ for arbitrary n using a constant-depth Clifford circuit with at most nine computational basis measurements, twelve single-qudit, and nine two-qudit Clifford gates.

TABLE II. Asymptotically good triorthogonal quantum codes: minimum qudit dimension q_{min}, bounds on encoding rate $\mathcal{R}$, and minimum code length $\mathcal{N}_{min}$. Previous works present various state and alphabet reduction procedures that allow for smaller q.

	q_{min}	$\mathcal{R}$	$\mathcal{N}_{min}$
Wills et al. [49]	2^{10}	$\frac{5}{118} \leq \mathcal{R} \leq \frac{5}{114}$	932,090
Nguyen [50]	2^8	$< \frac{1}{4}$ [a]	Not determined
Golowich et al. [51]	2^6	$> \frac{1}{100}$	Not determined
Present work	2^6	$< \frac{1}{2}$ [b]	≤ 55

[a] Deduced from [50, Corollary]
[b] Obtained in the limit $x \to 1$, although at $x = 1$ $\mathcal{D}_j = 0$

FIG. 1. The blue curve corresponds to a function field F_j. Then n pairwise distinct points P_i correspond to rational places of F_j. The divisor G_j specifies the Riemann-Roch space $\mathcal{L}(G_j)$. The points P_i on the curves and the divisor G_j specify an AG code of which the codewords are the vectors $(f(P_1), ..., f(P_n))$ where $f \in \mathcal{L}(G_j)$. The yellow curve F_{j+1} is an extension of F_j. An arrow $P_i \to P'_j$ indicates that P'_j lies above P_i. This relation allows us to lift the code on F_j into a code on F_{j+1} while preserving triorthogonality. Then, we lift the Riemann-Roch space similarly by taking the conorm map of $G_{j+1} = \text{Con}_{F_{j+1}/F_j}(G_j)$ to specify the lifted code. This builds sequences of triorthogonal codes by successive liftings.

III. BASIC NOTIONS OF ALGEBRAIC GEOMETRY CODES

Algebraic geometry (AG) codes are a class of error-correcting codes constructed from the framework of algebraic curves over finite fields. For a detailed review, we point readers toward Refs. [56, 57, 62], and we will further adopt notation following Refs. [49, 50]. The basic idea is to exploit the structure of a curve — specifically, its rational points and the associated function field — to define codewords. In particular, by evaluating chosen functions at a set of rational points, one obtains linear codes whose parameters can surpass classical bounds. The theory draws on concepts from algebraic geometry to systematically relate the properties of the curve to the performance of the code. This interplay between geometry and coding theory has led to highly efficient classical codes, including ones that achieve the TVZ bound [55]. Many of the same ideas can be adapted to quantum error-correcting codes by using the CSS construction combined with classical AG codes to achieve high rates and large distances. This connection allows algebraic geometry to inform the design of quantum codes, enabling quantum analogues that inherit favorable properties from their classical counterparts.
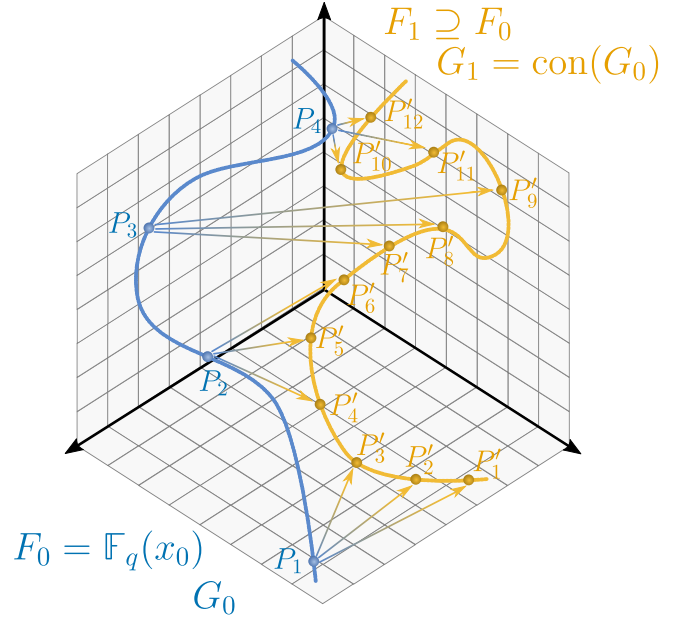
III.1. Algebraic Geometry

Before proceeding, let us define some preliminary notation that will be used throughout the paper. These concepts are well-known and basic to the field of algebraic geometry, and so describing our problem in these terms will allow us to borrow major results from that field to develop provably efficient AG codes for MSD purposes.

Definition 1 (Algebraic Function field)**.** *An algebraic function field F/K of one variable over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ that is transcendental over K. Associated with F is a non-negative integer $g := g(F)$, called the genus.*

We consider only the case where $K = \mathbb{F}_q$ is the full field of constants. From a function field we may build maximal ideals called "places" as well as divisors thereupon, which will serve as the central mathematical objects of AG code constructions. A place P is uniquely related to a valuation ring $\mathcal{O}_P$ of the function field; such a ring satisfies:

1. $\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq F$, and

2. If $x \in F$, then $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.

Definition 2 (Places). *A place P is the maximal ideal of a valuation ring $\mathcal{O}$. The set of all places of F will be denoted $\mathbb{P}(F)$. We note the following attributes:*

1. *A place P has degree $\deg(P) = [F_P : \mathbb{F}_q]$ where $F_P := \mathcal{O}_P/P$, the residue field. The place P is called rational if $\deg(P) = 1$.*

2. *The valuation v_P associated with a place P is a function evaluated on $x \in F$ as follows:*

   - *If $x \neq 0$ then, for any $t \in P$ such that $P = t O_P$, there exist unique $n \in \mathbb{Z}$ and $u, u^{-1} \in \mathcal{O}_P$ such that $x = t^n u$; define $v_P(x) := n$.*

   - *Define $v_P(0) := \infty$ otherwise.*

3. *For $x \in F$, a place P is a zero of order m if $v_P(x) = m > 0$; P is a pole of order m if $v_P(x) = -m < 0$.*

4. *A place P' of a function field extension F' lies above a place P of F if $\mathcal{O}_{P'} \cap F = \mathcal{O}_P$ (equivalently $P' \supseteq P$), and we denote $P' \mid P$. The ramification of P' over P is $e(P'|P) \geq 1$ such that $v_{P'}(x) = e(P'|P)v_P(x)$ for all $x \in F$.*

5. *A place P splits completely in an extension F'/F if $e(P'|P) = 1$ for all $P' \mid P$ (thereby ensuring $\sum_{P'|P} e(P'|P) = [F' : F]$ places P' lie above P).*

From places we can construct certain collections called divisors, which will be the fundamental structures of our AG codes.

Definition 3 (Divisors). *A divisor is a linear combination of places $M = \sum_P c_P P$, with degree $\deg(M) = \sum_P c_P \deg(P)$ and support $\mathrm{supp}(M) = \{P : c_P \neq 0\}$. Informally, we will say a place P is in a divisor M if $P \in \mathrm{supp}(M)$. We say $M \geq 0$ if $c_P \geq 0$ for all P in M. We note the following kinds that will be used later:*

1. *The canonical divisor associated with a differential ω is:*

$$(\omega) = \sum_{P \in \mathbb{P}(F)} v_P(\omega)P, \qquad (4)$$

   where $v_P(\omega) := v_P(z)$ given any decomposition $\omega = z\, dt$ with $z \in F$ and $t O_P = P$.[1]

2. *The conorm of a divisor $M = \sum_P c_P P$ over F with respect to a function field extension F'/F is*

$$\mathrm{Con}_{F'/F}(M) = \sum_P \sum_{P'|P} e(P'|P)c_P P', \qquad (5)$$

   also a divisor.

———

[1] (For further reading, see Ref. [62, Chapter 5] and Ref. [54, Chapter 12]).

3. *The cotrace $\mathrm{Cotr}_{F'/F}(\omega) := \omega'$ of a differential ω with respect to F'/F is the unique differential satisfying $\omega'(\alpha) = \omega(\mathrm{Tr}_{F'/F}(\alpha))$, where α is a map $\mathbb{P}(F') \to F'$ such that $\alpha_{P'} = \alpha_{Q'} \iff P' \cap F = Q' \cap F$. Moreover, the cotrace divisor is*

$$(\omega') = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F), \qquad (6)$$

in terms of the well-known, "different" divisor $\mathrm{Diff}(F'/F) \geq 0$. (For more details, see Ref. [62, Chapter 3].)

The well-known Riemann-Roch space of a divisor then constitutes a subspace of functions that we will use to realize the encoding in our AG codes.

Definition 4 (Riemann-Roch Space). *For a divisor G, the associated Riemann-Roch space denoted $\mathcal{L}(G)$ is the vector space*

$$\mathcal{L}(G) = \{x \in F : (x) + G \geq 0\} \cup \{0\}. \qquad (7)$$

Following the Riemann-Roch theorem [62], the Riemann-Roch space $\mathcal{L}(G)$ is characterized by the degree $\deg(G)$ and the genus $g(F)$.

III.2. Codes from Algebraic Geometry

Using the essential objects of algebraic geometry, we are ready to introduce generic AG codes.

Definition 5 (Algebraic geometry code). *Let $F/\mathbb{F}_q$ be an algebraic function field. Let $D = P_1 + \cdots + P_n$ be a divisor consisting of pairwise distinct rational places, and let $G = \sum_{P'} c_{P'} P'$ be another divisor of $F/\mathbb{F}_q$ disjoint from D. The AG code $C_{\mathcal{L}}(D, G)$ associated with the divisors D and G is the subspace*

$$C_{\mathcal{L}}(D, G) := \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\} \qquad (8)$$

mapped by function field elements in the Riemann-Roch space $\mathcal{L}(G)$.

Later, we will see that to construct suitable codes for MSD, it will be convenient to also characterize the dual of the AG code defined above. From Ref. [63], the dual to the AG code $C_{\mathcal{L}}(D, G)$ is also an AG code, see the proposition below reproduced without proof.

Definition 6 (Dual code). *For a code $C \subseteq \mathbb{F}_q^n$, the dual $C^\perp$ is*

$$C^\perp := \left\{ c' \in \mathbb{F}_q^n : \sum_{i=1}^n c_i c_i' = 0 \text{ for all } c \in C \right\}. \qquad (9)$$

Proposition III.1 (Dual of $C_{\mathcal{L}}(D, G)$ [63]). *For an AG code $C_{\mathcal{L}}(D, G)$, there exists a differential $\eta \in \Omega_F$ with simple poles at each $P_i \in \mathrm{supp}(D)$ such that its residue*

at each P_i is $\mathrm{res}_{P_i}(\eta) = 1$. *Moreover, the dual of the code* $C_{\mathcal{L}}(D, G)$ *is*

$$C_{\mathcal{L}}(D, G)^{\perp} := C_{\mathcal{L}}(D, D - G + (\eta)) \qquad (10)$$

where (η) is the canonical divisor associated with η. Finally, it follows from the Weak Approximation Theorem [62, Theorem 1.3.1], that there exists $z \in F$ such that the valuations $v_{P_i}(z) = 1$ for all $P_i \in \mathrm{supp}(D)$. Then, one choice of η is the logarithmic differential

$$\eta := \frac{dz}{z}. \qquad (11)$$

Clearly, $v_{P_i}(\eta) = -1$ and $\mathrm{res}_{P_i}(\eta) = 1$ for all $P_i \in \mathrm{supp}(D)$. Such a function $z \in F$ can be found when the function field $F = \mathbb{F}_q(x)$. Our procedure only requires computing η explicitly in the rational function field.

The parameters $[n, k, d]$ of the AG codes $C := C_{\mathcal{L}}(D, G)$ and $C^{\perp} = C_{\mathcal{L}}(D, G)^{\perp}$ can be calculated or bounded from the divisors D and G and the genus $g := g(F)$. If $2g - 2 < \deg(G) < n$, then k and d of C satisfy

$$\begin{aligned} k &= \deg(G) + 1 - g \\ d &\geq n - \deg(G). \end{aligned} \qquad (12)$$

The distance of the dual code, $d^{\perp}$, satisfies

$$d^{\perp} \geq \deg(G) - (2g - 2). \qquad (13)$$

Details can be found in Ref. [62, Corollary 2.2.3 and Theorem 2.2.7].

III.3. Triorthogonal codes

Triorthogonal codes were first proposed in [43] with the explicit purpose of making qubit magic state distillation more efficient. They are the most general stabilizer codes with transversal T gates, and important because they have low-overhead ($\gamma = \log_2(3) \approx 1.6$) for universal qubit fault-tolerant quantum computing.

A triorthogonal code is a stabilizer code that comes from a special kind of matrix $\mathcal{G}$ with two orthogonality conditions: *pairwise orthogonality* between any two rows and *triple orthogonality* where the product of any three rows is 0. Subsequent research extended the triorthogonal code framework to qudits [64–66]. For triorthogonality it is more practical formulate it via the star ($\star$) product of codes following Ref. [48, 50] where a code $C^{\star 2}$ is given by

$$C^{\star 2} := C \star C = \{c \star c' \mid c, c' \in C\} \qquad (14)$$

and $c \star c'$ is the point-wise product of codewords c and c',

$$c \star c' = (c_1 c_1', \dots, c_n c_n'). \qquad (15)$$

A code $C \subseteq \mathbb{F}_q^n$ satisfies the *star-square property* if $C^{\star 2} \subseteq C^{\perp}$ and is equivalent to triple orthogonality. In addition to triple orthogonality, requiring the code to contain the constant word $(1, \dots, 1)$ ensures the code has pairwise orthogonality.

Definition 7 (Triorthogonal code). *A linear code satisfying the Star-square property i.e. triple orthogonality i.e. triple orthogonality and containing the constant word $(1, \dots, 1)$ i.e. pairwise orthogonality is triorthogonal.*

In Lemma 2.3 of Ref. [50], it is shown that a classical triorthogonal code yields a quantum code $\mathcal{Q} : [[\mathcal{N}, \mathcal{K}, \mathcal{D}]]_{\mathbb{F}_q}$ where the transversal $(CCZ)^{\otimes \mathcal{N}}$ gate implements the logical $\overline{CCZ}^{\otimes \mathcal{K}}$ gate. Following Refs. [49, 50], it is possible to construct triorthogonal AG codes. From e.g. Ref. [50], there is a sufficient condition for an AG code to be triorthogonal for power of two qudits, $q = 2^m$. For completeness, we will present this sufficient condition using Prop. III.2 and Lemma 1.

Proposition III.2 (Some useful properties of AG codes). *Let $C := C_{\mathcal{L}}(D, G)$ and $C' := C_{\mathcal{L}}(D, G')$ be two AG codes with duals $C^{\perp} := C_{\mathcal{L}}(D, D - G + (\eta))$ and $(C')^{\perp} := C_{\mathcal{L}}(D, D - G' + (\eta'))$ respectively. Then*

1. If $G \leq G'$ then $C \subseteq C'$

2. $C^{\star 2} \subseteq C_{\mathcal{L}}(D, 2G)$.

Proof. The first statement simply follows from the fact that $G \leq G'$ implies $\mathcal{L}(G) \subseteq \mathcal{L}(G')$. Then, every codeword $(f(P_1), \dots, f(P_n)) \in C$ must also be in C'. Similarly, the second statement follows from the fact that for every pair $f, g \in \mathcal{L}(G)$, the product fg is in $\mathcal{L}(2G)$. $\square$

Using Proposition III.2, requiring $C_{\mathcal{L}}(D, 2G) \subseteq C_{\mathcal{L}}(D, G)^{\perp}$ ensures $C^{\star 2} \subseteq C^{\perp}$. The lemma below will present sufficient conditions on the divisor G to obtain a triorthogonal AG code.

Lemma 1 (Triorthogonal AG code). *Let $C := C_{\mathcal{L}}(D, G)$ with dual $C^{\perp} = C_{\mathcal{L}}(D, D - G + (\eta))$ where η is as given in Prop. III.1. If*

$$G \geq 0 \quad and \quad 3G \leq D + (\eta), \qquad (16)$$

then $(1, \dots, 1) \in C$ and $C^{\star 2} \subseteq C^{\perp}$.

Proof. The first statement follows from the fact that for $G \geq 0$, the constant function $f = 1$ is in $\mathcal{L}(G)$ since it has no poles (and no zeros). The second statement arises from the fact that $2G \leq D - G + (\eta) \Leftrightarrow 3G \leq D + (\eta)$. Therefore, under this condition, we have $C_{\mathcal{L}}(D, 2G) \subseteq C^{\perp}$ (Prop. III.2, first statement) and consequently $C^{\star 2} \subseteq C^{\perp}$ (Prop. III.2, second statement). $\square$

III.4. Tsfasman-Vladut-Zink bound

One of our main results is that our triorthogonal codes are the first to exceed the TVZ bound [55]. Below, we review asymptotic bounds of classical codes and the TVZ bound. For an $[n, k, d]$ classical code C over $\mathbb{F}_q$, the ratios:

$$R(C) := \frac{k}{n} \text{ and } \delta(C) := \frac{d}{n} \qquad (17)$$

are called encoding rate and relative distance respectively. The set

$$V_q := \{(\delta(C), R(C)) \mid C \text{ is a code over } \mathbb{F}_q\} \subseteq [0,1]^2 \tag{18}$$

contains all possible points $(\delta(C), R(C))$ where C is a code over $\mathbb{F}_q$. The asymptotic behavior of codes over $\mathbb{F}_q$ can be understood by studying the set of limit points of V_q, denoted U_q. That is, a point $(\delta, R) \in [0,1]^2$ is in U_q if and only if there exists a sequence of codes $\{C_i\}_{i \geq 0}$ such that as $i \to \infty$,

$$n_i \to \infty, R(C_i) \to R \text{ and } \delta(C_i) \to \delta. \tag{19}$$

There exists a continuous function α_q such that $0 \leq R \leq \alpha_q(\delta)$ for all δ. α_q satisfies $\alpha_q(0) = 1$ and $\alpha_q(\delta) = 0$ for $1 - 1/q \leq \delta \leq 1$. The exact value of $\alpha_q(\delta)$ in the interval $0 < \delta < 1 - 1/q$ is unknown. However, there are bounds. Lower bounds are important because a non-zero lower bound guarantees the existence of good codes. One lower bound is the GV bound which random codes typically exceed. A significant achievement of algebraic geometry code construction is that it yields an improved bound, the so-called TVZ bound. For a square $q = r^2$, the TVZ bound is

$$\alpha_q(\delta) \geq 1 - \frac{1}{r-1} - \delta. \tag{20}$$

For $q \geq 49$ – which is for all codes we consider – the TVZ bound is larger than the GV bound for an increasing interval around $\delta \sim 0.4$, showing that there are AG codes better than random codes. We will show that despite the extra algebraic constraint imposed by the triorthogonality requirement, our codes satisfy the TVZ bound. We call our codes triorthgonal TVZ codes.

IV. CLASSICAL CODE CONSTRUCTIONS

Following Refs. [49, 50], we construct a good family of triorthogonal codes $\{C_j\}_{j \to \infty}$ on qudits with dimension $q = r^2$ where $r \geq 8$ is a power of two. A "good" code means that both its rate k_j/n_j and the relative distance d_j/n_j do not vanish as $j \to \infty$. Since we preserve the triorthogonal property, this family of good classical codes will yield quantum codes with transversal CCZ gates for qudits of dimensions $q \geq 8^2$.

Our construction is recursive. We consider a tower of function fields $\mathcal{W} = (F_0, F_1, ...)$, where $F_0 = \mathbb{F}_q(x_0)$ is the rational function field, F_j is an extension of F_{j-1} (for $j \geq 1$), and $\mathbb{F}_q$ is the full field of constants for each function field F_j. Each code C_j is an AG code $C_j := C_{\mathcal{L}}(D_j, G_j)$, where each D_j and G_j are disjoint divisors in F_j and the places in D_j are rational.

The simplicity of our construction is that we only need to construct the base code C_0 explicitly. This construction is straightforward since F_0 is the rational function field. Then, we present our lifting procedure (Sec. IV.1) to obtain the code C_{j+1} using the C_j code. Remarkably, we will show that this lifting procedure preserves triorthogonality (Thm. 2). Another convenient property of our construction is that the parameters of the C_j codes can be derived or bounded using the parameters of C_0.

IV.1. Code lifting

Let the function field F_{j+1} be an extension of the function field F_j. We assume that both function fields have the same field of constants $\mathbb{F}_q$. We can now use the conorm divisor defined in Eq. (5) with respect to these field extensions to lift codes recursively.

Definition 8 (Code lifting). *Let $C_j := C_{\mathcal{L}}(D_j, G_j)$ where $D_j = P_1 + \cdots + P_{n_j}$ includes only places that split completely in the extension F_{j+1}/F_j. Set*

$$D_{j+1} := \text{Con}_{F_{j+1}/F_j}(D_j),$$
$$G_{j+1} := \text{Con}_{F_{j+1}/F_j}(G_j). \tag{21}$$

Then $C_{j+1} := C_{\mathcal{L}}(D_{j+1}, G_{j+1})$ is the lifting of C_j.

Note that C_{j+1} is a valid AG code (Sec. III) because

1. Since each place $P \in \text{supp}(D_j)$ splits completely in the extension F_{j+1}/F_j, the places $P' \in \text{supp}(D_{j+1})$ are rational places of F_{j+1}.

2. Since D_j and G_j are disjoint, so are D_{j+1} and G_{j+1}.

Moreover, we can relate $C_{j+1}^\perp$ to $C_j^\perp$.

Lemma 2 ($C_{j+1}^\perp$ code). *Let $C_j := C_{\mathcal{L}}(D_j, G_j)$. Suppose $z \in F_j$ is as in Prop. III.1 so that $C_j^\perp = C_{\mathcal{L}}(D_j, D_j - G_j + (\eta_j))$ where $\eta_j = dz/z$. Regarding z as an element of F_{j+1}, let us set $\eta_{j+1} = dz/z$, a differential in F_{j+1}. Then, $C_{j+1}^\perp = C_{\mathcal{L}}(D_{j+1}, D_{j+1} - G_{j+1} + (\eta_{j+1}))$.*

Proof. To prove this statement, we observe that any place $P' \in \text{supp}(D_{j+1})$ lies above some place $P \in \text{supp}(D_j)$. Then, $v_{P'}(z) = e(P'|P)v_P(z) = v_P(z) = 1$. Therefore, this choice of η_{j+1} satisfies Prop. III.1. $\qquad\square$

Now, we have all the ingredients to establish one of our main results. More precisely, we show that our lifting operation preserves the multiplication property $C^{*2} \subseteq C^\perp$.

Theorem 2 (Lifting theorem). *Suppose the code $C_j := C_{\mathcal{L}}(D_j, G_j)$ is as in Lemma 1, i.e.*

$$G_j \geq 0 \text{ and } 3G_j \leq D_j + (\eta_j). \tag{22}$$

Then, so is the lifted code C_{j+1}.

Proof. To prove this theorem, we observe that $G_{j+1} \geq 0$ is trivial since the Conorm of a positive divisor is also a

positive divisor. The rest is to establish that $3G_{j+1} \le D_{j+1} + (\eta_{j+1})$. In fact, one can derive the formula

$$3G_{j+1} - D_{j+1} - (\eta_{j+1)})$$
$$= \text{Con}_{F_{j+1}/F_j} (3G_j - D_j - (\eta_j)) - \text{Diff}(F_{j+1}/F_j) \quad (23)$$

by identifying our lifted differential with the cotrace of the lower differential, $\eta_{j+1} = \text{Cotr}_{F'/F}(\eta_j)$, and using the cotrace divisor formula of Eq. (6). By assumption, we have $3G_j - D_j - (\eta_j) \le 0$. Then, since the different divisor is positive, we arrive at $3G_{j+1} - D_{j+1} - (\eta_{j+1}) \le 0$, concluding the proof. $\square$

In other words, our lifting procedure allows one to obtain new triorthogonal codes from existing ones. Next, we relate the parameters of the C_{j+1} code to those of C_j.

Lemma 3 (Parameters of C_{j+1}). *Let $C_j = C_{\mathcal{L}}(D_j, G_j)$ and $C_{j+1} = C_{\mathcal{L}}(D_{j+1}, G_{j+1})$, where $D_{j+1} = \text{Con}_{F_{j+1}/F_j}(D_j)$ and $G_{j+1} = \text{Con}_{F_{j+1}/F_j}(G_j)$. Then*

1. Length n_{j+1} satisfies

$$n_{j+1} = \deg(D_{j+1})$$
$$= [F_{j+1} : F_j] \deg(D_j)$$
$$= [F_{j+1} : F_j] n_j. \quad (24)$$

2. Let $g_j := g(F_j)$ and $g_{j+1} := g(F_{j+1})$ be the genera of the two function fields respectively. Suppose $2g_{j+1} - 2 < \deg(G_{j+1}) < n_{j+1}$. Then, the dimension k_{j+1} is

$$k_{j+1} = \deg(G_{j+1}) + 1 - g_{j+1}$$
$$= [F_{j+1} : F_j] \deg(G_j) + 1 - g_{j+1}. \quad (25)$$

3. Distance d_{j+1} satisfies

$$d_{j+1} \ge n_{j+1} - \deg(G_{j+1})$$
$$= [F_{j+1} : F_j] (n_j - \deg(G_j)). \quad (26)$$

Proof. These statements follow from 12 and from the fact that for a divisor $A \in \text{Div}(F_j)$, $\deg(\text{Con}_{F_{j+1}/F_j}(A)) = [F_{j+1} : F_j] \deg(A)$.
$\square$

To end this discussion, we point that out there exists an alternative lifting method (provided in Appendix B) similar to that used in Ref. [57]. While such a lifting improves the dimension of the code, this improvement will be sub-leading for the family of codes we will build. Therefore, we will use the simpler lifting to analyze the asymptotic behavior of our codes.

IV.2. The Family of Codes

The family of codes $\{C_j\}_{j \to \infty}$ is constructed from a tower $\mathcal{W}$ of function fields over $\mathbb{F}_q$ with $q = r^2$. Using this tower, we show that for $r \ge 8$, there exists a good family of codes $\{C_j\}_{j \to \infty}$ in which each code C_j is triorthogonal. The tower we use is described in Refs. [54, 62].

Definition 9. *Let $\mathcal{W} = (F_0, F_1, F_2, \ldots)$ be the tower of function field over $\mathbb{F}_q$ with $q = r^2$ where*

1. $F_0 := \mathbb{F}_q(x_0)$ is the rational function field.

2. $F_{j+1} := F_j(x_{j+1})$ and each x_j and x_{j+1} satisfy the relation

$$x_{j+1}^r + x_{j+1} = \frac{x_j^r}{x_j^{r-1} + 1}. \quad (27)$$

Many useful properties of this tower are already known [54, Chapter 7].

Proposition IV.1 (Properties of tower). *Consider the tower $\mathcal{W}$ in Definition 9.*

1. For each $j \ge 0$, the extension F_j/F_0 has degree $[F_j : F_0] = r^j$.

2. The rational places in F_0 form the set

$$\mathcal{Z} := \{P_\alpha : \alpha \in \mathbb{F}_{r^2} \backslash \mathbb{F}_r\}, \quad (28)$$

and each splits completely in all extensions F_j/F_0. This set has cardinality $|\mathcal{Z}| = r(r-1)$.

3. The ramification locus of the tower is

$$\mathcal{V} := \{P_\alpha : \alpha \in \mathbb{F}_r\} \cup \{P_\infty\}. \quad (29)$$

This set has cardinality $|\mathcal{V}| = r + 1$.

4. The genus $g_j := g(F_j)$ of the function field F_j is

$$g_j = \begin{cases} \left(r^{\frac{j+1}{2}} - 1\right)^2 & \text{if } j \text{ is odd} \\ \left(r^{\frac{j}{2}} - 1\right)\left(r^{\frac{j+2}{2}} - 1\right) & \text{otherwise} \end{cases} \quad (30)$$

Often, we will use the expression

$$1 - g_j = \begin{cases} -r^{j+1} + 2r^{\frac{j+1}{2}} & \text{if } j \text{ is odd} \\ -r^{j+1} + r^{\frac{j}{2}}(1 + r) & \text{otherwise,} \end{cases} \quad (31)$$

which can be derived from Eq. (30).

Now, we are ready to present our family of triorthogonal codes. Our construction is recursive in a simple form: we first use the rational function field $F_0 := \mathbb{F}_q(x_0)$ to construct the base code C_0, and then obtain each subsequent code C_{j+1} from C_j via the triorthogonality-preserving lifting operation. Moreover, the parameters of all codes in the sequence can be computed or bounded from those of C_0. We summarize this result in the theorem below.

Theorem 3 (Good family of triorthogonal codes). *For $r = 2^m$ with $m \ge 3$, there exists a good family of triorthogonal codes $\{C_j\}_{j \to \infty}$ over the alphabet $\mathbb{F}_{r^2}$ with parameters $[n_j, k_j, d_j]$ given by*

$$n_j = r^j(r^2 - r)$$
$$k_j = r^j(r+1)\left\lfloor \frac{r-2}{3} \right\rfloor + 1 - g_j$$
$$d_j \ge \frac{2}{3} r^j(r^2 - r + 2). \quad (32)$$

One explicit family realizing these parameters is defined recursively by

$$C_0 = C_{\mathcal{L}}(D_0, G_0),$$
$$C_{j+1} = C_{\mathcal{L}}(\mathrm{Con}_{F_{j+1}/F_j}(D_j), \mathrm{Con}_{F_{j+1}/F_j}(G_j)), \quad (33)$$

where

$$D_0 = \sum_{P_\alpha \in \mathcal{Z}} P_\alpha, \quad G_0 = \left\lfloor \frac{r-2}{3} \right\rfloor \sum_{Q_\alpha \in \mathcal{V}} Q_\alpha. \quad (34)$$

and $F_j \in \mathcal{W}$, the tower of Def. 9.

Proof. We prove this theorem by construction. By Thm. 2, it is sufficient to explicitly construct the base code $C_0 := C_{\mathcal{L}}(D_0, G_0)$. We use the set $\mathcal{Z}$ to construct the divisor D_0 and the set $\mathcal{V}$ to construct G_0. Set

$$D_0 := \sum_{P \in \mathcal{Z}} P \qquad G_0 := \sum_{Q \in \mathcal{V}} a_Q Q \quad (35)$$

where the coefficients $a_Q \in \mathbb{Z}$ will be chosen so that C_0 is triorthogonal.

From Ref. [62, Prop. 8.1.2], a differential η_0 as in Prop. III.1 is given by

$$\eta_0 := \frac{dt_0}{t_0}, \quad t_0 := \prod_{\alpha \in \mathcal{Z}} (x_0 + \alpha). \quad (36)$$

A direct calculation gives the canonical divisor (outlined in Appendix A)

$$(\eta_0) = -D_0 + (r-2) \sum_{Q \in \mathcal{V}} Q. \quad (37)$$

Therefore, we can ensure C_0 is triorthogonal by setting $a_Q := \lfloor (r-2)/3 \rfloor$ for $r \geq 8$. Hence, the base code is $C_0 := C_{\mathcal{L}}(D_0, G_0)$ with

$$D_0 = \sum_{P \in \mathcal{Z}} P,$$
$$G_0 = \left\lfloor \frac{r-2}{3} \right\rfloor \sum_{Q \in \mathcal{V}} Q. \quad (38)$$

The parameters of C_0 are

$$n_0 = r(r-1),$$
$$k_0 = \deg(G_0) + 1 = (r+1) \left\lfloor \frac{r-2}{3} \right\rfloor + 1,$$
$$d_0 = r(r-1) - (r+1) \left\lfloor \frac{r-2}{3} \right\rfloor. \quad (39)$$

For example, for $r = 8$, C_0 is a triorthogonal code with parameters $[56, 19, 38]_{8^2}$.

We now define the family by successive lifting. Since $P \in \mathcal{Z}$ and $Q \in \mathcal{V}$, we can ensure that for each j:

1. Every place in $\mathrm{supp}(D_j)$ splits completely in the extension F_{j+1}/F_j.

2. The divisors D_{j+1} and G_{j+1} are disjoint.

Therefore, each C_j can be lifted to C_{j+1} by Def. 8:

$$C_0 = C_{\mathcal{L}}(D_0, G_0),$$
$$C_{j+1} = C_{\mathcal{L}}(\mathrm{Con}_{F_{j+1}/F_j}(D_j), \mathrm{Con}_{F_{j+1}/F_j}(G_j)), \quad (40)$$

with $F_j \in \mathcal{W}$. By Thm. 2, each C_j is triorthogonal. Lemma 3 in combination with Eq. (39) and

$$\deg G_j > 2g_j - 2 \text{ for } r \geq 8. \quad (41)$$

make clear that Eq. (32) holds.

Now, it is easy to show that this family is asymptotically good, i.e. the ratios d_j/n_j and k_j/n_j do not vanish.

$$\lim_{j \to \infty} \frac{d_j}{n_j} \geq \lim_{j \to \infty} \frac{r^j(r^2 - r + 2)}{r^j(r^2 - r)}$$
$$= \frac{2}{3} + \frac{4}{3r(r-1)} \quad (42)$$

For the dimension, we can use Eq (31) to get

$$\lim_{j \to \infty} \frac{k_j}{n_j} = \lim_{j \to \infty} \frac{r^j \left[(r+1) \left\lfloor \frac{r-2}{3} \right\rfloor - 1 \right]}{r^j r(r-1)}$$
$$\geq \frac{1}{3} - \frac{2r+7}{3r(r-1)} > 0 \text{ for } r \geq 8. \quad (43)$$

$\square$

These limits show that our codes have very good encoding rates for their relative distance. More precisely, these codes explicitly satisfy the TVZ bound for $r \geq 8$:

$$\lim_{j \to \infty} \frac{k_j}{n_j} + \frac{d_j}{n_j} \geq 1 - \frac{2r+3}{3r(r-1)} > 1 - \frac{1}{r-1}. \quad (44)$$

Thus, there exists a good family of triorthogonal codes $\{C_j\}$ exceeding the TVZ bound on finite Fields $\mathbb{F}_{r^2}$ for $r \geq 8$. Moreover, it can be verified by direct computations that these codes are also above the GV bound, thereby scaling better than random codes in all regimes. As we will see, such large encoding rates are beneficial when converting to quantum codes. Indeed, the dimension of the quantum code will be $\mathcal{K} \leq k$ and the length $\mathcal{N} = n - \mathcal{K}$. Hence, a large encoding rate in the classical code yields the possibility of quantum codes with correspondingly large encoding rates. In fact, a large encoding rate in the classical code will result in a large flexibility to either increase the distance of the quantum code or increase its dimension instead, as desired.

V. QUANTUM CODES

In this section, we outline how to obtain qudit CSS codes from the previously constructed family of classical triorthogonal codes that support a transversal CCZ gate. We first briefly review the basic elements of quantum

computation on qudits of dimension $q = 2^m$, $m \geq 1$, that are needed for constructing error-correcting codes.

The single-qudit Hilbert space is simply

$$\mathcal{H}_q := \text{span}\left\{ |\alpha\rangle \mid \alpha \in \mathbb{F}_q \right\}. \tag{45}$$

The qudit Pauli gates X^β and Z^β ($\beta \in \mathbb{F}_q$) act as

$$X^\beta |\alpha\rangle = |\alpha + \beta\rangle,$$
$$Z^\beta |\alpha\rangle = (-1)^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha\beta)} |\alpha\rangle. \tag{46}$$

Here, we have used the field trace operator $\text{Tr}_{\mathbb{F}_{r^n}/\mathbb{F}_r}(\cdot) : \mathbb{F}_{r^n} \to \mathbb{F}_r$ defined by

$$\text{Tr}_{\mathbb{F}_{r^n}/\mathbb{F}_r}(x) := x + x^r + x^{r^2} + \cdots + x^{r^{n-1}} \tag{47}$$

to describe these phase gates. These gates generate the qudit Pauli group $\mathcal{P} \subset U(q)$, whose elements take the form $i^a X^\alpha Z^\beta$ where $a \in \{0, 1, 2, 3\}$ and $\alpha, \beta \in \mathbb{F}_q$. The normalizer of the qudit Pauli group is the qudit Clifford group $\mathcal{C}$:

$$\mathcal{C} = \left\{ U \in U(q) \mid UPU^\dagger \in \mathcal{P} \text{ for all } P \in \mathcal{P} \right\}. \tag{48}$$

This qudit Clifford group and a non-Clifford gate element form a universal gate set for qudit-based quantum computation. For our construction of quantum codes, we consider the CCZ gate, a non-Clifford gate defined by

$$CCZ |x\rangle |y\rangle |z\rangle = (-1)^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(xyz)} |x\rangle |y\rangle |z\rangle. \tag{49}$$

This gate lies in the third level of the Clifford hierarchy, implying a $|CCZ\rangle$ state given in $\mathcal{H}_q^{\otimes 3}$ by

$$|CCZ\rangle := CCZ |+\rangle |+\rangle |+\rangle$$
$$= \frac{1}{q^{3/2}} \sum_{x,y,z \in \mathbb{F}_q} (-1)^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(xyz)} |x\rangle |y\rangle |z\rangle, \tag{50}$$

where $|+\rangle$ is the uniform superposition of basis states. The state $|CCZ\rangle$ can be injected using a Clifford circuit via gate teleportation [67]. So, the task of MSD in this paper is to distill this state. The next sections will describe the quantum codes that we will build for this procedure.

We can then discuss how to obtain a quantum code $\mathcal{Q}$ with parameters $[[\mathcal{N}, \mathcal{K}, \mathcal{D}]]_{r^2}$ from a triorthogonal code $C : [n, k, d]_{r^2}$ following a standard procedure [48, 50]. In short, the $k \times n$ generator matrix of a triorthogonal code C can be put in the convenient form

$$\mathcal{G}(C) = \begin{pmatrix} \mathbb{1}_\mathcal{K} & H_1 \\ 0 & H_0 \end{pmatrix}, \tag{51}$$

where $\mathcal{K} \leq k$. Because C is triorthogonal, the row vector subspaces, $\mathcal{H}_0 := \text{rowspace}(H_0)$ and $\mathcal{H}_1 := \text{rowspace}(H_1)$, are orthogonal (see, e.g., Ref. [50]). Let $\mathcal{H} := \text{rowspace}(H_0, H_1)$, so $\mathcal{H}_0 \subset \mathcal{H}$. From the qudit Pauli gates defined in Eq. (46) combined with these spaces, we can define the quantum CSS code

$$\mathcal{Q} = \text{CSS}\left(X, \mathcal{H}_0; Z, \mathcal{H}^\perp \right), \tag{52}$$

which has a transversal CCZ [50, Lemma 2.3].

The parameters $\mathcal{N}, \mathcal{K}$, and $\mathcal{D}$ of this quantum code can be estimated from those of the classical code. Clearly, the length is $\mathcal{N} = n - \mathcal{K}$, and $\mathcal{K}$ is the dimension. As a CSS code, its distance is given by $\mathcal{D} = \min(\mathcal{D}_X, \mathcal{D}_Z)$ where

$$\mathcal{D}_X = \min_{f \in \mathcal{H} \setminus \mathcal{H}_0} |f| \geq \text{dist}(\mathcal{H}) \geq d - \mathcal{K},$$
$$\mathcal{D}_Z = \min_{f \in \mathcal{H}_0^\perp \setminus \mathcal{H}^\perp} |f| \geq \text{dist}(\mathcal{H}_0^\perp) \tag{53}$$

and d is the distance of the classical code. Assuming $2g - 2 < \deg G < n$, Eq. 12 yields

$$\mathcal{D}_X \geq n - \deg G - \mathcal{K}. \tag{54}$$

Along with this, we can lower bound $\mathcal{D}_Z$. As explained in Ref. [50], the code $\mathcal{H}_0$ can be viewed as an AG code

$$\mathcal{H}_0 = C_\mathcal{L}(D', G'). \tag{55}$$

Here the divisor $D' = \sum_{i=\mathcal{K}+1}^n P_i$ corresponds to puncturing $\mathcal{K}$ positions, and $G' = G - \sum_{i=1}^\mathcal{K} P_i$. Equivalently, $\mathcal{H}_0$ is obtained by restricting the Riemann–Roch space $\mathcal{L}(G)$ to functions that vanish at all punctured positions, so that $\mathcal{L}(G') \subset \mathcal{L}(G)$. Then, using Eq. (13), we obtain

$$\mathcal{D}_Z \geq \text{dist}(\mathcal{H}_0^\perp) \geq \deg(G') - (2g - 2)$$
$$= \deg(G) - \mathcal{K} - (2g - 2). \tag{56}$$

In our case, we will show $\mathcal{D}_Z < \mathcal{D}_X$, implying that the distance of each of our quantum codes satisfy

$$\mathcal{D} \geq \deg(G) - \mathcal{K} - (2g - 2). \tag{57}$$

In particular, we may derive a family of quantum codes $\mathcal{Q}_j$ from the triorthogonal codes C_j constructed in Sec. IV. We summarize our quantum codes below:

Theorem 4 (Good quantum codes with a transversal CCZ gate)**.** *There exists a good family of quantum codes* $\{\mathcal{Q}_j\}$ *with transversal CCZ gates on qudits with dimension* $q = r^2 = 2^{2m}$ *for* $m \geq 3$. *Each code* $\mathcal{Q}_j$ *has parameters*

$$\mathcal{N}_j = r^j(r^2 - r) - \mathcal{K}_j$$
$$\mathcal{K}_j = x_1 r^j \left((r+1) \left\lfloor \frac{r-2}{3} \right\rfloor - 2r \right) + x_2 v(r, j)$$
$$\mathcal{D}_j \geq (1 - x_1) r^j \left((r+1) \left\lfloor \frac{r-2}{3} \right\rfloor - 2r \right)$$
$$+ (1 - x_2) v(r, j) \tag{58}$$

where

$$v(r, j) := \begin{cases} 4r^{\frac{j+1}{2}} & \text{if } j \text{ is odd} \\ 2r^{\frac{j}{2}} (1 + r) & \text{otherwise} \end{cases}$$

and the constants $x_1 \in (0, 1)$ *and* $x_2 \in [0, 1]$ *are chosen such that* $\mathcal{K}_j$ *is an integer.*
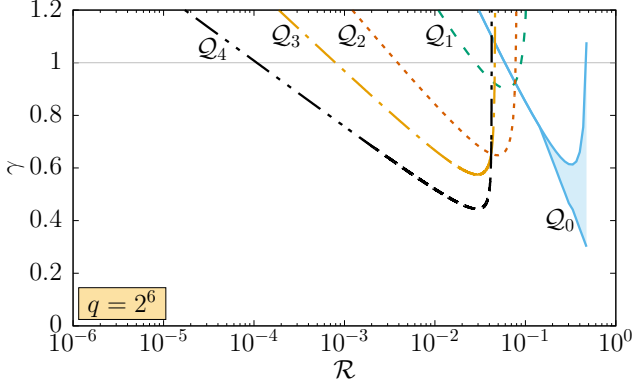
Proof. We show the proof in App. C. $\qquad\square$

FIG. 2. Bounds on γ vs. $\mathcal{R}$ for quantum codes $\mathcal{Q}_j$ at different levels of the lifting for $q = 2^6 = 64$. For $\mathcal{Q}_0$, we present two-sided bounds, while for the rest we have only upper bounds.

FIG. 3. Bounds on γ vs. $\mathcal{R}$ for quantum codes $\mathcal{Q}_j$ at different levels of the lifting for $q = 2^8 = 256$. For $\mathcal{Q}_0$, we present two-sided bounds, while for the rest we have only upper bounds.

VI. EXPLICIT CODE CONSTRUCTIONS

Having demonstrated the existences of new families of asymptotically or nearly asymptotically good codes, in this section we undertake to present explicit results for the properties of some $\mathcal{Q}_j = [[\mathcal{N}_j, \mathcal{K}_j, \mathcal{D}_j]]_q$ for low q and j. In particular, we are interested in understanding what overheads γ and encoding rates $\mathcal{R} = \mathcal{K}_j/\mathcal{N}_j$ are achievable. For reference in this discussion, comparisons will be made to the canonical code used in qubit MSD of $\mathcal{Q}_{BK} = [[15, 1, 3]]_2$ with $\gamma \approx 2.46$ and $\mathcal{R} \approx 0.07$ [68].

While $\mathcal{R}$ is straightforward once the code is constructed, computing the minimum-weight logical operator—and therefore the distance–for an arbitrary stabilizer code is NP-complete. For the large q codes that we will be considering, we thus have to suffice with bounds for now. For lower bounds $\mathcal{D}_j^{min}$, we use Eqs. (3) and (C1). To estimate upper bounds, for Q_0 we can leverage the QLDPC code available at [69] with a workstation. We leave the study of larger codes to future work.

The lowest q for which we can construct asymptotically good codes is the family of codes with $q = 2^6$. Their investigation is further motivated by the experimental demonstration of $q = 64$ state preparation, suggesting MSD with these codes is nearer to realization than larger q. For $j \leq 4$, the bounds on γ are presented as a function of $\mathcal{R}$ for all possible codes in our family with $q = 2^6$ in Fig. 2. The first point to observe is that $\gamma^{max} \to 0$ as $j \to \infty$ (as anticipated for an asymptotically good family). Moreover, all codes outperform $\mathcal{Q}_{BK}$. In particular, the best performing code in Q_0 is $[[42, 14, 6]]_{64}$, which has $\mathcal{R} = \frac{1}{3}$ and $\gamma^{max} \approx 0.613$. The codes within each $\mathcal{Q}_j$ with the lowest γ^{max} are tabulated in Table III.

Increasing the qudit dimension to $q = 2^8$; $\mathcal{N}_j$, $\mathcal{K}_j$, and $\mathcal{D}_j^{min}$ all grow by factors of 3-4. While the best code in $\mathcal{Q}_0$, $[[188, 52, 18]]$, demonstrates a smaller overhead at $\gamma^{max} = 0.445$ than the best code in $\mathcal{Q}_4$ of $d = 2^6$, it also comes at a cost of less efficient encoding rate $\mathcal{R}$ (See Table III). When $j > 0$, all $\mathcal{Q}_j$ have lower overhead
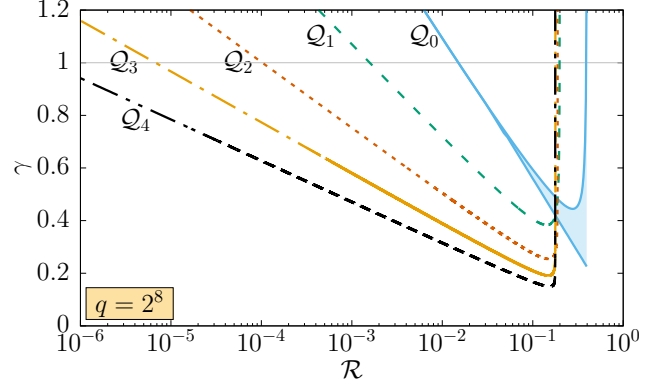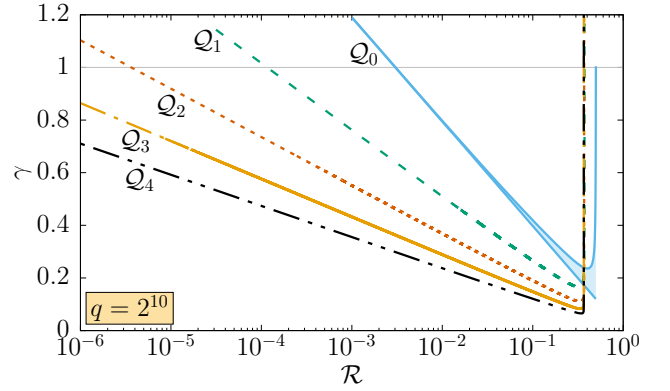

FIG. 4. Bounds on γ vs. $\mathcal{R}$ for quantum codes Q_j at different levels of the lifting for $q = 2^{10} = 1024$. For $\mathcal{Q}_0$, we present two-sided bounds, while for the rest we have only upper bounds.

γ^{max} than any code we have constructed with $d = 2^6$ and greater encoding rates by a factor of 3.

The final qudit dimension for which we explicitly construct codes is $q = 2^{10}$, so that we may compare with the family of asymptotically good codes identified in Ref. [49]. In that work, the codes had $\mathcal{R} \leq \frac{5}{114} \approx 0.04$ and $\mathcal{N} \geq 932,090$ were identified. In contrast, our families have $\mathcal{R} \geq 0.319$ and $\gamma^{max} \leq 0.236$ for the best codes in all $\mathcal{Q}_j$. Further, it is only in $\mathcal{Q}_2$ where our codes begin to exceed $\mathcal{N} = 932,090$. Instead, our best code in $\mathcal{Q}_0$ requires only $\mathcal{N} = 708$.

In all such cases considered here, we find low overhead costs to TVZ codes that we have constructed explicitly per the methods of Secs. IV and V. Typically, when constructing codes, one aims to guarantee constant overhead by choosing a sufficiently large code from a family, so that only a single round of MSD is required. However for practical implementation this task may be too ambitious and less cost-efficient overall. Indeed, we have constructed codes that are sufficiently small such that they would contribute a low cost even with overhead over multiple rounds of MSD.

One outstanding question is the error threshold for distillation of CCZ from these codes. Prior work on qutrits and ququints found low-overhead codes with thresholds to depolarizing noise as large as $\epsilon \approx 0.1$ exist [46, 64, 66]. Given the higher dimension of the qudits here, the many error channels likely result in lower thresholds, which would degrade the benefits from the codes proposed here. Therefore error thresholds should be investigated while varying $\mathcal{R}$. Another question would be to quantify the codes' maximum stabilizer weight checks, as prior work has shown them to be potentially non-constant in $\mathcal{N}$.

TABLE III. Summary of the codes Q_j for three values of r with the upper bound γ^{max} on their overhead. Reported are: the number of physical qudits used N_j, the number of logical qudits encoded K_j, and a lower bound on the code distance D_j^{min}, and the encoding rate $\mathcal{R}$.

r	j	$[[\mathcal{N}_j, \mathcal{K}_j, \mathcal{D}_j^{min}]]$	$\mathcal{R}$	γ^{max}
8	0	$[[42,14,6]]$	0.333	0.613
	1	$[[422,26,22]]$	0.062	0.902
	2	$[[3416,168,104]]$	0.049	0.649
	3	$[[27851,821,459]]$	0.030	0.575
	4	$[[222850,6526,2818]]$	0.029	0.444
16	0	$[[188,52,18]]$	0.277	0.445
	1	$[[3361,479,161]]$	0.143	0.383
	2	$[[53447,7993,1767]]$	0.150	0.254
	3	$[[855756,127284,21196]]$	0.149	0.191
	4	$[[13632492,2096148,271852]]$	0.154	0.150
32	0	$[[708,284,48]]$	0.401	0.236
	1	$[[24072,7672,968]]$	0.319	0.166
	2	$[[762355,253453,21043]]$	0.333	0.111
	3	$[[24292183,8213673,506711]]$	0.338	0.083
	4	$[[774113521,266073871,12914929]]$	0.344	0.065

VII. STATE REDUCTION

In Thm. 4, we have constructed good quantum codes allowing constant-overhead MSD on qudits of dimension $q = r^2$, where $r \geq 8$ is a power of two. What remains is to construct a protocol yielding a magic state for an arbitrary $q = 2^n$. Following Ref. [49], we treat each r^2-qudit as two r-qudits. Then, for a $r \geq 8$, we use our codes to distill a $|CCZ\rangle_{r^2}$ state. This state can reduced with a constant-depth Clifford circuit into a $|CCZ\rangle_r$. Below, we derive this state reduction procedure and show how any $|CCZ\rangle_{2^n}$ may be obtained with this procedure.

Lemma 4. *Given a state $|CCZ\rangle_{r^2}$, one can obtain the state $|CCZ\rangle_r$ using a Clifford circuit (Fig 5) consisting of 4 single-qudit gates and 3 two-qudit gates.*

Proof. We choose a normal basis $\{\theta, \theta^r\}$ of $\mathbb{F}_{r^2}$ over $\mathbb{F}_r$, which can always be chosen such that $\theta + \theta^r = 1$. In this
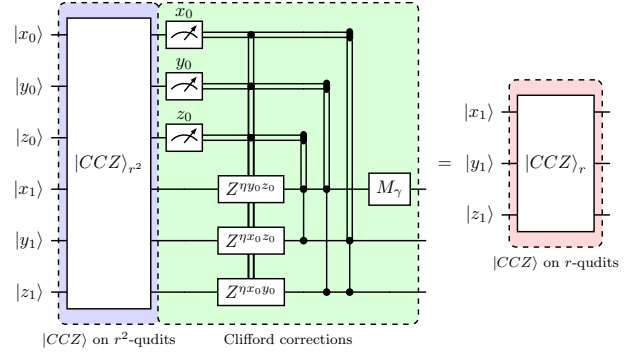

FIG. 5. Reduction of state $|CCZ\rangle_{r^2}$ to a state $|CCZ^\gamma\rangle_r$ where $\gamma := 1 + \eta$, $\eta := \theta^{r+1}$ and $\{\theta, \theta^r\}$ is a normal basis of $\mathbb{F}_{r^2}$ over $\mathbb{F}_r$ such that $\theta + \theta^r = 1$.

way, we can write

$$x = x_0\theta + x_1\theta^r, \; y = y_0\theta + y_1\theta^r, \text{ and } z = z_0\theta + z_1\theta^r \tag{59}$$

where $x_i, y_i, z_i \in \mathbb{F}_r$. Then, we can exploit the composition of field traces

$$\mathrm{Tr}_{\mathbb{F}_{r^2}/\mathbb{F}_2}(xyz) = \mathrm{Tr}_{\mathbb{F}_r/\mathbb{F}_2} \circ \mathrm{Tr}_{\mathbb{F}_{r^2}/\mathbb{F}_r}(xyz). \tag{60}$$

to rewrite

$$|CCZ\rangle_{r^2}$$
$$\propto \sum_{x,y,z} (-1)^{\mathrm{Tr}_{\mathbb{F}_r/\mathbb{F}_2} \circ \mathrm{Tr}_{\mathbb{F}_{r^2}/\mathbb{F}_r}(xyz)} |x_0, y_0, z_0,\rangle_r |x_1, y_1, z_1\rangle_r. \tag{61}$$

and evaluate only the first trace,

$$\mathrm{Tr}_{\mathbb{F}_{r^2}/\mathbb{F}_r}(xyz) = \gamma(x_0y_0z_0 + x_1y_1z_1) + \eta \sum_{i+j+k=1,2} x_iy_jz_k$$
$$\text{where } \gamma := 1 + \theta^{r+1}, \; \eta := \theta^{r+1}. \tag{62}$$

Thus, while the measurements in Fig. 5 fix the values of x_0, y_0, and z_0, the Clifford corrections cancel all phases proportional to η, so only the phase $\gamma x_1 y_1 z_1$ remains with the phase $\gamma x_0 y_0 z_0$ now a global one. These steps produce the state $|CCZ^\gamma\rangle_r$. Then, applying to register $|x_1\rangle_r$ the Clifford gate M_γ given by

$$M_\gamma |v\rangle_r = |\gamma v\rangle_r \text{ for } v \in \mathbb{F}_r, \tag{63}$$

we recover the $|CCZ\rangle_r$ state. $\square$

Theorem 5. *Suppose the state $|CCZ\rangle_{2^{2m}}$ for any $m \geq 3$ can be distilled (at constant space overhead with the codes of Thm. 4). Then, any $|CCZ\rangle_{2^n}$ can be obtained with a constant-depth Clifford circuit.*

Proof. We have a few cases to consider.

1. n is even and $n \geq 6$: set $r = 2^{n/2} \geq 8$ and use our codes to distill $|CCZ\rangle_{2^n}$.

2. $n > 2$ is odd or $n = 4$: set $r = 2^n \geq 8$ and distill $|CCZ\rangle_{r^2}$. Then, Fig. 5 is used to obtain $|CCZ\rangle_{2^n}$.

3. $n \leq 2$: set $r = 16$ and distill $|CCZ\rangle_{r^2}$. Then, Fig. 5 is used twice to obtain $|CCZ\rangle_4$ or thrice for $|CCZ\rangle_2$.

Thus the reduction circuit is used at most thrice. As a result, any $|CCZ\rangle_{2^n}$ gate may be obtained with at most 12 single-qudit and 9 two-qudit Clifford gates. $\square$

This procedure generalizes the result of Ref. [49] where it was shown how a non-Clifford single-qudit gate on 2^{10}-qudit can be converted to qubit $|CCZ\rangle$ gates.

VIII. CONCLUSIONS

In this work, we have presented explicit constructions of low-overhead magic state distillation protocols for qudits with dimensions 2^{2m} with $m \geq 3$ using triorthogonal codes that are asymptotically good. In this, we have identified a new family of triorthogonal codes that satisfy the TVZ bound through a lifting method. Of the codes identified, some can be implemented on $d = 2^6$ qudits – the same dimension as in Ref. [50] and smaller than in Ref. [49]. These are attractive design targets for qudit-based platforms like SRF-cavities where single $d \leq 100$ qudits have been demonstrated at varying levels of sophistication [40, 41] including a $[[42, 14, 6]]_{64}$ code.

Looking beyond these results, there are a number of interesting avenues of research. First, it is critical to identify within our family of codes those best suited for current and future qudit-based platforms in more detail. Numerics should be employed to determine the distillable states and regions with their thresholds. Further, continued exploration of the properties of single codes or families with smaller 2^n-dimension along the lines pursued for prime dimensions in [46] would be valuable. While they do not belong to a family of codes, we can construct a $[[25, 7, \geq 6]]_{32}$ and a $[[7, 1, 3]]_8$ codes with transversal CCZ gate, enabling protocols with low space footprint albeit higher overhead which are potentially practical on qudit-based platforms or even on qubit-based platforms with a small constant factor overhead. Another open question is whether qLDPC codes for qudits [70–73] can have low overhead. Finally, recent work has suggested that mildly relaxing the requirement for asymptotically good codes can improve the locality of the weight checks [74].

[1] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, Qudits and high-dimensional quantum computing, Frontiers in Physics **8**, 589504 (2020).

[2] E. O. Kiktenko, A. S. Nikolaeva, and A. K. Fedorov, Colloquium: Qudits for decomposing multiqubit gates and realizing quantum algorithms, Rev. Mod. Phys. **97**, 021003 (2025).

[3] L. B. Nguyen, N. Goss, K. Siva, Y. Kim, E. Younis, B. Qing, A. Hashim, D. I. Santiago, and I. Siddiqi, Empowering a qudit-based quantum processor by traversing the dual bosonic ladder, Nature Communications **15**, 7117 (2024).

[4] A. S. Nikolaeva, E. O. Kiktenko, and A. K. Fedorov, Efficient realization of quantum algorithms with qudits, EPJ Quant. Technol. **11**, 43 (2024), arXiv:2111.04384 [quant-ph].

[5] M. B. Mansky, S. L. n. Castillo, V. R. Puigvert, and C. Linnhoff-Popien, Near-optimal quantum circuit construction via Cartan decomposition, Phys. Rev. A **108**, 052607 (2023), arXiv:2212.12934 [quant-ph].

[6] D. Janković, J.-G. Hartmann, M. Ruben, and P.-A. Hervieux, Noisy qudit vs multiple qubits: conditions on gate efficiency for enhancing fidelity, npj Quantum Inf. **10**, 59 (2024), arXiv:2302.04543 [quant-ph].

[7] E. M. Murairi, M. Sohaib Alam, H. Lamm, S. Hadfield, and E. Gustafson, Highly-efficient quantum Fourier transformations for some nonabelian groups (2024), arXiv:2408.00075 [quant-ph].

[8] J. Keppens, Q. Eggerickx, V. Levajac, G. Simion, and B. Sorée, Qudit vs. Qubit: Simulated performance of error correction codes in higher dimensions (2025), arXiv:2502.05992 [quant-ph].

[9] A. S. Nikolaeva, E. O. Kiktenko, and A. K. Fedorov, Generalized Toffoli Gate Decomposition Using Ququints:

Towards Realizing Grover's Algorithm with Qudits, Entropy **25**, 387 (2023), arXiv:2212.12505 [quant-ph].

[10] Y. Iiyama, W. Jang, N. Kanazawa, R. Sawada, T. Onodera, and K. Terashi, Qudit-Generalization of the Qubit Echo and Its Application to a Qutrit-Based Toffoli Gate (2024), arXiv:2405.14752 [quant-ph].

[11] E. Champion, Z. Wang, R. Parker, and M. Blok, Multi-frequency control and measurement of a spin-7/2 system encoded in a transmon qudit (2024), arXiv:2405.15857 [quant-ph].

[12] E. O. Kiktenko, A. S. Nikolaeva, P. Xu, G. V. Shlyapnikov, and A. K. Fedorov, Scalable quantum computing with qudits on a graph, Phys. Rev. A **101**, 022304 (2020).

[13] T. Roy, Z. Li, E. Kapit, and D. Schuster, Two-qutrit quantum algorithms on a programmable superconducting processor, Phys. Rev. Appl. **19**, 064024 (2023).

[14] C. T. Hann, G. Lee, S. Girvin, and L. Jiang, Resilience of quantum random access memory to generic noise, PRX Quantum **2**, 020311 (2021).

[15] S. Zhu, A. Sundaram, and G. H. Low, Unified architecture for quantum lookup tables, Phys. Rev. Res. **7**, 043230 (2025).

[16] D. Tancara and F. Albarrán-Arriagada, High-dimensional counterdiabatic quantum computing (2024), arXiv:2410.10622 [quant-ph].

[17] S. Bravyi, A. Kliesch, R. Koenig, and E. Tang, Hybrid quantum-classical algorithms for approximate graph coloring, Quantum **6**, 678 (2022), arXiv:2011.13420 [quant-ph].

[18] M. Chizzini, F. Tacchino, A. Chiesa, I. Tavernelli, S. Carretta, and P. Santini, Qudit-based quantum simulation of fermionic systems, Phys. Rev. A **110**, 062602 (2024).

[19] S. Choi, N. Y. Yao, and M. D. Lukin, Dynamical engineering of interactions in qudit ensembles, Phys. Rev. Lett. **119**, 183603 (2017).

[20] L. Bassman Oftelie, K. Klymko, D. Liu, N. M. Tubman, and W. A. de Jong, Computing Free Energies with Fluctuation Relations on Quantum Computers, Phys. Rev. Lett. **129**, 130603 (2022).

[21] A. Young, Quantum Spin Systems (2023) arXiv:2308.07848 [math-ph].

[22] E. Gustafson, Prospects for Simulating a Qudit Based Model of (1+1)d Scalar QED, Phys. Rev. D **103**, 114505 (2021), arXiv:2104.10136 [quant-ph].

[23] D. González-Cuadra, T. V. Zache, J. Carrasco, B. Kraus, and P. Zoller, Hardware efficient quantum simulation of non-abelian gauge theories with qudits on Rydberg platforms (2022), arXiv:2203.15541 [quant-ph].

[24] P. P. Popov, M. Meth, M. Lewenstein, P. Hauke, M. Ringbauer, E. Zohar, and V. Kasper, Variational quantum simulation of U(1) lattice gauge theories with qudit systems, Phys. Rev. Res. **6**, 013202 (2024).

[25] G. Calajò, G. Magnifico, C. Edmunds, M. Ringbauer, S. Montangero, and P. Silvi, Digital quantum simulation of a (1+1)D SU(2) lattice gauge theory with ion qudits (2024), arXiv:2402.07987 [quant-ph].

[26] M. Illa, C. E. P. Robin, and M. J. Savage, Qu8its for quantum simulations of lattice quantum chromodynamics, Phys. Rev. D **110**, 014507 (2024), arXiv:2403.14537 [quant-ph].

[27] T. V. Zache, D. González-Cuadra, and P. Zoller, Fermion-qudit quantum processors for simulating lattice gauge theories with matter, Quantum **7**, 1140 (2023), arXiv:2303.08683 [quant-ph].

[28] M. Meth *et al.*, Simulating two-dimensional lattice gauge theories on a qudit quantum computer, Nature Phys. **21**, 570 (2025), arXiv:2310.12110 [quant-ph].

[29] D. M. Kürkçüoglu, H. Lamm, and A. Maestri, Qudit Gate Decomposition Dependence for Lattice Gauge Theories (2024), arXiv:2410.16414 [quant-ph].

[30] R. Joshi, M. Meth, J. C. Louw, J. J. Osborne, K. Mato, M. Ringbauer, and J. C. Halimeh, Efficient Qudit Circuit for Quench Dynamics of 2 + 1D Quantum Link Electrodynamics (2025), arXiv:2507.12589 [quant-ph].

[31] M. Ringbauer, M. Meth, L. Postler, R. Stricker, R. Blatt, P. Schindler, and T. Monz, A universal qudit quantum processor with trapped ions, Nature Phys. **18**, 1053 (2022), arXiv:2109.06903 [quant-ph].

[32] P. J. Low, B. White, and C. Senko, Control and Readout of a 13-level Trapped Ion Qudit (2023), arXiv:2306.03340 [quant-ph].

[33] X. Shi, J. Sinanan-Singh, T. J. Burke, J. Chiaverini, and I. L. Chuang, Efficient Implementation of a Quantum Algorithm with a Trapped Ion Qudit (2025), arXiv:2506.09371 [quant-ph].

[34] E. Champion, Z. Wang, R. W. Parker, and M. S. Blok, Efficient Control of a Transmon Qudit Using Effective Spin-7/2 Rotations, Phys. Rev. X **15**, 021096 (2025), arXiv:2405.15857 [quant-ph].

[35] Z. Wang, R. W. Parker, E. Champion, and M. S. Blok, Systematic study of High E_J/E_C transmon qudits up to $d = 12$ (2024), arXiv:2407.17407 [quant-ph].

[36] M. Mezzadri, A. Chiesa, L. Lepori, and S. Carretta, Fault-Tolerant Computing with Single Qudit Encoding (2023), arXiv:2307.10761 [quant-ph].

[37] S. Omanakuttan, A. Mitra, M. J. Martin, and I. H. Deutsch, Quantum optimal control of ten-level nuclear spin qudits in Sr87, Phys. Rev. A **104**, L060401 (2021), arXiv:2106.13705 [quant-ph].

[38] I. F. de Fuentes *et al.*, Navigating the 16-dimensional Hilbert space of a high-spin donor qudit with electric and magnetic fields, Nature Commun. **15**, 1380 (2024), arXiv:2306.07453 [quant-ph].

[39] M.-X. Dong, W.-H. Zhang, L. Zeng, Y.-H. Ye, D.-C. Li, G.-C. Guo, D.-S. Ding, and B.-S. Shi, Highly Efficient Storage of 25-Dimensional Photonic Qudit in a Cold-Atom-Based Quantum Memory, Phys. Rev. Lett. **131**, 240801 (2023), arXiv:2301.00999 [quant-ph].

[40] T. Kim *et al.*, Ultracoherent superconducting cavity-based multiqudit platform with error-resilient control (2025), arXiv:2506.03286 [quant-ph].

[41] X. Deng *et al.*, Quantum-enhanced metrology with large Fock states, Nature Phys. **20**, 1874 (2024), arXiv:2306.16919 [quant-ph].

[42] S. Bravyi and A. Kitaev, Universal quantum computation with ideal clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).

[43] S. Bravyi and J. Haah, Magic-state distillation with low overhead, Phys. Rev. A **86**, 052329 (2012).

[44] E. T. Campbell, H. Anwar, and D. E. Browne, Magic-State Distillation in All Prime Dimensions Using Quantum Reed-Muller Codes, Phys. Rev. X **2**, 041021 (2012).

[45] M. Howard and J. Vala, Qudit versions of the qubit $\pi/8$ gate, Phys. Rev. A **86**, 022316 (2012).

[46] T. Saha and S. Prakash, Sublogarithmic Distillation in all Prime Dimensions using Punctured Reed-Muller Codes (2025), arXiv:2510.10852 [quant-ph].

[47] M. B. Hastings and J. Haah, Distillation with sublogarithmic overhead, Phys. Rev. Lett. **120**, 050504 (2018).

[48] A. Krishna and J.-P. Tillich, Towards low overhead magic state distillation, Phys. Rev. Lett. **123**, 070507 (2019).

[49] A. Wills, M.-H. Hsieh, and H. Yamasaki, Constant-overhead magic state distillation, Nature Phys. 10.1038/s41567-025-03026-0 (2025).

[50] Q. T. Nguyen, Good binary quantum codes with transversal ccz gate, in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25 (Association for Computing Machinery, New York, NY, USA, 2025) p. 697–706.

[51] L. Golowich and V. Guruswami, Asymptotically Good Quantum Codes with Transversal Non-Clifford Gates, in *57th Annual ACM Symposium on Theory of Computing* (2024) arXiv:2408.09254 [quant-ph].

[52] E. N. Gilbert, A comparison of signalling alphabets, The Bell System Technical Journal **31**, 504 (1952).

[53] R. R. Varshamov, Estimate of the number of signals in error correcting codes, Doklady Akademii Nauk SSSR **117**, 739 (1957).

[54] M. Tsfasman, S. Vlăduţ, and D. Nogin, *Algebraic Geometry Codes: Advanced Chapters*, Mathematical Surveys and Monographs (American Mathematical Society, Providence, Rhode Island, 2019) pp. 335–396.

[55] M. A. Tsfasman, S. G. Vlădutx, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, Mathematische Nachrichten **109**, 21 (1982).

[56] M. Chara, R. Podestá, L. Quoos, and R. Toledano, Good iso-dual ag-codes from towers of function fields (2025), arXiv:2503.08899 [math.NT].

[57] M. Chara, R. Podestá, L. Quoos, and R. Toledano, Lifting iso-dual algebraic geometry codes, Designs, Codes and Cryptography **92**, 2743–2767 (2024).

[58] G. L. Matthews, T. Morrison, and A. W. Murphy, Curve-lifted codes for local recovery using lines, Des. Codes Cryptography **92**, 3645–3664 (2024).

[59] S. T. Dougherty, S. Y. Kim, and Y. H. Park, Lifted codes and their weight enumerators, Discrete Mathematics **305**, 123 (2005).

[60] V. Guemard, Lifts of quantum css codes, IEEE Transactions on Information Theory **71**, 5418 (2025).

[61] J. Old, M. Rispler, and M. Müller, Lift-connected surface codes, Quantum Science and Technology **9**, 045012 (2024).

[62] H. Stichtenoth, *Algebraic Function Fields and Codes* (Springer Berlin Heidelberg, 2009).

[63] H. Stichtenoth, Self-dual goppa codes, Journal of Pure and Applied Algebra **55**, 199 (1988).

[64] S. Prakash and R. Singhal, A Search for High-Threshold Qutrit Magic State Distillation Routines (2024), arXiv:2408.00436 [quant-ph].

[65] A. K. Sharma and S. S. Garani, Near-threshold qudit stabilizer codes with efficient encoding circuits for magic-state distillation, Phys. Rev. A **109**, 062426 (2024), [Erratum: Phys.Rev.A 110, 049902 (2024)].

[66] S. Prakash and T. Saha, Low Overhead Qutrit Magic State Distillation, Quantum **9**, 1768 (2025), arXiv:2403.06228 [quant-ph].

[67] E. Knill, Fault-Tolerant Postselected Quantum Computation: Schemes (2004), arXiv:quant-ph/0402171.

[68] S. Bravyi and A. Kitaev, Universal quantum computation with ideal clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).

[69] M. A. Perlin, qLDPC, https://github.com/qLDPCOrg/qLDPC (2023).

[70] S. A. Aly, *On Quantum and Classical Error Control Codes: Constructions and Applications*, Dissertation, Texas A&M University (2008), arXiv:0812.5104 [cs.IT].

[71] S. A. Aly, Families of LDPC codes derived from non-primitive BCH codes and cyclotomic cosets (2008), arXiv:0802.4079 [cs.IT].

[72] S. K. Borah, A. K. Pradhan, N. Raveendran, N. Rengaswamy, and B. Vasić, Non-binary hypergraph product codes for qudit error correction, in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Vol. 01 (2024) pp. 98–108.

[73] B. Vasic, V. Savin, M. Pacenti, S. Borah, and N. Raveendran, Quantum Low-Density Parity-Check Codes (2025), arXiv:2510.14090 [quant-ph].

[74] L. Golowich and V. Guruswami, Near-Asymptotically-Good Quantum Codes with Transversal CCZ Gates and Sublinear-Weight Parity-Checks (2025), arXiv:2510.06798 [quant-ph].

Appendix A: Canonical divisor (η_0)

In this section, we compute the canonical divisor (η_0) for

$$\eta_0 := \frac{dz_0}{z_0} \qquad \text{with } z_0 := \prod_{\alpha \in \mathcal{Z}} (x_0 + \alpha), \qquad \text{(A1)}$$

where Z are the rational places in $F_0 = \mathbb{F}_q(x_0)$. To perform this computation, we observe that for a finite field $\mathbb{F}_q$,

$$\prod_{\alpha \in \mathbb{F}_q} (x - \alpha) = x^q - x \qquad \text{(A2)}$$

and that $\mathbb{F}_{r^2} \backslash \mathcal{Z} = \mathbb{F}_r$. Then, noting that our fields have characteristics 2, we find that

$$z_0 = \frac{x_0^{r^2} + x_0}{x_0^r + x_0}. \qquad \text{(A3)}$$

where we have used the fact that $\mathbb{F}_{r^2} \backslash \mathcal{Z} = \mathbb{F}_r$. Computing the differential dz_0,

$$\begin{aligned} dz_0 &= \frac{x_0^{r^2} + x_0^r}{(x_0^r + x_0)^2} dx_0 \\ &= \frac{(x_0^r + x_0)^r}{(x_0^r + x_0)^2} dx_0 \\ &= (x_0^r + x_0)^{r-2} dx_0 \\ &= \prod_{\alpha \in \mathbb{F}_r} (x_0 + \alpha)^{r-2} \, dx_0. \qquad \text{(A4)} \end{aligned}$$

So far, we have used only ordinary calculus and recognized terms multiplied by r to be trivial. Putting the canonical divisor together,

$$\eta_0 = \frac{dz_0}{z_0} = \frac{\prod_{\alpha \in \mathbb{F}_r} (x_0 + \alpha)^{r-2}}{\prod_{\alpha \in \mathcal{Z}} (x_0 + \alpha)} dx_0, \qquad \text{(A5)}$$

it is clear now that

- The places P_α for $\alpha \in \mathcal{Z}$ are simple poles of η_0 with multiplicities 1.

- Each place Q_α for $\alpha \in \mathbb{F}_r$ is a zero of η_0, each with multiplicity $r - 2$.

- The place at infinity Q_∞ has valuation

$$v_{Q_\infty}(\eta_0) = (r^2 - r) - r(r - 2) - 2$$
$$= r - 2. \qquad \text{(A6)}$$

Thus, the divisor (η_0) is

$$(\eta_0) = -D_0 + (r - 2) \sum_{\alpha \in \mathbb{F}_r} Q_\alpha + (r - 2)Q_\infty$$
$$= -D_0 + (r - 2) \sum_{Q \in \mathcal{V}} Q. \qquad \text{(A7)}$$

Appendix B: Alternative Lifting Procedure

In Sec. IV, we demonstrate how a base AG code may be lifted repeatedly to generate a family of AG codes explicitly with good parameters. Here, we outline a similar lifting method, which offers some improvements upon these parameters, although their asymptotic behavior is the same.

This alternative lifting method is similar to that of Ref. [57]. As in our earlier method, the definition and the lifting of our first divisor D_j remain the same. Instead, we may lift the G_j divisor by

$$G_{j+1} := \text{Con}_{F_{j+1}/F_j}(G_j) + \Delta(F_{j+1}/F_j) \qquad \text{(B1)}$$

where

$$\Delta(F_{j+1}/F_j) := \sum_{P \in \mathbb{P}(F_j)} \sum_{P'|P} \left\lfloor \frac{d(P'|P)}{3} \right\rfloor P' \qquad \text{(B2)}$$

and $d(P'|P)$ is the different exponent of $P'|P$, defined as follows:

Definition 10 (Different exponent)**.** *The different exponent of a place $P'|P$ is $d(P'|P) = -v_{P'}(t) \geq 0$ for t forming the complementary module $tO'_P = C_P := \{x \in F' \mid \text{Tr}_{F'/F}(xO'_P) \subseteq \mathcal{O}_P\}$ of the integral closure $O'_P := \bigcap_{P'|P} \mathcal{O}_{P'}$ of O_P.*

The divisors D_{j+1} and G_{j+1} are disjoint by construction, because a place $P' \in \text{supp}\, D_{j+1}$ has $d(P'|P) = e(P'|P) - 1 = 0$ by Dedekind's different formula (Thm. 3.5.1 in Ref. [62]). Therefore, this lifting provides a valid AG code $C_{j+1} := C_{\mathcal{L}}(D_{j+1}, G_{j+1})$. Crucially, it is also triorthogonality-preserving since

$$3\Delta(F_{j+1}/F_j) \leq \text{Diff}(F_{j+1}/F_j), \qquad \text{(B3)}$$

where the different divisor Diff is related to the different exponent via the definition:

$$\text{Diff}(F'/F) := \sum_P \sum_{P'|P} d(P'|P)P'. \qquad \text{(B4)}$$

Appendix C: Proof of Good Quantum Codes' Parameters (Thm. 4)

To prove this theorem, we will explicitly derived the quantum codes from our triorthogonal codes following the discussion in Sec. V. First, we note that Eq. (57),

$$\mathcal{D}_j \geq \deg G_j - \mathcal{K}_j - (2g_j - 2) \qquad \text{(C1)}$$

can be verified simply by comparing the lower bounds on $\mathcal{D}_X$ and $\mathcal{D}_Z$. Then, in light of Eq. (C1), we must ensure

$$\mathcal{K}_j \leq \deg(G_j) + 2(1 - g_j), \qquad \text{(C2)}$$

which we may achieve simply by requiring

$$\mathcal{K}_j < r^j \left((r+1) \left\lfloor \frac{r-2}{3} \right\rfloor - 2r \right) + v, \qquad \text{(C3)}$$

where $v(r, j)$ is a positive function given by

$$v(r, j) := \begin{cases} 4r^{\frac{j+1}{2}} & \text{if } j \text{ is odd} \\ 2r^{\frac{j}{2}}(1 + r) & \text{otherwise} \end{cases}.$$

(Recall here that $\deg G_j = r^j \deg G_0 = r^j(r+1)\left\lfloor \frac{r-2}{3} \right\rfloor$, and our genus g_j is given in terms of our dimension r by Eq. (31).) Fixing $r \geq 8$, our strategy is to equivalently choose

$$\mathcal{K}_j = x_1 r^j \left((r+1) \left\lfloor \frac{r-2}{3} \right\rfloor - 2r \right) + x_2 v(r, j), \quad \text{(C4)}$$

where x_1, x_2 are constants such that $0 < x_1 < 1$, $0 \leq x_2 \leq 1$ and that $\mathcal{K}_j < k_j$ is an integer. Clearly, such constants always exist for $r \geq 8$, e.g. $x_1 = 1/2$ and $x_2 = 0$.

Having chosen $\mathcal{K}_j$, it follows then that

$$\mathcal{N}_j = n_j - \mathcal{K}_j$$
$$= r^j \left[r^2 - r - x_1 \left((r+1) \left\lfloor \frac{r-2}{3} \right\rfloor - 2r \right) \right]$$
$$\quad - x_2 v(r, j) \qquad \text{(C5)}$$

and the distance satsifies

$$\mathcal{D}_j \geq (1 - x_1) r^j \left((r+1) \left\lfloor \frac{r-2}{3} \right\rfloor - 2r \right)$$
$$\quad + (1 - x_2) v(r, j) \qquad \text{(C6)}$$

completing the proof. Note that the constants x_1 and x_2 have different roles. For example, $x_1 \notin \{0, 1\}$ guarantees that both the distance and the dimension are $\Theta(r^{j+2})$. The constant x_2, however, may be chosen to either increase the distance or the dimension.