HAL
open science

Towards low overhead magic state distillation

Anirudh Krishna, Jean-Pierre Tillich

To cite this version:

Anirudh Krishna, Jean-Pierre Tillich. Towards low overhead magic state distillation. 2019. hal-02120564

HAL Id: hal-02120564

https://inria.hal.science/hal-02120564

Preprint submitted on 6 May 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

arXiv:1811.08461v2 [quant-ph] 7 Jan 2019

Towards low overhead magic state distillation

Anirudh Krishna[1] and Jean-Pierre Tillich[2]

[1] *Université de Sherbrooke, 2500 Boulevard de l'Université, Sherbrooke, QC J1K 2R1, Canada*

[2] *Inria, Team SECRET, 2 Rue Simone IFF, CS 42112, 75589 Paris Cedex 12, France,*

(Dated: January 8, 2019)

Magic state distillation is a resource intensive sub-routine for quantum computation. The ratio of noisy input states to output states with error rate at most ϵ scales as $O(\log^{\gamma}(1/\epsilon))$ [1]. In a breakthrough paper, Hastings and Haah [2] showed that it is possible to construct distillation routines with sub-logarithmic overhead, achieving $\gamma \approx 0.6779$ and falsifying a conjecture that γ is lower bounded by 1. They then ask whether γ can be made arbitrarily close to 0. We answer this question in the affirmative for magic state distillation routines using qudits of prime dimension (d dimensional quantum systems for prime d).

Introduction – . One of the biggest obstacles we face as we endeavour to construct a fault-tolerant quantum computer is the tremendous resource overhead required to implement a universal set of gates. Analyses of the resource usage in quantum circuits point to *magic state distillation* as the biggest bottleneck [3–5]. This sub-routine consumes several impure copies of a resource state to produce fewer, but purer, copies of this state. The figure of merit used to measure the efficiency of this protocol is called the *overhead*, defined as the ratio of the number of input to output states. For a target error rate of ϵ, the overhead scales as $O\left(\log^{\gamma}\left(\frac{1}{\epsilon}\right)\right)$ where γ depends on the details of how the distillation sub-routine is constructed. It was conjectured that $\gamma \geq 1$, which if true would imply a strict bound on the efficiency of magic state distillation [1].

In a breakthrough article [2], Hastings and Haah have recently constructed codes for which $\gamma \approx 0.6779$ is achievable and thereby falsified the above conjecture. Their proof uses a quantum error correcting code with a very large block size (the number of qubits that will be addressed at one time step); they require a block size of roughly 2×10^{17}. This raises the question of whether γ can be reduced arbitrarily close to zero and whether this is possible with a smaller block size. In this paper, we answer these questions in the affirmative.

Our result employs quantum error correcting codes defined over qudits or d dimensional quantum systems. To the best of our knowledge, earlier qudit magic state distallation protocols such as [6–9] are only capable of distilling a single qudit. We construct quantum error correcting codes which can encode a growing number of logical qudits which also possess special symmetry properties desirable for fault tolerance. In particular, we build on the classification of diagonal gates in the Clifford hierarchy by Cui et al. [10] to generalize the framework of tri-orthogonality [1] to qudits of dimension p, where p is some prime. We then use Reed-Solomon codes over a prime field to show that we can achieve $\gamma = O(1/\log(p))$.

Gates from the third level of the Clifford hierarchy – . For a prime p, the state space of a qudit of dimension p is associated with the complex Euclidean space $\mathbb{C}^p$. The generalized Pauli group over $\mathbb{C}^p$ is defined using the shift and boost operators X and Z where for $j \in \mathbb{F}_p$,

$$X\left|j\right\rangle = \left|j+1\right\rangle, \quad Z\left|j\right\rangle = \omega^{j}\left|j\right\rangle \ , \tag{1}$$

where addition is modulo p and $\omega = \exp\left(2\pi i/p\right)$ is the p-th root of unity. As shorthand, we shall let $X^{g} = \bigotimes_i X^{g_i}$ and $Z^{f} = \bigotimes_j Z^{f_j}$ for $g, f \in \mathbb{F}_p^n$. For $p > 2$, the Pauli group is the group generated by X and Z along with a phase

$$\mathcal{P} = \langle \omega \mathbb{1}, X, Z \rangle \ . \tag{2}$$

The n-qudit Pauli group $\mathcal{P}_n = \mathcal{P}^{\otimes n}$ is then the n-fold tensor product of $\mathcal{P}$. aoeuidhtnspyfgcrlqjkxbmw Gottesman and Chuang introduced the Clifford hierarchy [11], which is defined recursively as

$$\mathcal{K}^{(t)} = \{U | UPU^{\dagger} \in \mathcal{K}^{(t-1)}, \forall P \in \mathcal{P}\} \ . \tag{3}$$

The second level of this hierarchy is the automorphism group of the Pauli group, denoted $\mathcal{K}^{(2)}$, and is called the Clifford group. Although Clifford gates form a closed finite group, we can use them together with any gate in the third level of the hierarchy to compose a universal set of gates for quantum computation [7]. We shall restrict our attention to diagonal gates in the Clifford hierarchy, and use $\mathcal{K}_d^{(t)}$ to denote the diagonal gates in the t-th level of the hierarchy.

For $m \in \mathbb{N}$ and $1 \leq a \leq p-1$, we let $U_{m,a}$ be the

single-qudit gate

$$U_{m,a} = \sum_j \exp\left(\frac{2\pi i}{p^m} j^a\right) |j\rangle \langle j| \ . \tag{4}$$

These gates are characterized by the parameter m known as the *precision* of the unitary gate and the degree a of the monomials j^a in the exponent of the phase.

The following result was shown by Cui et al. [10] (see theorem 2).

Lemma 1 (Cui et al.)**.** *For $m \in \mathbb{N}$, $1 \leq a \leq p-1$,*

$$U_{m,a} \in \mathcal{K}_d^{((p-1)(m-1)+a)} \setminus \mathcal{K}_d^{((p-1)(m-1)+a-1)} \ . \tag{5}$$

If the dimension of the qudit is $p = 3$ i.e. a qutrit, the third-level gate is $U_{2,1}$ whereas for qudits of dimension $p > 3$, the third-level gate is $U_{1,3}$. For the main body of the article, we shall restrict our attention to $p \geq 5$. We have dealt with the special case of $p = 3$ as well in appendix A.

Before proceeding to the next section, we recall that an n-qudit unitary gate U is *transversal* if it can be expressed as $\otimes_{i=1}^n V_i$, where V_i is some single-qudit unitary operator [12]. Since these gates act on each qudit independently, such gates prevent the spread of errors on one qudit from spreading to another and are therefore fault-tolerant by construction. We seek quantum error correcting codes such that logical gates from the third-level of the Clifford hierarchy can be implemented transversally and this motivates the framework of tri-orthogonality.

Generalized tri-orthogonality–. In this section, we extend the definition of a triply-even space and a tri-orthogonal code as given in [1], [13].

Definition 2 (**Tri-orthogonal matrix**)**.** *Let* $\mathrm{H} \in \mathbb{F}_p^{m\times n}$ *be a matrix whose rows are labeled* $\{h^a\}_{a=1}^m$*. We say that* H *is* tri-orthogonal *if*

1. *for* $1 \leq a < b \leq m$*,*

$$\sum_i h_i^a h_i^b = 0 \pmod p \ .$$

2. *for* $1 \leq a < b < c \leq m$*,*

$$\sum_i h_i^a h_i^b h_i^c = 0 \pmod p \ .$$

We shall partition H into two matrices H_0 and H_1, where H_0 contains the $(m-k)$ rows of H such that for $h \in \mathrm{H}_0$, its weight $\sum_i (h_i)^2 = 0 \pmod p$ and H_1 contains the k rows of H such that for $h \in \mathrm{H}_1$, its weight $\sum_j (h_j)^2 \neq 0 \pmod p$ for some natural number $k \leq M$. Let G be the matrix whose rows are orthogonal to H. Denote by $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}$ and $\mathcal{G}$ the span of the rows of the matrices H_0, H_1, H and G respectively. To obtain a tri-orthogonal quantum code $\mathsf{CSS}(X, \mathrm{H}_0; Z, \mathrm{G})$ from the tri-orthogonal matrix H, we associate

1. the rows of H_0 with the X stabilizer generators;
2. the rows of G with the Z stabilizer generators;
3. the rows of H_1 to both the X and Z logical operators.

Note that when we work with qubits, assuming that the weight of a vector $\sum_i (h_i)^2 = 1 \pmod 2$ implies that $\sum_i (h_i)^t = 1 \pmod 2$ for all $t \in \mathbb{N}$. However this is not the case when working with other primes. For instance, consider the vector $u := (0, 1, 2) \in \mathbb{F}_3$. It obeys $\sum_i (u_i)^3 = 0 \pmod 3$ but $\sum_i (u_i)^2 = 2 \pmod 3$. For this reason we define the quantity $\epsilon_a := \sum_i (h_i^a)^3$ for $1 \leq a \leq k$.

Lemma 14. *The code* $\mathsf{CSS}(X, \mathrm{H}_0; Z, \mathrm{G})$ *is a valid quantum code with dimension k and distance d, where*

$$d = \min_{v \in \mathcal{H}_1 \setminus \mathcal{G}} (v) \ .$$

The proof of this statement has been relegated to appendix B.

Since $\mathsf{CSS}(X, \mathrm{H}_0; Z, \mathrm{G})$ is a CSS code, for any $u \in \mathbb{F}_p^k$, the encoded state $|\overline{u}\rangle$ can be expressed as

$$|\overline{u}\rangle = \frac{1}{\sqrt{|\mathcal{H}_0|}} \sum_{h \in \mathcal{H}_0} \left| \sum_{a=1}^k u_a h^a + h \right\rangle \ ,$$

where the arithmetic within the ket is performed mod p.

Theorem 3. *Let* $\mathrm{H} \in \mathbb{F}_p^{m\times n}$ *be a tri-orthogonal matrix whose rows are labelled* $\{h^a\}_{a=1}^m$*.* $\mathcal{C}(\mathrm{H}) = \mathsf{CSS}(X, \mathrm{H}_0; Z, \mathrm{G})$ *be the tri-orthogonal code obtained from* H*. For* $1 \leq a \leq k$*,* $\epsilon_a := \sum_i (h_i^a)^3$*. The transversal physical gate* $U_{1,3}^{\otimes n}$ *performs the following transversal logical gate:*

$$U_{1,3}^{\otimes n} |\overline{u}\rangle = \bigotimes_{a=1}^k \left(\overline{U_{1,3}}\right)^{\epsilon_a} |\overline{u}\rangle \ .$$

Proof. Let $f \in \mathrm{span}\{h^a\}_{a=1}^m \subseteq \mathbb{F}_p^n$ be a vector in $\mathcal{H}$. The action of transversal $U_{1,3}$ on $|f\rangle$ can be

expressed as

$$U_{1,3}^{\otimes n}\,|f\rangle = \prod_{i=1}^{n} \exp\left(\frac{2\pi i}{p} f_i^3\right)|f\rangle \tag{6}$$

$$= \exp\left(\frac{2\pi i}{p}\sum_{i=1}^{n} f_i^3\right)|f\rangle \ . \tag{7}$$

By assumption, we may express $f = \sum_a u_a h^a$ for some constants $\{u_a\}_a \in \mathbb{F}_p$ and therefore for $i \in \{1,..,N\}$, we have

$$f_i^3 = \left(\sum_a u_a h_i^a\right)^3 \tag{8}$$

$$= \sum_a u_a^3 (h_i^a)^3 + \tag{9}$$

$$3\sum_{a<b}\left[(u_a)^2 u_b (h_i^a)^2 h_i^b + u_a (u_b)^2 h_i^a (h_i^b)^2\right]$$

$$+ \sum_{a<b<c} u_a u_b u_c h_i^a h_i^b h_i^c$$

We may use the definition of tri-orthogonality (definition 2) and ϵ to simplify this expression and obtain

$$\sum_{i=1}^{n} f_i^3 = \sum_{a=1}^{k} u_a^3 \epsilon_a \ . \tag{10}$$

Hence it follows that

$$U_{1,3}^{\otimes n}\,|f\rangle = \exp\left(\frac{2\pi i}{p}\sum_{a=1}^{k} u_a^3 \epsilon_a\right)|f\rangle \ , \tag{11}$$

which is the desired result. □

Triorthogonality can also be expressed simply using the $*$-product between two vectors u, v which is denoted $u * v$ and represents the vector $(u_i v_i)_i$. This can naturally be extended to the $*$-product between 3 or more vectors.

Definition 4 (**Triply even space**). *A subspace $\mathcal{V} \subseteq \mathbb{F}_p^N$ is said to be* triply-even *if for any triple $u, v, w \in \mathcal{V}$,*

$$|u * v * w| = 0 \pmod p \ .$$

For our purposes, it will be convenient to express the triply-even property slightly differently as

Lemma 5. *$\mathcal{V}$ is triply-even if and only if $\mathcal{V} * \mathcal{V} \subseteq \mathcal{V}^\perp$.*

Proof. If $\mathcal{V}$ is triply-even, then it means that for $u, v \in \mathcal{V}$, $u * v \in \mathcal{V}^\perp$. The other direction follows trivially. □

Let $\widetilde{\mathcal{C}} = [n+k, n+k-m]$ be a linear code over $\mathbb{F}_p$ defined by a parity check matrix $\widetilde{H}$ over $\mathbb{F}_p$ of dimension $m \times (n+k)$. If the dual code $\widetilde{\mathcal{C}}^\perp$ is triply-even and contains the all 1s vector, we may construct a quantum code by puncturing $\widetilde{\mathcal{C}}^\perp$. For simplicity, suppose we puncture the first k positions of the space; if not, we can always permute the qudits. We may then express the parity check matrix $\widetilde{H}$ of the code $\widetilde{\mathcal{C}}$ in (almost) systematic form with respect to the puncture:

$$\widetilde{H} = \begin{pmatrix} -\mathbb{1}_k & \mathrm{H}_1 \\ 0 & \mathrm{H}_0 \end{pmatrix} \ , \tag{12}$$

where $\mathbb{1}_k$ represents the $k \times k$ identity matrix, and H_1, H_0 are matrices of dimension $k \times n$ and $(m-k) \times n$ respectively. Note that this is not exactly systematic form because there is a minus sign preceding the identity $\mathbb{1}_k$.

Lemma 6. *Let $\widetilde{\mathcal{C}}$ be an $[n+k, n+k-m]$ code such that $\widetilde{\mathcal{C}}^\perp$ is triply-even and contains the all 1s vector. The parity check matrix H of the code $\mathcal{C}$*

$$\mathrm{H} = \begin{pmatrix} \mathrm{H}_1 \\ \mathrm{H}_0 \end{pmatrix} \tag{13}$$

is tri-orthogonal. Furthermore, for all $1 \le a \le k$, $h^a \in \mathrm{H}_1$, we must have $\epsilon_a = \sum_i (h_i^a)^3 = 1 \pmod p$ and $h^a \in \mathrm{H}_1$ that $\sum_i (h_i^a)^2 = -1 \pmod p$.

The proof of this claim can be found in the appendix 0 C.

The protocol for performing distillation has been presented in the paper by Bravyi and Haah [1]. Although this protocol and analysis was originally meant for qubits, it readily extends to qudit systems as well. For a target error rate of ϵ, the overhead for a $[\![n, k, d]\!]$ quantum error correcting code therefore scales as $\log^\gamma(1/\epsilon)$, where $\gamma = \log(n/k)/\log(d)$.

Reed-Solomon codes –. As noted, the condition of tri-orthogonality can be cast in terms of the star-product. Incidentally, this is a well-studied object in classical coding theory [14]. Based on this, we expect that satisfying the tri-orthogonality condition with a good minimum distance becomes easier as the size of the field over which the codes are defined increases.

Reed-Solomon codes are arguably the simplest class of algebraic codes that illustrate this idea. Let $\mathcal{R}$ be the ring of univariate polynomials over the field $\mathbb{F}_p$, i.e. $\mathcal{R} = \mathbb{F}_p[x]/(x^p - x)$. We define the evaluation map $\mathsf{ev} : \mathcal{R} \to \mathbb{F}_p$ for any polynomial as $\mathsf{ev}(\alpha) = (\alpha(u))_{u \in \mathbb{F}_p}$. Note that the map ev is a bijection and in particular, maps the $*$-product to the product of monomials, i.e. if $\alpha, \beta \in \mathcal{M}$, then

$$\mathsf{ev}(\alpha) * \mathsf{ev}(\beta) = \mathsf{ev}(\alpha\beta) \ . \tag{14}$$

We are now equipped to define the Reed-Solomon code.

Definition 7. *For $l \leq p$, the Reed-Solomon code RS_l is defined as*

$$\mathsf{RS}_l := \mathrm{span}\{\mathsf{ev}(\alpha) | \alpha \in \mathcal{R}, \deg \alpha < l\} \ .$$

We state some well known properties of Reed-Solomon codes and point the interested reader to [15] for proofs.

Lemma 8. *For $m \leq p$, the Reed-Solomon code RS_l is a $[p, l, p-l+1]$ code over $\mathbb{F}_p$. Its dual $\mathsf{RS}_l^\perp$ is*

$$\mathsf{RS}_l^\perp = \mathsf{RS}_{p-l} \ .$$

These observations imply the following simple condition to state when a Reed-Solomon code RS_l is triply-even.

Theorem 9. *The Reed-Solomon code RS_l is triply even if $3l < p+1$.*

Proof. According to lemma 5, the condition for a Reed-Solomon code to be triply even is

$$\mathsf{RS}_l * \mathsf{RS}_l \subseteq \mathsf{RS}_l^\perp = \mathsf{RS}_{p-l+1} \ ,$$

where the last equality follows from lemma 8. Since the map ev is a bijection,

$$\mathsf{ev}(\alpha) * \mathsf{ev}(\beta) = \mathsf{ev}(\alpha\beta) \ .$$

For $\alpha, \beta \in \mathsf{RS}_l$, $\deg(\alpha\beta) < 2l-1$. This implies that the code RS_l is triply even if $2l-1 < p-l$ or equivalently if $3l < p+1$. □

For $u \in \mathbb{F}_p^p$, and any set $\mathcal{A} \subseteq \mathbb{Z}_p$, let $u|_\mathcal{A}$ denote the restriction of the vector u to the indices in $\mathcal{A}$. In particular, if $\mathcal{A} = \{a_i\}_{i=1}^k \subseteq \mathbb{Z}_p$ is some set of punctured locations, then we can define a shortened Reed-Solomon code $\mathsf{SRS}_{p-l,\mathcal{A}}$ defined as

$$\mathsf{SRS}_{p-l,\mathcal{A}} = \{u|_{\mathcal{A}^c} | u \in \mathsf{RS}_{p-l}, u|_\mathcal{A} = 0\} \ , \qquad (15)$$

where $\mathcal{A}^c$ denotes the complement of $\mathcal{A}$ within $\mathbb{Z}_p$.

Let $\mathsf{SRS}_{p-l,\mathcal{A}}^\perp = \mathsf{PRS}_{l,\mathcal{A}}$ denote the punctured Reed-Solomon code defined as

$$\mathsf{PRS}_{l,\mathcal{A}} = \{u|_{\mathcal{A}^c} | u \in \mathsf{RS}_l\} \ . \qquad (16)$$

In constructing a tri-orthogonal quantum code by puncturing RS_l, the X stabilizers correspond to the set $\mathsf{SRS}_{l,\mathcal{A}}$ and the Z stabilizers correspond to the set $\mathsf{SRS}_{p-l,\mathcal{A}}$. Therefore the distance of the quantum code is the distance of $\mathsf{SRS}_{l,\mathcal{A}}^\perp = \mathsf{PRS}_{p-l,\mathcal{A}}$.

Lemma 10. *The punctured Reed-Solomon code $\mathsf{PRS}_{p-l,\mathcal{A}}$ has distance $l-k$.*

Proof. $\mathsf{PRS}_{p-l,\mathcal{A}}$ contains polynomials from RS_{p-l} with degree strictly less than $p-l$. If we puncture the code at locations in $\mathcal{A}$, the distance can drop by at most k. Let $\mathcal{A}^c = \mathbb{Z}_p \setminus \mathcal{A}$ and let $\mathcal{B} \subset \mathcal{A}^c$ be an arbitrary subset such that $|\mathcal{B}| = k$. This implies that the polynomial $g := \prod_{b \in \mathcal{B}}(x-b)$ is non-zero on the locations of the punctures and therefore, that $\mathsf{ev}(g)|_{\mathcal{A}^c}$ has weight $l-k$. □

Together with lemma 6, these results imply the following lemma:

Lemma 11. *For prime p, choose natural numbers l, k such that $3l \leq p+1$ and $k \leq l$. The tri-orthogonal quantum code $\mathcal{Q}$ whose X stabilizers are $\mathsf{SRS}_{l,\mathcal{A}}$ and Z stabilizers are $\mathsf{SRS}_{p-l,\mathcal{A}}$ is a $[\![p-k, k, l-k]\!]$ quantum code.*

The overhead associated with $\mathcal{Q}$ is then just

$$\gamma = \frac{\log((p-k)/k)}{\log(m-k)} \ . \qquad (17)$$

We find that $\gamma = 0.98 < 1$ for a $[\![35, 6, 6]\!]$ code over $p = 41$ and $\gamma = 0.657..$ for a $[\![83, 14, 15]\!]$ code for $p = 97$. Whereas Hastings and Haah required block sizes of roughly 2×10^{17} to achieve sub-logarithmic overhead, we find that it is possible to exceed the γ they could achieve using a block size of 83. We hasten to add this comes at the cost of using very large qudits whose dimension scales linearly with the block size.

Conclusion–. We have demonstrated that we can achieve arbitrarily close to constant overhead for magic state distillation using prime dimensional qudits. Furthermore, we have done so with relatively small block sizes, although the dimension of the qudits is fairly large. It still remains an open question to show that γ can be made arbitrarily close to 0 for qubit based protocols. Moreover, it is important to know whether this can be done for small block sizes.

Acknowledgements–. We would like to thank David Poulin for many helpful discussions and Colin Trout for detailed feedback on an earlier draft of this work. A.K. would like to thank Inria, Paris for their hospitality during his visit and the MITACS organization for the Globalink award which facilitated his visit to Inria, Paris. A.K. also acknowledges support from the Fonds de Recherche du Québec - Nature et Technologies (FRQNT) via the B2X scholarship for doctoral candidates. JPT acknowledges the support of the European Union and the French Agence Nationale de la Recherche through the QCDA project.

[1] S. Bravyi and J. Haah. Magic-state distillation with low overhead. *Physical Review A*, 86(5):052329, 2012.

[2] M. B. Hastings and J. Haah. Distillation with sublogarithmic overhead. *Physical Review Letters*, 120(5):050504, 2018.

[3] M. Suchara, A. Faruque, C.-Y. Lai, G. Paz, F. T. Chong, and J. Kubiatowicz. Comparing the overhead of topological and concatenated quantum error correction. *arXiv preprint arXiv:1312.2316*, 2013.

[4] C. Jones. Multilevel distillation of magic states for quantum computing. *Physical Review A*, 87(4):042305, 2013.

[5] J. O'Gorman and E. T. Campbell. Quantum computation with realistic magic-state factories. *Physical Review A*, 95(3):032338, 2017.

[6] H. Anwar, E. T. Campbell, and D. E. Browne. Qutrit magic state distillation. *New Journal of Physics*, 14(6):063006, 2012.

[7] E. T. Campbell, H. Anwar, and D. E. Browne. Magic-state distillation in all prime dimensions using quantum reed-muller codes. *Physical Review X*, 2(4):041021, 2012.

[8] M. Howard and J. Vala. Qudit versions of the qubit $\pi/8$ gate. *Physical Review A*, 86(2):022316, 2012.

[9] E. T. Campbell. Enhanced fault-tolerant quantum computing in d-level systems. *Physical Review Letters*, 113(23):230501, 2014.

[10] S. X. Cui, D. Gottesman, and A. Krishna. Diagonal gates in the clifford hierarchy. *Physical Review A*, 95(1):012329, 2017.

[11] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390, 1999.

[12] D. Gottesman. Stabilizer codes and quantum error correction. *arXiv preprint quant-ph/9705052*, 1997.

[13] J. Haah and M. B. Hastings. Codes and protocols for distilling t, controlled-s, and toffoli gates. *Quantum*, 2:71, 2018.

[14] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. *Algorithmic arithmetic, geometry, and coding theory. Contemp. Math*, 637:3–78, 2015.

[15] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. Elsevier, 1977.

APPENDICES

A. The special case of $p = 3$

In this appendix, we show that tri-orthogonality applies to $p = 3$ as well.

We first show how addition modulo 9 can be expressed in ternary. First we note that any element of $a \in \mathbb{Z}_9$ can be expressed as $a_0 + 3a_1$ for $a_0, a_1 \in \mathbb{F}_3$.

For any two elements $a, b \in \mathbb{Z}_9$, where $a = a_0 + 3a_1$ and $b = b_0 + 3b_1$, we can express addition over $\mathbb{Z}_9$ in terms of addition mod 3 as

$$a + b = (a_0 + b_0) - 3(a_0 b_0 + a_0^2 b_0 + a_0 b_0^2) + 3(a_1 + b_1) \ , \tag{18}$$

where the arithmetic within parthentheses is performed modulo 3. It is straightforward to check this equation explicitly. This can easily be extended to the sum over several elements as follows.

Lemma 12. *For $m \in \mathbb{N}$, let $\{a^i\}_{i=1}^m$ be elements of $\mathbb{Z}_9$, where for each i, we may express a^i in ternary as $a_0^i + 3a_1^i$. Then*

$$\begin{aligned}\sum_i a^i = &\left(\sum_i a_0^i\right) - 3\left(\sum_{i<j} a_0^i a_0^j\right) \\ &-3\left(\sum_{i<j} (a_0^i)^2 a_0^j + a_0^i (a_0^j)^2\right) \\ &+3\left(\sum_{i<j<k} a_0^i a_0^j a_0^k\right) + 3\left(\sum_i a_1^i\right) \ .\end{aligned} \tag{19}$$

Proof. The proof follows by induction on m. The base case for $m = 2$ follows from eq. 18.

Suppose we have proved eq. 19 for $m' < m$. If we add another element $b = b_0 + 3b_1$, then the non-trivial part emerges from the sum of the 0-components. We have

$$\begin{aligned}\sum_{i=1}^{m'} a^i + b = &\left(\sum_{i=1}^{m'} a_0^i + b_0\right) \\ &-3\left(\sum_{i<j} a_0^i a_0^j + \sum_i a_0^i b_0\right) \\ &-3\left(\left(\sum_i a_0^i\right)^2 b_0 + a_0^i b_0^2\right) \\ &+\left(\sum_{i<j} (a_0^i)^2 a_0^j + a_0^i (a_0^j)^2\right) \\ &+3\left(\sum_{i<j<k} a_0^i a_0^j a_0^k\right) + 3\left(\sum_i a_1^i + b_1\right) \ .\end{aligned}$$

Expanding the square of $\sum_i a_i$ yields the desired result. □

Theorem 13. *Let* $\mathrm{H} \in \mathbb{F}_p^{m\times n}$ *be a tri-orthogonal matrix whose rows are labelled* $\{h^a\}_{a=1}^m$. $\mathcal{C}(\mathrm{H}) = \mathsf{CSS}(X, \mathrm{H}_0; Z, \mathrm{G})$ *be the tri-orthogonal code obtained from* H. *For* $1 \le a \le K$, $\epsilon_a := \sum_i (h_i^a) \pmod 9$. *The transversal physical gate* $U_{2,1}^{\otimes n}$ *performs the following transversal logical gate:*

$$U_{2,1}^{\otimes n} |\overline{u}\rangle = \bigotimes_{a=1}^{k} \left(\overline{U_{2,1}}\right)^{\epsilon_a} |\overline{u}\rangle \ .$$

Proof. Let $f \in \mathrm{span}\{h^a\}_{a=1}^m \subseteq \mathbb{F}_3^n$ be a vector in the image of $\mathcal{H}$. The action of transversal $U_{2,1}$ on $|f\rangle$ can be expressed as

$$U_{2,1}^{\otimes n} |f\rangle = \prod_{i=1}^{n} \exp\left(\frac{2\pi i}{9} f_i\right) |f\rangle \tag{20}$$

$$= \exp\left(\frac{2\pi i}{9} \sum_{i=1}^{n} f_i\right) |f\rangle \ . \tag{21}$$

By assumption, we may express $f = \sum_a u_a h^a \pmod 9$ for some constants $\{u_a\}_a \in \mathbb{F}_3$. We express this sum in a ternary as

$$\begin{aligned} f_i &= \sum_a u_a h_i^a \pmod 9 \\ &= \sum_a u_a h_i^a \pmod 3 \\ &- 3\sum_{a<b} \big[u_a u_b h_i^a h_i^b + (u_a)^2 u_b (h_i^a)^2 h_i^b + \\ &u_a (u_b)^2 h_i^a (h_i^b)^2\big] \pmod 3 \\ &- 3\left[\sum_{a<b<c} u_a u_b u_c h_i^a h_i^b h_i^c \pmod 3\right] \ . \end{aligned}$$

This is especially convenient because each term in the sum above is expressed $\mathbb{F}_3$, the field over which tri-orthogonality is defined. This is proved in lemma 12. We may use definition 2 of tri-orthogonality to simplify this expression and obtain

$$\sum_{i=1}^{n} f_i = \sum_{a=1}^{k} u_a \epsilon_a \ . \tag{22}$$

Hence it follows that

$$U_{2,1}^{\otimes n} |f\rangle = \bigotimes_{a=1}^{k} \exp\left(\frac{2\pi i}{9} u_a \epsilon_a\right) |f\rangle \ , \tag{23}$$

which implies the desired result. □

B. $\mathsf{CSS}(X, \mathrm{H}_0; Z, \mathrm{G})$ is a valid code

Lemma 14. *The code* $\mathsf{CSS}(X, \mathrm{H}_0; Z, \mathrm{G})$ *is a valid quantum code with dimension* k *and distance* d, *where*

$$d = \min_{v \in \mathcal{H}_1 \setminus \mathcal{G}} (v) \ .$$

Proof. The logical Z operators corresponding to H_1 are going to commute with the X stabilizer generators corresponding to H_0 because of condition 1. Note that without loss of generality, we can always replace any row in $h \in \mathrm{H}_1$ with αh for $\alpha \in \mathbb{Z}_p$ such that we modify just the logical X operators. By doing so, we can force the X and Z logical operators to obey the canonical commutation relations as $[\overline{X}^a, \overline{Z}^b] = \delta_{a,b}$.

Following an argument identical to that of lemma 1 of [1], we can show that the vectors of H_1 are independent and that they do not overlap with H_0. Any vector $f \in \mathcal{H}_1$ can be expressed as $\sum_a x_a h^a$ for some $x_a \in \mathbb{F}_p$. It follows from the orthogonality condition that if $f = 0$, then each x_a must be identically 0. Similarly if we assume that a $u \in \mathcal{H}_0$ was in H_1, then we run into a contradiction for the same reason. Therefore the dimension of the code is k.

We have chosen these matrices such that $\mathcal{H}_0 \subseteq \mathcal{G}$. Therefore, the X distance d_X is at least as much as the Z distance d_Z since

$$d_Z = \min_{u \in \mathcal{H}_1 \setminus \mathcal{G}} (u) \le \min_{u \in \mathcal{H}_1 \setminus \mathcal{H}_0} (u) = d_X \ . \tag{24}$$

This is the distance of the code. □

C. Tri-orthogonality from triply-even codes

Lemma 6. *Let* $\widetilde{\mathcal{C}}$ *be an* $[n+k, n+k-m]$ *code such that* $\widetilde{\mathcal{C}}^\perp$ *is triply-even and contains the all* 1*s vector. The parity check matrix* H *of the code* $\mathcal{C}$

$$\mathrm{H} = \begin{pmatrix} \mathrm{H}_1 \\ \mathrm{H}_0 \end{pmatrix} \tag{13}$$

is tri-orthogonal. Furthermore, for all $1 \le a \le k$, $h^a \in \mathrm{H}_1$, *we must have* $\epsilon_a = \sum_i (h_i^a)^3 = 1 \pmod p$ *and* $h^a \in \mathrm{H}_1$ *that* $\sum_i (h_i^a)^2 = -1 \pmod p$.

Proof. Since $\widetilde{\mathcal{C}}^\perp$ is triply-even, it follows that for any three rows $\widetilde{H}^a, \widetilde{H}^b, \widetilde{H}^c \in \widetilde{\mathcal{C}}^\perp$, that $|\widetilde{H}^a * \widetilde{H}^b * \widetilde{H}^c| = 0 \pmod p$ by definition. If $1 \le a < b < c \le m$, then the same is true if we restrict these vectors to the

last n locations as they do not overlap on the first k locations. This in turn implies that $|h^a * h^b * h^c| = 0 \pmod p$ for $h^a, h^b, h^c \in \mathcal{C}^\perp$. It also implies that for $1 \leq a \leq k$, that $|h^a * h^a * h^a| = 1 \pmod p$. Since the all 1s vector is in $\widetilde{\mathcal{C}}^\perp$, it follows that if $a < b$ that $|h^a * h^b| = 0 \pmod p$ and that for $1 \leq a \leq k$, that $|h^a * h^a| = -1 \pmod p$. $\square$