Electronic Colloquium on Computational Complexity, Report No. 160 (2026)

Improved Transversal Non-Clifford Gates from Cup Products

Louis Golowich
UC Berkeley
lgolowich@berkeley.edu

Itzhak Tamo
Tel Aviv University
tamo@tauex.tau.ac.il

Guanyu Zhu
IBM Quantum
Guanyu.Zhu@ibm.com

August 19, 2026

Abstract

It is a major challenge in quantum fault-tolerance to obtain low-overhead protocols for performing non-Clifford gates. In this vein, we construct quantum codes with low-weight stabilizers that support transversal (i.e. low-depth) implementations of the non-Clifford $C^{r-1}Z$ gate, for every constant $r \geq 3$. In particular, we obtain length-n quantum LDPC codes (with constant-weight stabilizers) of polynomial distance $d \geq n^{(1-\epsilon)/r}$ supporting transversal $C^{r-1}Z$ gates on a close-to-linear number $k \geq n^{1-\epsilon}$ of disjoint tuples of logical qubits, for arbitrarily small $\epsilon > 0$. Our construction is the first with constant-weight stabilizers that obtains $dk \gg n$, and as a consequence achieves arbitrarily small magic state overhead exponent $\gamma = \log(n/k)/\log(d) > 0$. Comparable prior constructions instead required at least polylogarithmic stabilizer weight. We also show how to obtain linearly many $k = \Omega(n)$ logical $C^{r-1}Z$ gates, though with stabilizer weight and physical circuit depth n^{ϵ}. We show that our transversal gates also support addressing (i.e. targeting) of specific logical qubits.

To obtain our codes, we develop a general transformation based on cup products that maps classical codes satisfying a multiplication property to quantum codes with transversal $C^{r-1}Z$. We apply this transformation to a new family of classical Tanner codes that we construct from punctured tensor products of algebraic codes.

ISSN 1433-8092

Contents

1 Introduction

A major barrier to realizing large-scale quantum computation lies in our ability to efficiently perform quantum gates in a fault-tolerant manner. Indeed, in the absence of fault-tolerance, a computation would quickly become corrupted by the noise inherent to quantum devices. A key bottleneck limiting the efficiency of many fault-tolerance schemes is the implementation of *non-Clifford gates*. Such gates are required for universal quantum computation, but require specialized codes or distillation schemes to perform fault-tolerantly, which incur a large space-time overhead. Given the limited qubit counts and/or gate speeds of near-term quantum devices, reducing this overhead of non-Clifford gates could allow significantly larger computations to be executed in practice. Efficient non-Clifford gates similarly remain an important theoretical question, with the potential for significant asymptotic improvements that could reduce the space-time overhead of large-scale fault-tolerant computation.

One of the most powerful tools for performing fault-tolerant non-Clifford gates is a quantum code supporting *transversal* non-Clifford gates, meaning that there exists a low-depth[1] physical circuit to implement logical non-Clifford gates on the underlying encoded message. Indeed, low circuit depth implies an efficient implementation, and also ensures fault-tolerance by limiting the number of errors that can accumulate during the circuit.

Of particular interest are quantum codes with transversal non-Clifford gates that have low-weight stabilizers, so that the error-correction circuit that measures the stabilizers and applies an appropriate correction can also be performed in a low-depth or fault-tolerant manner. Indeed, quantum LDPC (qLDPC) codes, defined to have constant-weight stabilizers, underlie many proposed fault-tolerance schemes for both theoretical and practical applications (e.g. [Got14, NP25, XAP+23, YSR+25, CXK+26]). Good qLDPC codes supporting transversal non-Clifford gates could significantly improve the efficiency of such schemes. Yet such codes have proven difficult to construct. A line of works [BMD07a, BMD07b, Bom15, ZSP+23, Lin24, GL25, BDET24, SPW24, Zhu25, LLLN25, LSW+26, LLL26] has provided various constructions, though substantial room for improvement remains.

Following such prior works, we focus on the non-Clifford $C^{r-1}Z$ gate for $r \geq 3$ (see Definition 2.9). Of particular interest is the CCZ gate due to its close relationship[2] to the Toffoli gate, which is a common building block in many logical circuits of interest. For a code supporting transversal $C^{r-1}Z$, we define the *logical yield* s to be the number of disjoint logical $C^{r-1}Z$ gates induced by the physical circuit. Specifically, we allow a chosen set of logical qudits to be set to $|0\rangle$, but then require the remaining logical qudits to undergo $C^{r-1}Z$ gates on s disjoint r-tuples of qudits, with no additional gates acting between the different tuples. Intuitively, the logical yield measures how many logical $C^{r-1}Z$ gates we can "extract" from the physical transversal gate. Note that the logical yield is also a lower bound on the code's dimension.

Previously, all known qLDPC codes (with constant stabilizer weight) that support constant-depth transversal CCZ gates had length n, distance d, and logical yield s satisfying

$$ds \leq O(n). \tag{1}$$

[1] Sometimes the term "transversal" is used more restrictively to refer to depth-1 physical circuits, which are also sometimes required to apply the same gate to every qudit. In this work we use the looser definition allowing low-depth physical circuits, where we will always specify the precise circuit depth (or as a proxy, the number of gates touching each qudit; see Fact 2.11).

[2] Toffoli is equivalent to CCZ up to conjugation by Hadamard gates on the target qudit.

This bound was saturated up to polylogarithmic factors for every $d \leq n/\operatorname{poly}\log(n)$ by [LLL26], and up to constant factors for every $d \leq \alpha \cdot \sqrt{n}$ in [Zhu25], where $\alpha > 0$ is a sufficiently small constant.[3] However, this tradeoff in Equation (1) prohibits fault-tolerant computation with a high rate of logical non-Clifford gates and good error resilience. At an intuitive level, Equation (1) matches the parameters of the classical repetition code ($d = n$, $s = 1$), which is generally suboptimal. Indeed, to ensure exponentially low logical error rates, one typically requires polynomially large qLDPC code distance $d \geq n^{\Omega(1)}$ (see e.g. [KP13, Got14]), which implies that the logical yield $s \leq n^{1-\Omega(1)}$ in Equation (1) is a polynomially small fraction of the block length.

Our main result is the first known construction of qLDPC codes (with constant stabilizer weight) supporting constant-depth transversal CCZ gates that surpass the bound in Equation (1):

Theorem 1.1 (Informal statement of Corollary 5.1)**.** *For every integer $r \geq 3$, every $0 < \epsilon < 1$, and every prime power q, there exist quantum codes of length n, distance*

$$d \geq n^{(1-\epsilon)/r},$$

and alphabet size q with constant stabilizer weight, which support depth-1 transversal $C^{r-1}Z$ gates of logical yield

$$s \geq n^{1-\epsilon}.$$

These codes also have a $\operatorname{poly}(n)$-time decoding algorithm that corrects $n^{(1-\epsilon)/r}$ adversarial errors.

Formally, Theorem 1.1 follows immediately by applying the alphabet reduction in [GL25, Lemma 3.44] and the transversal-gate circuit-depth reduction in [GL25, Lemma 3.45] to the codes in Corollary 5.1 (see Section 5).[4]

Theorem 1.1 is most similar to the construction of [GL25], which provided the only previously known construction of quantum codes supporting transversal non-Clifford gates that beat the bound Equation (1) with subpolynomial (but still superconstant) stabilizer weight. Specifically, [GL25] showed a similar result as in Theorem 1.1, though with larger stabilizer weight $\operatorname{poly}\log(n)$, slightly larger distance $d \geq n^{1/r}/\operatorname{poly}\log(n)$, and without an efficient decoding algorithm.

While our general approach is related to that of [GL25], our construction and analysis are more modular and generalizable. Specifically, we first prove a general mapping from classical codes with appropriate properties to quantum codes with transversal $C^{r-1}Z$ gates (Theorem 3.1). We then prove Theorem 1.1 by instantiating this general mapping with a family of classical codes based on high-dimensional tensor products that we construct (Theorem 4.1). As one example of the flexibility of our approach, we show how to modify the instantiation in Theorem 1.1 to instead recover the precise parameters from [GL25] (see Corollary 5.2).

A disadvantage of both of these instantiations is that the logical yield bound $n^{1-\epsilon}$ remains sublinear in the block length n. We present a third instantiation that addresses this issue, at the cost of having larger stabilizer weight and transversal circuit depth:

[3] In particular, [LLL26] provide qLDPC codes of length n and distance $n/\operatorname{poly}\log(n)$ supporting transversal CCZ gates with logical yield 1. Taking s copies of a length-n/s code from this family therefore provides codes of length n, distance $n/(\operatorname{poly}\log(n) \cdot s)$, and logical yield s.

[4] The statement of Corollary 5.1 is analogous to that of Theorem 1.1, though for alphabet sizes $q = p^u$ where p is an arbitrary prime and u is a sufficiently large constant. The alphabet and circuit-depth reduction statements in [GL25, Lemma 3.44, Lemma 3.45] do not explicitly consider decoders, though their techniques for showing distance preservation do also imply that efficient decodability is preserved.

Theorem 1.2 (Informal statement of Corollary 5.3)**.** *For every integer $r \geq 3$, every $0 < \epsilon < 1$, and every prime power q, there exist quantum codes of length $n \to \infty$, distance*

$$d \geq \Omega(n^{1/r}),$$

and alphabet size q with stabilizer weight $\leq n^{\epsilon}$, which support depth $\leq n^{\epsilon}$ transversal $C^{r-1}Z$ gates of logical yield

$$s \geq \Omega(n).$$

These codes also have a $\mathrm{poly}(n)$*-time decoding algorithm that corrects $\Omega(n^{1/r})$ adversarial errors.*

Similarly as for Theorem 1.1, Theorem 1.2 follows immediately by applying the alphabet reduction in [GL25, Lemma 3.44] to the codes in Corollary 5.3 (see Section 5).

While our definition of a transversal $C^{r-1}Z$ gate of logical yield s applies $C^{r-1}Z$ to a fixed set of s disjoint tuples of logical qudits, it may be desirable to only apply $C^{r-1}Z$ to a chosen ("addressed") subset of these s tuples. Such *addressable* $C^{r-1}Z$ gates, which have previously been studied on non-LDPC codes [HVWZ25b, HVWZ25a], may be particularly useful on LDPC codes. Indeed, existing techniques for addressable/targeted fault-tolerant logical gates on LDPC codes such as code surgery (e.g. [CKBB22, CHRY24, CHWY26]) or code switching (e.g. [GCZ25, XZB+25]) typically require larger space-time overheads, especially when performing many logical gates in parallel. In contrast, in Appendix A we extend Theorems 1.1 and 1.2 to allow for addressable $C^{r-1}Z$ gates, while preserving the same code parameter and circuit depth bounds.

Many leading proposals for fault-tolerance schemes in both theory and practice perform non-Clifford gates by preparing *magic states*, such as $CCZ\,|+\rangle^{\otimes 3}$, which are then consumed to implement a non-Clifford gate via gate teleportation (e.g. [NP25, Gid25, CXK+26]). Such magic states are often distilled from noisier magic states using a code supporting a transversal non-Clifford gate. Higher code distance and logical yield allow a given number of good magic states to be distilled from fewer noisy states.

In particular, for a code of length n and distance d supporting a transversal non-Clifford gate with logical yield s, [BH12] showed how to distill m magic states[5] with infidelity $< \epsilon$ from $m \cdot \log^{\gamma}(1/\epsilon)$ states with some constant infidelity, where the *magic state overhead exponent*

$$\gamma := \log(n/s)/\log(d). \tag{2}$$

measures the scheme's overall performance. While lower-overhead distillation schemes have been constructed in certain settings (e.g. [WHY24]), the value of γ in Equation (2) remains a good measure of the resource overhead of distillation, especially when restricting attention to the leading-order term $\lim_{n\to\infty} \gamma$.

Theorem 1.1 provides the first known codes with constant stabilizer weight that obtain arbitrarily small values of $\gamma > 0$, improving upon the polylogarithmic stabilizer weight of [GL25]. Indeed, the codes of [Zhu25, LLL26] satisfying Equation (1) must have $\lim_{n\to\infty} \gamma \geq 1$. Previously, [WHY24, GG25a, Ngu25] constructed codes with $\gamma \to 0$, albeit with linear-weight stabilizers. [GG25b] also obtained $\gamma \to 0$ for codes with check weight[6] $O(\sqrt{n})$ (or $O(n^{1/3})$ over exponentially

[5] While [BH12] presented their protocol for the T gate, it can be extended to alternative non-Clifford gates such as CCZ, as observed by [PR13].

[6] Strictly speaking, the codes of [GG25b] have stabilizer weight $\Theta(n)$, but they are subsystem codes with gauge operators of weight $O(\sqrt{n})$.

large alphabets). Magic state distillation is still possible with such high-weight stabilizers, by concatenating with a code supporting fault-tolerant Clifford gates. However, low-weight stabilizers allow for more efficient stabilizer measurement circuits, and hence more efficient encoding and decoding, which translates to lower space-time overhead for magic state distillation.

It in particular remains an open question to construct a magic state distillation procedure with constant space-time overhead. While there exist schemes with a constant ratio of noisy input to low-error output states [WHY24], they still require polynomial space-time overhead to run encoding/decoding circuits. One approach to obtaining constant space-time overhead would be to remove the n^ϵ loss factors in Theorem 1.1 or in Theorem 1.2, to obtain codes with stabilizer weight $O(1)$, polynomial distance $n^{\Omega(1)}$, and logical yield $\Omega(n)$. If concatenated with a sufficiently low-overhead outer code supporting fault-tolerant Clifford gates, such constant stabilizer weight combined with linear logical yield could translate to constant overall space-time overhead for preparing low-error magic states.

We also emphasize that qLDPC codes supporting transversal non-Clifford gates of high logical yield raise the possibility for alternative approaches to low-overhead fault-tolerance, without using magic state distillation. For instance, because qLDPC codes natively support fault-tolerant stabilizer measurement and error-correction (see e.g. [Got14]), fault-tolerant computation could be performed directly on qLDPC codes with transversal non-Clifford gates. Such an approach removes the need for magic state preparation, but would still require additional techniques such as code switching (e.g. [Bom16, GCZ25, THL+25, XZB+25]), resource state preparation (e.g. [Got14, NP25]), or code surgery (e.g. [Lit19, CKBB22, CHRY24]) to perform fault-tolerant Clifford gates.

As an important technical remark, to obtain the quantum-code distance bounds in Theorems 1.1 and 1.2, we restrict attention to a subsystem of the entire code space, meaning our codes are strictly speaking *subsystem codes*. However, we emphasize that our codes still have truly low-weight stabilizers, rather than having low-weight gauge operators (which may be more difficult to measure fault-tolerantly; see e.g. [BFHS17]). Rather, our use of subsystem codes simply indicates the possibility of certain "bad" logical operators specifying "gauge" qudits that may not be protected by the code's distance, and hence are not used when encoding the message, or when determining the $C^{r-1}Z$ gate's logical yield s. These gauge qudits, along with all logical qudits outside of our s chosen disjoint tuples, must be set (i.e. "gauge-fixed") to $|0\rangle$ prior to performing the transversal $C^{r-1}Z$ gate.

After performing such gauge-fixing, our codes allow for fault-tolerant application of $C^{r-1}Z$ gates. Specifically, let $|\psi\rangle$ denote the gauge-fixed code state, and let C denote the physical transversal $C^{r-1}Z$ circuit. Assuming low-weight errors E and E' arise from gauge-fixing and from executing C respectively, the final state after applying transversal $C^{r-1}Z$ is

$$E'CE\,|\psi\rangle = E'(CEC^\dagger)C\,|\psi\rangle\,.$$

Assuming C is a constant-depth physical circuit, then the propagated error $CEC^\dagger$ has weight only a constant factor larger than that of E. Hence our output state consists of the noiseless post-transversal-gate state $C\,|\psi\rangle$, up to a low-weight residual error $E'' := E'(CEC^\dagger)$. Note that while E, E', E'' may not be Pauli errors (and E'' may not be Pauli even if E, E' are Pauli), we can decompose arbitrary such low-weight errors into linear combinations of low-weight Pauli errors. Our CSS code distance and decoding guarantees (see Section 2) can then be applied to each such Pauli term.

The design of fault-tolerant protocols for gauge-fixing, as well as for performing more general general Clifford gates, is beyond the scope of this paper. Indeed, it remains an active area of

research to construct such Clifford gate protocols, which when combined with non-Clifford gates yield universal quantum computation. We remark that our codes and gauge operators have a tensor product structure (see Section 3), so they may be particularly well-suited for performing Clifford gates via code switching (see e.g. [GCZ25, THL+25, XZB+25]). Also note that in the context of magic state distillation, the code with transversal non-Clifford gates is typically concatenated with a code supporting fault-tolerant Clifford gates. Hence in this setting the gauge-fixing procedure need not be fault-tolerant, which gives further flexibility.

1.1 Our Techniques

We now overview our techniques for proving Theorem 1.1 and Theorem 1.2. We construct our quantum codes as tensor products of cochain complexes associated to classical Tanner codes. We first prove a general result showing that classical Tanner codes that behave appropriately under component-wise multiplication yield quantum codes supporting transversal $C^{r-1}Z$. We then instantiate this result using a classical tensor product of algebraic codes, which we carefully puncture to express within the Tanner code framework. Our efficient decoding algorithms follow from known decoders for classical (folklore) as well as quantum [QC22] tensor product codes. Below, we provide more details on each of these steps. For simplicity, in this overview we restrict attention to constant-degree Tanner graphs as in Theorem 1.1, though the techniques generalize naturally to graphs with growing degree as in Theorem 1.2.

1.1.1 General Classical-to-Quantum Mapping

Our general mapping from classical Tanner codes to quantum codes supporting transversal $C^{r-1}Z$ is stated in Theorem 1.3 below. Here we specify a classical Tanner code over a field $\mathbb{F}$ by a graph Γ along with a *system of local codes* $\mathcal{F}$ on Γ, which assigns to every vertex v a local full-rank generator matrix $\mathcal{F}_{v\to E(v)} : \mathbb{F}^{m_v} \to \mathbb{F}^{E(v)}$. The Tanner code $\mathrm{T}(\Gamma, \mathcal{F}) \subseteq \mathbb{F}^{E(\Gamma)}$ then contains all length-$|E(\Gamma)|$ vectors whose restriction to the neighborhood $E(v)$ of each vertex v lies in the associated local code $\mathrm{im}(\mathcal{F}_{v\to E(v)})$.

Theorem 1.3 (Informal statement of Theorem 3.1)**.** *For a fixed integer $r \geq 3$, let $\mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(r)}$ be systems of local codes on a constant-degree graph Γ satisfying the* multiplication property

$$\mathrm{im}(\mathcal{F}^{(1)}_{v\to E(v)}) * \cdots * \mathrm{im}(\mathcal{F}^{(r-1)}_{v\to E(v)}) \subseteq \mathrm{im}(\mathcal{F}^{(r)}_{v\to E(v)}) \quad \text{for each } v \in V(\Gamma). \tag{3}$$

Assume that there exists a set $M \subseteq E(\Gamma)$ such that each classical Tanner code $\mathrm{T}(\Gamma, \mathcal{F}^{(i)})$ has distance $\geq d$, and has an information set[7] containing M. Then there exists an associated family of quantum codes of length $\Theta(|V(\Gamma)|^r)$ and distance $\Omega(d)$ supporting constant-depth transversal $C^{r-1}Z$ gates with logical yield $|M|^r$.

Our quantum codes in Theorem 1.3 are CSS codes given by the tensor products (sometimes

[7]Recall that an information set of a code $C \subseteq \mathbb{F}^n$ is a maximal set of coordinates $S \subseteq [n]$ for which $C|_S = \mathbb{F}^S$, so that in particular $|S| = \dim(C)$.

also called hypergraph products [TZ14])

$$\begin{aligned}
\mathcal{A}^{(1)} &= \mathcal{C}^*(\Gamma, \mathcal{F}^{(r)^\perp}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(1)}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(2)}) \otimes \cdots \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r-1)}) \\
\mathcal{A}^{(2)} &= \mathcal{C}^*(\Gamma, \mathcal{F}^{(r-1)}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r)^\perp}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(1)}) \otimes \cdots \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r-2)}) \\
&\vdots \\
\mathcal{A}^{(r)} &= \mathcal{C}^*(\Gamma, \mathcal{F}^{(1)}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(2)}) \otimes \cdots \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r-1)}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r)^\perp}),
\end{aligned}$$

of 1-dimensional cochain complexes $\mathcal{C}(\Gamma, \mathcal{F}^{(1)}), \ldots, \mathcal{C}(\Gamma, \mathcal{F}^{(r-1)}), \mathcal{C}(\Gamma, \mathcal{F}^{(r)^\perp})$ associated to the respective Tanner codes $\mathrm{T}(\Gamma, \mathcal{F}^{(1)}), \ldots, \mathrm{T}(\Gamma, \mathcal{F}^{(r-1)}), \mathrm{T}(\Gamma, \mathcal{F}^{(r)^\perp})$. Specifically, these 1-dimensional complexes are defined to have coboundary maps equal to the parity-check matrices of the associated Tanner codes. Here $\mathcal{F}^{(r)^\perp}$ denotes the system given by dualizing all local codes in $\mathcal{F}^{(r)}$.

To obtain the transversal $C^{r-1}Z$ gate in Theorem 1.3, we define a *cup product*

$$\smile : \mathcal{A}^{(1)} \times \cdots \times \mathcal{A}^{(r)} \to \mathcal{A}',$$

which is a multilinear map sending cochains $a^{(1)} \in \mathcal{A}^{(1)}, \ldots, a^{(r)} \in \mathcal{A}^{(r)}$ to some cochain $a^{(1)} \smile \cdots \smile a^{(r)}$ in an appropriate cochain complex $\mathcal{A}'$. Intuitively, the cup product provides a quantum/high-dimensional analogue of component-wise multiplication of classical codewords. More formally, we ensure the cup product induces a well-defined map on cohomology. We then fix a cycle $z_* \in Z_*(\mathcal{A}')$, and define our physical transversal gate to perform $C^{r-1}Z$ on every r-tuple of qudits whose cup product has nontrivial inner product with z_*. Here the multiplication property in Equation (3) ensures that there exists an appropriate such cycle z_*, which is given by the all-1s vector on an appropriate sector of the complex $\mathcal{A}'$.

This general strategy of constructing transversal $C^{r-1}Z$ gates from cup products was developed in prior works, e.g. [ZSP+23, Lin24, BDET24, Zhu25, LLLN25]. Our key to obtaining a simple and general statement in Theorem 1.3 is to first construct a cup product on the 1-dimensional complexes $\mathcal{C}(\Gamma, \mathcal{F}^{(1)}), \ldots, \mathcal{C}(\Gamma, \mathcal{F}^{(r-1)}), \mathcal{C}(\Gamma, \mathcal{F}^{(r)^\perp})$ using the multiplication property in Equation (3), following techniques in [Lin24, LLLN25]. We then extend this cup product to our higher-dimensional tensor product complexes $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(r)}$ via the formula

$$(a \otimes b) \smile (a' \otimes b') = (-1)^{i_b i_{a'}} (a \smile a') \otimes (b \smile b'), \tag{4}$$

where i_b (resp. $i_{a'}$) denotes the level of the cochain b (resp. a'). While Equation (4) was also used in [BDET24], the works [Lin24, LLLN25] proposed instead directly constructing cup products on high-dimensional complexes, which can complicate the analysis of the logical yield. Indeed, our bound on logical yield in Theorem 1.3 follows directly from the multiplication property on each factor in the tensor products defining $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(r)}$.

As a technical remark, to ensure that our quantum codes in Theorem 1.3 satisfy the distance bound of $\Omega(d)$, we construct them as subsystem codes, though still with truly low-weight stabilizers; see the discussion earlier in Section 1 above.

1.1.2 Instantiating the General Mapping

To instantiate the general mapping in Theorem 1.3, we construct new punctured versions of classical tensor products of algebraic codes. Here our goal is to construct classical LDPC Tanner codes

satisfying the multiplication property in Equation (3) that exhibit high dimension and distance. The construction of such classical codes has proven to be a difficult problem. A core difficulty is that traditional classical Tanner code constructions require local codes of rate $> 1/2$ to ensure positive global rate via constraint-counting (e.g. [SS96]). However, high-distance classical local codes with a multiplication property have rate $\leq 1/2$. Hence to obtain Tanner codes exhibiting both a multiplication property and large global rate, we need to carefully choose the local codes alongside the graph, and bound the rate using additional structure beyond simply constraint-counting.

Such an approach was taken to construct Tanner codes with the multiplication property in [DLZ23] and [GL25, Section 4]. However, these prior constructions required super-constant check weight in order to obtain large (i.e. close-to-linear) code dimension. We therefore provide a new construction of Tanner codes with constant check weight exhibiting a multiplication property.

To construct our LDPC Tanner codes, we begin with well-known *non-LDPC* families of good classical codes exhibiting a multiplication property, such as algebraic-geometry codes (see e.g. [CR21]). If we take a large constant-sized such code C of length n, dimension $k \geq n^{1-\epsilon}$, and distance $d \geq n^{1-\epsilon}$, the classical tensor powers $C^{\otimes t}$ for $t \to \infty$ provide a family of codes with a multiplication property that have length $N = n^t$, dimension $K = k^t \geq N^{1-\epsilon}$, distance $D = d^t \geq N^{1-\epsilon}$, and check weight $n = O(1)$. However, $C^{\otimes t}$ is not natively expressible as a Tanner code, i.e. there is no natural associated graph Γ and system of local codes $\mathcal{F}$.

To resolve this issue, we show how to puncture $C^{\otimes t}$ to obtain such a Tanner code, while retaining the same code properties and parameters up to a small loss. The main idea is to define a t-partite graph $\bar{\Gamma}$ whose vertices are axis-parallel columns (i.e. lines) in the hypercube $[n]^t$, and whose edges connect pairs of distinct columns that intersect. Each edge then has an associated point in $[n]^t$ given by the intersection of the two associated columns. However, a single point may have multiple associated edges. We therefore carefully choose a subgraph $\Gamma \subseteq \bar{\Gamma}$ for which each point in $[n]^t$ has at most one associated edge. We then define an associated system of local codes $\mathcal{F}$ given by puncturings of the base code C, so that the resulting Tanner code $\mathrm{T}(\Gamma, \mathcal{F})$ is a puncturing of $C^{\otimes t}$. See Theorem 4.1 in Section 4 for details (note that there the hypercube $[2n]^t$ replaces $[n]^t$ in this informal overview).

1.1.3 Efficient Decoding Algorithm

Our efficient decoding algorithms against adversarial errors in Theorems 1.1 and 1.2 follow from known decoders for tensor product codes. In particular, [QC22] show how to decode quantum codes obtained as tensor products of cochain complexes associated to classical codes, given access to decoders for the classical codes. As described in Section 1.1.2 above, we construct these classical codes by puncturing tensor products of classical algebraic-geometry codes. Such classical algebraic-geometry codes, and their (classical) tensor products, have well-known efficient decoding algorithms. Our choice of puncturing ensures our final classical codes can be viewed as the disjoint union of a small number of (unpunctured) classical tensor product codes (see Section 4), each of which we can decode with these known decoders. Hence we obtain efficient decoders for our quantum codes.

1.2 Directions for Future Work

Two natural areas for improvement in Theorem 1.1 are:

1. Improve the distance bound $d \geq n^{(1-\epsilon)/r}$ to (even close to) linear in n, and

2. Improve the logical yield bound $s \geq n^{1-\epsilon}$ to linear in n.

Theorem 1.2 provides one way to address the second point above, though at the cost of having super-constant stabilizer weight and physical transversal $C^{r-1}Z$ circuit depth. As described above, a family of polynomial-distance codes with linear logical yield and constant stabilizer weight could lead to asymptotically optimal (i.e. constant space-time overhead) magic state preparation under locally stochastic noise. Constructing such codes using Theorem 1.3 would require polynomial-distance constant-rate classical LDPC codes with a multiplication property, whose construction remains an intriguing open question.

In contrast, we could hope to improve the distance bounds in Theorem 1.1 and Theorem 1.2 by replacing the tensor product of cochain complexes used to prove Theorem 1.3 with a *balanced product* (also called a *lifted product*) [PK22b, BE21, PK22a]. Such balanced products can be viewed as tensor products quotiented by a group action, which have been shown to increase the resulting quantum code distance to nearly-linear in the block length, even in high-dimensional products [DLV24, KP25]. However, existing techniques to prove such near-linear distance only apply to Tanner codes on expander graphs whose local codes exhibit strong expansion properties. It remains an open question to adapt such proof techniques to our Tanner codes, or to modify our Tanner codes so that such techniques apply, while still preserving high-yield transversal $C^{r-1}Z$ gates. Some progress in this direction was made by the recent work [LLL26], which obtained algebraic local codes with sufficient expansion to show near-linear distance by the results of [DLV24]. However, the logical yield of the resulting transversal $C^{r-1}Z$ gate was constant.

While Theorems 1.1 and 1.2 give efficient decoding algorithms against adversarial errors, it also remains an interesting question to consider other noise models, such as locally stochastic noise, particularly in the context of constant space-time overhead magic state preparation.

1.3 Roadmap

The remainder of this paper is organized as follows. Section 2 presents preliminary definitions and results that we use throughout. Section 3 presents our formal statement and proof of Theorem 1.3, which provides our mapping from classical codes with a multiplication property to quantum codes with transversal $C^{r-1}Z$. Section 4 then provides the general family of classical Tanner codes from punctured tensor codes that we use to invoke Theorem 1.3, and Section 5 provides our specific instantiations.

2 Preliminaries

In this section, we present preliminary notions regarding classical and quantum codes.

2.1 Classical Codes

We begin with basic classical code definitions.

Definition 2.1. *A length-n* classical (linear) code *over a field $\mathbb{F}_q$ is a subspace $C \subseteq \mathbb{F}_q^n$. The code C has* dimension $k = \dim_{\mathbb{F}_q}(C)$ *and* distance $d = \min_{c \in C \setminus \{0\}} |c|$. *We summarize these parameters by saying C is a $[n, k, d]_q$ code.*

Definition 2.2. *For a classical code $C \subseteq \mathbb{F}_q^n$, the* dual code $C^\perp \subseteq \mathbb{F}_q^n$ *is given by*

$$C^\perp = \{x \in \mathbb{F}_q^n : \langle x, y\rangle = 0 \ \forall y \in C\}.$$

Our code constructions will be based on tensor products:

Definition 2.3. *For $i = 1, 2$, let C_i be an $[n_i, k_i, d_i]_q$ classical code. The* tensor product code $C_1 \otimes C_2$ *is the $[n_1 n_2, k_1 k_2, d_1 d_2]_q$ code consisting of all $n_1 \times n_2$ matrices for which every column lies in C_1 and every row lies in C_2.*

The following definition presents subsets of a code's coordinates to which we can view the restriction of a codeword as its encoded message.

Definition 2.4. *For a k-dimensional classical code $C \subseteq \mathbb{F}_q^n$, an* information set *is a subset $S \subseteq [n]$ of size $|S| = k$ such that $C|_S = \mathbb{F}_q^S \cong \mathbb{F}_q^k$. An* extendable set *$M \subseteq [n]$ is a set that can be extended into an information set, that is, M is extendable for C if there exists an information set $S \supseteq M$ for C.*

Below, we define the notion of a decoder for a classical code.

Definition 2.5. *A* radius-ρ time-T decoder *for a classical code $C \subseteq \mathbb{F}^n$ is a (classical) algorithm with running time $\leq T$ that takes as input a string $a = c + e \in \mathbb{F}^n$ for some codeword $c \in C$ and error $e \in \mathbb{F}^n$, and outputs c as long as $|e| < \rho$. If $|e| \geq \rho$, the output can be arbitrary.*

It is well-known that a tensor code $C \otimes C'$ can be decoded by first running a decoder for C in all columns of the corrupted codeword $x \in \mathbb{F}^{n \times n'}$, and then running a decoder for C' in all rows. The resulting product-code decoder has the following parameters:

Lemma 2.6 (Well-known; see e.g. Fact 2.15 in [KRRZ+21])**.** *For $i = 1, 2$, let $C_i \subseteq \mathbb{F}^{n_i}$ be a classical code with a radius-ρ_i time-T_i decoder. Then the tensor product code $C_1 \otimes C_2$ has a radius-$\rho_1\rho_2$ time-$(n_1 T_2 + n_2 T_1)$ decoder.*

2.2 Quantum Codes and Transversal Gates

We now present the notion of (subsystem) quantum CSS codes.

Definition 2.7. *A length-n* quantum (CSS) code *over $\mathbb{F}_q$ is a pair $Q = (Q_X, Q_Z)$ of classical codes $Q_X, Q_Z \subseteq \mathbb{F}_q^n$ satisfying $Q_X^\perp \subseteq Q_Z$.*

A k-dimensional subsystem *$L = (L_X, L_Z)$ of the quantum CSS code $Q = (Q_X, Q_Z)$ is a pair of k-dimensional subspaces $L_X \subseteq Q_X/Q_Z^\perp$, $L_Z \subseteq Q_Z/Q_X^\perp$ for which the restriction of the natural bilinear form $\langle \cdot, \cdot \rangle : Q_X/Q_Z^\perp \times Q_Z/Q_X^\perp \to \mathbb{F}_q$ to $L_X \times L_Z$ is nondegenerate. We call the data (Q, L) a* quantum CSS subsystem code. *The* distance *of the subsystem code is $d = \min\{d_X, d_Z\}$ for*

$$d_X = \min_{x \in Q_X \setminus L_Z^\perp} |x|$$
$$d_Z = \min_{z \in Q_Z \setminus L_X^\perp} |z|.$$

Here and below, by abuse of notation, we also write L_X and L_Z for their full preimages in Q_X and Q_Z, respectively. Thus $Q_Z^\perp \subseteq L_X \subseteq Q_X$ and $Q_X^\perp \subseteq L_Z \subseteq Q_Z$.

We summarize the parameters above by saying (Q, L) is a $[[n, k, d]]_q$ subsystem code.

We emphasize that we will only consider subsystem codes with low-weight (commuting) stabilizers. The subsystem property means that we specify a subsystem L of the logical qudit space in which we encode our message; the remainder of the logical qudit space may be corrupted by low-weight errors. By excluding these easily-corruptible logical qudits, our subsystem codes may have larger distance than the associated non-subsystem code.

Our usage of subsystem codes with low-weight stabilizers is in contrast to other works that use subsystem codes with high-weight stabilizers that are decomposed into low-weight non-commuting gauge operators. While such constructions are sometimes able to obtain improved rate and distance with low-weight checks (e.g. [BFHS17]), the checks are given by non-commuting gauge operators that may be difficult to measure fault-tolerantly.

Below, we define the notion of a decoder for a quantum code.

Definition 2.8. *A* radius-ρ time-T decoder *for a quantum CSS subsystem code (Q, L) is a (classical) algorithm with running time $\leq T$ that takes as input a pair of strings $a_X = c_X + e_X$, $a_Z = c_Z + e_Z \in \mathbb{F}^n$ for some codewords $c_X \in Q_X$, $c_Z \in Q_Z$ and errors $e_X, e_Z \in \mathbb{F}^n$, and outputs the pair of cosets $(c_X + L_Z^\perp,\ c_Z + L_X^\perp)$ as long as $|e_X|, |e_Z| < \rho$. If either $|e_X| \geq \rho$ or $|e_Z| \geq \rho$, the output can be arbitrary.*

We will not try to optimize the precise running time of our decoders, and will rather simply ensure the running time is polynomial in the block length. Our notion of a polynomial-time decoder in Definition 2.8 is equivalent to that of a polynomial-time decoder that needs to correct a weight-ρ error on a code state given as input a noise-free syndrome of the corrupted codeword. Indeed, given the syndrome, we can perform Gaussian elimination to compute some valid a_X and a_Z inducing that syndrome, and then compute the appropriate Pauli X and Z corrections as $a_X - c_X$ and $a_Z - c_Z$, respectively.

We now define transversal $C^{r-1}Z$ gates on quantum CSS (subsystem) codes. We begin by defining the $C^{r-1}Z$ gate.

Definition 2.9. *For a finite field $\mathbb{F}_q$ of characteristic p and for $a \in \mathbb{F}_q$, the unitary gate $C^{r-1}Z^a$ acts on r qudits of dimension q by*

$$C^{r-1}Z^a \left|x_1, \ldots, x_r\right\rangle = e^{2\pi i \operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a \cdot x_1 \cdots x_r)/p} \left|x_1, \ldots, x_r\right\rangle .$$

A physical circuit of $C^{r-1}Z$ gates acting across r quantum code states can be represented by a multilinear form, as defined below.

Definition 2.10. *Let $Q^{(1)}, \ldots, Q^{(r)}$ be quantum CSS codes over $\mathbb{F}_q$ of respective lengths $n^{(1)}, \ldots, n^{(r)}$, and let*

$$f : \mathbb{F}_q^{n^{(1)}} \times \cdots \times \mathbb{F}_q^{n^{(r)}} \to \mathbb{F}_q$$

be a multilinear form. We define an associated physical circuit $C^{r-1}Z^f$ acting on qudits labeled by $[n^{(1)}] \sqcup \cdots \sqcup [n^{(r)}]$, which applies the gate $C^{r-1}Z^{f(\mathbb{1}_{c^{(1)}}, \ldots, \mathbb{1}_{c^{(r)}})}$ to every r-tuple $(c^{(1)}, \ldots, c^{(r)}) \in [n^{(1)}] \times \cdots \times [n^{(r)}]$ of physical qudits.

We define the sparsity *of f to be the maximum number of non-identity[8] $C^{r-1}Z$ gates in which any single qudit participates.*

Fact 2.11 below shows that sparsity provides a good proxy for circuit depth.

[8] That is, gates $C^{r-1}Z^a$ for $a \neq 0$.

Fact 2.11. *If f has sparsity w, then $C^{r-1}Z^f$ can be implemented in circuit depth rw.*

Proof. Define a bipartite graph Γ whose left vertices are physical qudits, and whose right vertices are the physical $C^{r-1}Z$ gates performed in $C^{r-1}Z^f$, with edges connecting each qudit to the gates it participates in. By definition, Γ has maximum left-degree $\leq w$ and right-degree r. Let Γ_R^2 denote the right component of the square of Γ excluding self-loops, so that Γ_R^2 has vertices given by physical $C^{r-1}Z$ gates performed in $C^{r-1}Z^f$, and edges connecting every pair of distinct gates with a shared qudit. Then Γ_R^2 has maximum degree $\leq r(w-1)$, so its vertices can be properly colored by the set $[r(w-1)+1]$, i.e., no two vertices connected by an edge share the same color. It follows that we can perform each $C^{r-1}Z$ gate in $C^{r-1}Z^f$ in the time step given by its assigned color, and no two gates sharing a qudit will be executed in the same time step. This implementation has circuit depth $r(w-1)+1 \leq rw$, as desired. □

We next characterize when the physical circuit $C^{r-1}Z^f$ induces logical $C^{r-1}Z$ gates on r-tuples of logical qudits.

Definition 2.12. *We say the multilinear form f in Definition 2.10 is* cohomology-invariant *if it holds for every $(z^{(i)} \in Q_Z^{(i)})_{i\in[r]}$ and every $(b^{(i)} \in {Q_X^{(i)}}^{\perp})_{i\in[r]}$ that*

$$f(z^{(1)}+b^{(1)},\ldots,z^{(r)}+b^{(r)}) = f(z^{(1)},\ldots,z^{(r)}).$$

Such cohomology-invariance implies a well-defined induced multilinear form

$$\tilde{f} : Q_Z^{(1)}/{Q_X^{(1)}}^{\perp} \times \cdots \times Q_Z^{(r)}/{Q_X^{(r)}}^{\perp} \to \mathbb{F}_q.$$

The term *cohomology-invariant* arises from the view of quantum CSS codes as cochain complexes (see below). Cohomology-invariance ensures that the physical circuit $C^{r-1}Z^f$ maps an r-tuple of valid code states to valid states of the same codes. This physical circuit will always induce some logical circuit $C^{r-1}Z^{\tilde{f}}$ consisting of logical $C^{r-1}Z$ gates. We want this logical circuit to perform $C^{r-1}Z$ gates on as many disjoint r-tuples of logical qudits as possible, without any logical gates acting across different r-tuples. Indeed, such a circuit structure allows for performing many logical $C^{r-1}Z$ gates in parallel, without additional unwanted entangling operations. If we allow ourselves to choose any basis of logical operators for our codes, and we set all logical qudits outside of our chosen r-tuples to $|0\rangle$, then the maximum number of disjoint logical $C^{r-1}Z$ gates induced by $C^{r-1}Z^f$ is precisely the *subrank* of $\tilde{f}$:

Definition 2.13. *The* subrank *of a multilinear form $g : V^{(1)} \times \cdots \times V^{(r)} \to \mathbb{F}$ is the maximum integer s such that for every $j \in [r]$ there exist $v_1^{(j)},\ldots,v_s^{(j)} \in V^{(j)}$ satisfying*

$$g(v_{\ell_1}^{(1)},\ldots,v_{\ell_r}^{(r)}) = \mathbb{1}_{\ell_1=\cdots=\ell_r} \quad \forall \ell_1,\ldots,\ell_r \in [s].$$

Some of the codes $Q^{(i)}$ with cohomology-invariant multilinear forms that we will construct may have poor distance, but nevertheless have natural subsystems $L^{(i)}$ with better distance (Definition 2.7). Our goal is then to define such subsystem codes of large distance along with a multilinear form f such that the restriction of $\tilde{f}$ to the span of the specified $L_Z^{(i)}$ has large subrank:

Definition 2.14. *We say subsystem codes $(Q^{(i)}, L^{(i)})$ for $i \in [r]$ support a* transversal $C^{r-1}Z$ gate of sparsity w and logical yield s *if there exists a cohomology-invariant form f (see Definitions 2.10 and 2.12) of sparsity w for which $\tilde{f}|_{L_Z^{(1)}\times\cdots\times L_Z^{(r)}}$ has subrank s.*

More details on the motivation and implications of the definitions above can be found in [Lin24, Section 3], albeit with slightly different notation.

2.3 Quantum Codes from Cochain Complexes

In this section, we present basic definitions regarding (co)chain complexes, which provide useful language and machinery for quantum CSS codes.

Definition 2.15. *An* r-dimensional chain complex $\mathcal{C}_*$ *over a field* $\mathbb{F}$ *is a graded* $\mathbb{F}$*-vector space* $\mathcal{C} = \bigoplus_{i=0}^{r} \mathcal{C}_i$ *along with a* boundary map $\partial^{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ *satisfying* $\partial^{\mathcal{C}}(\mathcal{C}_i) \subseteq \mathcal{C}_{i-1}$ *and* $(\partial^{\mathcal{C}})^2 = 0$*. We write* $\partial_i^{\mathcal{C}} = \partial^{\mathcal{C}}|_{\mathcal{C}_i}$*. We restrict attention to* based *chain complexes, meaning that each* $\mathcal{C}_i = \mathbb{F}^{C_i}$ *for some specified basis* C_i*, and then* $\mathcal{C} = \mathbb{F}^C$ *with* $C = \bigsqcup_{i=0}^{r} C_i$*. The* locality w *of* $\mathcal{C}$ *is the maximum Hamming weight of any row or column of* $\partial^{\mathcal{C}} \in \mathbb{F}^{C \times C}$*.*

The cochain complex $\mathcal{C}^*$ associated to $\mathcal{C}_*$ *consists of the same graded vector space* $\mathcal{C} = \bigoplus_{i=0}^{r} \mathcal{C}^i$ *with each* $\mathcal{C}^i = \mathbb{F}^{C^i} = \mathbb{F}^{C_i} = \mathcal{C}_i$*, along with the* coboundary map $\delta^{\mathcal{C}} = (\partial^{\mathcal{C}})^\top$*. We write* $\delta_i^{\mathcal{C}} = \delta^{\mathcal{C}}|_{\mathcal{C}^i}$*.*

Writing $\partial = \partial^{\mathcal{C}}$*,* $\delta = \delta^{\mathcal{C}}$ *for the chain complex* $\mathcal{C}_*$*, we define the following spaces:*

$$\begin{aligned} &i\text{-chains } \mathcal{C}_i, && i\text{-cochains } \mathcal{C}^i \\ &i\text{-cycles } Z_i(\mathcal{C}) = \ker(\partial_i), && i\text{-cocycles } Z^i(\mathcal{C}) = \ker(\delta_i) \\ &i\text{-boundaries } B_i(\mathcal{C}) = \mathrm{im}(\partial_{i+1}), && i\text{-coboundaries } B^i(\mathcal{C}) = \mathrm{im}(\delta_{i-1}) \\ &i\text{-homology } H_i(\mathcal{C}) = Z_i(\mathcal{C})/B_i(\mathcal{C}), && i\text{-cohomology } H^i(\mathcal{C}) = Z^i(\mathcal{C})/B^i(\mathcal{C}). \end{aligned}$$

We also define the

$$i\text{-systolic distance } d_i(\mathcal{C}) = \min_{c \in Z_i(\mathcal{C}) \setminus B_i(\mathcal{C})} |c|, \qquad i\text{-cosystolic distance } d^i(\mathcal{C}) = \min_{c \in Z^i(\mathcal{C}) \setminus B^i(\mathcal{C})} |c|.$$

The quantum code $Q = (Q_X, Q_Z)$ associated to level i of $\mathcal{C}^*$ *is defined by* $Q_X = Z_i(\mathcal{C})$ *and* $Q_Z = Z^i(\mathcal{C})$*.*

Our codes will be constructed from tensor products of 1-dimensional cochain complexes, as defined below.

Definition 2.16. *For cochain complexes* $\mathcal{A}^*, \mathcal{B}^*$*, the* tensor product *is the cochain complex* $\mathcal{A}^* \otimes \mathcal{B}^*$ *given by*

$$(\mathcal{A} \otimes \mathcal{B})^i = \bigoplus_{j \in \mathbb{Z}} \mathcal{A}^j \otimes \mathcal{B}^{i-j},$$

with coboundary map acting on the product of $a \in \mathcal{A}^j$*,* $b \in \mathcal{B}^{i-j}$ *by*

$$\delta(a \otimes b) = \delta(a) \otimes b + (-1)^j a \otimes \delta(b).$$

The following well-known formula shows how (co)homology behaves under tensor products.

Lemma 2.17 (Künneth formula)**.** *For cochain complexes* $\mathcal{C}^* = \mathcal{A}^* \otimes \mathcal{B}^*$*, there exists an isomorphism*

$$H^i(\mathcal{C}) \cong \bigoplus_{j \in \mathbb{Z}} H^j(\mathcal{A}) \otimes H^{i-j}(\mathcal{B})$$

given by

$$a \otimes b + B^i(\mathcal{C}) \mapsto (a + B^j(\mathcal{A})) \otimes (b + B^{i-j}(\mathcal{B})).$$

for $a \in Z^j(\mathcal{A})$*,* $b \in Z^{i-j}(\mathcal{B})$*.*

The following lemma shows that a quantum code has an efficient decoder (Definition 2.8) if it is given by a tensor product of chain complexes specifying efficiently-decodable classical codes (Definition 2.5). The case where the factor complexes are 1-dimensional was shown by [QC22].

Lemma 2.18 (Generalization of [QC22])**.** *Let $\mathcal{A}^*$ and $\mathcal{B}^*$ be $r_{\mathcal{A}}$- and $r_{\mathcal{B}}$-dimensional cochain complexes respectively, and let $\mathcal{C}^* = \mathcal{A}^* \otimes \mathcal{B}^*$. Assume that the classical codes[9] $H^0(\mathcal{A})$ and $H_{r_{\mathcal{B}}}(\mathcal{B})$ both have radius-ρ time-T decoders. Let Q be the CSS code at level $r_{\mathcal{B}}$ of $\mathcal{C}$, and define the subsystem $L = (L_X, L_Z)$, where*

$$L_X = H_0(\mathcal{A}) \otimes H_{r_{\mathcal{B}}}(\mathcal{B}) \qquad \text{and} \qquad L_Z = H^0(\mathcal{A}) \otimes H^{r_{\mathcal{B}}}(\mathcal{B}).$$

Note that by the Künneth formula (Lemma 2.17) we may view L_X and L_Z as subspaces of $H_{r_{\mathcal{B}}}(\mathcal{C})$ and $H^{r_{\mathcal{B}}}(\mathcal{C})$ respectively. Then the quantum CSS subsystem code (Q, L) has a radius-ρ time-$\mathrm{poly}(T, |C|)$ decoder.[10]

Proof. We will present the Z-decoding algorithm for (Q, L), which takes as input the noisy codeword $x = c + e$ for $c \in Z^{r_{\mathcal{B}}}(\mathcal{C})$ and $e \in \mathcal{C}^{r_{\mathcal{B}}}$ of weight $|e| < \rho$, and outputs the coset $c + L_X^\perp$. The X-decoding algorithm is analogous (i.e. is obtained by running the Z-decoding algorithm on the dual chain complex $\mathcal{C}_* = \mathcal{A}_* \times \mathcal{B}_*$).

Letting $k_{\mathcal{A}} = \dim(H^0(\mathcal{A}))$ and $k_{\mathcal{B}} = \dim(H^{r_{\mathcal{B}}}(\mathcal{B}))$, we fix representative elements of dual homology-cohomology bases

$$\begin{aligned} a_1, \dots, a_{k_{\mathcal{A}}} \in Z_0(\mathcal{A}), \quad a^1, \dots, a^{k_{\mathcal{A}}} \in Z^0(\mathcal{A}), \\ b_1, \dots, b_{k_{\mathcal{B}}} \in Z_{r_{\mathcal{B}}}(\mathcal{B}), \quad b^1, \dots, b^{k_{\mathcal{B}}} \in Z^{r_{\mathcal{B}}}(\mathcal{B}), \end{aligned}$$

so that $\langle a_j, a^{j'} \rangle = \mathbb{1}_{j=j'}$ and $\langle b_j, b^{j'} \rangle = \mathbb{1}_{j=j'}$ (see e.g. [GG25c, Lemma 3.9]). Then

$$(a_i \otimes b_j \in Z_{r_{\mathcal{B}}}(\mathcal{C}))_{i \in [k_{\mathcal{A}}], j \in [k_{\mathcal{B}}]}, \quad (a^i \otimes b^j \in Z^{r_{\mathcal{B}}}(\mathcal{C}))_{i \in [k_{\mathcal{A}}], j \in [k_{\mathcal{B}}]}$$

form dual bases for $L_X/Q_Z^\perp$, $L_Z/Q_X^\perp$, so that

$$\langle a_i \otimes b_j, a^{i'} \otimes b^{j'} \rangle = \langle a_i, a^{i'} \rangle \langle b_j, b^{j'} \rangle = \mathbb{1}_{i=i'} \mathbb{1}_{j=j'} = \mathbb{1}_{(i,j)=(i',j')}.$$

Therefore, the coset $c + L_X^\perp \in Q_Z/L_X^\perp$ is uniquely determined (and can be computed in time $\mathrm{poly}(|C|)$ via Gaussian elimination) from the $k_{\mathcal{A}} k_{\mathcal{B}}$ values $\langle a_i \otimes b_j, c \rangle$ across all $(i, j) \in [k_{\mathcal{A}}] \times [k_{\mathcal{B}}]$.

Therefore given input $x = c + e$, to compute the coset $c + L_X^\perp$ it suffices to compute $(I \otimes b_j^\top)c$ for every $j \in [k_{\mathcal{B}}]$, as then $\langle a_i \otimes b_j, c \rangle = \langle a_i, (I \otimes b_j^\top)c \rangle$. For this purpose, we first compute

$$(I \otimes b_j^\top)x = (I \otimes b_j^\top)c + (I \otimes b_j^\top)e.$$

Because $b_j \in Z_{r_{\mathcal{B}}}(\mathcal{B})$ and $c \in Z^{r_{\mathcal{B}}}(\mathcal{C}) = Z^{r_{\mathcal{B}}}(\mathcal{A} \otimes \mathcal{B})$, the Künneth formula (Lemma 2.17) implies that $(I \otimes b_j^\top)c \in H^0(\mathcal{A})$. Meanwhile, $|(I \otimes b_j^\top)e| \le |e| < \rho$. Hence we may run our radius-ρ time-T decoder for $H^0(\mathcal{A})$ on $(I \otimes b_j^\top)x$ to recover $(I \otimes b_j^\top)c$. The total running time to compute the values $\langle a_i \otimes b_j, c \rangle$ across all $(i, j) \in [k_{\mathcal{A}}] \times [k_{\mathcal{B}}]$ is therefore $\mathrm{poly}(T, |C|)$, so we can compute the coset $c + L_X^\perp$ in time $\mathrm{poly}(T, |C|)$, as desired. □

[9] Here $H^0(\mathcal{A})$ and $H_{r_{\mathcal{B}}}(\mathcal{B})$ can be viewed as classical codes (i.e. subspaces) rather than quotient spaces because $B^0(\mathcal{A}) = 0$ and $B_{r_{\mathcal{B}}}(\mathcal{B}) = 0$.

[10] Recall here that C denotes the set of basis elements in $\mathcal{C} = \mathbb{F}^C$.

We specifically construct our quantum codes as tensor products of 1-dimensional complexes associated to classical Tanner codes, as defined below.

Definition 2.19. *Let Γ be a directed graph. For a field $\mathbb{F}$, we define a* system of local codes $\mathcal{F}$ on Γ *to assign to every vertex $v \in V(\Gamma)$ a local full-rank generator matrix $\mathcal{F}_{v\to E(v)} : \mathcal{F}_v \to \mathbb{F}^{E(v)}$ for some vector space $\mathcal{F}_v = \mathbb{F}^{m_v}$ of dimension $m_v \le |E(v)|$, so that $\mathrm{im}(\mathcal{F}_{v\to E(v)}) \subseteq \mathbb{F}^{E(v)}$ is a local code supported on the edges $E(v) \subseteq E(\Gamma)$ incident to v. For $e \in E(v)$, we let $\mathcal{F}_e = \mathbb{F}$, and we let $\mathcal{F}_{v\to e} = \mathcal{F}_{v\to E(v)}|_e : \mathcal{F}_v \to \mathcal{F}_e$ denote the restriction to edge e.*

We then define the associated Tanner code $\mathrm{T}(\Gamma, \mathcal{F}) \subseteq \mathbb{F}^{E(\Gamma)}$ to contain all vectors in $\mathbb{F}^{E(\Gamma)}$ whose restriction to every neighborhood $E(v)$ lies in the specified local code, that is,

$$\mathrm{T}(\Gamma, \mathcal{F}) = \{c \in \mathbb{F}^{E(\Gamma)} : c|_{E(v)} \in \mathrm{im}(\mathcal{F}_{v\to E(v)}) \ \forall v \in V(\Gamma)\}.$$

We also define an associated 1-dimensional cochain complex $\mathcal{C}^*(\Gamma, \mathcal{F})$ by

$$\mathcal{C}^0(\Gamma, \mathcal{F}) = \bigoplus_{v\in V(\Gamma)} \mathcal{F}_v$$
$$\mathcal{C}^1(\Gamma, \mathcal{F}) = \bigoplus_{e\in E(\Gamma)} \mathcal{F}_e = \mathbb{F}^{E(\Gamma)},$$

such that for $c \in \mathcal{C}^0(\Gamma, \mathcal{F})$ and $e = (v, v') \in E(\Gamma)$,

$$(\delta(c))_e = \mathcal{F}_{v\to e}(c_v) - \mathcal{F}_{v'\to e}(c_{v'}). \tag{5}$$

We use the following basic notation regarding systems of local codes.

Definition 2.20. *For a system of local codes $\mathcal{F}$, we let $\mathcal{F}^\perp$ be a system in which $\mathcal{F}^\perp_{v\to E(v)}$ is a generator matrix for the dual local code $\mathrm{im}(\mathcal{F}^\perp_{v\to E(v)}) = \mathrm{im}(\mathcal{F}_{v\to E(v)})^\perp$ for each vertex v.*

For $c, c' \in \mathbb{F}^n$, we let $c * c' = (c_i c'_i)_{i\in[n]} \in \mathbb{F}^n$ denote the component-wise product. We extend this notation to classical codes $C, C' \subseteq \mathbb{F}^n$ by letting $C * C' = \mathrm{span}\{c * c' : c \in C,\ c' \in C'\}$, and then to systems of local codes $\mathcal{F}, \mathcal{F}'$ by letting $\mathcal{F}'' = \mathcal{F} * \mathcal{F}'$ be a system with $\mathrm{im}(\mathcal{F}''_{v\to E(v)}) = \mathrm{im}(\mathcal{F}_{v\to E(v)}) * \mathrm{im}(\mathcal{F}'_{v\to E(v)})$ for every v.

Fact 2.21 below relates a Tanner code to the space of (co)cycles on associated (co)chain complexes.

Fact 2.21. *Let Γ be a graph with system of local codes $\mathcal{F}$ over a field $\mathbb{F}$. Assume that either Γ is bipartite (with all edges directed from left to right), or $\mathbb{F}$ has characteristic 2. Then*

$$Z_1(\Gamma, \mathcal{F}^\perp) = \mathrm{T}(\Gamma, \mathcal{F}) \cong Z^0(\Gamma, \mathcal{F}), \tag{6}$$

where the isomorphism maps $c \in \mathrm{T}(\Gamma, \mathcal{F})$ to $z \in Z^0(\Gamma, \mathcal{F})$ satisfying $c|_{E(v)} = \mathcal{F}_{v\to E(v)}(z_v)$ for every $v \in V(\Gamma)$. In particular, if Γ has maximum degree[11] Δ and $\mathrm{T}(\Gamma, \mathcal{F})$ has distance d, then

$$d_1(\Gamma, \mathcal{F}^\perp) = d \le \frac{\Delta}{2} \cdot d^0(\Gamma, \mathcal{F}) \tag{7}$$

Additionally, if $\mathrm{T}(\Gamma, \mathcal{F})$ has a radius-ρ time-T decoder, then $Z^0(\Gamma, \mathcal{F})$ has a radius-ρ/Δ time-$(T + O(\Delta^3|V(\Gamma)|))$-decoder.

[11] Here we count both incoming and outgoing edges in the degree.

Proof. By definition $Z_1(\Gamma, \mathcal{F}^\perp)$ equals the space of vectors $c \in \mathbb{F}^{E(\Gamma)}$ satisfying

$$(\mathcal{F}^\perp_{v \to E(v)})^\top (c|_{E(v)}) = 0 \tag{8}$$

for every vertex v, meaning that the restriction of c to the neighborhood $E(v)$ lies in $\mathrm{im}(\mathcal{F}^\perp_{v\to E(v)})^\perp = \mathrm{im}(\mathcal{F}_{v\to E(v)})$. Here we do not need to impose additional signs on the local code coordinates because if Γ is bipartite, then each vertex v only sees edges of a single orientation (incoming or outgoing), so the sign in the $v \to e$ term of Equation (5) is the same for all $e \in E(v)$. Meanwhile, if Γ is not bipartite but $\mathbb{F}$ has characteristic 2, then all signs are $+1 = -1$. Hence it follows by Equation (8) that $Z_1(\Gamma, \mathcal{F}^\perp)$ consists of all vectors $c \in \mathrm{T}(\Gamma, \mathcal{F})$, so the equality in Equation (6) holds.

The mapping from $c \in \mathrm{T}(\Gamma, \mathcal{F})$ to $z \in Z^0(\Gamma, \mathcal{F})$ in Equation (6) is an isomorphism because it is invertible. Specifically, let $\Phi : C^0(\Gamma, \mathcal{F}) \to \mathbb{F}^{E(\Gamma)}$ be the map that sends $z \in C^0(\Gamma, \mathcal{F})$ to $c = \Phi(z) \in \mathbb{F}^{E(\Gamma)}$ whose value on every edge $e = (v, v')$ is $c_e = \mathcal{F}_{v\to e}(z_v)$. If $z \in Z^0(\Gamma, \mathcal{F})$ is a cocycle, then we have $c_e = \mathcal{F}_{v\to e}(z_v) = \mathcal{F}_{v'\to e}(z_{v'})$, so $c \in \mathrm{T}(\Gamma, \mathcal{F})$, and hence the restriction $\Phi|_{Z^0(\Gamma,\mathcal{F})} : Z^0(\Gamma, \mathcal{F}) \to \mathrm{T}(\Gamma, \mathcal{F})$ indeed provides the desired inverse to the map $\mathrm{T}(\Gamma, \mathcal{F}) \to Z^0(\Gamma, \mathcal{F})$ above.

The inequality in Equation (7) holds because for every nonzero $c \in \mathrm{T}(\Gamma, \mathcal{F})$ with associated 0-cocycle $z \in Z^0(\Gamma, \mathcal{F})$, then if $c_e \neq 0$ for an edge $e = (v, v') \in E(\Gamma)$, we must have $z_v \neq 0$ and $z_{v'} \neq 0$. Hence each nonzero edge in c is incident to two nonzero vertices in z, and every vertex is incident to $\leq \Delta$ edges, so z must have $\geq 2|c|/\Delta$ nonzero vertices, and thus $|z| \geq 2|c|/\Delta$.

Assuming $\mathrm{T}(\Gamma, \mathcal{F})$ has a radius-ρ time-T decoder, we obtain a decoder for $Z^0(\Gamma, \mathcal{F})$ by first applying the map Φ defined above to the input $a = c + e$ where $c \in Z^0(\Gamma, \mathcal{F})$, $|e| < \rho/\Delta$, and then applying the decoder for $\mathrm{T}(\Gamma, \mathcal{F})$ before applying the inverse isomorphism $\Phi|^{-1}_{Z^0(\Gamma,\mathcal{F})} : \mathrm{T}(\Gamma, \mathcal{F}) \xrightarrow{\sim} Z^0(\Gamma, \mathcal{F})$. Because Φ can only map each element in the support of e (which lies on some vertex) to at most Δ edges, we run the decoder for $\mathrm{T}(\Gamma, \mathcal{F})$ on a corrupted codeword of $\mathrm{T}(\Gamma, \mathcal{F})$ with error weight $\leq \Delta \cdot |e| < \rho$, so the decoder gives the correct output. Each map takes time $O(\Delta^3|V(\Gamma)|)$ to implement, for a total running time of $T + O(\Delta^3|V(\Gamma)|)$. □

Remark 2.22. Reversing the direction of any set of edges in Γ does not change the Tanner code $\mathrm{T}(\Gamma, \mathcal{F})$, but does change the signs in Equation (5) defining the coboundary map of $\mathcal{C}(\Gamma, \mathcal{F})$. Hence a Tanner code $\mathrm{T}(\Gamma, \mathcal{F})$ on a bipartite graph Γ is preserved if we re-orient all edges to be directed from left to right, as required in Fact 2.21.

3 High-Yield Transversal Gates via Multiplication Property

In this section, we give a general construction of quantum codes supporting transversal $C^{r-1}Z$ gates from products of classical Tanner codes. We state this result in Section 3.1. We then describe the necessary cup product machinery in Section 3.2 that we subsequently use in Section 3.3 to prove the result. We show in Appendix A how to extend this result to allow for addressable $C^{r-1}Z$ gates, meaning that we can additionally choose which subset of logical qudits on which to perform $C^{r-1}Z$.

3.1 Result Statement

Fix a directed graph Γ of maximum degree $\Delta \geq 2$. For an integer $r \geq 2$, let $\mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(r)}$ be systems of local codes on Γ over a field $\mathbb{F}$. Assume that either Γ is bipartite (with all edges directed

from left to right), or $\mathbb{F}$ has characteristic 2 (so that Fact 2.21 holds; see also Remark 2.22). Let $M \subseteq E(\Gamma)$ be an extendable set for the classical code $\mathrm{T}(\Gamma, \mathcal{F}^{(i)})$ for every $1 \le i \le r-1$.

We define product cochain complexes

$$\begin{aligned}
\mathcal{A}^{(1)} &= \mathcal{C}^*(\Gamma, \mathcal{F}^{(r)^\perp}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(1)}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(2)}) \otimes \cdots \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r-1)}) \\
\mathcal{A}^{(2)} &= \mathcal{C}^*(\Gamma, \mathcal{F}^{(r-1)}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r)^\perp}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(1)}) \otimes \cdots \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r-2)}) \\
&\vdots \\
\mathcal{A}^{(r)} &= \mathcal{C}^*(\Gamma, \mathcal{F}^{(1)}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(2)}) \otimes \cdots \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r-1)}) \otimes \mathcal{C}^*(\Gamma, \mathcal{F}^{(r)^\perp}),
\end{aligned}$$

so that $\mathcal{A}^{(i)}$ is given by cyclically permuting the tensor factors of $\mathcal{A}^{(1)}$ by $i-1$ positions. We will construct transversal $C^{r-1}Z$ gates across the r codes associated to level 1 of these r cochain complexes $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(r)}$, respectively.

Theorem 3.1. *If it holds for each $v \in V(\Gamma)$ that*

$$\mathrm{im}(\mathcal{F}^{(1)}_{v \to E(v)}) * \cdots * \mathrm{im}(\mathcal{F}^{(r-1)}_{v \to E(v)}) \subseteq \mathrm{im}(\mathcal{F}^{(r)}_{v \to E(v)}), \tag{9}$$

then the quantum codes $Q^{(i)}$ at level 1 of $\mathcal{A}^{(i)}$ for $i \in [r]$ have subsystems $L^{(i)}$ that support a transversal $C^{r-1}Z$ gate of sparsity $\le (4\Delta)^{r^2}$ and logical yield $\ge |M|^r$. Furthermore, if each classical code $\mathrm{T}(\Gamma, \mathcal{F}^{(j)})$ has distance $d^{(j)}$ and supports a radius-$\rho^{(j)}$ time-$\mathrm{poly}(\Delta, |V(\Gamma)|)$ decoder, then $(Q^{(i)}, L^{(i)})$ is a quantum subsystem code of locality $\le r\Delta^2$, X-distance $d_X \ge d^{(r)}$, and Z-distance $d_Z \ge (2/\Delta)^{r-1} \cdot d^{(1)} d^{(2)} \cdots d^{(r-1)}$, which supports a radius-$\min\{\rho^{(1)} \cdots \rho^{(r-1)}/\Delta^{r-1},\ \rho^{(r)}\}$ time-$\mathrm{poly}(\Delta, |V(\Gamma)|)^r$ decoder.

3.2 Cup Products

To prove Theorem 3.1, we will construct the desired cohomology-invariant forms using *cup products* on cochain complexes:

Definition 3.2. *For cochain complexes $\mathcal{C}^*, \mathcal{C}'^*, \mathcal{C}''^*$, a* cup product *is a bilinear operation $\smile : \mathcal{C}^i \times \mathcal{C}'^j \to \mathcal{C}''^{i+j}$ for every $i, j \in \mathbb{Z}$ that satisfies the following* Leibniz rule *for every $c \in \mathcal{C}^i$, $c' \in \mathcal{C}'^j$:*

$$\delta(c \smile c') = \delta(c) \smile c' + (-1)^i c \smile \delta(c'). \tag{10}$$

Cup products have long been studied in algebraic topology, see e.g. [Hat01]. We only provide the minimal treatment necessary for our purposes.

The Leibniz rule ensures the following crucial cohomology-invariance property:

Fact 3.3. *A cup product satisfying the Leibniz rule as in Definition 3.2 induces a well-defined bilinear form on cohomology. That is, for every $c \in Z^i(\mathcal{C})$, $c' \in Z^j(\mathcal{C}')$,*

$$(c + B^i(\mathcal{C})) \smile (c' + B^j(\mathcal{C}')) \subseteq c \smile c' + B^{i+j}(\mathcal{C}'').$$

Proof. For every $a \in \mathcal{C}^{i-1}$ we have

$$\delta(a) \smile c' = \delta(a \smile c') - (-1)^{i-1} a \smile \delta(c') = \delta(a \smile c') \in B^{i+j}(\mathcal{C}''),$$

where the first equality above holds by the Leibniz rule, and the second equality holds because $c' \in Z^j(\mathcal{C}')$. Hence $(c + \delta(a)) \smile c'$ differs from $c \smile c'$ by the coboundary $\delta(a \smile c')$. Similar reasoning also implies that every element of $c \smile (c' + B^j(\mathcal{C}'))$ differs from $c \smile c'$ by a coboundary. □

We now show how to construct cup products on Tanner code complexes.

Definition 3.4. *Let $\mathcal{F}, \mathcal{F}'$ be systems of local codes on a graph Γ. For $i, j \in \mathbb{Z}$, we define the cup product*

$$\smile : \mathcal{C}^i(\Gamma, \mathcal{F}) \times \mathcal{C}^j(\Gamma, \mathcal{F}') \to \mathcal{C}^{i+j}(\Gamma, \mathcal{F}'' = \mathcal{F} * \mathcal{F}')$$

such that

$$\begin{aligned}
\forall c \in \mathcal{C}^0(\Gamma, \mathcal{F}),\ c' \in \mathcal{C}^0(\Gamma, \mathcal{F}'),\ v \in V(\Gamma): &\quad \mathcal{F}''_{v \to E(v)}((c \smile c')_v) = \mathcal{F}_{v \to E(v)}(c_v) * \mathcal{F}'_{v \to E(v)}(c'_v) \\
\forall c \in \mathcal{C}^0(\Gamma, \mathcal{F}),\ c' \in \mathcal{C}^1(\Gamma, \mathcal{F}'),\ e = (v, v') \in E(\Gamma): &\quad (c \smile c')_e = \mathcal{F}_{v \to e}(c_v) \cdot c'_e \\
\forall c \in \mathcal{C}^1(\Gamma, \mathcal{F}),\ c' \in \mathcal{C}^0(\Gamma, \mathcal{F}'),\ e = (v, v') \in E(\Gamma): &\quad (c \smile c')_e = c_e \cdot \mathcal{F}'_{v' \to e}(c'_{v'}).
\end{aligned}$$

Note that the first equality above uniquely determines $(c \smile c')_v$ because $\mathcal{F}''_{v \to E(v)}$ is by assumption a full-rank (injective) generator matrix.

Lemma 3.5. *The cup product in Definition 3.4 satisfies the Leibniz rule.*

Proof. Let $c \in \mathcal{C}^i(\Gamma, \mathcal{F})$, $c' \in \mathcal{C}^j(\Gamma, \mathcal{F}')$. If either i or j is nonzero then both sides of Equation (10) are 0. Thus assume $i = j = 0$. Then for every $e = (v, v') \in E(\Gamma)$,

$$\begin{aligned}
(\delta(c \smile c'))_e &= \mathcal{F}_{v \to e}(c_v) \cdot \mathcal{F}'_{v \to e}(c'_v) - \mathcal{F}_{v' \to e}(c_{v'}) \cdot \mathcal{F}'_{v' \to e}(c'_{v'}) \\
(\delta(c) \smile c')_e &= (\mathcal{F}_{v \to e}(c_v) - \mathcal{F}_{v' \to e}(c_{v'})) \cdot \mathcal{F}'_{v' \to e}(c'_{v'}) \\
(c \smile \delta(c'))_e &= \mathcal{F}_{v \to e}(c_v) \cdot (\mathcal{F}'_{v \to e}(c'_v) - \mathcal{F}'_{v' \to e}(c'_{v'})),
\end{aligned}$$

so Equation (10) follows. □

Lemma 3.6 below shows that the cup product respects tensor products.

Lemma 3.6. *Given cup products*

$$\begin{aligned}
\smile &: \mathcal{A} \times \mathcal{A}' \to \mathcal{A}'' \\
\smile &: \mathcal{B} \times \mathcal{B}' \to \mathcal{B}'',
\end{aligned}$$

then there exists a cup product (satisfying the Leibniz rule)

$$\smile : (\mathcal{A} \otimes \mathcal{B}) \times (\mathcal{A}' \otimes \mathcal{B}') \to \mathcal{A}'' \otimes \mathcal{B}''$$

defined for $a \in \mathcal{A}^{i_a}$, $a' \in \mathcal{A}'^{i_{a'}}$, $b \in \mathcal{B}^{i_b}$, $b' \in \mathcal{B}'^{i_{b'}}$ by

$$(a \otimes b) \smile (a' \otimes b') = (-1)^{i_b i_{a'}} (a \smile a') \otimes (b \smile b'). \tag{11}$$

Proof. We verify the Leibniz rule for the tensor product complexes, assuming that it holds for the factor complexes:

$$\begin{aligned}
&\delta((a \otimes b) \smile (a' \otimes b')) \\
&\quad = (-1)^{i_b i_{a'}} \cdot \delta((a \smile a') \otimes (b \smile b')) \\
&\quad = (-1)^{i_b i_{a'}} \cdot (\delta(a \smile a') \otimes (b \smile b') + (-1)^{i_a + i_{a'}} (a \smile a') \otimes \delta(b \smile b')) \\
&\quad = (-1)^{i_b i_{a'}} \cdot \big(\delta(a) \smile a' + (-1)^{i_a} a \smile \delta(a')\big) \otimes (b \smile b') \\
&\qquad + (-1)^{i_b i_{a'}} \cdot (-1)^{i_a + i_{a'}} (a \smile a') \otimes \big(\delta(b) \smile b' + (-1)^{i_b} b \smile \delta(b')\big) \\
&\quad = (\delta(a) \otimes b) \smile (a' \otimes b') + (-1)^{i_a} (a \otimes \delta(b)) \smile (a' \otimes b') \\
&\qquad + (-1)^{i_a + i_b} (a \otimes b) \smile (\delta(a') \otimes b') + (-1)^{i_a + i_b + i_{a'}} (a \otimes b) \smile (a' \otimes \delta(b')) \\
&\quad = \delta(a \otimes b) \smile (a' \otimes b') + (-1)^{i_a + i_b} (a \otimes b) \smile \delta(a' \otimes b').
\end{aligned}$$

□

3.3 Proof of Theorem 3.1

We first define the desired subsystems $L^{(i)} = (L_X^{(i)} \subseteq H_1(\mathcal{A}^{(i)}),\ L_Z^{(i)} \subseteq H^1(\mathcal{A}^{(i)}))$ of $Q^{(i)}$ for each $i \in [r]$. Specifically, using the isomorphism given by the Künneth formula (Lemma 2.17), we let

$$\begin{aligned} L_X^{(r)} &= H_0(\Gamma, \mathcal{F}^{(1)}) \otimes \cdots \otimes H_0(\Gamma, \mathcal{F}^{(r-1)}) \otimes H_1(\Gamma, \mathcal{F}^{(r)^\perp}) \\ L_Z^{(r)} &= H^0(\Gamma, \mathcal{F}^{(1)}) \otimes \cdots \otimes H^0(\Gamma, \mathcal{F}^{(r-1)}) \otimes H^1(\Gamma, \mathcal{F}^{(r)^\perp}). \end{aligned} \tag{12}$$

Then for $i \in [r]$, we let $L_X^{(i)}, L_Z^{(i)}$ be given by cyclically shifting the tensor factors in $L_X^{(r)}, L_Z^{(r)}$ to the right by i positions. The Künneth formula ensures that this subsystem is well defined.

Below we show the distance bounds in Theorem 3.1:

Claim 3.7. *For $i \in [r]$, the subsystem code $(Q^{(i)}, L^{(i)})$ has X-distance $d_X \geq d^{(r)}$ and Z-distance $d_Z \geq (2/\Delta)^{r-1} \cdot d^{(1)} d^{(2)} \cdots d^{(r-1)}$.*

Proof. By symmetry it suffices to consider the $i = r$ case. We bound the X- and Z-distances separately, using similar arguments:

X-distance: Let $a \in Z_1(\mathcal{A}^{(r)}) \setminus L_Z^{(r)^\perp}$. Since pure tensors span $L_Z^{(r)}$, there exists $z = z^{(1)} \otimes \cdots \otimes z^{(r)} \in L_Z^{(r)}$, where $z^{(1)} \in Z^0(\Gamma, \mathcal{F}^{(1)}), \ldots, z^{(r-1)} \in Z^0(\Gamma, \mathcal{F}^{(r-1)})$, $z^{(r)} \in Z^1(\Gamma, \mathcal{F}^{(r)^\perp})$, such that $\langle a, z \rangle \neq 0$. Let

$$a' = (z^{(1)} \otimes \cdots \otimes z^{(r-1)} \otimes I)^\top a \in \mathcal{C}_1(\Gamma, \mathcal{F}^{(r)^\perp})$$

be the vector obtained by restricting a to components in $C_0(\Gamma, \mathcal{F}^{(1)}) \times \cdots \times C_0(\Gamma, \mathcal{F}^{(r-1)}) \times C_1(\Gamma, \mathcal{F}^{(r)^\perp}) \subseteq A_1^{(r)}$ (yielding an r-dimensional tensor), and then applying $\langle \cdot, z^{(i)} \rangle$ to each direction-i column for $i = 1, \ldots, r-1$. By the Künneth formula

$$a' \in Z_1(\Gamma, \mathcal{F}^{(r)^\perp}),$$

and $\langle a', z^{(r)} \rangle = \langle a, z \rangle \neq 0$ so that $a' \neq 0$. Thus

$$|a| \geq |a'| \geq d_1(\Gamma, \mathcal{F}^{(r)^\perp}) = d^{(r)},$$

where the final equality holds by Fact 2.21.

Z-distance: Now let $a \in Z^1(\mathcal{A}^{(r)}) \setminus L_X^{(r)^\perp}$. Since pure tensors span $L_X^{(r)}$, there exists $z = z^{(1)} \otimes \cdots \otimes z^{(r)} \in L_X^{(r)}$, where $z^{(1)} \in Z_0(\Gamma, \mathcal{F}^{(1)}), \ldots, z^{(r-1)} \in Z_0(\Gamma, \mathcal{F}^{(r-1)})$, $z^{(r)} \in Z_1(\Gamma, \mathcal{F}^{(r)^\perp})$, such that $\langle z, a \rangle \neq 0$. Let

$$a' = (I^{\otimes r-1} \otimes z^{(r)})^\top a \in \mathcal{C}^0(\Gamma, \mathcal{F}^{(1)}) \otimes \cdots \otimes \mathcal{C}^0(\Gamma, \mathcal{F}^{(r-1)}).$$

By the Künneth formula

$$a' \in Z^0(\Gamma, \mathcal{F}^{(1)}) \otimes \cdots \otimes Z^0(\Gamma, \mathcal{F}^{(r-1)}),$$

and $\langle z^{(1)} \otimes \cdots \otimes z^{(r-1)}, a' \rangle = \langle z, a \rangle \neq 0$ so that $a' \neq 0$. Thus

$$|a| \geq |a'| \geq d^0(\Gamma, \mathcal{F}^{(1)}) \cdots d^0(\Gamma, \mathcal{F}^{(r-1)}) \geq \frac{2d^{(1)}}{\Delta} \cdots \frac{2d^{(r-1)}}{\Delta},$$

where the final inequality holds by Fact 2.21. □

Below we present the decoder in Theorem 3.1:

Claim 3.8. *For $i \in [r]$, the subsystem code $(Q^{(i)}, L^{(i)})$ has a radius-$\min\{\rho^{(1)} \cdots \rho^{(r-1)}/\Delta^{r-1},\ \rho^{(r)}\}$ time-$\text{poly}(\Delta, |V(\Gamma)|)^r$ decoder.*

Proof. By symmetry it again suffices to consider the $i = r$ case. Let

$$\mathcal{A}' = \mathcal{C}(\Gamma, \mathcal{F}^{(1)}) \otimes \cdots \otimes \mathcal{C}(\Gamma, \mathcal{F}^{(r-1)})$$
$$\mathcal{B}' = \mathcal{C}(\Gamma, \mathcal{F}^{(r)^\perp}),$$

so that $\mathcal{A}^{(r)} = \mathcal{A}' \otimes \mathcal{B}'$. Recall we assume that each $\mathrm{T}(\Gamma, \mathcal{F}^{(j)}) = Z_1(\Gamma, \mathcal{F}^{(j)^\perp})$ has a radius-$\rho^{(j)}$ time-$\text{poly}(\Delta, |V(\Gamma)|)$ decoder. Then

$$Z^0(\mathcal{A}') = Z^0(\Gamma, \mathcal{F}^{(1)}) \otimes \cdots \otimes Z^0(\Gamma, \mathcal{F}^{(r-1)}),$$

so by Lemma 2.6 and Fact 2.21, $Z^0(\mathcal{A}')$ has a radius-$\rho^{(1)} \cdots \rho^{(r-1)}/\Delta^{r-1}$ time-$\text{poly}(\Delta, |V(\Gamma)|)^{r-1}$ decoder. Therefore by Lemma 2.18, $(Q^{(r)}, L^{(r)})$ has a radius-$\min\{\rho^{(1)} \cdots \rho^{(r-1)}/\Delta^{r-1},\ \rho^{(r)}\}$ time-$\text{poly}(\Delta, |V(\Gamma)|)^r$ decoder, as desired. □

We now construct the desired multilinear form for the transversal $C^{r-1}Z$ gate in Theorem 3.1. Let

$$\mathcal{C}' = \mathcal{C}^*(\Gamma, \mathcal{F}^{(1)} * \cdots * \mathcal{F}^{(r-1)} * \mathcal{F}^{(r)^\perp}) \quad \text{and} \quad \mathcal{A}' = \mathcal{C}'^{\otimes r}. \tag{13}$$

For each $v \in V(\Gamma)$, the assumption in Equation (9) implies that all codewords in $\mathrm{im}(\mathcal{F}^{(1)}_{v \to E(v)}) * \cdots * \mathrm{im}(\mathcal{F}^{(r-1)}_{v \to E(v)}) * \mathrm{im}(\mathcal{F}^{(r)}_{v \to E(v)})^\perp$ have entries summing to 0, or equivalently, the dual $(\mathrm{im}(\mathcal{F}^{(1)}_{v \to E(v)}) * \cdots * \mathrm{im}(\mathcal{F}^{(r-1)}_{v \to E(v)}) * \mathrm{im}(\mathcal{F}^{(r)}_{v \to E(v)})^\perp)^\perp$ contains the all-1s vector $\mathbb{1}_{E(v)}$. Hence $\mathrm{T}(\Gamma, (\mathcal{F}^{(1)} * \cdots * \mathcal{F}^{(r-1)} * \mathcal{F}^{(r)^\perp})^\perp) = Z_1(\mathcal{C}')$ (see Fact 2.21) contains the all-1s vector $\mathbb{1}_{E(\Gamma)}$.

We then define a multilinear form

$$f : \mathcal{A}^{(1)^1} \times \cdots \times \mathcal{A}^{(r)^1} \to \mathbb{F}$$

by

$$f(a^{(1)}, \ldots, a^{(r)}) = \langle \mathbb{1}^{\otimes r}_{E(\Gamma)}, a^{(1)} \smile \cdots \smile a^{(r)} \rangle. \tag{14}$$

Specifically, to define the cup product

$$a^{(1)} \smile \cdots \smile a^{(r)} \in \mathcal{A}'^r$$

in Equation (14), we first define the cup product from Definition 3.4 on the factor complexes $\mathcal{C}^*(\Gamma, \mathcal{F}^{(i)})$, and then we obtain the cup product on the tensor product complexes $\mathcal{A}^{(i)}$ by Lemma 3.6. Here we process the cup products from left to right, i.e. we take $((a^{(1)} \smile a^{(2)}) \smile a^{(3)}) \cdots$. Also note in Equation (14) that $\mathbb{1}_{E(\Gamma)} \in Z_1(\mathcal{C}')$, so $\mathbb{1}^{\otimes r}_{E(\Gamma)} \in Z_r(\mathcal{A}')$.

Claim 3.9. *f has sparsity $\leq (4\Delta)^{r^2}$.*

We do not attempt to make the bound in Claim 3.9 tight. Rather, the important point is that it grows polynomially in Δ when r is constant. To prove Claim 3.9, recall that basis elements in $A^{(1)}, \dots, A^{(r)}$ are by definition associated to vertices and edges in the Cartesian product $\Gamma^{\times r}$ of r copies of Γ. The main idea is that the cup product in Equation (14) can only have nonzero terms for basis elements that are adjacent in $\Gamma^{\times r}$. Once we fix one basis element, the number of adjacent basis elements is then bounded in terms of the graph degree Δ. We now present the details.

Proof of Claim 3.9. If $C^{r-1}Z^f$ applies a non-identity gate on qudits $c^{(1)} \in {A^{(1)}}^1, \dots, c^{(r)} \in {A^{(r)}}^1$, then we must have $f(\mathbb{1}_{c^{(1)}}, \dots, \mathbb{1}_{c^{(r)}}) \neq 0$, and therefore

$$\mathbb{1}_{c^{(1)}} \smile \cdots \smile \mathbb{1}_{c^{(r)}} \neq 0. \tag{15}$$

As each $\mathcal{A}^{(i)}$ is the tensor product of r complexes $\mathcal{C}(\Gamma, \mathcal{F})$ (for different $\mathcal{F}$), we can write each $c^{(i)} = (c_1^{(i)}, \dots, c_r^{(i)})$ for basis elements $c_j^{(i)}$ in the factor complexes $C(\Gamma, \mathcal{F})$. Then Equation (15) implies that for every $j \in [r]$,

$$\mathbb{1}_{c_j^{(1)}} \smile \cdots \smile \mathbb{1}_{c_j^{(r)}} \neq 0. \tag{16}$$

Recall that each basis element in $C^0(\Gamma, \mathcal{F})$ is associated to a vertex in Γ (with $\dim(\mathcal{F}_v) \leq \Delta$ basis elements for each vertex v), and $C^1(\Gamma, \mathcal{F}) = E(\Gamma)$ is the set of edges. By Definition 3.4, Equation (16) can only hold if there exists some edge $e_j = (v_j, v_j') \in E(\Gamma)$ such that each of $c_j^{(1)}, \dots, c_j^{(r)}$ either equal e_j, or else are associated to v_j or v_j'.

Hence once we fix $c^{(i)} = (c_1^{(i)}, \dots, c_r^{(i)})$ for a single $i \in [r]$, then for each $j \in [r]$ there are $\leq \Delta$ choices of a valid edge $e_j = (v_j, v_j')$ incident (or equal) to $c_j^{(i)}$, and then there are $\leq 2\Delta + 1$ choices of $c_j^{(i')}$ for each $i' \in [r] \setminus \{i\}$ that are associated to e_j, v_j, or v_j'. Thus for each $j \in [r]$ there are $\leq \Delta \cdot (2\Delta + 1)^{r-1}$ choices of $(c_j^{(i')})_{i' \in [r] \setminus \{i\}}$ satisfying Equation (16), so the total number of choices of $(c^{(i')})_{i' \in [r] \setminus \{i\}}$ satisfying Equation (15) is $\leq (\Delta \cdot (2\Delta + 1)^{r-1})^r \leq (4\Delta)^{r^2}$.

□

Claim 3.10. *f is cohomology-invariant.*

Proof. The claim follows from the cohomology-invariance of the cup product from Fact 3.3. That is, for every $a^{(1)} \in Z^1(\mathcal{A}^{(1)}), \dots, a^{(r)} \in Z^1(\mathcal{A}^{(r)})$ and every $b^{(1)} \in B^1(\mathcal{A}^{(1)}), \dots, b^{(r)} \in B^1(\mathcal{A}^{(r)})$,

$$(a^{(1)} + b^{(1)}) \smile \cdots \smile (a^{(r)} + b^{(r)}) \in a^{(1)} \smile \cdots \smile a^{(r)} + B^r(\mathcal{A}').$$

Then it follows because $\mathbb{1}_{E(\Gamma)}^{\otimes r} \in Z_r(\mathcal{A}')$ that $\langle \mathbb{1}_{E(\Gamma)}^{\otimes r}, B^r(\mathcal{A}') \rangle = 0$, so

$$f(a^{(1)} + b^{(1)}, \dots, a^{(r)} + b^{(r)}) = \langle \mathbb{1}_{E(\Gamma)}^{\otimes r}, a^{(1)} \smile \cdots \smile a^{(r)} \rangle = f(a^{(1)}, \dots, a^{(r)}).$$

□

We now show that the transversal gate $C^{r-1}Z^f$ has logical yield $|M|^r$ (see Definition 2.14):

Claim 3.11. *The restriction of the induced form*

$$\tilde{f} : H^1(\mathcal{A}^{(1)}) \times \cdots \times H^1(\mathcal{A}^{(r)}) \to \mathbb{F}$$

to $L_Z^{(1)} \times \cdots \times L_Z^{(r)}$ has subrank $\geq |M|^r$.

Proof. For every $i \in [r-1]$ because M is extendable for $\mathrm{T}(\Gamma, \mathcal{F}^{(i)})$, there exists for every $e \in M$ a codeword $c_e^{(i)} \in \mathrm{T}(\Gamma, \mathcal{F}^{(i)})$ whose restriction $c_e^{(i)}|_M = \mathbb{1}_e \in \mathbb{F}^M$ to components in M equals the indicator function for edge e. Let $z_e^{(i)} \in Z^0(\Gamma, \mathcal{F}^{(i)})$ be the 0-cocycle associated to $c_e^{(i)}$ under the isomorphism in Fact 2.21. Also let $z_e^{(r)} = c_e^{(r)} = \mathbb{1}_e \in Z^1(\Gamma, \mathcal{F}^{(r)^\perp})$.

Then by the definition of the cup product on 1-dimensional complexes in Definition 3.4, for every $e^{(1)}, \dots, e^{(r)} \in M$ and every $i \in [r]$,

$$z_{e^{(1)}}^{(1-i)} \smile z_{e^{(2)}}^{(2-i)} \smile \cdots \smile z_{e^{(r)}}^{(r-i)} = c_{e^{(1)}}^{(i-1)} * c_{e^{(2)}}^{(i-2)} * \cdots * c_{e^{(r)}}^{(i-r)} = \begin{cases} \mathbb{1}_{e^{(r)}} & \text{if } e^{(1)} = \cdots = e^{(r)} \\ 0 & \text{otherwise,} \end{cases}$$

where above we take the superscripts $1-i, 2-i, \dots, r-i$ modulo r to obtain indices in $[r]$. Therefore for every tuple of edges $e^{(i)} = (e_1^{(i)}, \dots, e_r^{(i)}) \in M^r$ for $i \in [r]$, letting

$$z_{e^{(i)}}^{(i)} = z_{e_1^{(i)}}^{(1-i)} \otimes z_{e_2^{(i)}}^{(2-i)} \otimes \cdots \otimes z_{e_r^{(i)}}^{(r-i)} \in Z^1(\mathcal{A}^{(i)}) \tag{17}$$

(where we again take superscripts modulo r), then by the definition of the cup product on $\mathcal{A}^{(1)} \times \cdots \times \mathcal{A}^{(r)}$ from Lemma 3.6,

$$\begin{aligned} z_{e^{(1)}}^{(1)} \smile \cdots \smile z_{e^{(r)}}^{(r)} &= \bigotimes_{i \in [r]} \left(z_{e_i^{(1)}}^{(1-i)} \smile z_{e_i^{(2)}}^{(2-i)} \smile \cdots \smile z_{e_i^{(r)}}^{(r-i)} \right) \\ &= \begin{cases} \bigotimes_{i \in [r]} \mathbb{1}_{e_i^{(1)}} & \text{if } e^{(1)} = \cdots = e^{(r)} \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{18}$$

Specifically, the first equality above follows by repeatedly applying Equation (11) to transform the cup product of tensor products on the LHS into a tensor product of cup products; the sign $(-1)^{i_b i_{a'}}$ in Equation (11) is $+1$ in every one of these applications because $z_e^{(r)} = z_e^{(0)}$ is a 1-cocycle whereas every $z_e^{(i)}$ for $i \not\equiv 0 \pmod r$ is a 0-cocycle. Therefore

$$f(z_{e^{(1)}}^{(1)}, \dots, z_{e^{(r)}}^{(r)}) = \langle \mathbb{1}_{E(\Gamma)}^{\otimes r}, z_{e^{(1)}}^{(1)} \smile \cdots \smile z_{e^{(r)}}^{(r)} \rangle = \begin{cases} 1 & \text{if } e_i^{(1)} = \cdots = e_i^{(r)} \ \forall i \in [r] \\ 0 & \text{otherwise.} \end{cases}$$

Thus for $i \in [r]$, the cohomology classes $z_{e^{(i)}}^{(i)} + B^1(\mathcal{A}^{(i)}) \in H^1(\mathcal{A}^{(i)})$ across all possible choices of $e^{(i)} = (e_1^{(i)}, \dots, e_r^{(i)}) \in M^r$ satisfy the precise condition in Definition 2.13 needed to imply that $\tilde{f}$ has subrank $\geq |M|^r$. Because each $z_{e^{(i)}}^{(i)} + B^1(\mathcal{A}^{(i)})$ in fact lies in $L_Z^{(i)} \subseteq H^1(\mathcal{A}^{(i)})$ by Equations (12) and (17), the same subrank bound holds for the restriction of $\tilde{f}$ to $L_Z^{(1)} \times \cdots \times L_Z^{(r)}$. □

Theorem 3.1 follows from the claims above (below recall Definition 2.14):

Proof of Theorem 3.1. The transversal $C^{r-1}Z$ gate is constructed in Equation (14), and cohomology-invariance is shown in Claim 3.10. The desired logical yield is shown in Claim 3.11, and the sparsity in Claim 3.9. The locality bound of $r\Delta^2$ follows because $\mathcal{A}^{(i)}$ is the tensor product of r 1-dimensional complexes each of locality $\leq \Delta^2$. The distance bounds are shown in Claim 3.7, and the decoder is constructed in Claim 3.8. □

4 Classical Tanner Codes with Multiplication Property

In this section, we present a classical Tanner code construction that has large dimension even for local codes of rate $< 1/2$. Hence as shown in Section 5 below, we can instantiate this construction with algebraic local codes that respect component-wise multiplication, and hence apply Theorem 3.1 to obtain quantum codes with transversal $C^{r-1}Z$ gates of large logical yield. In the statement below, we denote $[a : b] = \{a, a+1, \ldots, b\}$ for $a, b \in \mathbb{Z}$.

Theorem 4.1. *For every $n, t \in \mathbb{N}$ with $t \geq 2$, there exists a bipartite graph $\Gamma = \Gamma(n, t)$ of maximum degree $2n$ with the following property. For every choice of classical codes $C_i \subseteq \mathbb{F}_q^{2n}$ for $i \in [t]$ of length $2n$, dimension $k_i \leq n$, and distance $d_i > n$, there exists a system of local codes $\mathcal{F} = \mathcal{F}(C_1, \ldots, C_t)$ on Γ such that the Tanner code $\mathrm{T}(\Gamma, \mathcal{F})$ has parameters*

$$\left[N = (t-1)n^t,\ K = \prod_{i \in [t]} k_i,\ D \geq \prod_{i \in [t]} (d_i - n) \right]_q .$$

Furthermore, for each $v \in V(\Gamma)$, the local code $\mathrm{im}(\mathcal{F}_{v \to E(v)})$ equals the puncturing $C_{i_v}|_{P_v}$ of some C_{i_v} down to some set $P_v \subseteq [2n]$ of components, where $i_v \in [t]$, P_v, and the bijection $P_v \cong E(v)$ used to define the Tanner code[12] depend only on n, t, v (and not on the choice of codes $C_1, \ldots, C_t$). Specifically, each P_v equals either $[1 : n]$, $[n+1 : 2n]$, or $[1 : 2n]$.

Additionally suppose for each $i \in [t]$ that we have a radius-ρ_i time-T_i decoder for $C_i|_{[1:n]}$ and for $C_i|_{[n+1:2n]}$. Then there exists a radius $\rho = \prod_{i \in [t]} \rho_i$ time $T = (t-1)n^{t-1} \sum_{i \in [t]} T_i$ decoder for $\mathrm{T}(\Gamma, \mathcal{F})$.

4.1 Proof of Theorem 4.1

We will construct $\Gamma, \mathcal{F}$ so that $\mathrm{T}(\Gamma, \mathcal{F})$ is a puncturing of the tensor code $\bigotimes_{i \in [t]} C_i$. The dimension and distance bounds, as well as the decoding algorithm, will then follow from those of the tensor code.

To begin, we define a t-partite graph $\bar{\Gamma}$ that has vertices corresponding to columns (in any of the t directions) in the t-dimensional hypercube $[2n]^t$, and edges connecting pairs of columns that intersect. Formally,

$$V(\bar{\Gamma}) = \bar{V}_1 \sqcup \cdots \sqcup \bar{V}_t \quad \text{with each} \quad \bar{V}_i = [2n]^{[t] \setminus \{i\}} \cong [2n]^{t-1}.$$

A vertex $v \in \bar{V}_i$ corresponds to the direction-i column

$$\mathrm{col}_i(v) = [2n]^{\{i\}} \times v \subseteq [2n]^t,$$

where above the $[2n]^{\{i\}}$ factor is moved into the ith position in $v_i \in [2n]^{[t] \setminus \{i\}}$. A pair of vertices $(v_i \in \bar{V}_i,\ v_j \in \bar{V}_j)$ forms an edge in $E(\bar{\Gamma})$ if $i < j$ and the projections of v_i, v_j onto all components in $[t] \setminus \{i, j\}$ are equal, or equivalently, if $\mathrm{col}_i(v_i) \cap \mathrm{col}_j(v_j) \neq \emptyset$.

To define Γ, recalling the notation $[a : b] = \{a, a+1, \ldots, b\}$ for $a, b \in \mathbb{Z}$, we let

$$V(\Gamma) = V_1 \sqcup \cdots \sqcup V_t \quad \text{with each} \quad V_i = [n+1 : 2n]^{[1:i-1]} \times [1 : n]^{[i+1:t]} \subseteq \bar{V}_i.$$

We let Γ be the subgraph of $\bar{\Gamma}$ induced by $V(\Gamma)$.

[12] Specifically, the bijection is used to associate the components of $C_{i_v}|_{P_v} \subseteq \mathbb{F}_q^{P_v}$ with the components of $\mathcal{F}_v \subseteq \mathbb{F}_q^{E(v)}$.

Claim 4.2. *Define sets* $E_1, \dots, E_{t-1}, E \subseteq [2n]^t$ *by*

$$E_i = [n+1:2n]^{[1:i]} \times [1:n]^{[i+1:t]} \quad \forall 1 \le i \le t-1$$
$$E = \bigsqcup_{i \in [t-1]} E_i.$$

Then there is an isomorphism

$$\mathrm{ed} : E \xrightarrow{\sim} E(\Gamma)$$

that maps $e = (e_1, \dots, e_t) \in E_i$ *to* $\mathrm{ed}(e) = (v, v') \in E(\Gamma)$ *where*

$$v = (e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_t) \in V_i, \quad v' = (e_1, \dots, e_i, e_{i+2}, \dots, e_t) \in V_{i+1}.$$

In particular, Γ *is bipartite, and for* $v \in V(\Gamma)$,

$$\deg(v) = \begin{cases} n, & v \in V_1 \sqcup V_t \\ 2n, & v \in V_2 \sqcup \cdots \sqcup V_{t-1}. \end{cases} \tag{19}$$

Proof. For $i, j \in [t]$ with $i < j - 1$, the projections of V_i and V_j onto component $i+1$ are $[1:n]$ and $[n+1:2n]$ respectively, so Γ has no edges between V_i and V_j.

Therefore all edges in $E(\Gamma)$ lie in $V_i \times V_{i+1}$ for $i \in [t-1]$. Each $v = (e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_t) \in V_i$ by definition has an edge to $v' = (e_1, \dots, e_i, e_{i+2}, \dots, e_t) \in V_{i+1}$ for every $e_i \in [n+1:2n]$, so the claim follows.

It also follows that Γ is bipartite, with left vertices $V_1 \sqcup V_3 \sqcup \cdots$ and right vertices $V_2 \sqcup V_4 \sqcup \cdots$. Each vertex in V_i has n neighbors in V_{i-1} (unless $i = 1$) and n neighbors in V_{i+1} (unless $i = t$), so Equation (19) follows. □

In light of Claim 4.2, we may view edges in $E(\Gamma)$ as elements of $E = \bigsqcup_{i \in [t-1]} E_i$, where a vertex $v \in V_i$ lies in an edge $e \in E$ if $e \in \mathrm{col}_i(v)$.

With this view, we are ready to define the system of local codes $\mathcal{F} = \mathcal{F}(C_1, \dots, C_t)$ on Γ. For a vertex $v \in V_i$ for some $i \in [t]$, we choose $\mathcal{F}_{v \to E(v)}$ to give local code

$$\mathrm{im}(\mathcal{F}_{v \to E(v)}) = C_i|_{\mathrm{col}_i(v) \cap E}.$$

To make sense of this definition, recall that the set $\mathrm{col}_i(v) = [2n]^{\{i\}} \times v \cong [2n]$ is naturally in bijection with the $2n$ components of $C_i \subseteq \mathbb{F}_q^{2n}$. Meanwhile, the first n elements of $\mathrm{col}_i(v)$ lie in E_{i-1} (unless $i = 1$ in which case they lie outside E), and the last n elements of $\mathrm{col}_i(v)$ lie in E_i (unless $i = t$ in which case they lie outside E). Hence $\mathrm{im}(\mathcal{F}_{v \to E(v)}) = C_i$ for every $2 \le i \le t-1$, while for $i = 1$ or $i = t$ then $\mathrm{im}(\mathcal{F}_{v \to E(v)})$ is obtained by restricting C_i to the last or first n components, respectively.

Claim 4.3. *Let* $C = \bigotimes_{i \in [t]} C_i \subseteq \mathbb{F}_q^{[2n]^t}$. *Then the restriction map* $\mathrm{Res}_E : \mathbb{F}_q^{[2n]^t} \to \mathbb{F}_q^E$ *induces an isomorphism* $\mathrm{Res}_E|_C : C \xrightarrow{\sim} \mathrm{T}(\Gamma, \mathcal{F})$.

Proof. We show the result by induction on t. For the base case, when $t = 2$, we have $E = E_1 = [n+1:2n] \times [1:n]$. Hence by definition of the local codes,

$$\mathrm{T}(\Gamma, \mathcal{F}) = (C_1|_{[n+1:2n]}) \otimes (C_2|_{[1:n]}).$$

On the other hand, $C|_E = (C_1|_{[n+1:2n]}) \otimes (C_2|_{[1:n]})$, and hence $\mathrm{T}(\Gamma, \mathcal{F}) = C|_E$.

Furthermore, since $d_1, d_2 > n$, the restriction map from each C_i to its puncturing is an isomorphism. Therefore $\mathrm{Res}_E|_C : C \to \mathrm{T}(\Gamma, \mathcal{F})$ is an isomorphism.

For the inductive step, let $t > 2$, and assume the claim holds for $t-1$. By definition $\mathrm{Res}_E(C) = C|_E$ lies inside $\mathrm{T}(\Gamma, \mathcal{F})$, as every constraint of $\mathrm{T}(\Gamma, \mathcal{F})$ simply checks consistency with C_i inside some subset of some direction-i column for some $i \in [t]$. Furthermore, $\mathrm{Res}_E|_C$ is injective: for $c \in C$ with $c|_E = 0$, then $c|_{E_1} = c|_{[n+1:2n]\times[1:n]^{t-1}} = 0$, so $c = 0$ because every C_i has distance $d_i > n$ (similarly as in the $t = 2$ case above).

Hence it remains to show that $\mathrm{Res}_E|_C$ is surjective onto $\mathrm{T}(\Gamma, \mathcal{F})$. For this purpose, fix some $c \in \mathrm{T}(\Gamma, \mathcal{F})$. We will construct some $c'' \in C$ with $c''|_E = c$. First, for each $j \in [1 : n]$, we define a subgraph $\Gamma|_{t\to j}$ of Γ consisting of those vertices and edges that are entirely contained in $[2n]^{[t-1]} \times \{j\}^{\{t\}} \subseteq [2n]^{[t]}$. Formally, for $i \in [t-1]$, let $V_i|_{t\to j} \subseteq V_i$ be the set of vertices $v \in V_i$ with $v_t = j$, and let $E_i|_{t\to j} \subseteq E_i$ be the set of edges $e \in E_i$ with $e_t = j$. Then we let

$$V(\Gamma|_{t\to j}) = \bigsqcup_{i\in[t-1]} V_i|_{t\to j}$$
$$E(\Gamma|_{t\to j}) = \bigsqcup_{i\in[t-2]} E_i|_{t\to j}$$

For each $j \in [1 : n]$, by definition $\Gamma|_{t\to j}$ is isomorphic to $\Gamma(n, t-1)$ (recall here that $\Gamma = \Gamma(n, t)$). It follows that the restriction of $\mathrm{T}(\Gamma, \mathcal{F})$ to components in $E(\Gamma|_{t\to j})$ must lie inside the code $\mathrm{T}(\Gamma(n, t-1), \mathcal{F}(C_1, \ldots, C_{t-1}))$ (recall that $\mathcal{F} = \mathcal{F}(C_1, \ldots, C_t)$), as every local code constraint in the latter Tanner code is also a constraint in the former. Then by the inductive hypothesis, for each $j \in [1 : n]$ there exists some $c'_j \in C_1 \otimes \cdots \otimes C_{t-1}$ such that $c'_j|_{E(\Gamma(n,t-1))} = c|_{E(\Gamma|_{t\to j})}$. Letting $c' = (c'_1, \ldots, c'_n) \in (C_1 \otimes \cdots \otimes C_{t-1}) \otimes \mathbb{F}_q^{[1:n]}$, then it follows that

$$c'|_{E_i} = c|_{E_i} \quad \forall i \in [t-2]. \tag{20}$$

Now recall that every vertex $v \in V_{t-1}$ imposes a constraint on $c \in \mathrm{T}(\Gamma, \mathcal{F})$ that requires the $2n$ components of c in $\mathrm{col}_{t-1}(v) \subseteq E$ to form a codeword in C_{t-1}. The first n components of c in $\mathrm{col}_{t-1}(v)$ lie inside E_{t-2}, and hence agree with c' by Equation (20). Then because C_{t-1} has distance $d_{t-1} > n$, the last n components of c in $\mathrm{col}_{t-1}(v)$, which lie inside E_{t-1}, also must agree with c'. Applying this argument to every $v \in V_{t-1}$, we conclude that

$$c'|_{E_{t-1}} = c|_{E_{t-1}}. \tag{21}$$

Now every vertex $v \in V_t$ imposes a constraint on $c \in \mathrm{T}(\Gamma, \mathcal{F})$ that requires the n components of c in $\mathrm{col}_t(v) \cap E_{t-1} \subseteq E$ to form a codeword in $C_t|_{[1:n]}$. It follows that $c'|_{E_{t-1}} = c|_{E_{t-1}}$ in fact lies inside $(C_1 \otimes \cdots \otimes C_{t-1}) \otimes C_t|_{[1:n]}$. Then because $E_{t-1} = [n+1 : 2n]^{[1:t-1]} \times [1 : n]^{\{t\}}$ and every C_i has distance $d_i > n$, there exists a unique $c'' \in C = C_1 \otimes \cdots \otimes C_t$ for which $c''|_{E_{t-1}} = c'|_{E_{t-1}}$, and $c''|_{[2n]^{t-1}\times[1:n]} = c'$. Thus $c''|_E = c'|_E$, which equals $c|_E$ by Equations (20) and (21), as desired. □

Proof of Theorem 4.1. It only remains to show that $\mathrm{T}(\Gamma, \mathcal{F})$ has parameters $[N, K, D]_q$ and a radius-ρ time-T decoder as given in the statement of Theorem 4.1. The length is by definition

$$N = |E| = \sum_{i\in[t-1]} |E_i| = (t-1)n^t.$$

Letting $C = \bigotimes_{i\in[t]} C_i$, by Claim 4.3 the dimension of $\mathrm{T}(\Gamma, \mathcal{F})$ is

$$K = \dim(C) = \prod_{i\in[t]} k_i.$$

Also by Claim 4.3, the distance D of $\mathrm{T}(\Gamma, \mathcal{F})$ is at least the minimum value of $|c|_{E_1}|$ for any nonzero $c \in C$. Because $E_1 = [n+1:2n] \times [1:n]^{t-1}$, we have

$$C|_{E_1} = \left(C_1|_{[n+1:2n]}\right) \otimes \bigotimes_{i=2}^{t} \left(C_i|_{[1:n]}\right)$$

and each factor has distance at least $d_i - n$. Hence the minimum distance of $C|_{E_1}$ is at least $\prod_{i\in[t]}(d_i - n)$.

To show that $\mathrm{T}(\Gamma, \mathcal{F})$ has a radius-$\rho = \prod_{i\in[t]} \rho_i$ time-$T = (t-1)n^{t-1} \sum_{i\in[t]} T_i$ decoder, it suffices to show that the restriction $\mathrm{T}(\Gamma, \mathcal{F})|_{E_i}$ to each E_i has a radius-ρ time-$n^{t-1} \sum_{i\in[t]} T_i$ decoder, as then we can decode the restriction to each E_i independently. But by Claim 4.3, each such restriction $\mathrm{T}(\Gamma, \mathcal{F})|_{E_i}$ is the tensor product of t length-n codes, where the ith factor is either $C_i|_{[1:n]}$ or $C_i|_{[n+1:2n]}$. The statement of Theorem 4.1 assumes that each such factor code has a radius-ρ_i time-T_i decoder. Hence by Lemma 2.6, their tensor product $\mathrm{T}(\Gamma, \mathcal{F})|_{E_i}$ has a radius-ρ time-$n^{t-1} \sum_{i\in[t]} T_i$ decoder, as desired. □

5 Instantiations of High-Yield Transversal Gates

In this section, we present instantiations of quantum codes that have transversal gates with close-to-linear logical yield and good locality. Specifically, we instantiate the transversal gate construction in Theorem 3.1 with classical Tanner codes from Theorem 4.1, in various parameter regimes. Our main instantiations are described in the corollaries below, which we will prove in Section 5.2.

We begin with the construction in Corollary 5.1 below, which has constant locality (i.e. constant stabilizer weight). In this construction, we apply Theorem 4.1 with a high-dimensional tensor product of constant-sized algebraic geometry codes.

Corollary 5.1. *For every integer $r \geq 3$, every $0 < \epsilon < 1$, and every prime p, there exists an infinite family of r-tuples of*

$$[[N,\ K \geq N^{1-\epsilon},\ D \geq N^{(1-\epsilon)/r}]]_q$$

quantum codes $(Q^{(i)}, L^{(i)})_{i\in[r]}$ of locality $O_{r,\epsilon}(1)$ and alphabet size $q = p^u$ for $u = O_r(1)$ with block lengths $N \to \infty$, which support transversal $C^{r-1}Z$ gates of sparsity $O_{r,\epsilon}(1)$ and logical yield $\geq N^{1-\epsilon}$. These codes support radius-$N^{(1-\epsilon)/r}$ time-$\mathrm{poly}(N)$ decoders.

We next show how to slightly improve the distance, from $N^{(1-\epsilon)/r}$ in Corollary 5.1 above to $N^{1/r}/\mathrm{poly}(\log N)$ in Corollary 5.2 below, by applying Theorem 4.1 with slowly growing factor codes. Specifically, the length of the factor codes grows polylogarithmically with respect to the length of the final product code. As a result, our codes in Corollary 5.2 also have polylogarithmic locality (rather than the constant locality in Corollary 5.1). We include Corollary 5.2 below primarily to demonstrate that we can recover the precise parameter regimes achieved in [GL25].

Corollary 5.2. *For every integer $r \geq 3$, every $0 < \epsilon < 1$, and every prime p, there exists an infinite family of r-tuples of*

$$[[N,\ K \geq N^{1-\epsilon},\ D \geq N^{1/r}/(\log N)^{O_{r,\epsilon}(1)}]]_q$$

quantum codes $(Q^{(i)}, L^{(i)})_{i\in[r]}$ of locality $(\log N)^{O_{r,\epsilon}(1)}$ and alphabet size $q = p^u$ for $u = \Theta_{r,\epsilon}(\log_p(\log N))$ with block lengths $N \to \infty$, which support transversal $C^{r-1}Z$ gates of sparsity $(\log N)^{O_{r,\epsilon}(1)}$ and logical yield $\geq N^{1-\epsilon}$.

Whereas Corollaries 5.1 and 5.2 above both have dimension and logical yield $N^{1-\epsilon}$, we show in Corollary 5.3 below how to achieve linear dimension and logical yield $\Theta(N)$. The cost is that the locality now grows as a small polynomial N^ϵ.

Corollary 5.3. *For every integer $r \geq 3$, every $0 < \epsilon < 1$, and every prime p, there exists an infinite family of r-tuples of*

$$[[N,\ K \geq \Omega_{r,\epsilon}(N),\ D \geq \Omega_{r,\epsilon}(N^{1/r})]]_q$$

quantum codes $(Q^{(i)}, L^{(i)})_{i\in[r]}$ of locality N^ϵ and alphabet size $q = p^u$ for $u = O_r(1)$ with block lengths $N \to \infty$, which support transversal $C^{r-1}Z$ gates of sparsity N^ϵ and logical yield $\geq \Omega_{r,\epsilon}(N)$. These codes support radius-$\Omega_{r,\epsilon}(N^{1/r})$ time-$\mathrm{poly}(N)$ decoders.

The alphabet sizes, as well as the sparsities of the transversal gates, in Corollaries 5.1 to 5.3 above are large constants or slowly-growing functions of the block length. However, these quantities can be reduced to small constants using known techniques, with just a small degradation in other parameters. Specifically, [GL25, Lemma 3.44] shows that the alphabet size can be reduced from $q = p^u$ down to an arbitrary power of p (including down to p itself) with just a multiplicative $u^{O_r(1)}$ loss in other parameters. Similarly, [GL25, Lemma 3.45] shows that the transversal gate sparsity can be reduced from w to 1, with just a multiplicative $w^{O(1)}$ loss in other parameters. We omit the details on these transformations to avoid redundancy with [GL25], and rather refer the reader to the statements there.

While we use the classical Tanner codes from Theorem 4.1 to prove all three corollaries above, we remark that Corollary 5.2 can be recovered by instead using the classical codes in [GL25, Section 4]. Also, a result similar to Corollary 5.3 can be recovered by instead using the classical codes in [KT26], though the codes of [KT26] have alphabet size growing with the block length, and hence would require alphabet reduction to recover the constant alphabet size in Corollary 5.3. Indeed, both [GL25, Section 4] and [KT26] provide classical Tanner codes on carefully designed graphs to ensure high rate when using local Reed-Solomon codes with a multiplication property. These graphs have the additional advantage of being good spectral expanders, which may have benefits such as for single-shot error-correction (see e.g. [FGL18, GTC+24]). In contrast, while we do not show any spectral expansion bound for our graphs in Theorem 4.1, our Tanner codes are arguably simpler to construct. Furthermore, the constructions of [GL25, Section 4] and [KT26] require graphs of super-constant degree, so they cannot be used to obtain codes of constant locality (i.e. LDPC) as in Corollary 5.1.

5.1 Algebraic Classical Codes

In this section, we state the parameters of some well-known families of (non-LDPC) classical codes with a multiplication property. We will instantiate the Tanner codes in Theorem 4.1 with these codes.

We first state the parameters of Reed-Solomon codes in Lemma 5.4 below, whose codewords consist of evaluations on $2n$ points of degree $< k$ polynomials over a finite field $\mathbb{F}_q$. These codes satisfy a multiplication property because the product of r polynomials of degree $< k$ is a polynomial of degree $< r(k-1)+1$. For details on Reed-Solomon codes, see for instance [GRS22, Chapter 5].

Lemma 5.4 (Reed-Solomon codes; well known, see e.g. [GRS22])**.** *For every integer $r \geq 2$, every prime power q, and every choice of integers $n \leq q/2$ and $k < 2n/r + 1$, there exists a $[2n, k, 2n-k+1]_q$ classical code C, such that C^{*r} is a $[2n, r(k-1)+1, 2n-r(k-1)]_q$ code.*

We state the parameters of algebraic geometry (AG) codes in Lemma 5.5 below. These codes reduce the alphabet size of Reed-Solomon codes to a constant, at the cost of a slightly worse rate-distance tradeoff. The statement below for instance follows directly from [CR21, Theorem 21, & Section 4.2] (rate and distance bounds), [CR21, Equation (17)] (multiplication property, i.e. expression for C^{*r-1}), and [CR21, Theorem 75] (polynomial-time decoder).

Lemma 5.5 (Algebraic geometry codes [GS95, SV90])**.** *Fix an integer $r \geq 2$ and a prime p. Then for infinitely many $n \in \mathbb{N}$, there exist codes C with parameters $[2n, k, d]_q$ such that $k \geq n/4r$, $d \geq 3n/2$, $q = p^u$ for some integer $u = O_r(1)$, and such that C^{*r-1} has distance $d' \geq 3n/2$. Furthermore, all four restricted codes*

$$C|_{[1:n]},\ C|_{[n+1:2n]},\ C^{*r-1}|_{[1:n]},\ C^{*r-1}|_{[n+1:2n]} \tag{22}$$

have radius-$n/4$ time-$\mathrm{poly}(n)$ decoders.

Note that in Lemma 5.5, the restriction (i.e. puncturing) of an AG code to a subset of coordinates is still an AG code, so known decoders (e.g. [SV90]) can be applied.

5.2 Tanner Code Instantiations

We now apply the codes in Section 5.1 to prove the corollaries stated at the start of Section 5.

Proof of Corollary 5.1. By Lemma 5.5, for infinitely many $n \in \mathbb{N}$ there exist codes C with parameters $[2n, k, d]_q$ such that $k \geq n/4r$, $d \geq 3n/2$, $q = p^u$ for some integer $u = O_r(1)$, and such that C^{*r-1} has distance $d' \geq 3n/2$. Furthermore, all four restricted codes in Equation (22) have radius-$n/4$ time-$\mathrm{poly}(n)$ decoders. We fix some $n = n(r, \epsilon)$ sufficiently large such that $k \geq n/4r \geq n^{1-\epsilon/2}$, so that $n/4$ and $d' - n,\ d - n \geq n/2$ are also at least $n^{1-\epsilon/2}$.

Then for $t \in \mathbb{N}$, let $\Gamma = \Gamma(n, t)$ and $\mathcal{F} = \mathcal{F}(C_1 = C, \ldots, C_t = C)$ be defined as in Theorem 4.1. We now think of r, ϵ and $n = n(r, \epsilon)$ as fixed while $t \to \infty$. Then by Theorem 4.1, $\mathrm{T}(\Gamma, \mathcal{F})$ has length $N_0 = (t-1)n^t$ with $t = \Theta_{r,\epsilon}(\log N_0)$, and has dimension $K_0 = k^t \geq n^{(1-\epsilon/2)t}$ and distance $D_0 \geq (d-n)^t \geq n^{(1-\epsilon/2)t}$, such that $\mathrm{T}(\Gamma, \mathcal{F}^{*r-1})$ also has distance $D_0' \geq (d'-n)^t \geq n^{(1-\epsilon/2)t}$. Theorem 4.1 also implies that $\mathrm{T}(\Gamma, \mathcal{F})$ and $\mathrm{T}(\Gamma, \mathcal{F}^{*r-1})$ have radius-$\rho_0 = (n/4)^t \geq n^{(1-\epsilon/2)t}$ time-$\mathrm{poly}(n^t) = \mathrm{poly}(N_0)$ decoders. Here by definition $n^{(1-\epsilon/2)t} \geq \Omega_{r,\epsilon}(N_0/\log N_0)^{1-\epsilon/2}$.

We now apply Theorem 3.1 with Γ and with $\mathcal{F}^{(1)} = \cdots = \mathcal{F}^{(r-1)} = \mathcal{F}$ and $\mathcal{F}^{(r)} = \mathcal{F}^{*r-1}$. We let M be any maximal extendable set of $\mathrm{T}(\Gamma, \mathcal{F})$, so that $|M| = K_0$. Assuming t is sufficiently large, then by Theorem 3.1, the resulting subsystem codes $(Q^{(i)}, L^{(i)})$ have length $N = \Theta_r(N_0)^r$, distance

$$D \geq \min\{(D_0/n)^{r-1}, D_0'\} \geq N^{(1-\epsilon)/r},$$

locality $O_{r,\epsilon}(1)$, and support transversal $C^{r-1}Z$ gates of sparsity $O_{r,\epsilon}(1)$ with logical yield at least

$$|M|^r = K_0^r \geq N^{1-\epsilon}.$$

The codes' dimension is at least the logical yield $K \geq |M|^r \geq N^{1-\epsilon}$. Theorem 3.1 also implies that each $(Q^{(i)}, L^{(i)})$ has a radius-$\rho = \min\{(\rho_0/2n)^{r-1}, \rho_0\} \geq N^{(1-\epsilon)/r}$ time-poly(N) decoder. □

Proof of Corollary 5.2. By Lemma 5.4, for every $n \in \mathbb{N}$ there exists a code C with parameters $[2n, k, d]_q$ such that $k = \lceil n^{1-\epsilon/2} \rceil$, $d = 2n - (k-1)$, $q = p^u$ where $u = \lceil \log_p(2n) \rceil$, and such that C^{*r-1} has distance $d' = 2n - (r-1)(k-1)$. We let $t = t(\epsilon, n) = \lceil n^{\epsilon/4} \rceil$, and we think of $n \to \infty$ as r, ϵ remain fixed.

Then let $\Gamma = \Gamma(n, t)$ and $\mathcal{F} = \mathcal{F}(C_1 = C, \ldots, C_t = C)$ be defined as in Theorem 4.1. By Theorem 4.1, $\mathrm{T}(\Gamma, \mathcal{F})$ has length $N_0 = (t-1)n^t$ with $t, n = (\log N_0)^{\Theta_\epsilon(1)}$, dimension

$$K_0 = k^t \geq n^{(1-\epsilon/2)t} \geq N_0^{1-\epsilon/2}/(\log N_0)^{\Theta_\epsilon(1)},$$

and distance

$$D_0 \geq (d-n)^t \geq (n - n^{1-\epsilon/2})^t \geq n^t \cdot (1 - n^{-\epsilon/2})^{n^{\epsilon/4}} = \Theta(n^t) \geq N_0/(\log N_0)^{\Theta_{r,\epsilon}(1)},$$

such that $\mathrm{T}(\Gamma, \mathcal{F}^{*r-1})$ has distance satisfying the same bound $D_0' \geq (d'-n)^t \geq N_0/(\log N_0)^{\Theta_{r,\epsilon}(1)}$.

We now apply Theorem 3.1 with Γ and with $\mathcal{F}^{(1)} = \cdots = \mathcal{F}^{(r-1)} = \mathcal{F}$ and $\mathcal{F}^{(r)} = \mathcal{F}^{*r-1}$. We let M be any maximal extendable set of $\mathrm{T}(\Gamma, \mathcal{F})$, so that $|M| = K_0$. Assuming n is sufficiently large, then by Theorem 3.1, the resulting subsystem codes $(Q^{(i)}, L^{(i)})$ have length $N = \Theta_r(N_0)^r/n^{O_r(1)} = \Theta_r(N_0)^r/(\log N_0)^{O_{r,\epsilon}(1)}$ (where here we divide $\Theta_r(N_0)^r$ by $n^{O_r(1)}$ to account for the fact that $|C^0(\Gamma, \mathcal{F}^{(i)})|$ may be smaller than $N_0 = |C^1(\Gamma, \mathcal{F}^{(i)})|$ by a factor of $O(n^{\epsilon/2})$, as the local code C has dimension $\lceil n^{1-\epsilon/2} \rceil$), distance

$$D \geq \min\{(D_0/n)^{r-1}, D_0'\} \geq N^{1/r}/(\log N)^{\Theta_{r,\epsilon}(1)},$$

locality $\leq r(2n)^2 \leq (\log N)^{\Theta_{r,\epsilon}(1)}$, and support transversal $C^{r-1}Z$ gates of sparsity $\leq (8n)^{r^2} \leq (\log N)^{\Theta_{r,\epsilon}(1)}$ with logical yield at least

$$|M|^r = K_0^r \geq N^{1-\epsilon}.$$

The codes' dimension is at least the logical yield $K \geq |M|^r \geq N^{1-\epsilon}$.

Because $n = (\log N_0)^{\Theta_\epsilon(1)} = (\log N)^{\Theta_{r,\epsilon}(1)}$, our codes have alphabet size $q = p^u$ for

$$u = \lceil \log_p(2n) \rceil = \Theta_{r,\epsilon}(\log_p(\log N)).$$

□

Proof of Corollary 5.3. By Lemma 5.5, for infinitely many $n \in \mathbb{N}$ there exist codes C with parameters $[2n, k, d]_q$ such that $k \geq n/4r$, $d \geq 3n/2$, $q = p^u$ for some integer $u = O_r(1)$, and such that C^{*r-1} has distance $d' \geq 3n/2$. Furthermore, all four restricted codes in Equation (22) have radius-$n/4$ time-poly(n) decoders. We fix $t = t(r, \epsilon) = \lceil 2r^2/\epsilon \rceil$, and think of $n \to \infty$ as r, ϵ, t remain fixed.

Then let $\Gamma = \Gamma(n, t)$ and $\mathcal{F} = \mathcal{F}(C_1 = C, \ldots, C_t = C)$ be defined as in Theorem 4.1. By Theorem 4.1, $\mathrm{T}(\Gamma, \mathcal{F})$ has length $N_0 = (t-1)n^t = \Theta_{r,\epsilon}(n^t)$, dimension $K_0 = k^t \geq \Omega_{r,\epsilon}(N_0)$, and

distance $D_0 \geq (d-n)^t \geq \Omega_{r,\epsilon}(N_0)$, such that $\mathrm{T}(\Gamma, \mathcal{F}^{*r-1})$ also has distance $D_0' \geq (d'-n)^t \geq \Omega_{r,\epsilon}(N_0)$. Theorem 4.1 also implies that $\mathrm{T}(\Gamma, \mathcal{F})$ and $\mathrm{T}(\Gamma, \mathcal{F}^{*r-1})$ have radius-$\rho_0 = (n/4)^t \geq \Omega_{r,\epsilon}(N_0)$ time-poly$(n^t) = \mathrm{poly}(N_0)$ decoders.

We now apply Theorem 3.1 with Γ and with $\mathcal{F}^{(1)} = \cdots = \mathcal{F}^{(r-1)} = \mathcal{F}$ and $\mathcal{F}^{(r)} = \mathcal{F}^{*r-1}$. We let M be any maximal extendable set of $\mathrm{T}(\Gamma, \mathcal{F})$, so that $|M| = K_0$. Assuming n is sufficiently large, and recalling that

$$N = \Theta_{r,\epsilon}(N_0^r) = \Theta_{r,\epsilon}(n^{rt}) \geq \Omega_{r,\epsilon}(n^{2r^3/\epsilon}),$$

then by Theorem 3.1, the resulting subsystem codes $(Q^{(i)}, L^{(i)})$ have length N, distance

$$D \geq \min\{(D_0/n)^{r-1}, D_0'\} \geq \Omega_{r,\epsilon}(N^{1/r}),$$

locality $\leq r(2n)^2 \leq N^\epsilon$, and support transversal $C^{r-1}Z$ gates of sparsity $\leq (8n)^{r^2} \leq N^\epsilon$ with logical yield at least

$$|M|^r = K_0^r \geq \Omega_{r,\epsilon}(N).$$

The codes' dimension is at least the logical yield $K \geq |M|^r \geq \Omega_{r,\epsilon}(N)$. Theorem 3.1 also implies that each $(Q^{(i)}, L^{(i)})$ has a radius-$\rho = \min\{(\rho_0/2n)^{r-1}, \rho_0\} \geq \Omega_{r,\epsilon}(N^{1/r})$ time-poly(N) decoder. □

6 Acknowledgments

L.G. acknowledges support from ONR grant N00014-24-1-2491, a UC Noyce initiative award, a Google PhD Fellowship, and a National Science Foundation Graduate Research Fellowship under Grant No. DGE 2146752. G.Z. is supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Co-design Center for Quantum Advantage (C2QA) under contract number DE-SC0012704.

AI disclosure: All proofs and writing are the work of the human authors. ChatGPT Pro was used to check the draft for typos and minor inconsistencies, and to find references.

References

[BDET24] Nikolas P. Breuckmann, Margarita Davydova, Jens N. Eberhardt, and Nathanan Tantivasadakarn. Cups and Gates I: Cohomology invariants and logical quantum operations, October 2024. arXiv:2410.16250.

[BE21] Nikolas P. Breuckmann and Jens N. Eberhardt. Balanced Product Quantum Codes. *IEEE Transactions on Information Theory*, 67(10):6653–6674, October 2021. Conference Name: IEEE Transactions on Information Theory.

[BFHS17] Dave Bacon, Steven T. Flammia, Aram W. Harrow, and Jonathan Shi. Sparse Quantum Codes from Quantum Circuits. *IEEE Transactions on Information Theory*, 63(4):2464–2479, April 2017. arXiv:1411.3334 [quant-ph].

[BH12] Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Physical Review A*, 86(5):052329, November 2012.

[BMD07a] H. Bombin and M. A. Martin-Delgado. Exact topological quantum order in $D=3$ and beyond: Branyons and brane-net condensates. *Physical Review B*, 75(7):075103, February 2007.

[BMD07b] H. Bombin and M. A. Martin-Delgado. Topological Computation without Braiding. *Physical Review Letters*, 98(16):160502, April 2007.

[Bom15] Héctor Bombín. Gauge color codes: optimal transversal gates and gauge fixing in topological stabilizer codes. *New Journal of Physics*, 17(8):083002, August 2015.

[Bom16] H. Bombin. Dimensional Jump in Quantum Error Correction, May 2016. arXiv:1412.5079 [quant-ph].

[CHRY24] Andrew Cross, Zhiyang He, Patrick Rall, and Theodore Yoder. Improved QLDPC Surgery: Logical Measurements and Bridging Codes, November 2024. arXiv:2407.18393 [quant-ph].

[CHWY26] Alexander Cowtan, Zhiyang He, Dominic J. Williamson, and Theodore J. Yoder. Parallel Logical Measurements via Quantum Code Surgery. *PRX Quantum*, 7(2):020325, May 2026.

[CKBB22] Lawrence Z. Cohen, Isaac H. Kim, Stephen D. Bartlett, and Benjamin J. Brown. Low-overhead fault-tolerant quantum computing using long-range connectivity. *Science Advances*, 8(20):eabn1717, May 2022.

[CR21] Alain Couvreur and Hugues Randriambololona. Algebraic Geometry Codes and Some Applications. In *Concise Encyclopedia of Coding Theory*. Chapman and Hall/CRC, 2021. Num Pages: 56.

[CXK+26] Madelyn Cain, Qian Xu, Robbie King, Lewis R. B. Picard, Harry Levine, Manuel Endres, John Preskill, Hsin-Yuan Huang, and Dolev Bluvstein. Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits, March 2026. arXiv:2603.28627 [quant-ph].

[DLV24] Irit Dinur, Ting-Chun Lin, and Thomas Vidick. Expansion of High-Dimensional Cubical Complexes: with Application to Quantum Locally Testable Codes. pages 379–385. IEEE Computer Society, October 2024.

[DLZ23] Irit Dinur, Siqi Liu, and Rachel Zhang. New Codes on High Dimensional Expanders, August 2023. ISSN: 1433-8092.

[FGL18] Omar Fawzi, Antoine Grospellier, and Anthony Leverrier. Constant overhead quantum fault-tolerance with quantum expander codes. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 743–754, October 2018. arXiv:1808.03821 [quant-ph].

[GCZ25] Louis Golowich, Kathleen Chang, and Guanyu Zhu. Constant-Overhead Addressable Gates via Single-Shot Code Switching, October 2025. arXiv:2510.06760 [quant-ph].

[GG25a] Louis Golowich and Venkatesan Guruswami. Asymptotically Good Quantum Codes with Transversal Non-Clifford Gates. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 707–717, New York, NY, USA, June 2025. Association for Computing Machinery.

[GG25b] Louis Golowich and Venkatesan Guruswami. Near-Asymptotically-Good Quantum Codes with Transversal CCZ Gates and Sublinear-Weight Parity-Checks. In *2025 IEEE 66th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1561–1569, December 2025. ISSN: 2575-8454.

[GG25c] Louis Golowich and Venkatesan Guruswami. Quantum LDPC Codes of Almost Linear Distance via Iterated Homological Products. In *Proceedings of the 40th Computational Complexity Conference*, CCC '25, pages 25:1–25:11, Dagstuhl, DEU, July 2025. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[Gid25] Craig Gidney. How to factor 2048 bit RSA integers with less than a million noisy qubits, May 2025. arXiv:2505.15917 [quant-ph].

[GL25] Louis Golowich and Ting-Chun Lin. Quantum LDPC Codes with Transversal Non-Clifford Gates via Products of Algebraic Codes. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 689–696, New York, NY, USA, June 2025. Association for Computing Machinery.

[Got14] Daniel Gottesman. Fault-tolerant quantum computation with constant overhead. *Quantum Information & Computation*, 14(15-16):1338–1372, November 2014.

[GRS22] Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. Essential coding theory. *Draft available at http://www. cse. buffalo. edu/ atri/courses/coding-theory/book*, 2022.

[GS95] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Inventiones mathematicae*, 121(1):211–222, December 1995.

[GTC+24] Shouzhen Gu, Eugene Tang, Libor Caha, Shin Ho Choe, Zhiyang He, and Aleksander Kubica. Single-Shot Decoding of Good Quantum LDPC Codes. *Communications in Mathematical Physics*, 405(3):85, March 2024.

[Hat01] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, Cambridge, UK, 2001.

[HVWZ25a] Zhiyang He, Vinod Vaikuntanathan, Adam Wills, and Rachel Yun Zhang. Asymptotically Good Quantum Codes with Addressable and Transversal Non-Clifford Gates, July 2025. arXiv:2507.05392 [quant-ph].

[HVWZ25b] Zhiyang He, Vinod Vaikuntanathan, Adam Wills, and Rachel Yun Zhang. Quantum Codes with Addressable and Transversal Non-Clifford Gates, February 2025. arXiv:2502.01864 [quant-ph].

[KP13] Alexey A. Kovalev and Leonid P. Pryadko. Fault tolerance of quantum low-density parity check codes with sublinear distance scaling. *Physical Review A*, 87(2):020304, February 2013.

[KP25] Gleb Kalachev and Pavel Panteleev. Maximally Extendable Product Codes are Good Coboundary Expanders. In *2025 IEEE 66th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1512–1524, December 2025. ISSN: 2575-8454.

[KRRZ+21] Swastik Kopparty, Nicolas Resch, Noga Ron-Zewi, Shubhangi Saraf, and Shashwat Silas. On List Recovery of High-Rate Tensor Codes. *IEEE Transactions on Information Theory*, 67(1):296–316, January 2021.

[KT26] Swastik Kopparty and Itzhak Tamo. Algebraic Expander Codes, March 2026. arXiv:2603.24788 [cs].

[Lin24] Ting-Chun Lin. Transversal non-Clifford gates for quantum LDPC codes on sheaves, October 2024. arXiv:2410.14631 [quant-ph].

[Lit19] Daniel Litinski. A Game of Surface Codes: Large-Scale Quantum Computing with Lattice Surgery. *Quantum*, 3:128, March 2019.

[LLL26] Yiming Li, Zimu Li, and Zi-Wen Liu. Transversal non-Clifford gates on almost-good quantum LDPC and quantum locally testable codes, July 2026. arXiv:2604.01874 [quant-ph] version: 2.

[LLLN25] Yiming Li, Zimu Li, Zi-Wen Liu, and Quynh T. Nguyen. Poincaré Duality and Multiplicative Structures on Quantum Codes, December 2025. arXiv:2512.21922 [quant-ph].

[LSW+26] Zimu Li, Yuguo Shao, Fuchuan Wei, Yiming Li, and Zi-Wen Liu. Theory of (Co)homological Invariants on Quantum LDPC Codes, March 2026. arXiv:2603.25831 [quant-ph].

[Ngu25] Quynh T. Nguyen. Good Binary Quantum Codes with Transversal CCZ Gate. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 697–706, New York, NY, USA, June 2025. Association for Computing Machinery.

[NP25] Quynh T. Nguyen and Christopher A. Pattison. Quantum Fault Tolerance with Constant-Space and Logarithmic-Time Overheads. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 730–737, New York, NY, USA, June 2025. Association for Computing Machinery.

[PK22a] Pavel Panteleev and Gleb Kalachev. Asymptotically good Quantum and locally testable classical LDPC codes. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022, pages 375–388, New York, NY, USA, June 2022. Association for Computing Machinery.

[PK22b] Pavel Panteleev and Gleb Kalachev. Quantum LDPC Codes With Almost Linear Minimum Distance. *IEEE Transactions on Information Theory*, 68(1):213–229, January 2022. Conference Name: IEEE Transactions on Information Theory.

[PR13] Adam Paetznick and Ben W. Reichardt. Universal Fault-Tolerant Quantum Computation with Only Transversal Gates and Error Correction. *Physical Review Letters*, 111(9):090505, August 2013.

[QC22] Armanda O. Quintavalle and Earl T. Campbell. ReShape: A Decoder for Hypergraph Product Codes. *IEEE Transactions on Information Theory*, 68(10):6569–6584, October 2022. Conference Name: IEEE Transactions on Information Theory.

[SPW24] Thomas R. Scruby, Arthur Pesah, and Mark Webster. Quantum Rainbow Codes, August 2024. arXiv:2408.13130 [quant-ph].

[SS96] M. Sipser and D.A. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, November 1996.

[SV90] A.N. Skorobogatov and S.G. Vladut. On the decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 36(5):1051–1060, September 1990.

[THL+25] Shi Jie Samuel Tan, Yifan Hong, Ting-Chun Lin, Michael J. Gullans, and Min-Hsiu Hsieh. Single-Shot Universality in Quantum LDPC Codes via Code-Switching, October 2025. arXiv:2510.08552 [quant-ph].

[TZ14] Jean-Pierre Tillich and Gilles Zemor. Quantum LDPC codes with positive rate and minimum distance proportional to n^{1/2}. *IEEE Transactions on Information Theory*, 60(2):1193–1202, February 2014. arXiv: 0903.0566.

[WHY24] Adam Wills, Min-Hsiu Hsieh, and Hayata Yamasaki. Constant-Overhead Magic State Distillation, August 2024. arXiv:2408.07764 [quant-ph].

[XAP+23] Qian Xu, J. Pablo Bonilla Ataides, Christopher A. Pattison, Nithin Raveendran, Dolev Bluvstein, Jonathan Wurtz, Bane Vasic, Mikhail D. Lukin, Liang Jiang, and Hengyun Zhou. Constant-Overhead Fault-Tolerant Quantum Computation with Reconfigurable Atom Arrays, August 2023. arXiv:2308.08648 [quant-ph].

[XZB+25] Qian Xu, Hengyun Zhou, Dolev Bluvstein, Madelyn Cain, Marcin Kalinowski, John Preskill, Mikhail D. Lukin, and Nishad Maskara. Batched high-rate logical operations for quantum LDPC codes, October 2025. arXiv:2510.06159 [quant-ph].

[YSR+25] Theodore J. Yoder, Eddie Schoute, Patrick Rall, Emily Pritchett, Jay M. Gambetta, Andrew W. Cross, Malcolm Carroll, and Michael E. Beverland. Tour de gross: A modular quantum computer based on bivariate bicycle codes, June 2025. arXiv:2506.03094 [quant-ph].

[Zhu25] Guanyu Zhu. A topological theory for qLDPC: non-Clifford gates and magic state fountain on homological product codes with constant rate and beyond the $N^{1/3}$ distance barrier, January 2025. arXiv:2501.19375 [quant-ph].

[ZSP+23] Guanyu Zhu, Shehryar Sikander, Elia Portnoy, Andrew W. Cross, and Benjamin J. Brown. Non-Clifford and parallelizable fault-tolerant logical gates on constant and almost-constant rate homological quantum LDPC codes via higher symmetries, October 2023. arXiv:2310.16982 [cond-mat, physics:hep-th, physics:quant-ph].

A Addressable Gates

In this section, we describe how to render our transversal $C^{r-1}Z$ gates *addressable*. That is, in Section 2.2 we defined a transversal $C^{r-1}Z$ gate with logical yield s to be a (low-depth) physical circuit that induces logical $C^{r-1}Z$ gates on some s disjoint r-tuples of qudits under some choice of logical basis. However, if we fix the code and logical basis, we could ask for different low-depth

physical circuits implementing logical $C^{r-1}Z$ gates on different choices of qudits. Such flexibility in the choice of logical action is referred to as *addressability* (see e.g. [HVWZ25b, HVWZ25a]). We will specifically show how to extend Theorem 3.1, and as a consequence Corollaries 5.1 to 5.3, to obtain such addressability.

A typical form of addressability is the ability to perform $C^{r-1}Z$ gates on arbitrary subsets of a pre-specified collection of r-tuples of logical qudits (with a pre-specified choice of basis). This form of addressability is immediately implied by the ability to perform C^rZ gates. Specifically, we can partition qudits into $(r+1)$-tuples, and place the first qudit in each tuple in a computational basis "control" state. A control value of $|a\rangle$ ensures that applying C^rZ to the tuple induces the action of $C^{r-1}Z^a$ on the remaining r qudits in the tuple.

In our setting of transversal gates across code blocks, this idea allows us to use transversal C^rZ across $r+1$ code blocks to implement addressable $C^{r-1}Z$ across r code blocks. Indeed, we simply use the first code block as a control block. This block's logical state is always a computational basis state, and can be modified by applying (depth-1) logical Pauli-X operators. Applying our transversal C^rZ gate then induces addressable $C^{r-1}Z$ on the remaining r code blocks.

One downside of this approach is that our main constructions of codes supporting transversal $C^{r-1}Z$ all have distance at most $O(N^{1/r})$, where N denotes the block length (Corollaries 5.1 to 5.3). Therefore addressable $C^{r-1}Z$ via transversal C^rZ would require codes of distance $O(N^{1/(r+1)})$, which is lower than the distance $O(N^{1/r})$ of our codes with non-addressable transversal $C^{r-1}Z$. Below, we describe how to modify our construction to increase the distance back to $O(N^{1/r})$ while retaining addressable $C^{r-1}Z$. We begin with a formal definition of addressable gates.

Definition A.1. *We say subsystem codes $(Q^{(i)}, L^{(i)})$ over $\mathbb{F}_q$ for $i \in [r]$ support a* addressable $C^{r-1}Z$ gates of sparsity w and logical yield s *if for every $i \in [r]$ there exist $z_1^{(i)}, \dots, z_s^{(i)} \in L_Z^{(i)}$ with the following property: for every $a \in \mathbb{F}_q^s$, there exists a cohomology-invariant form f_a (see Definitions 2.10 and 2.12) of sparsity w for which*

$$\tilde{f}_a(z_{\ell_1}^{(1)}, \dots, z_{\ell_r}^{(r)}) = a_{\ell_1} \cdot \mathbb{1}_{\ell_1 = \dots = \ell_r} \quad \forall \ell_1, \dots, \ell_r \in [s].$$

Similarly as described for (non-addressable) transversal gates in Section 2.2, an addressable $C^{r-1}Z$ gate of sparsity w and logical yield s in the sense of Definition A.1 provides, for every $a \in \mathbb{F}_q^s$, a physical circuit $C^{r-1}Z^{f_a}$ of depth rw (Fact 2.11) that implements logical $C^{r-1}Z^a = \bigotimes_{\ell=1}^s C^{r-1}Z^{a_\ell}$ on the s tuples of logical qudits respectively specified by $(z_\ell^{(1)}, \dots, z_\ell^{(r)})$ for $\ell \in [s]$.

We now provide our extension of Theorem 3.1 to addressable gates:

Theorem A.2. *Define all variables as in Section 3.1. Assume that we have an additional system of local codes $\mathcal{F}^{(0)}$ on Γ such that $M \subseteq E(\Gamma)$ is also an extendable set for $\mathrm{T}(\Gamma, \mathcal{F}^{(0)})$, and such that in place of Equation (9) we have*

$$\mathrm{im}(\mathcal{F}^{(0)}_{v \to E(v)}) * \mathrm{im}(\mathcal{F}^{(1)}_{v \to E(v)}) * \cdots * \mathrm{im}(\mathcal{F}^{(r-1)}_{v \to E(v)}) \subseteq \mathrm{im}(\mathcal{F}^{(r)}_{v \to E(v)}). \tag{23}$$

Then the quantum codes $Q^{(i)}$ at level 1 of $\mathcal{A}^{(i)}$ for $i \in [r]$ have subsystems $L^{(i)}$ that support addressable $C^{r-1}Z$ gates of sparsity $\leq (4\Delta)^{r^2}$ and logical yield $\geq |M|^r$. Furthermore, if for every $j \in [r]$ the classical code $\mathrm{T}(\Gamma, \mathcal{F}^{(j)})$ has distance $d^{(j)}$ and supports a radius-$\rho^{(j)}$ time-$\mathrm{poly}(\Delta, |V(\Gamma)|)$ decoder, then $(Q^{(i)}, L^{(i)})$ is a quantum subsystem code of locality $\leq r\Delta^2$, X-distance $d_X \geq d^{(r)}$, and Z-distance $d_Z \geq (2/\Delta)^{r-1} \cdot d^{(1)} d^{(2)} \cdots d^{(r-1)}$, which supports a radius-$\min\{\rho^{(1)} \cdots \rho^{(r-1)}/\Delta^{r-1}, \rho^{(r)}\}$ time-$\mathrm{poly}(\Delta, |V(\Gamma)|)^r$ decoder.

The proof of Theorem A.2 is similar to that of Theorem 3.1, with just some minor modifications. We therefore simply describe the necessary changes:

Proof sketch of Theorem A.2. The choice of subsystems $L^{(i)}$, and the associated distance and decoder analysis, are identical to those in Equation (12), Claim 3.7, Claim 3.8 respectively in the proof of Theorem 3.1. Therefore it remains to be shown that assuming Equation (23), the subsystem codes $(Q^{(i)}, L^{(i)})$ support addressable $C^{r-1}Z$ gates of sparsity $\leq (4\Delta)^{r^2}$ and logical yield $\geq |M|^r$.

For this purpose, for every $e^{(i)} = (e_1^{(i)}, \dots, e_r^{(i)}) \in M^r$, we define $z^{(i)}_{e^{(i)}} \in Z^1(\mathcal{A}^{(i)})$ as in Equation (17), so that the associated cohomology class $z^{(i)}_{e^{(i)}} + B^1(\mathcal{A}^{(i)})$ lies in $L_Z^{(i)}$, as shown in the proof of Theorem 3.1.

Our goal is then to show that for every $a \in \mathbb{F}_q^{M^r}$, there exists a cohomology-invariant form f_a of sparsity $\leq (4\Delta)^{r^2}$ for which

$$\tilde{f}_a(z^{(1)}_{e^{(1)}}, \dots, z^{(r)}_{e^{(r)}}) = a_{e^{(1)}} \cdot \mathbb{1}_{e^{(1)}=\cdots=e^{(r)}} \quad \forall e^{(1)}, \dots, e^{(r)} \in M^r. \tag{24}$$

To define f_a, we first observe that Equation (23) implies that all codewords in $\mathrm{im}(\mathcal{F}^{(0)}_{v\to E(v)}) * \mathrm{im}(\mathcal{F}^{(1)}_{v\to E(v)}) * \cdots * \mathrm{im}(\mathcal{F}^{(r-1)}_{v\to E(v)}) * \mathrm{im}(\mathcal{F}^{(r)}_{v\to E(v)})^\perp$ have entries summing to 0, or equivalently, that

$$\mathrm{im}(\mathcal{F}^{(1)}_{v\to E(v)}) * \cdots * \mathrm{im}(\mathcal{F}^{(r-1)}_{v\to E(v)}) * \mathrm{im}(\mathcal{F}^{(r)}_{v\to E(v)})^\perp \subseteq \mathrm{im}(\mathcal{F}^{(0)}_{v\to E(v)})^\perp.$$

Therefore because $M \subseteq E(\Gamma)$ is extendable for $\mathrm{T}(\Gamma, \mathcal{F}^{(0)}) = Z_1(\Gamma, \mathcal{F}^{(0)^\perp})$ (see Fact 2.21), then defining $\mathcal{C}' = \mathcal{C}^*(\Gamma, \mathcal{F}^{(1)} * \cdots * \mathcal{F}^{(r-1)} * \mathcal{F}^{(r)^\perp})$ as in Equation (13), it follows that $Z_1(\mathcal{C}') \supseteq \mathrm{T}(\Gamma, \mathcal{F}^{(0)})$, so M is also extendable for $Z_1(\mathcal{C}')$. Also defining $\mathcal{A}' = \mathcal{C}'^{\otimes r}$ as in Equation (13), then it furthermore follows that $M^r \subseteq E(\Gamma)^r$ is extendable for $Z_1(\mathcal{C}')^{\otimes r} = Z_r(\mathcal{A}')$, where the final equality holds by the Künneth formula. Thus there exists a cycle $z_a \in Z_r(\mathcal{A}')$ for which the restriction

$$z_a|_{M^r} = a. \tag{25}$$

We then define the multilinear form

$$f_a : \mathcal{A}^{(1)^1} \times \cdots \times \mathcal{A}^{(r)^1} \to \mathbb{F}$$

by

$$f_a(b^{(1)}, \dots, b^{(r)}) = \langle z_a, b^{(1)} \smile \cdots \smile b^{(r)} \rangle, \tag{26}$$

where the cup product $b^{(1)} \smile \cdots \smile b^{(r)} \in \mathcal{A}'^r$ in Equation (26) is defined using Definition 3.4 and Lemma 3.6 as in the proof of Claim 3.8 in Theorem 3.1.

Cohomology-invariance of f_a follows by an analogous argument as used to show Claim 3.10. Equation (24) then follows immediately from Equations (18) and (25). Meanwhile, f_a has sparsity $\leq (4\Delta)^{r^2}$ by the exact same proof as given in Claim 3.9 in the proof of Theorem 3.1. Thus the subsystem codes $(Q^{(i)}, L^{(i)})$ support addressable $C^{r-1}Z$ gates of sparsity $\leq (4\Delta)^{r^2}$ and logical yield $\geq |M|^r$, as desired. □

Theorem A.2 provides quantum codes with addressable $C^{r-1}Z$ gates given as input classical Tanner codes satisfying the multiplication property in Equation (23), analogously to how Theorem 3.1 provides quantum codes with (non-addressable) transversal $C^{r-1}Z$ gates given as input

classical Tanner codes satisfying the multiplication property in Equation (9). The only difference between these two multiplication properties is that Equation (23) takes the component-wise product of r factor codes, whereas Equation (9) only takes the product of $r-1$ factor codes. Our instantiations of Theorem 3.1 in Corollaries 5.1 to 5.3 (using Theorem 4.1) are based on the Reed-Solomon and algebraic-geometry codes in Lemmas 5.4 and 5.5, which satisfy multiplication properties for arbitrary constants r, up to changes in constant factors in the dimension and distance bounds. Hence Corollaries 5.1 to 5.3 also hold for addressable gates (as opposed to simply transversal gates), with the same parameters up to changes in the constants hidden by the big-Os.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il