Quantum Tanner codes

Anthony Leverrier, Gilles Zemor

Quantum Tanner codes

Anthony Leverrier* Gilles Zémor†

September 19, 2022

Abstract

Tanner codes are long error correcting codes obtained from short codes and a graph, with bits on the edges and parity-check constraints from the short codes enforced at the vertices of the graph. Combining good short codes together with a spectral expander graph yields the celebrated expander codes of Sipser and Spielman, which are asymptotically good classical LDPC codes.

In this work we apply this prescription to the left-right Cayley complex that lies at the heart of the recent construction of a c^3 locally testable code by Dinur *et al.* Specifically, we view this complex as two graphs that share the same set of edges. By defining a Tanner code on each of those graphs we obtain two classical codes that together define a quantum code. This construction can be seen as a simplified variant of the Panteleev and Kalachev asymptotically good quantum LDPC code, with improved estimates for its minimum distance. This quantum code is closely related to the Dinur *et al.* code in more than one sense: indeed, we prove a theorem that simultaneously gives a linearly growing minimum distance for the quantum code and recovers the local testability of the Dinur *et al.* code.

1 Introduction

1.1 Contributions

Constructing good linear error correcting codes has been a major endeavor of the information theory community since the early existence results of Shannon. In the past decades, codes have found new playgrounds in fields such as program checking, probabilistically checkable proofs or even quantum computing. Such applications require additional properties beside the capability to correct errors. For instance, a *locally testable code* (LTC) comes with the remarkable feature that it is possible to read a contant number of bits of a noisy message and estimate how far the message is from the code. In a recent breakthrough, Dinur *et al.* [DEL+21] showed that LTCs exist even when requiring constant rate, constant distance and constant locality. For quantum computing, codes must be able to correct two types of errors: (classical) bit flips and (quantum) phase flips. For this reason, one can define *quantum codes* by giving a pair of linear codes $\mathcal{C}_0, \mathcal{C}_1$ that

*Inria, France. anthony.leverrier@inria.fr
†Institut de Mathématiques de Bordeaux, UMR 5251, France. zemor@math.u-bordeaux.fr

will each correct one type of errors. These codes cannot be chosen arbitrarily: they must satisfy some compatibility condition that reads $\mathcal{C}_1 \supset \mathcal{C}_0^\perp$. Of major interest — for theory and experiments — are quantum low-density parity-check (LDPC) codes corresponding to the case when both $\mathcal{C}_0 = \ker H_0$ and $\mathcal{C}_1 = \ker H_1$ are defined by *sparse* parity-check matrices H_0 and H_1. Here, the major open question concerned the existence of good quantum LDPC codes displaying a constant rate and a constant (relative) distance, and was answered positively in the breakthrough work of Panteleev and Kalachev [PK21], which also provided an alternative construction of classical LTC.

A specific combinatorial object lies at the heart of the construction of the LTC of Dinur *et al.* [DEL$^+$21]: a *square complex*, and more specifically a *left-right Cayley complex*, which is a generalisation of expander graphs in higher dimension with cells of dimension 0 (vertices), 1 (edges) and 2 (squares, hence the name). We note that left-right Cayley complexes are also equal to balanced products of Cayley graphs, as introduced by Breuckmann and Eberhardt [BE21a]. Recalling the seminal expander codes of Sipser and Spielman [SS96] building on the ideas of Tanner [Tan81] to obtain good classical LDPC codes by putting the bits on the edges of an expander graph and the parity-check constraints on its vertices *via* codes of constant size, it is tempting to apply a similar recipe with higher dimensional objects such as square complexes. In that case, the bits are naturally placed on the 2-dimensional cells of the complex (squares) and the constraints are again enforced at the vertices. The novelty then is that the local view of a vertex becomes a matrix of bits, and allows one to put constraints corresponding to a small tensor product code. The consequence is far reaching: the redundancy between the row constraints and column constraints of the small tensor codes translates into a form of robustness, which can then propagate to the entire code through the square complex, giving in particular the LTCs of Dinur *et al.* when the square complex is sufficiently expanding.

In the present paper, we apply the Tanner code prescription to the quantum case and construct quantum codes with qubits on the squares and constraints on the vertices of a left-right Cayley complex. The condition $\mathcal{C}_1 \supset \mathcal{C}_0^\perp$ prevents the constraints to be those of small tensor codes, but should come from the dual of such tensor codes. We show that if the complex is sufficiently expanding (*e.g.* the complex of [DEL$^+$21]) and if the small dual tensor codes exhibit robustness (which is true with high probability for random codes [PK21]), then the construction gives rise to a family of asymptotically good LDPC codes displaying constant rate and linear minimal distance. The present construction borrows a lot from [PK21], indeed it uses the same ingredients, since [PK21] also uses Tanner codes and has a left-right Cayley complex embedded in its construction: the proposed code family may therefore be seen as a simplified variant of [PK21]. However, we wish to stress that it also involves a conceptual shift: the recent series of breakthrough asymptotic constructions of LPDC codes with large distances [HHO20, PK20, BE21b, PK21] arguably relies upon increasingly refined notions of chain-complex products that improve upon the simple product idea of [TZ14]. Our approach breaks away from this paradigm by proposing to take a geometric (square) complex and directly apply to it

the Tanner code strategy. Indeed, we show that the square complex can be viewed as two ordinary graphs that share the same set of edges, and the two classical codes $\mathcal{C}_0, \mathcal{C}_1$ that make up the quantum code are simply defined as classical Tanner codes on these two graphs. We obtain improved estimates for the minimum distance of the resulting quantum code, which for any given code rate scales like $n/\Delta^{3/2+\varepsilon}$, where n is the code length, Δ is the degree of the underlying Cayley graphs, and $\varepsilon > 0$ can be taken to be arbitrarily close to 0.

Interestingly, Panteleev and Kalachev showed that there is often a classical LTC hiding behind a good quantum LDPC code, and it turns out that we can recover exactly the LTC of Dinur *et al.* from our quantum Tanner codes.[1] It can indeed be argued that the present construction is the missing link between the quantum code construction of [PK21] and the LTC construction of [DEL⁺21], for we show that the linear minimum distance of our quantum code and the local testability of the Dinur *et al.* code are direct consequences of a uniting Theorem that is the main technical result of the present work.

1.2 Context and history

Locally testable codes. A binary linear code is a subspace of $\mathbb{F}_2^n$. A κ-locally testable code with q queries is a code C that comes with a tester: the tester requires access to at most q of bits of any given n-bit word x, accepts all words of the code, and rejects a word $x \notin C$ with probability $\geqslant \frac{\kappa}{n} d(x, C)$, where $d(x, C)$ is the Hamming distance from x to the code, and κ is a constant called the detection probability. A c^3-LTC, as constructed in [DEL⁺21], is such that the rate and distance of the code, as well as the number q of queries, are all constant. In that example, the test simply picks a vertex of the left-right Cayley complex and checks whether the local conditions corresponding to the small tensor code are satisfied.

LTCs were defined in the early 90s [BFLS91] and were first studied in the context of probabilistically checkable proofs (PCPs), before being investigated as mathematical objects of interest notably in [GS06]. A good overview of the field can be found in [Gol10]. Let us note that a third construction of c^3-LTC, besides those of [DEL⁺21] and [PK21], was obtained by Lin and Hsieh [LH22] through a method similar to that of [PK21], but relying on lossless expanders rather than spectral expanders.

Quantum LDPC codes. Defining the distance of a quantum code is slightly more complicated than in the classical case (where it is the minimum Hamming weight of a nonzero codeword). It is the minimum of two distances, d_X and d_Z, that basically characterize how well the code behaves against the two possible types of errors occurring in the quantum case: X-type errors, also called bit flips (swapping the basis states $|0\rangle$ and $|1\rangle$) and Z-type errors, or phase flips (adding a phase -1 to the state $|1\rangle$ while acting trivially on $|0\rangle$). Recall that a quantum CSS code [CS96, Ste96] is defined by a pair of classical codes $\mathcal{C}_0 = \ker H_0, \mathcal{C}_1 = \ker H_1$ such that $\mathcal{C}_1 \supset \mathcal{C}_0^\perp$ (or equivalently $H_0 \cdot H_1^T = 0$).

[1] Note however that it is not recovered through the prescription of Lemma 1 in [PK21] which would give another c^3-LTC, namely $\ker H_0^T$, with degraded parameters.

The distance of the code is then given by $d = \min(d_X, d_Z)$ with

$$d_X = \min_{w \in \mathcal{C}_0 \setminus \mathcal{C}_1^\perp} |w|, \quad d_Z = \min_{w \in \mathcal{C}_1 \setminus \mathcal{C}_0^\perp} |w|.$$

It is worth noting that for a quantum LDPC code, the sparsity of H_0 and H_1 implies that both $\mathcal{C}_0^\perp$ and $\mathcal{C}_1^\perp$, and therefore $\mathcal{C}_0$ and $\mathcal{C}_1$ contain (many) words of constant weight. In particular, the codes $\mathcal{C}_0$ and $\mathcal{C}_1$ are not asymptotically good, quite the opposite!

The study of quantum LDPC codes arguably started around 1997 with the paradigmatic surface code construction of Kitaev [Kit03] that encodes a constant number of logical qubits into n physical qubits and achieves a distance of $\sqrt{n}$. Improving on this scaling turned out to be challenging: despite an early construction of [FML02] achieving $n^{1/2} \log^{1/4} n$ in 2002, no further progress was made on this question until 2020. In the meantime, a major development was the idea of taking a special product of classical codes [TZ14], which turned out to correspond to the tensor product of chain complexes that represent the two classical codes, and yielded quantum codes of contant rate and minimum distance $\Theta(\sqrt{n})$. Things accelerated quickly in 2020 when the logarithmic dependence of [FML02] was first improved for constructions based on high-dimensional expanders [EKZ20, KT20], and then much more decisively in a series of works [HHO20, PK20, BE21b] introducing various combinations of chain complex products together with graph lifts. Already well known in the classical case, lifts turned out to be crucial to significantly break the $\sqrt{n}$ barrier on the distance of quantum LDPC codes. Finally, Panteleev and Kalachev proved the existence of asymptotically good quantum LDPC codes by considering non-abelian lifts of products of (classical) Tanner codes [PK21].

We also remark that it is possible to define quantum locally testable codes [AE15]. The existence of such codes would have implications in Hamiltonian complexity, which is the quantum version of computational complexity. In particular, such codes would imply the NLTS conjecture formulated by Hastings [Has13, EH17], and which is itself implied by the quantum PCP conjecture [AAV13]. Current constructions of quantum LTC are still very weak at the moment and far from sufficient for such applications, however: they only encode a constant number of logical qubits with a minimum distance bounded by $O(\sqrt{n})$ [Has17, LLZ21].

A very fruitful approach to prove the existence of certain objects is the probabilistic method and it is indeed very effective to prove that good classical LDPC codes [Gal62] and good quantum (non LDPC) codes [CS96, Ste96] exist. This method has failed, however, to produce c^3-LTCs or good quantum LDPC codes. On the one hand, it is well known that a good LDPC code cannot be locally testable since removing a single constraint will yield another good code and therefore a word violating this single constraint will actually be far from the code; on the other hand, picking a good LDPC code for $\mathcal{C}_0$ in the quantum case forces one to choose $\mathcal{C}_1^\perp$ to contain words of large weight and $\mathcal{C}_1$ will then not be LDPC. For both problems, it seems essential to enforce some minimal structure, and left-right Cayley complexes have provided this fitting, long-awaited framework.

The paper is organised as follows. Section 2 gives an overview of the paper, describes the quantum code construction, states the main theorem and its consequences, with

sketches of proofs. It is structured as a stand-alone extended summary and concludes with some open problems. Section 3 is a preliminary to the detailed part of the paper and introduces the required technical material. Section 4 is the core of the paper, giving the detailed construction of the quantum code, proving the main theorem and showing how it implies a linear distance for the quantum code and also how it implies that the Dinur *et al.* code is locally testable. An appendix is devoted to proving the required behaviour of random dual tensor codes.

2 Overview

The left-right Cayley complex. Let us summarise the construction of the square complex of Dinur *et al.* [DEL+21]. It is an incidence structure X between a set V of vertices, two sets of edges E_A and E_B, that we will refer to as A-edges and B-edges, and a set Q of squares (or quadrangles). The vertex-set V is defined from a group G: it will be useful for us that the complex is bipartite, *i.e.* the vertex set is partitioned as $V = V_0 \cup V_1$, with V_0 and V_1 both identified as a copy of the group G. Formally, we set $V_0 = G \times \{0\}$ and $V_1 = G \times \{1\}$. Next we have two self-inverse subsets $A = A^{-1}$ and $B = B^{-1}$ of the group G: a vertex $v_0 = (g, 0) \in V_0$ and a vertex $v_1 = (g, 1)$ are said to be related by an A-edge if $g' = ag$ for some $a \in A$. Similarly, v_0 and v_1 are said to be related by a B-edge if $g' = gb$ for some $b \in B$. The sets E_A and E_B make up the set of A-edges and B-edges respectively. In other words, the graph $\mathcal{G}_A = (V, E_A)$ is the double cover of the *left* Cayley graph $\mathsf{Cay}(G, A)$ and likewise $\mathcal{G}_B = (V, E_B)$ is the double cover of the *right* Cayley graph $\mathsf{Cay}(G, B)$.

Next, the set Q of squares is defined as the set of 4-subsets of vertices of the form

$$\{(g, 0), (ag, 1), (gb, 1), (agb, 0)\}.$$

A square is therefore made up of two vertices of V_0, two vertices of V_1 as represented on Figure 1.

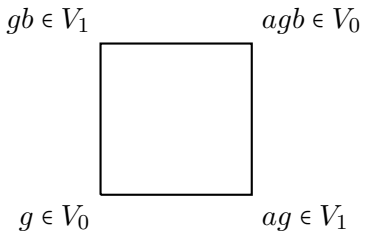

Figure 1: Square of the complex, with edges $(g, ag), (agb, gb) \in E_A, (g, gb), (agb, ag) \in E_B$.

Let us remark that, if we restrict the vertex set to V_0, every square is now incident to only two vertices (those in V_0). The set of squares can now be seen as a set of edges on V_0, and it therefore defines a graph that we denote by $\mathcal{G}_0^{\square} = (V_0, Q)$. Similarly, restricting

to vertices of V_1 defines the graph $\mathcal{G}_1^{\square}$, which is an exact replica of $\mathcal{G}_0^{\square}$: both graphs are defined over a copy of the group G, with $g, g, ' \in G$ being related by an edge whenever $g' = agb$ for some $a \in A, b \in B$. We assume for simplicity that A and B are of the same cardinality Δ.

Tanner codes on the complex X. Recall the definition of a Tanner code, or expander code, on a graph, [Tan81, SS96]. For $\mathcal{G} = (V, E)$ a regular graph of degree n_0 and C_0 a binary linear code of length n_0, we define the Tanner code $T(\mathcal{G}, C_0)$ on $\mathbb{F}_2^E$ as the set of binary vectors indexed by E (functions from E to $\mathbb{F}_2$), such that on the edge neighbourhood of every vertex $v \in V$, we see a codeword of C_0[2]. Sipser and Spielman's celebrated result is that if the graph $\mathcal{G}$ is chosen from a family of n_0-regular expander graphs, and if the base code C_0 has sufficiently large minimum distance and sufficiently large rate, then the Tanner codes $T(\mathcal{G}, C_0)$ form a family of asymptotically good codes.

Now for every vertex v of the graph $\mathcal{G}_0^{\square} = (V_0, Q)$ (or of $\mathcal{G}_1^{\square}$) associated to the square complex X, there is a natural identification[3] of its neighbourhood with the product set $A \times B$. It therefore makes sense to consider codes C_0 on the coordinate set $A \times B$ that are obtained from two small codes C_A and C_B of length $\Delta = |A| = |B|$, defined on coordinate sets A and B, respectively. We will refer to the restriction of an assignment $x \in \mathbb{F}_2^Q$ to the Q-neighbourhood $Q(v)$ of some vertex $v \in V_0$ as the *local view* of x in v. The Tanner code construction therefore consists in constraining the local views of x to belong to the code C_0.

The locally testable code of Dinur *et al.* Let C_0 be defined as the tensor code $C_A \otimes C_B$ on the coordinate set $A \times B$. In other words, this is the code such that for every fixed $b \in B$, we see a codeword of C_A on $\{(a, b), a \in A\}$, and for every fixed a we see a codeword of C_B on $\{(a, b), b \in B\}$. The Tanner code $T(\mathcal{G}_0^{\square}, C_0)$ is exactly the locally testable code of Dinur *et al.* [DEL+21]. If $C_A = C_B$ is a linear code with parameters $[\Delta, \rho\Delta, \delta\Delta]$, the resulting Tanner code $T(\mathcal{G}_0^{\square}, C_0)$ has length $\Delta^2|G|/2$, a rate at least $2\rho^2 - 1$ and is shown to have a normalized minimum distance $\geqslant \delta^2(\delta - \lambda/\Delta)$, where λ is the (common) second largest eigenvalue of the Cayley graphs $\mathsf{Cay}(G, A)$ and $\mathsf{Cay}(G, B)$ [DEL+21].

Two Tanner codes that define a quantum LDPC code. Besides the base code $C_0 = C_A \otimes C_B$ that we have defined over $A \times B$, define the code $C_1 = C_A^{\perp} \otimes C_B^{\perp}$. Now consider the two Tanner codes $\mathcal{C}_0 = T(\mathcal{G}_0^{\square}, C_0^{\perp})$ and $\mathcal{C}_1 = T(\mathcal{G}_1^{\square}, C_1^{\perp})$ that are defined over the same coordinate set Q. We claim that this pair of codes $(\mathcal{C}_0, \mathcal{C}_1)$ satisfies the definition of a quantum CSS code, namely that $\mathcal{C}_1 \supset \mathcal{C}_0^{\perp}$. Note crucially that we now enforce constraints corresponding to the dual of a tensor code at each vertex.

[2]This implies some identification, or map, between the edge neighbourhood of each vertex and the coordinate set $[n_0]$ on which C_0 is defined

[3]Formally, this identification is well-defined provided that the complex satisfies the *Total No-Conjugacy* condition, see Section 3.2 for a precise statement.

This last fact is best seen by looking at the generators (in quantum coding jargon) or parity-checks for these codes. Define a C_0-*generator* for $\mathcal{C}_0$ (resp. a C_1-generator for $\mathcal{C}_1$) as a vector of $\mathbb{F}_2^Q$ whose support lies entirely in the Q-neighbourhood $Q(v)$ of a vertex v of V_0 (resp. V_1), and which is equal to a codeword of C_0 (resp. C_1) on $Q(v)$. (The codes C_i and $\mathcal{C}_i$ should not be confused!) The code $\mathcal{C}_0$ (resp. $\mathcal{C}_1$) is by definition the space of vectors orthogonal to all C_0-generators (C_1-generators). Now consider a C_0-generator and a C_1-generator on vertices v_0 and v_1. If the generators have intersecting supports then the vertices v_0 and v_1 must be neighbours. If they are connected by a B-edge, then their Q-neighbourhoods $A \times B$ share an A-set $\{(a, b), a \in A\}$ for a fixed b, on which the C_0-generator must equal a codeword of C_A and the C_1-generator must equal a codeword of $C_A^\perp$. The two generators must therefore be orthogonal to each other. We reach the same conclusion analogously if v_0 and v_1 are connected by an A-edge.

For reasons of symmetry, we will wish the base codes C_0 and C_1 to have the same rate: we will require C_A to have some rate ρ and C_B to have rate $1 - \rho$. In this case, the length of the quantum code $\mathcal{Q} = (\mathcal{C}_0, \mathcal{C}_1)$ is given by the number of squares in the complex, namely $\Delta^2|G|/2$, and the number of parity check constraints is $2\rho(1-\rho)\Delta^2|G|$. We conclude that the quantum code has rate at least $(2\rho-1)^2$ which is non-zero for every $\rho \neq 1/2$.

We will show that under the right conditions for the choice of the left-right Cayley complex X and the component codes C_A and C_B, we obtain an asymptotically good family of quantum codes $\mathcal{Q} = (\mathcal{C}_0, \mathcal{C}_1)$. The required conditions on the choice of X are the same as in [DEL+21], namely that the two Cayley graphs $\mathsf{Cay}(G, A)$ and $\mathsf{Cay}(G, B)$ should be Ramanujan graphs or almost Ramanujan graphs, *i.e.* with a second largest eigenvalue $\lambda \leqslant c\sqrt{\Delta}$ for some small constant c, and that a non-degeneracy condition (called Total No-Conjugacy or TNC) is satisfied by the sets A, B, ensuring that for all choices of $g \in G, a \in A$ and $b \in B$, it holds that $ag \neq gb$.

It is worth noting that the good asymptotic properties of classical expander codes follow as soon as the distance of the small code is larger than the second eigenvalue of the expander graph, since the normalized minimum distance is known to be at least $\delta(\delta - \lambda/\Delta) > 0$. In the case we are considering however, the distance of the small code is upper bounded by Δ while the second eigenvalue scales like 2Δ. It is therefore necessary to inspect more closely the structure of the small dual codes $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ in order to get a nontrivial bound on the distance of the quantum Tanner code.

Robustness of the component codes C_A, C_B. The required conditions for the codes C_A, C_B are that the minimum distances of $C_A, C_B, C_A^\perp$ and $C_B^\perp$ are all sufficiently large, and that the two dual tensor codes $(C_A \otimes C_B)^\perp$ and $(C_A^\perp \otimes C_B^\perp)^\perp$ are sufficiently *robust.* Viewing the sets A and B as the row and column sets respectively of $\Delta \times \Delta$ matrices, let us say that a dual tensor code $(C_A^\perp \otimes C_B^\perp)^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ is w-robust if any codeword x of weight $\leqslant w$ has its support included in the union of $|x|/d_A$ columns and $|x|/d_B$ rows, where d_A and d_B are the minimum distances of C_A and C_B. A similar notion is used both in [DEL+21] and [PK21]. In particular, w-robustness is equivalent to a notion of robustness for the tensor code $C_A \otimes C_B$, which loosely speaking, says that if

a vector of $\mathbb{F}_2^{A\times B}$ is close to the column code $C_A \otimes \mathbb{F}_2^B$ as well as to the row code $\mathbb{F}_2^A \otimes C_B$, then it must also be close to the tensor code $C_A \otimes C_B$. We shall be more precise with this notion later on.

To obtain asymptotically good quantum codes, we are however not quite able to prove the existence of component codes C_A, C_B that yield robust dual tensor codes for a large enough parameter w. To overcome this problem, following [PK21], we introduce the following tweak: recall that if C is a code defined on the coordinate set S, and $T \subset S$ is a subset of S, then we may define the punctured code that we will denote by $(C)_T$, as the set of codewords of C restricted the set of coordinates T. Let us say that the dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ has w-robustness *with resistance to puncturing* p, if, for any subsets $A' \subset A$ and $B' \subset B$ of cardinality $\geqslant \Delta - w'$, $w' \leqslant p$, it remains w-robust when punctured outside of the set $A' \times B'$. Equivalently, if the dual tensor code obtained from the punctured codes $(C_A)_{A'}$ and $(C_B)_{B'}$ is w-robust.

Using the method of [PK21], we will obtain that for any $\varepsilon \in (0, 1/2)$ and $\gamma \in (1/2+\varepsilon, 1)$, and for random pairs of codes C_A, C_B of given fixed rates, the associated dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ is, with high probability, w-robust with resistance to puncturing w', for $w = \Delta^{3/2-\varepsilon}$ and $w' = \Delta^\gamma$.

Our main technical result will now take the following form.

Theorem 1. *Fix $\varepsilon \in (0, 1/2)$, $\gamma \in (1/2+\varepsilon, 1)$ and $\delta > 0$. For any fixed large enough Δ, if the component codes C_A and C_B have minimum distance $\geqslant \delta\Delta$ and if the dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B = C_1^\perp$ is w-robust with p-resistance to puncturing for $w = \Delta^{3/2-\varepsilon/2}$ and $p = \Delta^\gamma$, then there exists an infinite family of square complexes X for which the Tanner code $\mathcal{C}_1 = T(\mathcal{G}_1^\square, C_1^\perp)$ of length $n = |Q|$ has the following property:*

for any codeword $x \in \mathcal{C}_1$ of non-zero weight $< \delta n/4\Delta^{3/2+\varepsilon}$, there exists a vertex $v \in V_0$, and a codeword y of $\mathcal{C}_1$ entirely supported by the Q-neighbourhood of v, on which it coincides with a codeword of the tensor code $C_A \otimes C_B$, and such that $|x + y| < |x|$.

We recall from [DEL+21] that there exists an infinite sequence of degrees Δ (namely $q + 1$, for q an odd prime power), such that for each fixed degree Δ, there exists an infinite family of left-right Cayley complexes (over the groups $G = \mathrm{PSL}_2(q^i)$), satisfying the TNC condition, for which both the (left) Cayley graph $\mathsf{Cay}(G, A)$ and the (right) Cayley graph $\mathsf{Cay}(G, B)$ are Ramanujan graphs. These complexes provide the infinite families of Theorem 1. Let us also mention that randomly chosen codes C_A and C_B will typically achieve the requirements of the above theorem. In the quantum case, the codeword y will in fact belong to $\mathcal{C}_0^\perp$.

Sketch of proof of Theorem 1. Let $x \in \mathcal{C}_1$ be a codeword of sufficiently low weight. It induces a subgraph $\mathcal{G}_{1,x}^\square$ of $\mathcal{G}_1^\square$ with vertex set $S \subset V_1$. The local view for any $v \in S$ corresponds to a codeword of $C_1^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$. The w-robustness of this code guarantees that codewords of weight less than $w = \Delta^{3/2-\varepsilon}$ have a support restricted to a small number of rows and columns: in particular, and this is the crucial consequence of the robustness property, it implies that the view restricted to any column (or row) is at distance $O(\Delta^{1/2-\varepsilon})$ from a word of C_A (or C_B).

Let us call *normal vertices* the vertices of S with degree less than $\Delta^{3/2-\varepsilon}$ in $\mathcal{G}_{1,x}^{\square}$. Expansion in $\mathcal{G}_1$ ensures that the set of exceptional (*i.e.* not normal) vertices is small compared to S and we will neglect it in this sketch. Dealing with exceptional vertices, however, is slightly technical since their number is not *that* small, and this is the reason why we will require robust codes that are resistant to puncturing (in order to discard rows or columns belonging to an exceptional vertex).

Define $T \subset V_0$ to be vertices of V_0 sharing a column (or a row) with a normal vertex in S, and such that the local view on this column (or row) is close to a nonzero codeword of C_A (or C_B). The global codeword x induces a subgraph of $\mathcal{G}_A \cup \mathcal{G}_B$ in which the vertices of T have a degree $\Omega(\Delta)$. Expansion in the graph $\mathcal{G}_A \cup \mathcal{G}_B$ then implies that when $|x|$ is too small, there can't be too many vertices in T, which in turn implies that a typical vertex in T must be adjacent to a large number $\Omega(\Delta)$ of vertices in S. In other words, the rows and columns that are close to codewords of C_A and C_B in the local views of normal vertices of S, must cluster around the vertices of T. So the local view of a typical vertex of T consist of many columns (or rows) containing almost undisturbed codewords of C_A (or C_B). The robustness of $C_A \otimes C_B$ then implies that the local view of such a vertex must be $\Delta^{3/2-\varepsilon}$-close to a codeword y of the tensor code, which cannot be the zero codeword since the local view has weight $\Omega(\Delta^2)$. Adding this codeword will decrease the weight of x.

Asymptotically good quantum codes. A straightforward consequence of Theorem 1 is that the quantum code $\mathcal{Q} = (\mathcal{C}_0, \mathcal{C}_1)$ described above has constant rate and minimum distance linear in its length n.

Theorem 2. *Let X be the infinite family of square complexes from Theorem 1. For any $\rho \in (0, 1/2)$, $\varepsilon \in (0, 1/2)$ and $\delta > 0$ satisfying $-\delta \log_2 \delta - (1-\delta)\log_2(1-\delta) < \rho$, randomly choosing C_A and C_B of rates ρ and $1-\rho$ yields, with probability > 0 for Δ large enough, an infinite sequence of quantum codes $\mathcal{Q} = (\mathcal{C}_0, \mathcal{C}_1)$ of rate $(2\rho - 1)^2$, length n and minimum distance $\geqslant \delta n / 4\Delta^{3/2+\varepsilon}$.*

For a more precise statement see Theorems 17 and 18.

Sketch of proof of Theorem 2. Recall that the minimum distance of a quantum code $(\mathcal{C}_0, \mathcal{C}_1)$ is the smallest weight of a vector that is either in $\mathcal{C}_0 \setminus \mathcal{C}_1^{\perp}$ or in $\mathcal{C}_1 \setminus C_0^{\perp}$. The vector y in Theorem 1 is in $\mathcal{C}_0^{\perp}$, so by applying repeatedly the existence a such a y, we obtain that any codeword x of $\mathcal{C}_1$ of weight $< \delta n / 4\Delta^{3/2+\varepsilon}$ must belong to $\mathcal{C}_0^{\perp}$. To similarly bound from below the weight of a vector in $\mathcal{C}_0$ but not in $\mathcal{C}_1^{\perp}$, one must apply Theorem 1 to the code $\mathcal{C}_0$ instead of $\mathcal{C}_1$, which just means that we need to ensure that the distance and robustness properties required of C_A and C_B are also satisfied by $C_A^{\perp}$ and $C_B^{\perp}$. We choose C_A and C_B randomly by picking a uniform random parity-check matrix for one code and a uniform random generator matrix for the other, so that properties typically satisfied by the pair C_A, C_B will also be satisfied by the pair $C_A^{\perp}, C_B^{\perp}$. □

Recovering the local testability of the construction of [DEL+21]. Recall that the tester picks randomly a vertex $v \in V_0$ and checks whether the local view x_v of the

input vector $x \in \mathbb{F}_2^Q$ belongs to the small tensor code $C_0 = C_A \otimes C_B$. Proving local testability amounts to proving that the distance $d(x, \mathcal{C})$ of x to the LTC $\mathcal{C}$ is always proportional to the size $|S|$ of the subset $S \subset V_0$ of vertices for which x_v is not a codeword of C_0. To this end we consider the collection $\mathcal{Z} = (c_v)_{v \in V_0}$ of all the closest C_0-codewords to the local views x_v of x. Conflating the small vector $c_v \in C_0$ with a vector in $\mathbb{F}_2^Q$ that equals c_v on the Q-neighbourhood of v and is zero elsewhere, we then define the vector $z = \sum_{v \in V_0} c_v \in \mathbb{F}_2^Q$ that we call the mismatch of the collection $\mathcal{Z}$. If we have $z = 0$ then $\mathcal{Z}$ is the collection of local views of a global codeword $c \in \mathcal{C}$, and its distance to x must be proportional (up to a Δ^2 factor) to $|S|$. Otherwise the key observation is that the local views of the mismatch z at all the vertices of V_1, must consist of codewords of $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$, in other words z must belong to the code $\mathcal{C}_1$ of Theorem 1. The same Theorem 1 then states that there exists a vector $y_v \in \mathbb{F}_2^Q$, that is equal to a codeword of C_0 on the Q-neighbourhood of some vertex $v \in V_0$, and such that $|z + y_v| < |z|$. Consequently, if one replaces c_v by $c_v + y_v$ in the collection $\mathcal{Z}$, one reduces the weight of the mismatch, and by repeatedly applying the procedure (which we can think of as decoding the mismatch), we obtain a updated list $\mathcal{Z}$ than coincides with the set of local views of a codeword of $\mathcal{C}$ whose distance to x is again easily shown to be proportional to the size of the original set S.

Comments and open problems. A natural follow up problem is to devise an efficient decoding algorithm for quantum Tanner codes. At the moment, to the best of our knowledge, the only efficient decoder for quantum codes that corrects adversarial errors of weight larger than $\sqrt{n}$ is that of [EKZ20] which can correct errors of weight $\Omega(\sqrt{n} \log n)$.

While the construction of quantum Tanner codes described above is arguably conceptually simpler than the balanced product and lifted product constructions of [BE21a, PK21], it comes at the price of larger weights for the generators, namely $\Theta(\Delta^2)$ instead of $\Theta(\Delta)$. Even if they are constant, it would be very useful to decrease these weights as much as possible and it would be interesting to explore how the weight reduction technique of Hastings [Has21] can help on this issue.

It would be naturally very interesting to find other complexes, besides left-right Caley complexes, on which the Tanner construction can be applied to yield good families of quantum LDPC codes.

It would also be desirable to have completely explicit constructions. Reed-Solomon codes (binarised versions) come close, but tensor codes of Reed-Solomon codes are only known to have the required robustness when the sum of the rates of the component codes is < 1 [PS94], which is insufficient for the above constructions. In a similar vein, we remark that if one could improve the robustness of the component dual tensor codes to values above $\Delta^{3/2}$, we could improve the dependence on Δ of the relative minimum distance of the quantum code, potentially up to $\Omega(1/\Delta)$. We also remark that we cannot hope to improve the dependence on Δ of the relative minimum distance above $O(1/\Delta)$. Indeed, we will prove the existence of words of $\mathcal{C}_1 \setminus \mathcal{C}_0^\perp$ of weight less than n/Δ (see Section 4.3 for details). This shows that there is little room for improvement in our estimation of the quantum code minimum distance.

Acknowledgements. We would like to thank Benjamin Audoux, Alain Couvreur, Shai Evra, Omar Fawzi, Tali Kaufman, Jean-Pierre Tillich, and Christophe Vuillot for many fruitful discussions on quantum codes over the years. We also thank Max Hopkins for spotting a technical error in the application of Proposition 7 in an earlier version of this manuscript. We acknowledge support from the Plan France 2030 through the project ANR-22-PETQ-0006. AL acknowledges support from the ANR through the QuantERA project QCDA, and GZ acknowledges support from the ANR through the project QUDATA, ANR-18-CE47-0010.

3 Preliminaries

3.1 Expander Graphs

Let $\mathcal{G} = (V, E)$ be a graph. Graphs will be undirected but may have multiple edges. For $S, T \subset V$, let $E(S,T)$ denote the multiset of edges with one endpoint in S and one endpoint in T[4]. Let $\mathcal{G}$ be a Δ-regular graph on n vertices, and let $\Delta = \lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n$ be the eigenvalues of the adjacency matrix of $\mathcal{G}$. For $n \geqslant 3$, we define $\lambda(\mathcal{G}) := \max\{|\lambda_i|, \lambda_i \neq \pm\Delta\}$. The connected graph $\mathcal{G}$ is said to be Ramanujan if $\lambda(\mathcal{G}) \leqslant 2\sqrt{\Delta - 1}$.

We recall the following version of the expander mixing lemma (see e.g. [HLW06]).

Lemma 3 (Expander mixing lemma)**.** *For a Δ-regular non-bipartite, connected graph $\mathcal{G}$ and any sets $S, T \subset V(\mathcal{G})$, it holds that*

$$|E(S,T)| \leqslant \frac{\Delta}{|V|}|S||T| + \lambda(\mathcal{G})\sqrt{|S||T|}.$$

For a Δ-regular bipartite connected graph $\mathcal{G}$ over the vertex set $V = V_0 \cup V_1$ and any sets $S \subset V_0$, $T \subset V_1$, it holds that

$$|E(S,T)| \leqslant \frac{\Delta}{|V_0|}|S||T| + \lambda(\mathcal{G})\sqrt{|S||T|}.$$

3.2 Left-right Cayley complexes.

A *left-right Cayley complex* X is introduced in [DEL⁺21] from a group G and two sets of generators $A = A^{-1}$ and $B = B^{-1}$. As in [DEL⁺21] we will restrict ourselves, for the sake of simplicity, to the case $|A| = |B| = \Delta$. The complex is made up of vertices, A-edges, B-edges, and squares. The vertex set is G, the A-edges are pairs of vertices of the form $\{g, ag\}$ and B-edges are of the form $\{g, gb\}$ for $g \in G, a \in A, b \in B$. A *square* is a set of group elements of the form $\{g, ag, gb, agb\}$. The *Total No-Conjugacy* condition (TNC) requires that

$$\forall a \in A, b \in B, g \in G, \quad ag \neq gb. \tag{1}$$

[4] with the convention that an edge with both endpoints in $S \cap T$ appears twice in $E(S,T)$

This condition ensures that a square contains exactly 4 distinct vertices and that every vertex is incident to exactly Δ^2 squares. For a vertex v, the set of incident squares is called the *link* of v, and denoted X_v. The TNC condition implies that the link of any vertex is in bijection with the set $A \times B$ (see Claim 3.7 of [DEL+21]). We will naturally refer to sets of the form $\{a\} \times B$ as rows and sets $A \times \{b\}$ as columns.

We recall from [DEL+21] that there exists an infinite sequence of degrees Δ (namely $q+1$, for q an odd prime power) such that each fixed degree Δ, there exists an infinite family of left-right Cayley complexes (over the groups $G = \mathrm{PSL}_2(q^i)$), satisfying the TNC condition, for which both the (left) Cayley graph $\mathsf{Cay}(G, A)$ and the (right) Cayley graph $\mathsf{Cay}(G, B)$ are Ramanujan graphs.

When the Cayley graphs $\mathsf{Cay}(G, A)$ and $\mathsf{Cay}(G, B)$ are not bipartite (as is the case of the above family[5]), it will be convenient for us to make them so by replacing them by their double covers. So we make two copies $V_0 = G \times \{0\}$ and $V_1 = G \times \{1\}$ of G and define the graphs $\mathcal{G}_A = (V = V_0 \cup V_1, E_A)$ and $\mathcal{G}_B = (V, E_B)$ with the edge set E_A made up of pairs $\{(g,0),(ag,1)\}$, $a \in A$, and E_B consisting of the pairs $\{(g,0),(gb,1)\}$, $b \in B$.

Finally, the set Q of squares of the square complex X is defined as the set of 4-subsets of vertices of the form

$$\{(g,0),(ag,1),(gb,1),(agb,0)\}.$$

Let us introduce two further graphs that exist on the complex X. The first is just the union of $\mathcal{G}_A$ and $\mathcal{G}_B$, and we denote it by $\mathcal{G}^{\cup} = (V, E_A \cup E_B)$. The second graph we denote by $\mathcal{G}^{\square} = (V, E^{\square})$: it puts an edge between all pairs of vertices of the form $\{(g,i),(agb,i)\}$, $g \in G, a \in A, b \in B, i = 0,1$. The graph $\mathcal{G}^{\square}$ is therefore made up of two connected components, on V_0 and V_1, that we denote by $\mathcal{G}_0^{\square}$ and $\mathcal{G}_1^{\square}$. We note that $\mathcal{G}^{\square}$ is regular of degree Δ^2, and may have multiple edges.

If $\mathcal{G}_A$ and $\mathcal{G}_B$ are Ramanujan, then $\mathcal{G}^{\cup}$ and $\mathcal{G}^{\square}$ inherit most of their expansion properties. Specifically:

Lemma 4. *Assume that $\mathcal{G}_A$ and $\mathcal{G}_B$ are Ramanujan graphs, then*

$$\lambda(\mathcal{G}^{\cup}) \leqslant 4\sqrt{\Delta}, \quad \lambda(\mathcal{G}_0^{\square}) \leqslant 4\Delta, \quad \lambda(\mathcal{G}_1^{\square}) \leqslant 4\Delta.$$

Proof. Let M_A and M_B be the adjacency matrices of $\mathcal{G}_A$ and $\mathcal{G}_B$. Since these graphs are bipartite, they admit two eigenvalues Δ and $-\Delta$ and the remaining eigenvalues have an absolute value less than $2\sqrt{\Delta}$. The adjacency matrices of $\mathcal{G}^{\cup}$ and $\mathcal{G}^{\square}$ are respectively $M_A + M_B$ and $M_A M_B = M_B M_A$. Since M_A and M_B commute, they can be made to have the same eigenspaces: therefore the eigenvalues of $M_A + M_B$ are the sum of the eigenvalues of M_A and M_B and the eigenvalues of $M_A M_B$ are the products of the eigenvalues of M_A and M_B. The eigenvalue $-\Delta$ has the same eigenspace in M_A and M_B, therefore the eigenvalue Δ^2 has an eigenspace of dimension 2 in $M_A M_B$, meaning that $\mathcal{G}^{\square}$ splits into the two connected components $\mathcal{G}_0^{\square}$ and $\mathcal{G}_1^{\square}$. ∎

[5] Thanks to Shai Evra for spelling this out.

The quadripartite version. A way of avoiding the somewhat cumbersome TNC condition is to make the complex quadripartite rather than simply bipartite. In this case we construct the vertex set V as the disjoint union of four copies of the group G: we set $V = V_0 \cup V_1$ with $V_0 = V_{00} \cup V_{11}$ and $V_1 = V_{10} \cup V_{01}$, where $V_{ij} = G \times \{i, j\}$, $i, j \in \{0, 1\}$. The set Q of squares is then defined as the set of 4-subsets of vertices of the form

$$\{(g, 00), (ag, 01), (gb, 10), (agb, 11)\}.$$

We see that this time the Q-neighbourhood of any vertex becomes naturally in bijection with $A \times B$ without requiring any special properties of $A = A^{-1}$ and $B = B^{-1}$. In the present case the edge set E_A of $\mathcal{G}_A$ becomes the set of pairs of the form $\{(g, 00), (ag, 01)\}$ and of the form $\{(g, 10), (ag, 11)\}$, and the edge set E_B of $\mathcal{G}_B$ becomes the set of pairs $\{(g, 00), (gb, 10)\}$ and $\{(g, 01), (gb, 11)\}$. The graphs $\mathcal{G}_A$ and $\mathcal{G}_B$ are therefore both made up of two connected components. As before, we may set $\mathcal{G}^{\cup} = (V, E_A \cup E_B)$, and finally the graph $\mathcal{G}^{\square}$ over the vertex set V puts an edge between $(g, 00)$ and $(agb, 11)$ as well as between $(g, 01)$ and $(agb, 10)$ for all $g \in G, a \in A, b \in B$. The two connected components $\mathcal{G}_0^{\square}$ and $\mathcal{G}_1^{\square}$ have now become bipartite, the vertex set of $\mathcal{G}_0^{\square}$ being $V_{00} \cup V_{11}$ and that of $\mathcal{G}_1^{\square}$ being $V_{01} \cup V_{10}$.

It is readily seen that Lemma 4 also holds in the quadripartite case with the eigenvalue analysis being similar. In the sequel we will not need the bipartite structure of $\mathcal{G}_0^{\square}$ and $\mathcal{G}_1^{\square}$, and to lighten notation we will just assume the complex to be bipartite and not necessarily quadripartite. The quantum code construction presented in Section 4.1 is however straightforwardly adapted to the quadripartite case, and its analysis is essentially unchanged.

We note that the quadripartite version of the square left-right Cayley complex appears in [PK21].

3.3 Tanner codes

A binary linear code of length n is an $\mathbb{F}_2$-linear subspace of $\mathbb{F}_2^n$. For sets E of cardinality $|E| = n$, it will be convenient for us to identify $\mathbb{F}_2^n$ with $\mathbb{F}_2^E$, which we can think of as the space of functions from E to $\mathbb{F}_2$. Identication with $\mathbb{F}_2^n$ amounts to defining a one-to-one map between E and $[n] = \{1, 2, \ldots, n\}$, *i.e.* a numbering of the elements of E.

Let $\mathcal{G} = (V, E)$ be a regular graph of degree Δ, and for any vertex v denote by $E(v)$ the set of edges incident to v. Assume an identification of $\mathbb{F}_2^{E(v)}$ with $\mathbb{F}_2^{\Delta}$ for every $v \in V$. Let $x \in \mathbb{F}_2^E$ be a vector indexed by (or a function defined on) the set E. Let us define the *local view* of x at vertex v as the subvector $x_v = (x_e)_{e \in E(v)}$, *i.e.* x restricted to the edge-neighbourhood $E(v)$ of v.

Let C_0 be a linear code of length Δ, dimension $k_0 = \rho_0 \Delta$, and minimum distance $d_0 = \delta_0 \Delta$. We define the Tanner code [Tan81] associated to $\mathcal{G}$ and C_0 as

$$T(\mathcal{G}, C_0) = \{x \in \mathbb{F}_2^E : x_v \in C_0 \text{ for all } v \in V\}.$$

In words, the Tanner code is the set of vectors over E all of whose local views lie in C_0. By counting the number of linear equations satisfied by the Tanner code, we obtain

$$\dim T(\mathcal{G}, C_0) \geqslant (2\rho_0 - 1)n. \tag{2}$$

We also have the bound [SS96, Gur10] on the minimum distance d of the Tanner code:

$$d \geqslant \delta_0(\delta_0 - \lambda(\mathcal{G})/\Delta)n.$$

Therefore, if $(\mathcal{G}_i)$ is a family of Δ-regular expander graphs with $\lambda(\mathcal{G}_i) \leqslant \lambda < d_0$, and if $\rho_0 > 1/2$, then the associated family of Tanner codes has rate and minimum distance which are both $\Omega(n)$, meaning we have an asymptotically good family of codes, as was first shown in [SS96].

3.4 Quantum CSS codes

A quantum CSS code is specific instance of a stabilizer code [Got97] that can be defined by two classical codes $\mathcal{C}_0$ and $\mathcal{C}_1$ in the ambient space $\mathbb{F}_2^n$, with the property that $\mathcal{C}_0^\perp \subset \mathcal{C}_1$ [CS96, Ste96]. If both codes are defined by their parity-check matrix, $\mathcal{C}_0 = \ker H_0, \mathcal{C}_1 = \ker H_1$, then the condition is equivalent to $H_0 H_1^T = 0$. The resulting quantum code $\mathcal{Q} = (\mathcal{C}_0, \mathcal{C}_1)$ is the following subspace of $(\mathbb{C}_2)^{\otimes n}$, the space of n qubits:

$$\mathcal{Q} := \mathrm{Span}\left\{ \sum_{z \in \mathcal{C}_1^\perp} |x + z\rangle \ : \ x \in \mathcal{C}_0 \right\},$$

where $\{|x\rangle \ : \ x \in \mathbb{F}_2^n\}$ is the canonical basis of $(\mathbb{C}_2)^{\otimes n}$.

In practice, it is convenient to describe the code *via* its *generators*. A CSS code admits X-type generators which correspond to the rows of H_1 and and Z-type generators, corresponding to the rows of H_0. The condition $\mathcal{C}_0^\perp \subset \mathcal{C}_1$ is simply that the rows of H_0 are orthogonal to the rows of H_1, where orthogonality is with respect to the standard inner product over $\mathbb{F}_2^n$. A CSS code is called *LDPC* is both H_0 and H_1 are sparse matrices, *i.e.* each row and column has constant weight independent of the code length n. Equivalently, each generator acts nontrivially on a constant number of qubits, and each qubit is only involved in a constant number of generators.

The dimension k of the code counts the number of logical qubits and is given by

$$k = \dim\left(\mathcal{C}_0/\mathcal{C}_1^\perp\right) = \dim \mathcal{C}_0 + \dim \mathcal{C}_1 - n.$$

Its minimum distance is $d = \min(d_X, d_Z)$ with

$$d_X = \min_{w \in \mathcal{C}_0 \setminus \mathcal{C}_1^\perp} |w|, \quad d_Z = \min_{w \in \mathcal{C}_1 \setminus \mathcal{C}_0^\perp} |w|.$$

We denote the resulting code parameters by $[\![n, k, d]\!]$. We say that a code family $(\mathcal{Q}_n)_n$ is *asymptotically good* if its parameters are of the form

$$[\![n, k = \Theta(n), d = \Theta(n)]\!].$$

3.5 Tensor codes and dual tensor codes: robustness

Let A and B be two sets of size Δ. We define codes on the ambient space $\mathbb{F}_2^{A\times B}$ that we may think of the space of matrices whose rows (columns) are indexed by A (by B). If $C_A \subset \mathbb{F}_2^A$ and $C_B \subset \mathbb{F}_2^B$ are two linear codes, we define the *tensor* (or product) code $C_A \otimes C_B$ as the space of matrices x such that for every $b \in B$ the column vector $(x_{ab})_{a\in A}$ belongs to C_A and for every $a \in A$ the row vector $(x_{ab})_{b\in B}$ belongs to C_B. It is well known that $\dim(C_A \otimes C_B) = \dim(C_A)\dim(C_B)$ and that the minimum distance of the tensor code is $d(C_A \otimes C_B) = d(C_A)d(C_B)$.

Consider the codes $C_A \otimes \mathbb{F}_2^B$ and $\mathbb{F}_2^A \otimes C_B$ consisting respectively of the space of matrices whose columns are codewords of C_A and whose rows are codewords of C_B. We may consider their sum $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ which is called a *dual tensor* code, since it is the dual code of the tensor code $C_A^\perp \otimes C_B^\perp = (C_A^\perp \otimes \mathbb{F}_2^B) \cap (\mathbb{F}_2^A \otimes C_B^\perp)$. It is relatively straightforward to check that $d(C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B) = \min(d(C_A), d(C_B))$.

Definition 5. *Let $0 \leqslant w \leqslant \Delta^2$. Let C_A and C_B be codes of length Δ with minimum distances d_A and d_B. We shall say that the dual tensor code $C = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ is* w-robust*, if for any codeword $x \in C$ of Hamming weight $|x| \leqslant w$, there exist $A' \subset A, B' \subset B$, $|A'| \leqslant |x|/d_B$, $|B'| \leqslant |x|/d_A$, such that $x_{ab} = 0$ whenever $a \notin A', b \notin B'$.*

In words, w-robustness means that any dual tensor codeword of weight at most w is entirely supported within the union of a set of at most $|c|/d_A$ columns and a set of at most $|c|/d_B$ rows. In fact, the following proposition shows that any such codeword is the sum of a word of $C_A \otimes \mathbb{F}_2^B$ and of a word of $\mathbb{F}_2^A \otimes C_B$ supported on a few columns or rows.

Proposition 6. *Let C_A and C_B be codes of length Δ with minimum distances d_A and d_B, and suppose $C = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ is w-robust with $0 < w < d_A d_B$. Then for any codeword $x \in C$ such that $|x| \leqslant w$, there exist $A' \subset A, B' \subset B$, $|A'| \leqslant |x|/d_B$, $|B'| \leqslant |x|/d_A$ and a decomposition $x = c + r$, with $c \in C_A \otimes \mathbb{F}_2^{B'}$ and $r \in \mathbb{F}_2^{A'} \otimes C_B$.*

Proof. To see this, apply the definition and write $x = r' + c'$, with $r'_{ab} = c'_{ab}$ for any $(a, b) \in (A \setminus A') \times (B \setminus B')$. The restrictions of r' and c' to $(A \setminus A') \times (B \setminus B')$ both belong to the code obtained by tensoring C'_A and C'_B, the punctured codes deduced from C_A and C_B by throwing away coordinates of A' and B'. This code is the same as the punctured code obtained from $C_A \otimes C_B$ by throwing away the coordinates $A' \times B \cup A \times B'$. Therefore, there exists a tensor codeword of $C_A \otimes C_B = C_A \otimes \mathbb{F}_2^B \cap \mathbb{F}_2^A \otimes C_B$ that coincides with $c' = r'$ on $(A \setminus A') \times (B \setminus B')$: adding this tensor codeword to both c' and r' yields the required pair r, c such that $x = r + c$. □

Our notion of robustness for the dual tensor code also implies a form of robustness for the corresponding tensor code.

Proposition 7. *Let C_A and C_B be codes of length Δ and minimum distances d_A, d_B such that the dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ is w-robust with $w \leqslant d_A d_B/2$. Then, any word x close to both the column and row code is also close to the tensor code: precisely,*

if $d(x, C_A \otimes \mathbb{F}_2^B) + d(x, \mathbb{F}_2^A \otimes C_B) \leqslant w$ *then*

$$d(x, C_A \otimes C_B) \leqslant \frac{3}{2}\left(d(x, C_A \otimes \mathbb{F}_2^B) + d(x, \mathbb{F}_2^A \otimes C_B)\right). \tag{3}$$

The conclusion of Proposition 7 is very close to a property called "robustly testable" in [DEL+21]. The difference is that robustly testable tensor codes are required to satisfy (3) without any condition on its right hand side (equivalently, with $w = 2\Delta^2$), at the expense of allowing a looser constant than 3/2. We note that the constant 3/2 in Proposition 7 is tight[6].

Proof. Let x be an $A \times B$ matrix that we write as $x = C + e_C = R + e_R$ with $C \in C_A \otimes \mathbb{F}_2^B$, $R \in \mathbb{F}_2^A \otimes C_B$ and

$$|e_C| = d(x, C_A \otimes \mathbb{F}_2^B), \quad |e_R| = d(x, \mathbb{F}_2^A \otimes C_B).$$

Let us suppose $|e_C| + |e_R| \leqslant w$. From $C + R = e_C + e_R$, we obtain that $|C + R| \leqslant w$ and the robust testability of the dual product code implies that there exist $c \in C_A \otimes \mathbb{F}_2^B$, $r \in \mathbb{F}_2^A \otimes C_B$, supported respectively, since $w \leqslant d_A d_B/2$, on at most $d_B/2$ columns and at most $d_A/2$ rows, and such that $C + R = c + r$. Since c is supported by at most $d_B/2$ columns, we have that $|c + r| \geqslant |c|$, and similarly $|c + r| \geqslant |r|$.

Note in particular that $R + r = C + c$ is a codeword of the tensor code $C_A \otimes C_B$. One can therefore write $x = (C + c) + c + e_C$, from which we have:

$$d(x, C_A \otimes C_B) \leqslant |c + e_C| \leqslant |c| + |e_C| \leqslant |c + r| + |e_C| = |e_C + e_R| + |e_C| \leqslant 2|e_C| + |e_R|.$$

Writing $x = (R + r) + r + e_R$, we similarly get $d(x, C_A \otimes C_B) \leqslant 2|e_R| + |e_C|$, and adding the two inequalities we conclude that

$$d(x, C_A \otimes C_B) \leqslant \frac{3}{2}\left(d(x, C_A \otimes \mathbb{F}_2^B) + d(x, \mathbb{F}_2^A \otimes C_B)\right). \qquad \square$$

If $C_A \subset \mathbb{F}_2^A$ is a code and $A' \subseteq A$, let us denote by $C_{A'} \subset \mathbb{F}_2^{A'}$ the *punctured code* consisting of all subvectors $(c_a)_{a \in A'}$ of all codewords $(c_a)_{a \in A}$ of C_A. Similarly, for a code C_B we denote by $C_{B'}$ the punctured code on B' for $B' \subseteq B$.

Let us introduce the following twist on the above definition of robustness for dual tensor codes, which allows us to boost its potential.

Definition 8. *Let* $C_A \subset \mathbb{F}_2^A$ *and* $C_B \subset \mathbb{F}_2^B$. *For integers* w, p, *let us say that the dual tensor code* $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ *is* w*-robust with* p*-resistance to puncturing, if for any* $A' \subset A$ *and* $B' \subset B$ *such that* $|A'| = |B'| = \Delta - w'$, *with* $w' \leqslant p$, *the dual tensor code*

$$C_{A'} \otimes \mathbb{F}_2^{B'} + \mathbb{F}_2^{A'} \otimes C_{B'}$$

is w*-robust.*

[6] For example, consider $C_A = C_B = \mathrm{Span}(111100, 110011)$ and define $x = \begin{bmatrix} 11 & 11 & 00 \\ 11 & 00 & 11 \\ 10 & 00 & 00 \\ 10 & 00 & 00 \\ 01 & 00 & 00 \\ 01 & 00 & 00 \end{bmatrix}$. One checks that $d(x, C_A \otimes \mathbb{F}_2^B) = d(x, \mathbb{F}_2^A \otimes C_B) = 4$ and $d(x, C_A \otimes C_B) = 6$.

We shall need the following result on the robustness of random dual tensor codes.

Theorem 9. *Let $0 < \rho_A < 1$ and $0 < \rho_B < 1$. Let $0 < \varepsilon < 1/2$ and $1/2 + \varepsilon < \gamma < 1$. Let C_A be a random code obtained from a random uniform $\rho_A\Delta \times \Delta$ generator matrix, and let C_B be a random code obtained from a random uniform $(1-\rho_B)\Delta \times \Delta$ parity-check matrix. With probability tending to 1 when Δ goes to infinity, the dual tensor code*

$$C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$$

is $\Delta^{3/2-\varepsilon}$-robust with Δ^γ-resistance to puncturing.

Except for the fact that we allow a larger robustness parameter, (namely $\Delta^{1/2-\varepsilon}$), this result is essentially in [PK21]. We provide a proof in the appendix, which closely follows the approach of [PK21].

4 Asymptotically good quantum Tanner codes

4.1 The construction

Let G belong to an infinite family of groups with size $|G| \to \infty$, together with two sets of generators $A = A^{-1}$ and $B = B^{-1}$ of fixed cardinality Δ. We form the associated family of left-right Cayley complexes X, and will assume throughout that they satisfy the TNC condition (1).

Recall that the square-neighbourhood (or link) $Q(v)$ of a vertex $v = (g, i) \in G \times \{0, 1\}$ is the set of squares incident to v. To lighten notation, let us write, for $a \in A, b \in B$, $av = (ag, 1-i), vb = (gb, 1-i), avb = (agb, i)$, so that $\{v, av, vb, avb\}$ is a square incident to v. The TNC condition implies in particular that the map

$$\begin{array}{rcl} A \times B & \to & Q(v) \\ (a, b) & \mapsto & \{v, av, vb, avb\} \end{array}$$

is one-to-one, and let ϕ_v denote the inverse of this map. A crucial consequence of the TNC condition is that for two adjacent vertices $v, v' \in V$, the intersection $Q(v) \cap Q(v')$ has cardinality Δ, and more specifically,

$$\begin{array}{ll} \phi_v(Q(v) \cap Q(vb)) = A \times \{b\} & \phi_{vb}(Q(v) \cap Q(vb)) = A \times \{b^{-1}\} \\ \phi_v(Q(v) \cap Q(av)) = \{a\} \times B & \phi_{av}(Q(v) \cap Q(av)) = \{a^{-1}\} \times B. \end{array}$$

For a vector $x \in \mathbb{F}_2^Q$, we may define its local view x_v as the restriction $(x_q)_{q \in Q(v)}$ of x to the link $Q(v)$ of v. Through the indexation map ϕ_v, the local view at any vertex v can be seen as an $A \times B$ array, all of its rows being shared by the local views of the A-neighbours of v, and all of its columns being shared by the local views of its B-neighbours. The situation is illustrated on Figure 2.

We define a quantum CSS code $\mathcal{Q} = (\mathcal{C}_0, \mathcal{C}_1)$ by associating qubits to the squares of the complex X and enforcing constraints on the local view of each vertex. The idea is

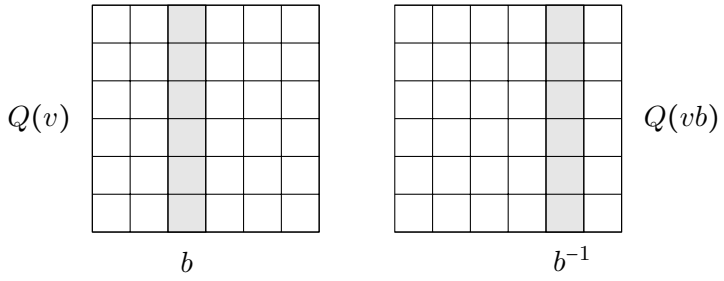

Figure 2: The structure of $Q(v)$ and $Q(vb)$ at neighbouring vertices v and vb. Both square-neighbourhoods are isomorphic to $A \times B$ and share a common column, which is column b for the $A \times B$ grid $Q(v)$ and column b^{-1} for the grid $Q(vb)$.

to associate Z-type generators with vertices of V_0 and X-type generators with V_1. Since their support can only overlap on a column or on a row, it suffices to impose orthogonality constraints between the two types of generators on each row and column to obtain a CSS code satisfying $\mathcal{C}_0^\perp \subset \mathcal{C}_1$. More precisely, we choose two codes $C_A \subset \mathbb{F}_2^A$ and $C_B \subset \mathbb{F}_2^B$ and define the two tensor codes $C_0 = C_A \otimes C_B$ and $C_1 = C_A^\perp \otimes C_B^\perp$. To define the two sets of generators, choose a basis β_0 of C_0 and a basis β_1 of C_1. For every vertex $v \in V_0$ we define $\dim C_0$ generators $x \in \mathbb{F}_2^Q$ of type Z by requiring that their local views x_v at v be equal (through ϕ_v) to a basis element in β_0 and that $x_q = 0$ for all $q \notin Q(v)$. Similarly, we define $|V_1| \dim C_1$ generators of type X by imposing a local view equal to a basis element of β_1 on a single vertex $v \in V_1$ and requiring $x_q = 0$ for all values outside the neighbourhood $Q(v)$ of v. We see that X-generators and Z-generators are orthogonal by design.

Equivalently, the code $\mathcal{C}_0$ ($\mathcal{C}_1$) orthogonal to all Z-generators (X-generators) is defined as the set of vectors $x \in \mathbb{F}_2^Q$ such that x_v is in $C_0^\perp$ (in $C_1^\perp$). In other words, the quantum code $\mathcal{Q} = (\mathcal{C}_0, \mathcal{C}_1)$ is the pair of Tanner codes

$$\mathcal{C}_0 = T(\mathcal{G}_0^\square, C_0^\perp), \qquad \mathcal{C}_1 = T(\mathcal{G}_1^\square, C_1^\perp). \tag{4}$$

To have the same number of X and Z-type generators, we shall set $\rho = \dim C_A/\Delta$ and require $\dim C_B = \Delta - \dim C_A$: consequently we shall have $\dim C_0 = \dim C_1 = \rho(1-\rho)\Delta^2$.

It is immediate that this code is LDPC since all its generators have weight at most Δ^2, which is a constant, and any qubit is involved in at most $4\rho(1-\rho)\Delta^2 \leqslant \Delta^2$ generators[7]. The code length is the number of squares in the complex, $n = \Delta^2|G|/2$. While computing the exact dimension k of the code would require to check for possible dependencies among generators, it is straightforward to get a lower bound by counting the number of generators, namely $|V_0| \dim C_0 + |V_1| \dim C_1 = 2\rho(1-\rho)\Delta^2|G|$. This yields the following bound for the rate of the quantum code:

$$\frac{1}{n} \dim \mathcal{Q} \geqslant (2\rho - 1)^2, \tag{5}$$

[7]By comparison, the quantum code of [PK21] admits generators of weight $O(\Delta)$.

with equality when all the generators are independent. In particular, the rate is > 0 for any value of $\rho \neq 1/2$.

Most of the rest of this section is devoted to establishing a linear lower bound for the minimum distance of this quantum code, provided that the Cayley graphs associated to X are sufficiently expanding and the dual tensor codes $C_0^\perp$ and $C_1^\perp$ are sufficiently robust. This in turn requires Δ to be large enough and G to be non Abelian (since the Cayley graph of an Abelian group cannot be an expander if the degree is constant). But the quantum Tanner code construction is more general, and even small examples where $C_A = C_B^\perp$ is a small Hamming code could display good performance. For instance, one could consider $G = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $A = \{(a, 0) : a \neq 0\}$, $B = \{(b, 1) : b \neq 1\}$ and C_A, C_B to be the $[7, 4, 3]$ Hamming code and its dual $[7, 3, 4]$. The associated quantum Tanner code has length 392, dimension at least 8, and generators of weight 12.

4.2 Proof of Theorem 1

Let us recall our main technical theorem:

Theorem 1. *Fix $\varepsilon \in (0, 1/2)$, $\gamma \in (1/2 + \varepsilon, 1)$ and $\delta > 0$. For any fixed large enough Δ, if the component codes C_A and C_B have minimum distance $\geqslant \delta\Delta$ and if the dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B = C_1^\perp$ is w-robust with p-resistance to puncturing for $w = \Delta^{3/2-\varepsilon/2}$ and $p = \Delta^\gamma$, then there exists an infinite family of square complexes X for which the Tanner code $\mathcal{C}_1 = T(\mathcal{G}_1^\square, C_1^\perp)$ of length $n = |Q|$ has the following property:*

for any codeword $x \in \mathcal{C}_1$ of non-zero weight $< \delta n/4\Delta^{3/2+\varepsilon}$, there exists a vertex $v \in V_0$, and a codeword y of $\mathcal{C}_1$ entirely supported by the Q-neighbourhood of v, on which it coincides with a codeword of the tensor code $C_A \otimes C_B$, and such that $|x + y| < |x|$.

Proof. We consider a left-right Cayley complex X from Section 3.2 over a group G, satisfying the TNC condition and such that $\mathsf{Cay}(G, A)$ and $\mathsf{Cay}(G, B)$ are Ramanujan graphs.

Let $x \in \mathcal{C}_1$ be a codeword of weight $|x| < \delta n/4\Delta^{3/2+\varepsilon}$. It induces a subgraph $\mathcal{G}_{1,x}^\square$ of $\mathcal{G}_1^\square$ with vertex set $S \subset V_1$. The local view for any $v \in S$ corresponds to a codeword of $C_1^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$. This code is w-robust so codewords of weight less than $w = \Delta^{3/2-\varepsilon}$ have a support restricted to a small number $\leqslant w/(\delta\Delta)$ of rows and columns: in particular, the local view restricted to any column (or row) is at distance at most $\Delta^{1/2-\varepsilon}/\delta$ from a codeword of C_A (or C_B).

Let us call *normal vertices* the vertices of S with degree less than $\Delta^{3/2-\varepsilon}$ in $\mathcal{G}_{1,x}^\square$, and define S_e, the set of *exceptional vertices* with degree greater than $\Delta^{3/2-\varepsilon}$. Expansion in $\mathcal{G}_1^\square$ ensures that the set of exceptional vertices is small compared to S.

Claim 10. *The set of exceptional vertices has size*

$$|S_e| \leqslant \frac{64}{\Delta^{1-2\varepsilon}}|S|. \tag{6}$$

Proof. The degree of each vertex $v \in S$ in the subgraph $\mathcal{G}_{1,x}^{\square}$ is at least $\delta\Delta$ since the local view must correspond to a codeword of $C_1^{\perp} = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$. It implies that

$$|S| \leqslant \frac{2|x|}{\delta\Delta} \leqslant \frac{1}{4\Delta^{1/2+\varepsilon}}|V_1|. \tag{7}$$

Applying the Expander Mixing Lemma 3 to $E(S_e, S)$ in $\mathcal{G}_1^{\square}$, regardless of whether $\mathcal{G}_1^{\square}$ is bipartite or not, we obtain from Lemma 4 that:

$$\begin{aligned} |E(S_e,S)| &\leqslant \frac{\Delta^2}{|V_1|}|S_e||S| + 4\Delta\sqrt{|S_e||S|} \\ &\leqslant \frac{1}{2}\Delta^{3/2-\varepsilon}|S_e| + 4\Delta\sqrt{|S_e||S|} \end{aligned}$$

By definition of S_e, it also holds that $|E(S_e, S)| \geqslant \Delta^{3/2-\varepsilon}|S_e|$. Combining both inequalities, we obtain $\Delta^{1/2-\varepsilon}\sqrt{|S_e|} \leqslant 8\sqrt{|S|}$ and the claim follows. □

The support of the local view of any normal vertex of S decomposes into a small number of rows and columns, which are shared with vertices in V_0. We now introduce the set T of vertices of V_0 whose local views share with a normal vertex of S either a row or a column of large weight. Formally:

Defining the subset $T \subset V_0$. The vector x, viewed as a set of squares, defines a subset E_x of edges of $\mathcal{G}^{\cup}$, namely the edges incident to a square in x. Let us say that an edge of E_x is *heavy,* if it is incident to at least $\delta\Delta - \Delta^{1/2-\varepsilon}/\delta$ squares of x. Let T be the set of vertices of V_0 that are connected to (at least) one *normal* vertex of S *through a heavy edge*. Let us keep in mind that the local view of a normal vertex of S is supported by at most $\Delta^{1/2-\varepsilon}/\delta$ rows and at most $\Delta^{1/2-\varepsilon}/\delta$ columns, so a heavy edge between a normal vertex of S and a vertex of T corresponds to either a row or a column shared by the two local views, which is at distance at most $\Delta^{1/2-\varepsilon}/\delta$ from a nonzero codeword of C_A (or C_B).

Claim 11. *The degree in E_x of any vertex of T is at least $\delta\Delta - \Delta^{1/2-\varepsilon}/\delta$.*

Proof. This follows simply from the fact that a row of weight w in a local view is incident to w columns. □

Claim 12. *For Δ large enough, the size of the set T satisfies:*

$$|T| \leqslant \frac{64}{\delta^2\Delta}|S|. \tag{8}$$

Proof. From Claim 11 we have the following lower bound on the number of edges of $\mathcal{G}^{\cup}$ between S and T,

$$|E(S,T)| \geqslant \delta\Delta\Big(1 - \frac{1}{\delta^2\Delta^{1/2+\varepsilon}}\Big)|T|.$$

Applying the Expander mixing Lemma 3 to $E(S,T)$, we have, from Lemma 4,

$$|E(S,T)| \leqslant \frac{4\Delta}{|V|}|S||T| + 4\sqrt{\Delta}\sqrt{|S||T|}.$$

Recalling (7), we have $|S| \leqslant |V|/8\Delta^{1/2+\varepsilon}$, we have therefore

$$|T|\delta\Delta\left(1 - \frac{1}{\delta^2\Delta^{1/2+\varepsilon}} - \frac{1}{2\delta\Delta^{1/2+\varepsilon}}\right) \leqslant 4\sqrt{\Delta}\sqrt{|S||T|}$$

which implies

$$\delta\Delta\sqrt{|T|} \leqslant 8\sqrt{\Delta}\sqrt{|S|}$$

for Δ large enough, from which the claim follows. □

From this last claim we infer that a typical vertex in T must be adjacent to a large number of vertices in S, linear in Δ, which means that its local view should consist of many columns (or rows) containing almost undisturbed codewords of C_A (or C_B). The robustness of $C_A \otimes C_B$ then implies that the local view of such a vertex must be close to a codeword of the tensor code, and that adding the corresponding word will decrease the weight of x. We now detail the argument.

Define $\bar{d}_T$ to be the average (over T) number of heavy edges incident to a vertex of T. The number of edges between T and $S \setminus S_e$ is $|E(T, S \setminus S_e)| = \bar{d}_T|T| \geqslant |S| - |S_e|$. Applying (6) and (8), we have

$$\bar{d}_T \geqslant \frac{|S| - |S_e|}{|T|} \geqslant \frac{\delta^2}{64}\left(1 - \frac{64}{\Delta^{1-2\varepsilon}}\right)\Delta =: 2\alpha\Delta.$$

Let η be the fraction of vertices of T with degree greater than $\alpha\Delta$. Since the maximum degree of a vertex in $\mathcal{G}^\cup$ is 2Δ, it holds that

$$2\alpha\Delta \leqslant \bar{d}_T \leqslant 2\Delta\eta + (1-\eta)\alpha\Delta$$

and $\eta \geqslant \alpha/(2-\alpha) \geqslant \alpha/2$. We have just shown:

Claim 13. *At least a fraction $\alpha/2$ of vertices of T are incident to at least $\alpha\Delta$ heavy edges.*

We will need to single out a vertex v of T whose existence is guaranteed by claim 13, but we also need this vertex to not be incident to too many exceptional vertices of S. To this end we estimate the total number of edges of $\mathcal{G}^\cup$ between T and S_e.

From the Expander mixing Lemma 3,

$$\begin{aligned} E(S_e,T) &\leqslant \frac{4\Delta}{|V|}|S_e||T| + 4\sqrt{\Delta}\sqrt{|T||S_e|} \\ &\leqslant \frac{256\Delta^{2\varepsilon}}{|V|}|T||S| + 32\Delta^{\varepsilon}\sqrt{|T||S|} \\ &\leqslant \frac{32}{\Delta^{1/2-\varepsilon}}|T| + 32\Delta^{\varepsilon}\sqrt{|T||S|} \end{aligned} \tag{9}$$

by first applying (6), and then (7). Now every vertex of $S \setminus S_e$ is, by definition of T, adjacent to a vertex of T in $\mathcal{G}^\cup$. Since the degree of $\mathcal{G}^\cup$ is 2Δ we get that $|S|-|S_e| \leqslant 2\Delta|T|$. From (8), we have that, for Δ large enough, $|S_e| \leqslant |S|/2$, whence $|S| \leqslant 4\Delta|T|$. From (9) we therefore obtain

$$E(S_e, T) \leqslant \beta\Delta^{1/2+\varepsilon}|T|$$

with $\beta = 64+32/\Delta$. We therefore have that at most an $\alpha/4$ proportion of vertices of T are adjacent to more than $\frac{4}{\alpha}\beta\Delta^{1/2+\varepsilon}$ vertices of S_e. Summarising, we have shown, together with claim 13

Claim 14. *At least a fraction $\alpha/4$ of vertices of T*

- *are incident to at least $\alpha\Delta$ heavy edges.*
- *are adjacent to at most $d_1 = \frac{4\beta}{\alpha}\Delta^{1/2+\varepsilon}$ vertices of S_e.*

Pick any vertex v whose existence is guaranteed by claim 14. The local view at v is illustrated on Figure 3.

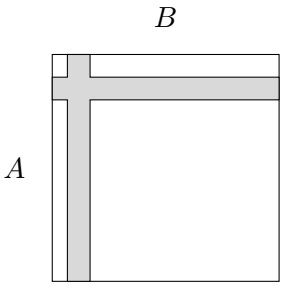

Figure 3: The local view at v from Claim 14. There are at most $d_1 \leqslant \Delta^\gamma$ rows and d_1 columns (shaded) that are shared with local views from exceptional vertices of S. All other rows and columns are shared with normal vertices of S, and differ from a codeword of C_B or C_A on at most $\Delta^{1/2-\varepsilon}/\delta$ coordinates.

We may therefore define two subsets $A' \subset A$, $B' \subset B$, with $|A'| = |B'| = \Delta - d_1$, and such that in the view of v, all rows and columns indexed by A' and B' are normal, *i.e.* are not shared with the local views of vertices in S_e. Observe that for Δ large enough we have $d_1 \leqslant \Delta^\gamma$, since we have imposed $\gamma > 1/2 + \varepsilon$. The theorem's hypothesis on resistance to puncturing implies therefore that the punctured code $C_{A'} \otimes \mathbb{F}_2^{B'} + \mathbb{F}_2^{A'} \otimes C_{B'}$ is $\Delta^{3/2-\varepsilon/2}$-robust.

Denote by $x_v \in \mathbb{F}_2^{A\times B}$ the local view of x at vertex v, and by x'_v its restriction to coordinates in $A' \times B'$. Proposition 7, applied for large enough Δ, states that there exists a codeword $c' \in C_{A'} \otimes C_{B'}$ of the punctured code $C_{A'} \otimes C_{B'}$ close to x'_v: specifically,

$$d(x'_v, c') \leqslant \frac{3}{2}\left(d(x'_v, C_{A'} \otimes \mathbb{F}_2^{B'}) + d(x'_v, \mathbb{F}_2^{A'} \otimes C_{B'})\right) \leqslant 3\Delta\frac{\Delta^{1/2-\varepsilon}}{\delta}$$

since each column (or row) of x_v is at distance at most $\frac{\Delta^{1/2-\varepsilon}}{\delta}$ from C_A (or C_B), and there are not more than Δ columns (rows) altogether.

Since $d_1 < \delta\Delta$, there is a unique tensor codeword $c \in C_A \otimes C_B$ that coincides with c' on $A' \times B'$, and we have, since $|(A \times B) \setminus (A' \times B')| \leqslant 2d_1\Delta$,

$$d(x_v, c) \leqslant d(x'_v, c') + 2d_1\Delta.$$

This last upper bound scales like $\Delta^{3/2+\varepsilon}$, but the first point of Claim 14 implies that the weight of x_v is a quantity that scales like Δ^2, so for large enough values of Δ it must be that $d(x_v, c) = |x_v + c| < |x_v|$ (implying in particular that c is non-zero). Defining the vector $y \in \mathbb{F}_2^Q$ to coincide with c on the Q-neighbourhood of v and to be zero elsewhere, we have just shown that $|x| - |x+y| = |x_v| - |x_v + c|$ is positive, which concludes the proof of the theorem. □

Remark 15. *The last part of the proof of Theorem 1 shows that when Δ is large enough, not only do we have $|x| - |x+y| > 0$ for y thus constructed, but there is furthermore a constant a such that we have $|x| - |x+y| > a\Delta^2$.*

Remark 16. *Theorem 1 stays valid for negative values of ε, i.e. when $\varepsilon \in (-1/2, 0)$. In this case however, there is no need for any resistance to puncturing, because the exceptional rows and columns at the local view of v from Claim 14 will number $o(\Delta^{3/2})$ and contribute a negligible amount to the distance between x_v and the tensor codeword c.*

4.3 Consequences of Theorem 1: asymptotically good quantum LDPC codes

The following theorem is a direct consequence of Theorem 1.

Theorem 17. *Fix $\rho \in (0, 1/2)$, $\varepsilon \in (0, 1/2)$, $\gamma \in (1/2 + \varepsilon, 1)$ and $\delta > 0$. If Δ is large enough and C_A and C_B are codes of length Δ such that*

1. *$0 < \dim C_A \leqslant \rho\Delta$ and $\dim C_B = \Delta - \dim C_A$,*
2. *the minimum distances of $C_A, C_B, C_A^\perp, C_B^\perp$ are all $\geqslant \delta\Delta$,*
3. *both dual tensor codes $C_0^\perp = (C_A \otimes C_B)^\perp$ and $C_1^\perp = (C_A^\perp \otimes C_B^\perp)^\perp$ are $\Delta^{3/2-\varepsilon/2}$-robust with Δ^γ-resistance to puncturing,*

then the quantum code $\mathcal{Q} = (\mathcal{C}_0, \mathcal{C}_1)$ defined in (4) has parameters

$$[\![n, k \geqslant (1-2\rho)^2 n, d \geqslant \frac{\delta}{4\Delta^{3/2+\varepsilon}} n]\!].$$

Proof. The statement on the dimension k is formula (5). Recall that the minimum distance of the quantum code $\mathcal{Q}$ is the smallest weight of a vector that is either in $\mathcal{C}_0 \setminus \mathcal{C}_1^\perp$ or in $\mathcal{C}_1 \setminus \mathcal{C}_0^\perp$. Let $x \in \mathcal{C}_1$ be a non-zero vector of weight $< \delta n / 4\Delta^{3/2+\varepsilon}$. The vector y guaranteed by Theorem 1 is in $\mathcal{C}_0^\perp \subset \mathcal{C}_1$, and since $|x + y| < |x|$, we may apply repeatedly

Theorem 1 to create a sequence of vectors of $\mathcal{C}_1$ of decreasing weights, and ultimately obtain that x must be a sum of vectors of $\mathcal{C}_0^\perp$. The same argument applies symmetrically to the weight of vectors of $\mathcal{C}_0 \setminus \mathcal{C}_1^\perp$, since we have imposed that $C_A^\perp$ and $C_B^\perp$ also satisfy the hypotheses of Theorem 1. □

To obtain asymptotically good families of quantum codes it remains to show that codes C_A, C_B satisfying the conditions 1,2,3 of Theorem 17 exist. This is achieved through the random choice result of Theorem 9.

Specifically, we have:

Theorem 18. *Fix $\rho \in (0, 1/2)$, $\varepsilon \in (0, 1/2)$, $\gamma \in (1/2+\varepsilon, 1)$ and $\delta > 0$ such that $-\delta \log_2 \delta - (1-\delta)\log_2(1-\delta) < \rho$. Fix some large enough Δ and let $r = \lfloor \rho\Delta \rfloor$. Let C_A be the random code defined by a random uniform $r \times \Delta$ generator matrix and let C_B be the random code defined by a random uniform $r \times \Delta$ parity-check matrix. With non-zero probability C_A and C_B satisfy conditions 1,2,3 of Theorem 17 yielding an infinite family of quantum codes of parameters*

$$[\![n, k \geqslant (1-2\rho)^2 n, d \geqslant \frac{\delta}{4\Delta^{3/2+\varepsilon}} n]\!].$$

Proof. It is well-known that for $r < \Delta$, a random uniform $r \times \Delta$ matrix has rank r with probability at least $1 - 1/2^{\Delta - r}$ so condition 1 will hold with probability tending to 1 when Δ goes to infinity.

The value δ has been chosen to be below the Gilbert-Varshamov bound for the imposed rates of all 4 codes $C_A, C_B, C_A^\perp, C_B^\perp$, so all their minimum distances will be $\geqslant \delta\Delta$ with probability tending to 1 when Δ goes to infinity.

Finally, both the pair (C_A, C_B) and the pair $(C_A^\perp, C_B^\perp)$ are chosen according to the same probability distribution, namely one random uniform generator matrix and one random uniform parity-check matrix, therefore, with probability tending to 1 when Δ goes to infinity, both dual tensor codes $C_0^\perp$ and $C_1^\perp$ will satisfy the conclusion of Theorem 9 in other words condition 3. □

An upper bound on the minimum distance of $\mathcal{Q}$. To evaluate the tightness of the lower bound on the minimum distance d of the quantum code $\mathcal{Q}$ given by Theorem 17, we now derive the following upper bound on d.

Proposition 19. *The minimum distance d of the quantum code $\mathcal{Q}$ is not more than n/Δ.*

Recalling Remark 16, we have that if we could find the required dual tensor codes $C_0^\perp$ and $C_1^\perp$ that are both $\Delta^{3/2-\varepsilon}$-robust for $\varepsilon \to -1/2$, we would obtain a lower bound on the quantum code minimum distance that practically closes the gap with the upper bound of Proposition 19.

To prove Proposition 19 we shall show the existence of small-weight ($\leqslant n/\Delta$) codewords of $\mathcal{C}_1 \setminus \mathcal{C}_0^\perp$. We do this by constructing many small-weight codewords of $\mathcal{C}_1$, that are too numerous to all be in $\mathcal{C}_0^\perp$. Those codewords are best described when using the quadripartite version of the Left-Right Cayley complex described at the end of Section 3.2. In this case the graph $\mathcal{G}_1^\square$ is bipartite, with its vertex set V_1 split into the disjoint union

of two sets V_{10} and V_{01}. We have that for every vertex $v \in V_1$, all squares in its local view that are indexed by row a, are indexed by row a^{-1} in all neighbouring local views. Therefore, if for every vertex $v \in V_{10}$ we restrict its Q-neighbourhood $Q(v)$ to row a for a fixed a, and similarly restrict all Q-neighbourhoods of vertices of V_{01} to row a^{-1}, we obtain a subgraph $\mathcal{G}_{1a}^{\square}$ of $\mathcal{G}_1^{\square}$ that is a copy of the double cover of the graph $\mathsf{Cay}(G, B)$. Furthermore, the edge set of $\mathcal{G}_1^{\square}$ is the disjoint union of the edge sets of the graphs $\mathcal{G}_{1a}^{\square}$ for a ranging in A.

Now we see that any codeword of the Tanner code $T(\mathcal{G}_{1a}^{\square}, C_B)$ yields a codeword of $\mathcal{C}_1$, where every non-zero local view at any vertex of V_{10} must be entirely supported by row a (and row a^{-1} for vertices of V_{01}) and coincide with a codeword of C_B. Any such codeword has weight at most n/Δ: expanding $T(\mathcal{G}_{1a}^{\square}, C_B)$ to the whole index set $\mathcal{G}_1^{\square}$ by padding its words with 0s, we may define the disjoint direct sum

$$\mathcal{L} = \sum_{a \in A} T(\mathcal{G}_{1a}^{\square}, C_B).$$

We claim that:

Lemma 20. $\dim \mathcal{L} \cap \mathcal{C}_0^{\perp} \leqslant 2 \dim C_A . \dim T(\mathcal{G}_{1a}^{\square}, C_B)$ *for any given* $a \in A$. *In particular when* $\dim C_A < \Delta/2$ *we have* $\mathcal{L} \not\subset \mathcal{C}_0^{\perp}$.

The second claim of Lemma 20 follows from the first, since clearly $\dim \mathcal{L} = \Delta \ell$ where ℓ is the common dimension of the Δ isomorphic Tanner codes $T(\mathcal{G}_{1a}^{\square}, C_B)$. Lemma 20 implies therefore that at least one non-zero Tanner codeword in some $T(\mathcal{G}_{1a}^{\square}, C_B)$ (which must be of weight $\leqslant n/\Delta$) cannot be in $\mathcal{C}_0^{\perp}$ which proves Proposition 19. It remains therefore to prove Lemma 20. We will need the following easy fact on Tanner codes on bipartite graphs:

Lemma 21. *Let* $\mathcal{G} = (W, E)$ *be a regular bipartite graph on the vertex set* $W = W_0 \cup W_1$, *and let* $C = T(\mathcal{G}, C_0)$ *be a Tanner code on it for some inner code* C_0. *Let* $x = \sum_{w \in W} c_v$ *be a vector in* $\mathbb{F}_2^E$ *such that every* c_w *is a word supported by the edge-neighbourhood* $E(w)$ *of* w *and that coincides with a codeword of* C_0 *on* $E(w)$. *Then if* x *is a Tanner codeword of* C, *then so are the partial sums* $\sum_{w \in W_0} c_w$ *and* $\sum_{w \in W_1} c_w$.

Proof. We have that $x = \sum_{w \in W_0} x_w = \sum_{w \in W_1} x_w$ where x_w is the local view of x at vertex w. Therefore $\sum_{w \in W} c_w + \sum_{w \in W_1} x_w = 0$, so that

$$\sum_{w \in W_0} c_w = \sum_{w \in W_1} c_w + x_w$$

and therefore $\sum_{w \in W_0} c_w$ is a vector whose local views, both at vertices of W_0 and at vertices of W_1, are all in C_0, so $\sum_{w \in W_0} c_w$ is a Tanner codeword. Similarly, so is $\sum_{w \in W_1} c_w$. □

Proof of Lemma 20. Let $e_1, \dots e_k$ be a basis of C_A corresponding to some information set $a_1, \dots, a_k$, for $k = \dim C_A$. This means that e_i has value 1 on index a_i and has value 0 on all indices $a_j, j \neq i$.

Let $x \in \mathcal{L} \cap \mathcal{C}_0^\perp$. Since $x \in \mathcal{C}_0^\perp$, it decomposes as

$$x = \sum_{i=1}^{k} \sum_{v \in V_{00}} e_i \otimes x_v^i + \sum_{i=1}^{k} \sum_{w \in V_{11}} e_i \otimes x_w^i. \tag{10}$$

where x_v^i, x_w^i are all codewords of C_B. We have abused notation somewhat by identifying the local view of x at a vertex v with its decomposition expressed as a tensor codeword. But the point is that every term of the form $e_i \otimes x_v^i$ contributes to the sum (10) a codeword of C_B to the local view at v on row a_i. Since we must see on column a_i a Tanner codeword of $T(\mathcal{G}_{1a_i}^\square, C_B)$ (because $x \in \mathcal{L}$), we have from Lemma 21 that the whole sum

$$\sum_{v \in V_{00}} e_i \otimes x_v^i$$

must be equal, when restricted to row a_i, to a codeword of $T(\mathcal{G}_{1a_i}^\square, C_B)$. Therefore, the left part of the sum (10) must belong to a sum of $\dim C_A$ codes all isomorphic to a $T(\mathcal{G}_{1a}^\square, C_B)$ Tanner code, and by a similar argument, so must the right part of the sum, which concludes the proof. □

4.4 Consequences of Theorem 1: classical locally testable codes

Let X be the left right Cayley complex of Theorem 1, and let $C_A = C_B$ be a code of length Δ, rate $\rho \in (0,1)$ and distance $\delta\Delta$ and suppose that the associated dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ satisfies Theorem 1.

Let $C_0 = C_A \otimes C_B$: the Tanner code $\mathcal{C} = T(\mathcal{G}_0^\square, C_0)$ is precisely the locally testable code defined of Dinur *et al.* and is shown ([DEL+21]) to have parameters

$$[n, k \geqslant (2\rho^2 - 1)n, d \geqslant \delta^2(\delta - \lambda/\Delta)n]$$

where λ is the (common) second largest eigenvalue of the constituent Ramanujan Cayley graphs.

Recall from [DEL+21] the tester for this code: given a word $x \in \mathbb{F}_2^Q$, pick a random vertex $v \in V_0$, accept if the local view x_v belongs to the tensor code C_0 and reject if $x_v \notin C_0$. Let $T \subset V_0$ be the set of vertices for which the local test rejects,

$$T = \{v \in V_0 \,:\, x_v \notin C_0\}.$$

The fraction of rejecting local tests is therefore $\zeta(x) := \frac{|T|}{|V_0|}$.

Recall that a code is said to be locally testable with q queries and detection probability κ, if the tester accesses at most q bits from x, always accepts when x is a codeword, and otherwise satisfies

$$\zeta(x) \geqslant \kappa \frac{1}{n} d(x, \mathcal{C}). \tag{11}$$

In the present case, the number of queries is $q = \Delta^2$, the size of the Q-neighbourhood of a vertex. The goal is to establish (11) for some constant κ.

The strategy to establish the local testability of the code $\mathcal{C}$ is to define a decoder that is guaranteed to always find a codeword close to x if $\zeta(x)$ (or $|T|$) is sufficiently small. The difference with a classical decoder is that we make no assumption on how far x actually is from the code $\mathcal{C}$.

Theorem 1 can be converted into such a decoding algorithm. Let $x \in \mathbb{F}_2^Q$ be an initial vector. Our goal is to find a close enough codeword $c \in \mathcal{C}$. For each vertex $v \in V_0$, let $c_v \in C_0$ be the closest codeword to the local view x_v (breaking ties arbitrarily), and let $e_v := x_v + c_v$ be the local corresponding error (of minimum weight). We slightly abuse notation here and write c_v or e_v for both the vectors in $\mathbb{F}_2^{Q(v)}$ and the vectors in $\mathbb{F}_2^Q$ coinciding with e_v, c_v on $Q(v)$ and equal to zero elsewhere.

The decoder. The decoder starts by computing the list $(c_v)_{v\in V_0}$ from the decompositions $x_v = c_v + e_v$. Note that this local decoding can be achieved by brute-force if need be since the local code has constant length Δ^2. Note also that the list of these local views is not necessarily equal to the list of local views of a codeword $c \in \mathcal{C}$ (if it does then the decoder outputs c). The decoder then computes what we may call the *mismatch* of the list (c_v), and which is defined as $z = \sum_v c_v$. If the weight $|z|$ is too large, namely $\geqslant \delta n/4\Delta^{3/2+\varepsilon}$, then the decoder will refuse to continue and output "far from the code". Otherwise the decoder proceeds by looking for a vertex $v \in V_0$ on which it will update the value of c_v, replacing it by $c'_v = c_v + y_v$ for some non-zero $y_v \in C_0$, so as to decrease the weight of the new value $z + y_v$ of the mismatch. Among all possible vertices v and small codewords $y_v \in C_0$, let it choose the one that maximizes $|z| - |z + y_v|$.

The decoder proceeds iteratively in this way until it has a list of local views with a zero mismatch, corresponding therefore to the list of local views of a global codeword $c' \in \mathcal{C}$ which it outputs.

Claim 22. *If $|z| < \delta n/4\Delta^{3/2+\varepsilon}$, then the decoder always converges to the zero mismatch and a codeword c' of $\mathcal{C}$.*

Proof. The crucial observation is that z is a codeword of $\mathcal{C}_1 = T(\mathcal{G}_1^{\square}, C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B)$, the Tanner code defined on the graph $\mathcal{G}_1^{\square}$ (with vertices in V_1), and local code given by the *dual* tensor code. In the language of the quantum codes of the previous section, this is simply because $\sum_{v\in V_0} c_v$ is a sum of generators. Theorem 1 asserts that there exists a generator $y_v \in C_0$ such that $|z| - |z + y_v| > a\Delta^2$, for some constant $a > 0$, independent of n (and mentioned in Remark 15). □

Claim 23. *If $|z| < \delta n/4\Delta^{3/2+\varepsilon}$, then the distance from x to $\mathcal{C}$ is bounded by*

$$d(x, \mathcal{C}) \leqslant n\Big(1 + \frac{1}{a}\Big)\zeta(x). \tag{12}$$

Proof. Let $(c'_v)_{v\in V_0}$ be the list of local views of the output codeword c'. Writing $x = c' + e'$, we have that the local views e'_v of e' satisfy $x'_v = c'_v + e'_v$ and

$$d(x, c') = |e'| = \frac{1}{2}\sum_{v\in V_0} |e'_v|.$$

Let S be the list of vertices of V_0 whose output value c'_v differs from the original value c_v. Writing $x = c' + e'$, and remembering that T is the set of vertices v for which the original e_v is non-zero, we may bound from above $|e'|$ by

$$\sum_{v\in T} |e_v| + \sum_{v\in S} |e'_v| \leqslant \Delta^2(|T| + |S|).$$

We must have $|S| \leqslant |z|/(a\Delta^2)$. Furthermore, since each bit of the word x appears twice in the sum $\sum_{v\in V_0} x_v = \sum_{v\in V_0}(c_v + e_v)$, we have that $\sum_{v\in V_0} c_v = \sum_{v\in V_0} e_v = z$, from which we infer that $|z| \leqslant |T|\Delta^2$. Putting this together, we obtain

$$|e'| \leqslant \Delta^2(|T| + |T|/a) = \Delta^2|V_0|\Big(1 + \frac{1}{a}\Big)\zeta(x)$$

whence

$$d(x, \mathcal{C}) \leqslant n\Big(1 + \frac{1}{a}\Big)\zeta(x). \qquad \square$$

Let us now consider a word $x \in \mathbb{F}_2^Q$ such that $|z| \geqslant \delta n/4\Delta^{3/2+\varepsilon}$, in which case the decoder gives us nothing. We nevertheless have that, again using $|z| \leqslant \Delta^2|T|$,

$$\frac{1}{n}d(x, \mathcal{C}) \leqslant 1 \leqslant \frac{4\Delta^{3/2+\varepsilon}|z|}{\delta n} \leqslant \frac{4\Delta^{7/2+\varepsilon}|T|}{\delta n} = \frac{4\Delta^{7/2+\varepsilon}|V_0|}{\delta n}\zeta(x) = \frac{8\Delta^{3/2+\varepsilon}}{\delta}\zeta(x). \tag{13}$$

From (12) and (13), we obtain that the Tanner code $\mathcal{C} = T(\mathcal{G}_0^{\square}, C_0)$ is κ-locally testable with Δ^2 queries and

$$\kappa = \min\Big(\frac{a}{a+1}, \frac{\delta}{8\Delta^{3/2+\varepsilon}}\Big).$$

We conclude this section with a word of comment on the choice of the small component code $C_A = C_B$. To obtain an LTC we need it to satisfy the hypotheses of Theorem 1. One way is to obtain this by random choice, namely by applying Theorem 9, as we did in Section 4.3. But since this time we have no need for the robustness of $C_A^\perp \otimes C_B^\perp$, there are alternatives: in [DEL⁺21], the component codes that are used have better robustness than what is guaranteed by Theorem 9.

A Appendix: proof of Theorem 9

The proof follows the blueprint of [PK21], though puncturing is handled a little differently.

Let $C_A \subset \mathbb{F}_2^A$ and $C_B \subset \mathbb{F}_2^B$ and let C be the dual tensor code $C = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$. Let $X \subset \mathbb{F}_2^{A\times B}$ be a $\Delta \times \Delta$ matrix. Let H_A be an $r_A \times \Delta$ parity-check matrix for the column code C_A. The $r_A \times \Delta$ matrix $H_A X$ is such that, for every $b \in B$, its b-th column is the H_A-syndrome of the b-th column of X. We note that $X \in C$ iff $H_A X$ is such that everyone of its r_A rows is a codeword of C_B.

Lemma 24. *Let V be a set of vectors of $\mathbb{F}_2^A$. Suppose that the union of the supports in A of the vectors of V has size $t < d_A/2$, where d_A is the minimum distance of C_A. Then* $\mathrm{rk}\{H_A v : v \in V\} = \mathrm{rk} V$, *where* rk *denotes the rank function.*

Proof. The syndrome map $x \mapsto H_A x^\top$ is injective on the Hamming ball of radius t, therefore for a subset W of vectors x of V, $\sum_W H_A x = 0$ implies $\sum_W x = 0$. So if $W \subset V$ is a set of linearly independent vectors, $\mathrm{rk}\{H_A x : x \in W\} = |W|$. □

Let $d > 2\alpha\Delta_A$ be a lower bound on the minimum distance d_A of C_A, for some constant α.

Lemma 25. *Let X be a $\Delta \times n$ matrix such that all of its columns are of weight $\leqslant \sqrt{\Delta}/\log_2 \Delta$ and such that the number of its non-zero rows is at least $d/2$. Then, for Δ large enough, X has rank at least $\alpha\sqrt{\Delta}\log\Delta$.*

Proof. Let $x_1, x_2, \ldots, x_m$ be a maximum sequence of non-zero columns of X with the property that $\mathrm{supp}(x_i) \notin \cup_{1\leqslant j<i} \mathrm{supp}(x_j)$. We clearly have that $x_1 \ldots, x_m$ are linearly independent, and we have $m \geqslant d/2w$ where w is the maximum weight of a vector x_i, otherwise the union of the supports of all columns of X would be less than $d/2$, contrary to our hypothesis. From $w \leqslant \sqrt{\Delta}/\log_2 \Delta$ we have the result. □

Corollary 26. *Let X be a $\Delta \times n$ matrix such that all of its columns are of weight $\leqslant \sqrt{\Delta}/\log_2 \Delta$ and that has at least $d/2$ non-zero rows. Then $H_A X$ has rank at least $\alpha\sqrt{\Delta}\log\Delta$.*

Proof. Choose $\alpha\sqrt{\Delta}\log\Delta$ linearly independent columns of X, which is possible by Lemma 25. Since the weight of these vectors is not more than $\leqslant \sqrt{\Delta}/\log_2 \Delta$, the sum of all the weights of these vectors is less than $d/2$, therefore Lemma 24 applies and the claim is proved. □

Lemma 27. *Let $\mathbf{C}$ be a random linear code of length n, defined by an $r \times n$ uniform random matrix $\mathbf{H}$. Let V be a set of linearly independent vectors of $\mathbb{F}_2^n$. The probability that all vectors of V fall into the random code $\mathbf{C}$ is equal to $1/2^{r|V|}$.*

Proof. The $\mathbf{H}$-syndrome of a fixed non-zero vector x is uniformly distributed in $\mathbb{F}_2^r$ and the probability that it equals zero is therefore $1/2^r$. When the fixed vectors $x \in V$ are independent in the sense of linear algebra, their $\mathbf{H}$-syndromes are independent in the sense of probability, hence the lemma. □

Lemma 28. *Let $\mathbf{C}$ be a random linear code of length n, defined by an $r \times n$ uniform random matrix $\mathbf{H}$. Let $\mathbf{C}_p$ be the punctured code obtained from $\mathbf{C}$ by throwing away the first p coordinates. Let V be a set of linearly independent vectors of $\mathbb{F}_2^{n-p}$ defined on the set of coordinates $\{p+1, \dots n\}$. Then the probability that all vectors of V fall into the random code $\mathbf{C}_p$ is at most $1/2^{(r-p)|V|}$.*

Proof. Let $\mathbf{W}$ be the random linear subspace of $\mathbb{F}_2^r$ generated by the first p columns of $\mathbf{H}$. Let $\mathbf{H}_p$ be the $r \times (n-p)$ matrix deduced from $\mathbf{H}$ by throwing away its first p columns. A vector $x \in \mathbb{F}_2^{n-p}$ is in the punctured code $\mathbf{C}_p$ iff its $\mathbf{H}_p$-syndrome $\mathbf{H}_p x^\top$ belongs to $\mathbf{W}$. Denote by E_V the event whereby all vectors of V fall into the punctured code $\mathbf{C}_p$. Let W be a fixed subspace of $\mathbb{F}_2^r$ of dimension $w \leqslant p$. Denote by E_W the event whereby the first p columns of $\mathbf{H}$ generate W. We have that the projections onto $\mathbb{F}_2^r/W$ of the columns of $\mathbf{H}_p$ are uniformly distributed and independent in the sense of probability. Therefore, if the first p columns of $\mathbf{H}$ generate the fixed subspace W, Lemma 27 applies and we have $P(E_V|E_W) = 1/2^{(r-w)|V|}$. Now we have

$$P(E_V) = \sum_W P(E_W) P(E_V|E_W)$$

where the sum is over all subspaces W of $\mathbb{F}_2^r$ of dimension at most p. Hence,

$$P(E_V) \leqslant \sum_W P(E_W) \frac{1}{2^{(r-p)|V|}} = \frac{1}{2^{(r-p)|V|}}. \qquad \square$$

Lemma 29. *Let p, r_B be integers such that $0 < p < r_B < \Delta$. Let X_p be a fixed $\Delta \times (\Delta - p)$ binary matrix such that all its columns are of weight $\leqslant \sqrt{\Delta}/\log_2 \Delta$ and that has at least $d/2$ non-zero rows. Let P be a subset of B of cardinality p. Let $\mathcal{X}_P$ be the subset of $\Delta \times \Delta$ matrices that, when leaving out all columns indexed by P, are all equal to X_p.*

Let $\mathbf{C}$ be the random code defined by a uniform random $r_B \times \Delta$ parity-check matrix $\mathbf{H}$. Then the probability that the dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes \mathbf{C}$ contains at least one matrix in $\mathcal{X}_P$ is at most $1/2^{(r_B - p)\alpha\sqrt{\Delta}\log\Delta}$.

Proof. Identifying B with $\{1, \dots, \Delta\}$, we may suppose without loss of generality that P is equal to the set $\{1, \dots, p\}$ of the first p coordinates. Let $\mathbf{C}_p$ be deduced from $\mathbf{C}$ by puncturing the first p coordinates. If $\mathcal{X}_P$ contains one matrix in the dual tensor code, then it must be that all rows of $H_A X_p$ fall into $\mathbf{C}_p$, where H_A is the parity-check matrix of C_A. By Corollary 26 we have that the rank of $H_A X_p$ is at least $\alpha\sqrt{\Delta}\log\Delta$. We now apply Lemma 28 to conclude. $\square$

Let $0 < \rho < 1$ and let $0 < \delta < 1$ be such that $\delta < h^{-1}(1-\rho)$, where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ denotes the binary entropy function. In other words we take δ to be less than the Gilbert-Varshamov bound on the relative minimum distance for codes of rate ρ. This means in particular that, with probability tending to 1 when Δ goes to infinity (more precisely, behaving as $1 - 1/2^{\Omega(\Delta)}$), a random code of rate ρ and length Δ has relative minimum distance at least δ.

Theorem 30. *Let C_A be a fixed code of length Δ and of minimum distance at least $\delta\Delta$. Let $\mathbf{C}$ be a random code obtained from a uniform random parity-check matrix of size $r \times \Delta$ with $r \geqslant \Delta(1-\rho)$. With probability at least $1 - 1/2^{c\Delta^{3/2}}$, with c depending only on ρ, we have that:*

every matrix X of weight at most $\frac{\delta}{2}\Delta^{3/2}/\log_2 \Delta$ is

- *either supported by at most $\delta\Delta/2$ rows and at most $\delta\Delta/2$ columns,*
- *or not in the dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes \mathbf{C}$.*

Proof. A matrix X whose weight is thus upper bounded contains at most $p = \delta\Delta/2$ columns of weight $> \sqrt{\Delta}/\log\Delta$. Therefore, if X is not supported by at most $\delta\Delta/2$ rows and at most $\delta\Delta/2$ columns, it must fall into a subset $\mathcal{X}_P$ of matrices as defined in Lemma 29. So we apply Lemma 29 and count the expected number of sets $\mathcal{X}_P$ that contain a matrix in the dual tensor code. The number of sets $\mathcal{X}_P$ is not more than the number $\binom{\Delta}{p} \leqslant 2^{\Delta}$ of ways of choosing P, times the number of ways of choosing X_p, which is not more than $\binom{\Delta}{\sqrt{\Delta}/\log_2 \Delta}^{\Delta} \leqslant 2^{\Delta^{3/2}}$. Therefore the number of $\mathcal{X}_P$'s is $2^{O(\Delta^{3/2})}$ while the probability that any given $\mathcal{X}_P$ contains a matrix in the dual tensor code is $1/2^{\Omega(\Delta^{3/2}\log\Delta)}$. Hence the result. □

Finally we shall need this last lemma.

Lemma 31. *Let c be a codeword of weight w of the dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ where C_A and C_B have minimum distances d_A and d_B. If c is supported by at most $d_A/2$ rows and at most $d_B/2$ columns, then it is supported by at most w/d_A columns and at most w/d_B rows.*

Proof. Write $c = \mathbf{r} + \mathbf{c}$ where $\mathbf{r} \in \mathbb{F}_2^A \otimes C_B$ is a vector supported by at most $d_A/2$ rows, all of which are in C_B, and where likewise $\mathbf{c} \in C_A \otimes \mathbb{F}_2^B$ has at most $d_B/2$ non-zero columns, all of which are in C_A. We have obviously that $\mathbf{r}$ is supported by at most $|\mathbf{r}|/d_B$ rows and that $\mathbf{c}$ is supported by at most $|\mathbf{c}|/d_A$ columns. Since we clearly have $w = |\mathbf{r}+\mathbf{c}| \geqslant |\mathbf{r}|$ and likewise $w \geqslant |\mathbf{c}|$, the result follows. □

We are now ready to prove Theorem 9, which we recall.

Theorem 9. *Let $0 < \rho_A < 1$ and $0 < \rho_B < 1$. Let $0 < \varepsilon < 1/2$ and $1/2 + \varepsilon < \gamma < 1$. Let C_A be a random code obtained from a random uniform $\rho_A\Delta \times \Delta$ generator matrix, and let C_B be a random code obtained from a random uniform $(1-\rho_B)\Delta \times \Delta$ parity-check matrix. With probability tending to 1 when Δ goes to infinity, the dual tensor code*

$$C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$$

is $\Delta^{3/2-\varepsilon}$-robust with Δ^{γ}-resistance to puncturing.

Proof. Let us fix $\delta < \min(h^{-1}(1-\rho_A), h^{-1}(1-\rho_B))$. By standard union bound arguments, we have that the minimum distances d_A and d_B of C_A and C_B satisfy $\min(d_A, d_B) > \delta\Delta$

with probability $1 - 1/2^{\Omega(\Delta)}$. Set $w = \Delta^{3/2-\varepsilon}$: we have that $w < \frac{\delta}{2}\Delta^{3/2}/\log_2 \Delta$ for Δ large enough. Applying Theorem 30, we have that with probability $1 - 1/2^{\Omega(\Delta)}$, every codeword c of weight $|c| \leqslant w$ of the dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ is supported by at most $d_A/2$ rows and at most $d_B/2$ columns, from which we infer, applying Lemma 31, that c is supported by at most $|c|/d_A$ columns and at most $|c|/d_B$ rows. In other words the dual tensor code $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ is w-robust with probability $1 - 1/2^{\Omega(\Delta)}$.

To obtain resistance to puncturing, we repeat the argument for every pair of subsets $A' \subset A$, $B' \subset B$, $|A'| = |B'| \geqslant \Delta - \Delta^\gamma$. We will obtain that every dual tensor code $C_{A'} \otimes \mathbb{F}_2^{B'} + \mathbb{F}_2^{A'} \otimes C_{B'}$ is *not* w-robust with probability $1/2^{\Omega(\Delta)}$, from which it will follow that all such dual tensor codes are w-robust, except with probability

$$\sum_{i \leqslant \Delta^\gamma} \binom{\Delta}{i}^2 \frac{1}{2^{\Omega(\Delta)}} = \frac{1}{2^{\Omega(\Delta)}}.$$

We note that, for $|A'| = |B'| = \Delta'$, the punctured code $C_{A'}$ is obtained from a random uniform generator matrix of size $\rho_A \Delta \times \Delta'$ and the punctured code $C_{B'}$ is obtained by first choosing a random variable $r \geqslant \Delta' - \rho_B \Delta$ and then, a random uniform $r \times \Delta'$ parity-check matrix for $C_{B'}$. Since Δ'/Δ must tend to 1 when Δ tends to infinity, this justifies applying Theorem 30 to every $C_{A'} \otimes \mathbb{F}_2^{B'} + \mathbb{F}_2^{A'} \otimes C_{B'}$, as just argued. □

References

[AAV13] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum PCP conjecture. *ACM SIGACT news*, 44(2):47–79, 2013. 4

[AE15] Dorit Aharonov and Lior Eldar. Quantum locally testable codes. *SIAM Journal on Computing*, 44(5):1230–1262, 2015. 4

[BE21a] Nikolas P Breuckmann and Jens N Eberhardt. Balanced product quantum codes. *IEEE Transactions on Information Theory*, 67(10):6653–6674, 2021. 2, 10

[BE21b] Nikolas P Breuckmann and Jens N Eberhardt. Quantum low-density parity-check codes. *PRX Quantum*, 2:040101, Oct 2021. 2, 4

[BFLS91] László Babai, Lance Fortnow, Leonid A Levin, and Mario Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing*, STOC '91, page 21–32, New York, NY, USA, 1991. Association for Computing Machinery. 3

[CS96] Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54:1098–1105, Aug 1996. 3, 4, 14

[DEL+21] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. Locally Testable Codes with constant rate, distance, and locality. *arXiv preprint arXiv:2111.04808*, 2021. 1, 2, 3, 5, 6, 7, 8, 9, 11, 12, 16, 26, 28

[EH17] Lior Eldar and Aram W Harrow. Local Hamiltonians whose ground states are hard to approximate. In *Foundations of Computer Science (FOCS), 2017 IEEE 58th Annual Symposium on*, pages 427–438. IEEE, 2017. 4

[EKZ20] Shai Evra, Tali Kaufman, and Gilles Zémor. Decodable quantum LDPC codes beyond the square root distance barrier using high dimensional expanders. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 218–227, 2020. 4, 10

[FML02] Michael H Freedman, David A Meyer, and Feng Luo. Z_2-systolic freedom and quantum codes. *Mathematics of quantum computation, Chapman & Hall/CRC*, pages 287–320, 2002. 4

[Gal62] Robert Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8(1):21–28, 1962. 4

[Gol10] Oded Goldreich. *Short Locally Testable Codes and Proofs: A Survey in Two Parts*, pages 65–104. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010. 3

[Got97] Daniel Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997. 14

[GS06] Oded Goldreich and Madhu Sudan. Locally Testable Codes and PCPs of Almost-Linear Length. *J. ACM*, 53(4):558–655, jul 2006. 3

[Gur10] Venkatesan Guruswami. Expander codes and their decoding. https://www.cs.cmu.edu/~venkatg/teaching/codingtheory/notes/notes8.pdf, 2010. 14

[Has13] Matthew B Hastings. Trivial low energy states for commuting Hamiltonians, and the quantum PCP conjecture. *Quantum Information & Computation*, 13(5-6):393–429, 2013. 4

[Has17] Matthew B Hastings. Quantum codes from high-dimensional manifolds. In *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017. 4

[Has21] Matthew B Hastings. On quantum weight reduction. *arXiv preprint arXiv:2102.10030*, 2021. 10

[HHO20] Matthew B Hastings, Jeongwan Haah, and Ryan O'Donnell. Fiber Bundle Codes: Breaking the $N^{1/2}$polylog(N) Barrier for Quantum LDPC Codes. *arXiv preprint arXiv:2009.03921*, 2020. 2, 4

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006. 11

[Kit03] Alexei Yu Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, 2003. 4

[KT20] Tali Kaufman and Ran J Tessler. Quantum LDPC codes with $\Omega(\sqrt{n}\log^k n)$ distance, for any k. *arXiv preprint arXiv:2008.09495*, 2020. 4

[LH22] Ting-Chun Lin and Min-Hsiu Hsieh. c^3-local testable codes from lossless expanders. *arXiv preprint arXiv:2201.11369*, 2022. 3

[LLZ21] Anthony Leverrier, Vivien Londe, and Gilles Zémor. Towards Local Testability for Quantum Coding. In James R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, volume 185, pages 65:1–65:11. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2021. 4

[PK20] Pavel Panteleev and Gleb Kalachev. Quantum LDPC Codes with Almost Linear Minimum Distance. *arXiv preprint arXiv:2012.04068*, 2020. 2, 4

[PK21] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical LDPC codes. *arXiv preprint arXiv:2111.03654*, 2021. 2, 3, 4, 7, 8, 10, 13, 17, 18, 29

[PS94] Alexander Polishchuk and Daniel A Spielman. Nearly-linear size holographic proofs. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 194–203, 1994. 10

[SS96] Michael Sipser and Daniel A. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, 1996. 2, 6, 14

[Ste96] Andrew M. Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77:793–797, Jul 1996. 3, 4, 14

[Tan81] R. Tanner. A recursive approach to low complexity codes. *IEEE Transactions on Information Theory*, 27(5):533–547, 1981. 2, 6, 13

[TZ14] Jean-Pierre Tillich and Gilles Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2014. 2, 4