Good quantum low-density parity-check codes

Fanny Terrier

Good quantum low-density parity-check codes

Fanny TERRIER
Master Quantum Information - Sorbonne university
Supervisor: Anthony LEVERRIER

Abstract

This manuscript is a report of an internship done at INRIA on the subject of quantum error correction. In particular, some theoretical aspects of the quantum Tanner codes are explored such as the non-trivial logical operators bases, the number of logical qubits and the modified minimal distance when constructing the code from a Abelian group.

Contributions :

- Oral presentation of an article proving the No-Low Energy Stabilizer states conjecture, which is an implication of the Quantum PCP conjecture, using the Quantum Tanner codes construction [Cob+23]. The slides are available at https://t.ly/lqKz3,
- Adaptation of the proof for the minimal distance of the quantum Tanner codes when considering a Abelian group,
- Derivation of the non-trivial logical operators bases and the number of logical qubits for the non-lifted quantum Tanner codes obtained by modification of a Hypergraph Product code.
- Attempts to derive the non-trivial logical operators bases and the number of logical qubits for the lifted quantum Tanner codes, i.e the ones achieving a linear minimal distance.
- Numerical simulations to conjecture or corroborate the theoretical results. Some of the Python code implemented can be found at https://t.ly/FShcS

To clarify the contributions, the following color code is used throughout this manuscript:

Properties or lemmas
from the litterature

Properties or lemmas
derived during this internship

Contents

I Preliminaries **3**
- A Classical error correction . . . 3
  - A.1 Linear code . . . 3
  - A.2 Classical product code . . . 4
  - A.3 Tensor and dual tensor codes . . . 4
- B Quantum error correction . . . 5
  - B.1 Stabilizer codes . . . 5
  - B.2 Logical operators . . . 6
- C Graph theory . . . 6
  - C.1 Cayley graphs . . . 6
  - C.2 Left-right Cayley Complexes . . . 7
- D Description of quantum Tanner codes . . . 7

II From hypergraph product codes to quantum Tanner codes **9**
- A Description of hypergraph product code (HGP code) . . . 9
- B From HGP code to non-lifted quantum Tanner codes . . . 11
- C Rank of $\widetilde{H_X}$ . . . 13
- D Logical operators bases for the non-lifted quantum Tanner codes . . . 14
  - D.1 Basis for logical operators under a tensor form . . . 15
  - D.2 Bases for every logical operators . . . 17

III Lifted quantum Tanner codes **19**
- A Graph lift . . . 19
- B Exploration into the basis of logical operators . . . 20

IV Abelian quantum Tanner codes **21**
- A Cayley graphs expanding property for Abelian groups . . . 21
- B Minimal distance with Abelian groups . . . 21

V Conclusion and perspectives **24**

Appendices **26**

A Parameters of the hypergraph product code **26**

B Proofs of Section III-D **26**
- A Proof of Lemma 14 . . . 26
- B Proof of Lemma 15 . . . 27
- C Proof of Property 17 . . . 27

I Preliminaries

A Classical error correction

A.1 Linear code

An error correcting code is encoding k bits in a string of length n. The message to be transmitted has length k and the encoded message has length n.

Definition (Error correcting code). *Let Σ be an alphabet. An error correcting code is a subset $C \subset \Sigma^n$ of size $|C| = |\Sigma|^k$ equipped with an encoding map*

$$E : \Sigma^k \longrightarrow C \,,$$

and a decoding map

$$D : \Sigma^n \longrightarrow \Sigma^k$$

In the following, we will only consider codes over the binary alphabet, i.e $\Sigma = \mathbb{F}_2$.

The error correcting capability to detect and correct errors can be described by the minimal distance of the code.

Definition (Minimal distance). *Let $x, y \in C$ be two codewords. The distance d between x and y is the number of symbols on which they differ, i.e*

$$d(x, y) = |i \in [n] | x_i \neq y_i|$$

The minimal distance of the code C is the minimal distance between any two distinct codewords x, y belonging to the code

$$d_{\min}(C) = \min_{x,y \in C, x \neq y} d(x, y)$$

A code C encoding a message of length n into k bits and with minimal distance d is denoted as $C = [n, k, d]$. An $[n, k, d]$ code is said to be asymptotically good if $k = \Theta(n)$ and $d = \Theta(n)$.

Definition (Linear code). *Let $\mathbb{F}$ be a finite field. In a linear code, $\Sigma = \mathbb{F}$ and $C \subset \mathbb{F}^n$ is a k-dimensional subspace. The encoding map is a linear map: $E(x) = xG$ where G is a $k \times n$ matrix over $\mathbb{F}$ named the generator matrix.*

Since a linear code is a subspace of a vector space, it is the kernel of some linear transformation and as a result another useful way to describe a linear code is to define it as the kernel of a matrix $H \in \mathbb{F}_2^{(n-k)\times n}$, the *parity-check* matrix, for which each row corresponds to a linear constraint every codeword has to respect :

$$\forall x \in C,\ Hx = 0 \bmod 2. \tag{1}$$

A Tanner graph is a bipartite graph allowing to visualize the linear constraints of a code as depicted on Fig.1 for the Hamming code $[7, 4, 3]$. One set of vertices corresponds to the set of bits nodes, the other one to the different parity-check constraints, and the adjacency matrix corresponds to the parity-check matrix.
By construction, the rows of G are orthogonal to the rows of H, i.e $HG^T = 0 (mod\ 2)$. The orthogonal complement of C in $\mathbb{F}_2^n$, denoted $C^\perp$ and called the *dual code*, is defined by $GH^T = 0$. In other words, the generator matrix G of C is the parity matrix of $C^\perp$ and the parity matrix H of C is the generator matrix of $C^\perp$. As a vector of even weight is self-orthogonal, it is possible for C and $C^\perp$ to intersect. For a dual pair, all the members of one code satisfy all parity checks represented by members of the other code.

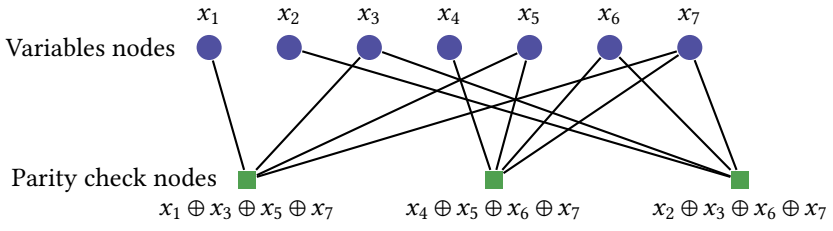

Figure 1: Tanner graph associated to the Hamming code $[7, 4, 3]$.

The Gilbert-Varshamov bound for linear codes gives an upper bound on the rate of a code given length and minimal distance [Gil52; Var57]. The proof of this bound by a probabilistic method also gave rise to Theorem 1 which states that a random binary code is asymptotically good with high probability. From this, it follows that to find a good random linear code of length n would take time $e^{\Omega(n)}$.

Theorem 1 (Gilbert-Varshamov). *For any $0 < \delta < 1/2$, there is $\alpha > 0$, such that for sufficiently large n and $k = \alpha n$, the random binary code C is a $[n, k, \delta n]$ code with probability $1 - e^{-\Omega(n)}$.*

A.2 Classical product code

Classical product codes are a class of classical codes obtained by taking the product of two codes and are useful for studying the hypergraph product and quantum Tanner codes introduced later.

Definition (Product code [MS78]). *Let $\mathscr{C}_1, \mathscr{C}_2$ be two classical codes of respective parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ with parity-check matrices H_1, H_2.*
The product code $\mathscr{C} = \mathscr{C}_1 \otimes \mathscr{C}_2$ has parameters $[n_1 n_2, k_1 k_2, d_1 d_2]$ and its parity-check matrix is

$$H = \begin{pmatrix} \mathbb{I}^{n_1} \otimes H_2 \\ H_1 \otimes \mathbb{I}^{n_2} \end{pmatrix}.$$

The set of $n_1 n_2$ bits can be represented as matrix $w \in \mathcal{M}^{n_1 \times n_2}(\mathbb{F}_2)$ and w is a codeword of $\mathscr{C} = \mathscr{C}_1 \otimes \mathscr{C}_2$ if and only if each of its rows is a codeword of $\mathscr{C}_2$ and each of its column a codeword of $\mathscr{C}_1$ as depicted in Figure 2.

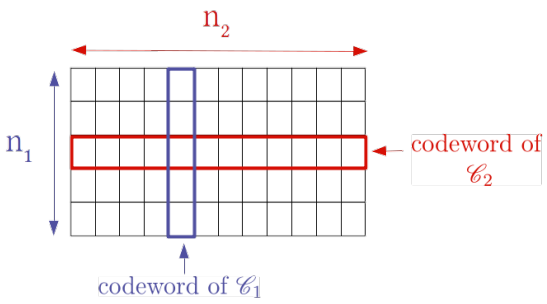

Figure 2: Caption

A.3 Tensor and dual tensor codes

Let C_A be a $[n_A, k_A, d_A]$ code and C_B a $[n_B, k_B, d_B]$ code. One can define a *tensor code* $C_A \otimes C_B \subseteq \mathbb{F}_2^{n_A \times n_B}$ as the set of $n_B \times n_A$ matrices whose rows correspond to codewords in C_A and columns to codewords in C_B. The tensor code has dimension $dim(C_A \otimes C_B) = dim(C_A)dim(C_B)$ and minimal distance $d_{AB} = d_A d_B$. The associated *dual tensor code* is $(C_A \otimes C_B)^\perp = C_A^\perp \otimes \mathbb{F}_2^{n_B} + \mathbb{F}_2^{n_A} \otimes C_B^\perp$.

Definition (ω-robustness). *Let $C_A \subseteq \mathbb{F}_2^\Delta$, $C_B \subseteq \mathbb{F}_2^\Delta$ be two classical codes with distances d_A and d_B respectively. The dual tensor code $C^\perp = (C_A \otimes C_B)^\perp = C_A \otimes \mathbb{F}_2^\Delta + \mathbb{F}_2^\Delta \otimes C_B$ is said to be ω-robust if any $x \in C^\perp$ such that $|x| < \omega$ has its supports included in $|x|/d_A$ rows and $|x|/d_B$ columns.*

Leverrier and Zémor showed that the robustness of the dual tensor code also implies a kind of robustness for the associated tensor code which is closed to the notion of robustly testable tensor code defined by Dinur et al. [LZ22b; Din+21]. Informally, a code $C = [n, k, d]$ is said to be κ-locally testable if a randomized local tester reading a constant number of bits from a message always accepts a valid codeword and rejects non-valid codewords with probability greater than κd. A test is said to be *robust* if non-valid codewords are rejected with high probability and the view of the tester is also far from any accepting view with high probability [BS04].
Let C be a code defined on the coordinate set S and let $T \subset S$. The *punctured* code derived from C, denoted $(C)_T$, is the set of codewords of C restricted to the set of coordinates T.

Definition (p-Resistance to puncturing). *Let $C_A \subseteq \mathbb{F}_2^\Delta$, $C_B \subseteq \mathbb{F}_2^\Delta$ be two codes. For $\omega, p \in \mathbb{N}$, the dual tensor code $(C_A \otimes C_B)^\perp = C_A \otimes \mathbb{F}_2^\Delta + \mathbb{F}_2^\Delta \otimes C_B$ is ω-robust with p-resistance to puncturing, if for any $A' \subset A$, $B' \subset B$ and $\omega' \leq p$ such that $|A'| = |B'| = \Delta - \omega' = \Delta'$, the dual tensor code $(C_A)_{A'} \otimes \mathbb{F}_2^{\Delta'} + \mathbb{F}_2^{\Delta'} \otimes (C_B)_{B'}$ is ω-robust.*

Informally, p-resistance to puncturing can be seen as the persistence of the ω-robustness when the codes C_A and C_B are restricted to subsets of coordinates of size $\leq \Delta - p$. These notions of robustness and resistance to puncturing have been at the core of proving the bound of the minimal distance of Quantum Tanner codes when considering dual tensor codes constructed from linear random codes.
Kalachev and Panteleev recently showed a stronger form of robustness for dual tensor codes constructed from uniformly random linear codes [KP22] which is stated in Theorem 3 .

Property 2 (Robustness of the dual tensor code). *Let $C_A, C_B \subset \mathbb{F}_2^\Delta$. The dual tensor code $C_A \otimes \mathbb{F}_2^\Delta + \mathbb{F}_2^\Delta \otimes C_B$ is said to be κ-robust if any $x \in C_A \otimes \mathbb{F}_2^\Delta + \mathbb{F}_2^\Delta \otimes C_B$ can be written as $x = r + c$, with $c \in C_A \otimes \mathbb{F}_2^\Delta$, $r \in \mathbb{F}_2^\Delta \otimes C_B$ and*

$$|c + r| \geq \kappa\Delta(||c|| + ||r||),$$

where $|.|$ is the Hamming weight and $||c||$ (resp. $||r||$) denotes the number of non zero column (resp. row) codewords.

Theorem 3. *For every $\rho \in (0,1)$, the dual tensor codes $(C_A \otimes C_B)^\perp$ and $(C_A^\perp \otimes C_B^\perp)^\perp$ obtained from uniformly random linear codes C_A, C_B of length Δ and of respective rate ρ and $1-\rho$ is κ-robust with high probability and with*

$$\kappa = \frac{1}{2}\min\left(\frac{1}{4}h^{-1}\left(\frac{\rho}{8}\right)h^{-1}\left(\frac{1-\rho}{8}\right), h^{-1}\left(\frac{\rho(1-\rho)}{8}\right)\right),$$

where h^{-1} is the inverse of the binary entropy function.

B Quantum error correction

Quantum mechanics raise several challenges in designing error correcting. Firstly, the no-cloning theorem asserts that quantum information cannot be copied, hence quantum repetition codes cannot be designed. Besides, a qubit is no longer a binary number but is equivalent to a point on a three-dimensional sphere and can undergo two types of errors, bit flip errors and phase flip errors, corresponding respectively to the action of Pauli X and Pauli Z. Lastly, measuring a quantum system usually change its state, which is known as the *collapse of the wavefunction*, and the parity-check operators should not collapse the encoded quantum information.
A quantum error correcting code C is referred to as a $[\![n,k,d]\!]$ code, where n is the number of physical qubits, k the number of logical qubits, *i.e.*, the dimension of the code-space and d is the distance of the code, which is now defined as the minimum number of errors that can occur on a codeword that causes it to be mapped to a different codeword. The code C has *constant rate* if $k = \Omega(n)$, and has *linear distance* if the distance between any two codewords is linear in the code length n. A quantum code with constant rate and a linear distance is said to be *good.*

B.1 Stabilizer codes

A useful formalism to describe quantum error correcting code is the stabilizer formalism, in which an operator in the stabilizer group corresponds to a non-disturbing measurement, i.e it leaves the state unchanged. The *Stabilizer codes* are quantum error correcting codes where the parity-check operators are generators of a stabilizer group [Got97]. Recall that the Pauli group acting on n qubits is defined as

$$\mathbb{G}_n = \left\{\alpha P_n \mid \alpha \in \{\pm 1, \pm i\}, P_n \in \{\mathbb{I}, X, Y, Z\}^{\otimes n}\right\},$$

and it is closed under multiplication.

Definition (Stabilizer code)**.** *Let $\mathbb{S}$ be an Abelian subgroup of $\mathbb{G}_n/-\mathbb{I}$. The stabilizer code $C(\mathbb{S})$ associated to the stabilizer group $\mathbb{S}$ is defined as*

$$C(\mathbb{S}) = \{|\Psi\rangle \mid \forall M \in \mathbb{S}, M|\Psi\rangle = |\Psi\rangle\}, \tag{2}$$

which is the simultaneous eigenspace with eigenvalue 1 of all elements of $\mathbb{S}$.

In order to obtain a non trivial vector space, two conditions must be satisfied by the stabilizer group $\mathbb{S}$. On the one hand, $-\mathbb{I} \notin \mathbb{S}$ since otherwise, $-\mathbb{I}|\Phi\rangle = |\Phi\rangle$ and it implies $|\Phi\rangle = 0$. On the other hand, the elements of $\mathbb{S}$ must not anticommute. Indeed, consider $M, N \in \mathbb{S}$ such that $\{M, N\} = 0$, then $|\Phi\rangle = MN|\Phi\rangle = -NM|\Phi\rangle = -|\Phi\rangle$.

Let $C(\mathbb{S})$ be a $[\![n,k,d]\!]$ quantum stabilizer code. Then, the stabilizer group can be define by a set of $n-k$ generators $M = \{m | m \in \mathbb{G}_n\}$ such that $\mathbb{S} = \mathrm{Span}(M)$. Similarly to the classical case, these $n-k$ stabilizer generators may be looked upon as the check operators of the code.
In 1996, Calderbank and Shor; Steane shed light on a new class of quantum error correcting code called CSS codes [CS96; Ste96]. These codes are stabilizer codes with the special property that each stabilizer is either composed only of X and $\mathbb{I}$ operators or of Z and $\mathbb{I}$ operators. It is described by a pair of mutually orthogonal binary codes C_X, C_Z such that $C_Z^\perp \subseteq C_X$. Parity-check matrix H_X (resp. H_Z) can be defined as the matrix for which each row correspond to a stabilizer generator of C_X (resp. C_Z) such that a row $[0\ 1\ 1\ 0]$ correspond to the generator $\mathbb{I} \otimes X \otimes X \otimes \mathbb{I}$. The condition $C_Z^\perp \subseteq C_X$ can then be rewriting as $H_X H_Z^T = 0$.

Proposition 4 (Parameters of a CSS code)**.** *A CSS code $C = (C_X, C_Z)$ described by parity-check matrices $(H_X, H_Z) \in \mathbb{F}_2^{r_X \times n} \times \mathbb{F}_2^{r_Z \times n}$ has length n, dimension 2^k where $k = n - rank(H_X) - rank(H_Z)$ and minimal distance*

$$d = \min\{|w| : w \in C_X \setminus C_Z^\perp \cup C_Z \setminus C_X^\perp\}$$

A nice property of CSS codes is that the decoding procedure can be split in two : a procedure to correct bit flip errors and one to correct phase flip errors.

Quantum codes described by sparse parity-check matrices are said to be *Low-Density Parity-check codes* (LDPC codes). These codes raise a lot of attention as they would necessitate a smaller number of physical qubits to construct a fault-tolerant quantum circuit that can run interesting algorithm in comparison to other kind of quantum error correcting.

B.2 Logical operators

Consider $\mathscr{C}$ to be a stabilizer code associated to the stabilizer group $\mathbb{S}$. A logical gate is a unitary operator L that preserves the codespace. In other word, the unitary L is a logical gate if and only if $\forall S \in \mathbb{S}, L^\dagger SL \in \mathbb{S}$, i.e if and only if L belongs to the normalizer $N(\mathbb{S})$ of the group $\mathbb{S}$. A special type of logical gates are Pauli logical operators that corresponds to the Pauli operators that commute with all the stabilizers, i.e the Pauli operators belonging to the centralizer $C(\mathbb{S})$. It can be noted that for Pauli operators, $N(\mathbb{S}) = C(\mathbb{S})$.
The non-trivial logical operators or logical errors are defined as Pauli operators that do not belong to the stabilizer group but commute with all the stabilizers, i.e Pauli operators that belongs to $N(\mathbb{S})\backslash\mathbb{S}$. The minimal distance of a stabilizer code corresponds to the weight of the smallest logical error.

Property 5 (Non-trivial logical operators for a CSS code)**.** *Let $\mathscr{C} = (\mathscr{C}_X, \mathscr{C}_Z)$ be a CSS code defined by the parity-check matrices (H_X, H_Z). The Z logical errors belong to Ker $H_X\backslash$Im H_Z^T and the X logical errors to Ker $H_Z\backslash$Im H_X^T.*

The logical operations are essential to perform fault-tolerant computation since they allow to manipulate the information contained in the code states while keeping the protection of the error correcting code.
Throughout this manuscript, the non-trivial logical operators will be only called logical operators for concision.

C Graph theory

We denote an edge between two vertices a and b in a text as $\{a, b\}$.

Definition (Tensor product of graphs)**.** *Let $\mathcal{G} = (V_G, E_G)$ and $\mathcal{H} = (V_H, E_H)$ be two graphs. $\mathcal{T} = \mathcal{G} \otimes \mathcal{H} = (V_T, E_T)$ is the tensor product of G and H, whose vertex set is $V_T = V_G \times V_H$, and edge set is $E_T = \left\{\{(g,h),(g',h')\} \middle| (g,g') \in E_G, (h,h') \in E_H\right\}$.*

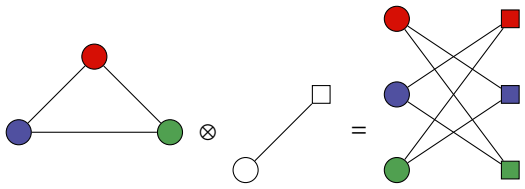

Figure 3: Illustration of tensor product of two graphs.

Informally, each vertex in $\mathcal{T}$ represents a pair of vertices made of one vertex of $\mathcal{G}$ and one vertex of $\mathcal{H}$.Given that, there is an edge between to vertices of $\mathcal{T}$ if the vertices represented are adjacent in their respective graphs.

Definition (Cover of a graph)**.** *Let $\mathcal{G} = (V_1, E_1)$ and $\mathscr{C}_G = (V_2, E_2)$. Let $f : V_2 \to V_1$ be a surjection. The map f is a covering map from $\mathscr{C}_G$ to $\mathcal{G}$ if for all $v \in V_2$, the restriction of f to the neighborhood of v is a bijection onto the neighborhood of $f(v)$ in G. The resulting graph $\mathscr{C}_G$ is called a cover of the graph $\mathcal{G}$.*

We say that $\mathscr{C}_G$ is a *double cover* of $\mathcal{G}$, which we denote $\mathscr{C}_G^2$, if each vertex of G has exactly two preimages in $\mathscr{C}_G$. A *bipartite double cover* of $\mathcal{G}$ is given by $\mathscr{C}_G^2 := G \otimes K_2$. The vertex set of $\mathscr{C}^2_{G=(V,E)}$ is by construction uniquely described by the elements of $V \times \{0,1\}$, its edge set is the set $\left\{\{(a,i),(b,1-i)\} \middle| (a,b) \in E, i \in \{0,1\}\right\}$.

C.1 Cayley graphs

Let $\mathcal{G}$ be a connected Δ-regular graph with n vertices, so that its eigenvalues satisfy $\Delta := \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_n \geq -\Delta$. We define $\lambda(\mathcal{G}) := \max_{|\lambda_i|<d} \lambda_i$ as the second largest eigenvalue of G in magnitude and call it the spectral gap. The link used between graph theory and group theory is the that of Cayley graph.

Definition (Cayley graph)**.** *Let G be a group.*
The Cayley graph of G with respect to S is the graph $Cay(G,S) = (V,E)$ where the set of vertices is $V = G$ and the set of edges is $E = \{\{x,y\} \mid \exists s \in S, x \cdot s = y\}$.

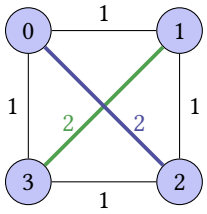

Figure 4: Example of the Cayley graph for $G = \mathbb{Z}/4\mathbb{Z}$ and $S = \{1, 2\}$.

Cayley graphs are good candidates to build expander graphs, *i.e.*, graphs that are sparse yet very well-connected. *Sparse* means here that the degree of the graph is a slowly growing function of the number of vertices. One significant property of expander graphs is the *Expander Mixing Lemma*:

Lemma 6 (Expander mixing lemma)**.** *Let $\mathcal{G}$ be a connected Δ-regular bipartite graph on the vertex set $V_0 \cup V_1$. For any $S \subset V_0$,$T \subset V_1$,*

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

Lemma 6 states that, in a good expander (a Δ-regular graph $\mathcal{G}$ where $\lambda(\mathcal{G})$ is small compared to Δ), the number of edges between every pair of sizeable subsets of vertices is approximately equal to what one would expect in a random Δ-regular graph. This pseudorandom property of expanders is the key ingredient in the analysis of both the distance property of expander codes as well as the error-correction algorithms.
A Ramanujan graph is a Δ-regular graph whose spectral gap is almost as large as possible (formally $\lambda(\mathcal{G}) \leq \sqrt{\Delta - 1}$). In addition, note that if $\mathcal{G}$ is a Ramanujan graph, then $\mathscr{C}^2_{\mathcal{G}}$ is a bipartite Ramanujan graph.

C.2 Left-right Cayley Complexes

Let G be a group and $A, B \subset G$ two self-inverse subsets of G, such that $|A| = |B| = \Delta$.
In 2021, Dinur et al. described a new two-dimensional complex, named *left-right Cayley complex*, constructed from Cayley graphs [Din+21]. We will consider the two Cayley graphs $Cay(G,A)$ and $Cay(G,B)$, and more precisely their bipartite double covers $Cay^2(G,A)$ and $Cay^2(G,B)$. We assume we generate $Cay(G,A)$ by left multiplication of the elements from A, and $Cay(G,B)$ by the right multiplication of the elements from B. We define the two edge sets $E_A = \big\{\{(g,0),(ag,1)\}\big|g \in G, a \in A\big\}$ and $E_B = \big\{\{(g,0),(gb,1)\}\big|g \in G, b \in B\big\}$ together with the vertex set $V = G \times \{0,1\}$. As such, the bipartite double covers of $Cay^2(G,A)$ and $Cay^2(G,B)$ are respectively $Cay^2(G,A) = (V,E_A)$ and $Cay^2(G,B) = (V,E_B)$. The central structure of the quantum Tanner codes is that of Left-right Cayley complex, denoted by $Cay(G,A,B)$, which is the graph resulting of the tensor product between $Cay^2(G,A)$ and $Cay^2(G,B)$.

Definition (Left-right Cayley Complexes)**.**

$$Cay(G,A,B) = (V,E) := Cay^2(G,A) \otimes Cay^2(G,B)\,.$$

It is rather clear that the edge set of $Cay(G,A,B)$ is uniquely described by $V = G \times \{0,1\}$ since both A and B are generators of G. $Cay(G,A,B)$ is bipartite by construction, hence we can write $V = V_0 \cup V_1$ where $V_i := \mathcal{G} \times \{i\}$ is the set of vertices of the form (g,i) for $i = 0,1$ and g an element of G.

Definition (Square in a complex)**.** *The complex $Cay(G,A,B)$ is made up from the two bipartite double covers $Cay^2(G,A) = (V,E_A)$ and $Cay^2(G,B) = (V,E_B)$ where $V = V_0 \cup V_1$. A square is a 4-subset of vertices of $Cay(G,A,B)$ of the form $\{(g,0),(ag,1),(agb,0),(gb,1)\}$.*

A square is therefore made of two vertices of V_0, two vertices of V_1, two edges of E_A and two edges of E_B. When using a bipartite complex, the *Total Non-Conjugacy* condition (formally, $\forall a \in A, b \in B, g \in G, ag \neq gb$), has to be satisfied to ensure that all the squares have four distinct vertices.

D Description of quantum Tanner codes

In 1981, Tanner devised a recursive approach to construct classical code allowing a low-complexity decoding [Tan81]. To this aim, let $\mathcal{G} = (V,E)$ be a Δ-regular graph with $|V| = n$ and $|E| = \frac{\Delta n}{2}$ and $C_0 \subseteq \mathbb{F}_2^{\Delta}$ a linear code. A Tanner code can be defined as

$$\mathcal{T}(\mathcal{G},C_0) = \left\{\mathbf{c} \in \mathbb{F}_2^{\frac{n\Delta}{2}} \,|\forall v \in V, \mathbf{c}|_{N(v)} \in C_0\right\} \tag{3}$$

where $N(v)$ is the neighborhood of the vertex v. As $|E| = \frac{\Delta n}{2}$, the support of the codewords can be identified to the set of edges, i.e the code $\mathcal{T}(\mathcal{G}, C_0)$ has bits sitting on the edges E which form a codeword $\mathbf{c} \in \mathbb{F}_2^{\frac{n\Delta}{2}}$. The local view $x(v)$ of a vertex $v \in V$ is the restriction of the support to the edges incident to v and this restricted codeword must belongs to the smaller code C_0. Hence, at each vertex v, local constraints are enforced: $x(v)$ must satisfy the parity-checks of the local code C_0.
Quantum Tanner codes are constructed from a pair of Tanner codes and a left-right Cayley complex [LZ22b]. Let G be a group and $A, B \subset G$ two sets of self-inverse generators such that $|A| = |B| = \Delta$. We consider a quadripartite version of $Cay(G, A, B)$ in which

- the vertex set V set corresponds to four copies of the group G, i.e $V = \cup_{i,j\in\{0,1\}} V_{ij}$ with $V_{ij} = G \times \{ij\}$,
- the edge set is $E = E_A \cup E_B$ with

$$E_A = \{\{(g, i0), (ag, i1)\} : g \in G, a \in A, i = 0, 1\},$$

$$E_B = \{\{(g, 0j), (gb, 1j)\} : g \in G, b \in B, j = 0, 1\},$$

- the square set is

$$Q = \{\{(g, 00), (ag, 01), (gb, 10), (agb, 11)\} : g \in G, a \in A, b \in B\}.$$

Hence, the left-right Cayley complex is made up of two copies of the double cover of $\mathcal{G}_A = Cay(G, A)$ and two copies of the double cover of $\mathcal{G}_B = Cay(G, B)$, where $\mathcal{G}_A$ is obtained by left multiplication and $\mathcal{G}_B$ by right multiplication.

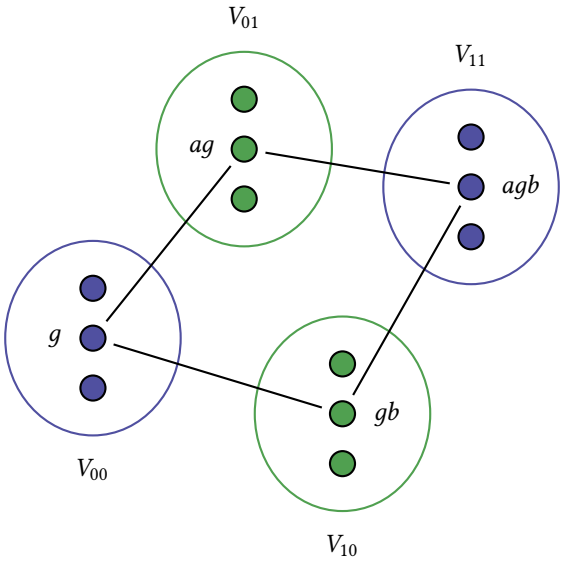

Figure 5: Representation of quadripartite version of the left-right Cayley complex where one square is exhibited.

A schematic representation of the quadripartite complex can be found in Figure 5. It exhibits $|G|\Delta^2$ squares and each vertex has Δ^2 incident squares as Δ edges from E_A and Δ edges from E_B are incident to it. Similarly to classical Tanner codes, the qubits sit on the squares, i.e the support of the codewords is isomorphic to Q. In the following, the local view of a vertex v corresponds to the restriction of the codeword support to the squares incident in v and it will be denoted $Q(v)$ and called the Q-neighborhood. For every vertex v, $Q(v)$ is isomorphic to $A \times B$ and there exists an bijective map $\phi_v : A \times B \to Q(v)$ such that

$$\phi_v(a, b) = \begin{cases} \{(g, 00), (ag, 01), (gb, 10), (agb, 11)\} & \text{for } v = (g, 00) \in V_{00} \\ \{(g, 01), (a^{-1}g, 00), (gb, 11), (a^{-1}gb, 10)\} & \text{for } v = (g, 01) \in V_{01} \\ \{(g, 10), (ag, 11), (gb^{-1}, 00), (agb^{-1}, 01)\} & \text{for } v = (g, 10) \in V_{10} \\ \{(g, 11), (a^{-1}g, 10), (gb^{-1}, 01), (a^{-1}gb^{-1}, 00)\} & \text{for } v = (g, 11) \in V_{11} \end{cases}$$

Two codes $C_A \subset \mathbb{F}_2^\Delta$ and $C_B \subset \mathbb{F}_2^\Delta$ are chosen and two tensor codes are defined as $C_0 = C_A \otimes C_B$ and $C_1 = C_A^\perp \otimes C_B^\perp$. The distance of C_A, C_B and the tensor codes will be at least $\delta\Delta$. At each vertex, local constraints are enforced: in the local view of $v \in V_0 = V_{00} \cup V_{11}$, a codeword of $C_0^\perp$ must be seen and in the local view of $v \in V_1 = V_{10} \cup V_{01}$, a codeword of $C_1^\perp$. C_A, C_B are chosen such that their minimal distance is at least $\delta\Delta$ and their respective dimensions are $\rho\Delta$ and $(1-\rho)\Delta$, for some rate ρ. We have then

$$\text{Dim } C_A = \text{Dim } C_B^\perp = \rho\Delta$$

$$\text{Dim } C_B = \text{Dim } C_A^\perp = (1-\rho)\Delta$$

A linear error correcting code $[n,k,d]$ exhibits $n-k$ parity check constraints. Therefore, the tensor codes C_0 and C_1 both exhibit $(1-\rho)\rho\Delta^2$ constraints. Since there are $4|G|$ vertices in the complex and each of them has $(1-\rho)\rho\Delta^2$ stabilizer generators corresponding to either the generators of C_0 or C_1, the quantum Tanner codes has $4(1-\rho)\rho|Q|$ stabilizer generators and its dimension is $k_Q \geq (2\rho-1)^2|Q|$, with equality when all the generators are independent.
The complex also exhibits another graph, denoted $\mathcal{G}^\square$, which is obtained by putting an edge between all pairs of vertices $\{(g,i),(agb,i)\}$ for $g \in G, a \in A, b \in B, i = 0,1$. This graph is therefore made up of two connected components, one on V_0 and one on V_1, denoted $\mathcal{G}_0^\square$ and $\mathcal{G}_1^\square$. To rephrase it, $\mathcal{G}_i^\square$, $i = 0,1$, has vertex set V_i and edge set Q.
Let $\mathcal{G}_A = Cay(G,A)$ and $\mathcal{G}_B = Cay(G,B)$. In the following, we suppose that $\mathcal{G}_A$, $\mathcal{G}_B$ are Ramananujan graphs, i.e $\lambda(\mathcal{G}_A), \lambda(\mathcal{G}_B) \leq 2\sqrt{\Delta-1}$. This assumption has been one of the key ingredients to show the lower bound on the minimal distance.

Lemma 7 ([LZ22b]). *If $\mathcal{G}_A, \mathcal{G}_B$ are Ramanujan graphs, then*

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

Let $\{e_i\},\{f_j\},\{g_k\},\{k_l\}$ be basis for respectively $C_A, C_B, C_A^\perp$ and $C_B^\perp$. Then, $C_0 = \text{Span}\left(\beta_0 = \{e_i \otimes f_j\}\right)$ and $C_1 = \text{Span}\left(\beta_1 = \{g_k \otimes k_l\}\right)$.
The matrix H_X has $|V_0| \cdot \text{Dim } C_0$ rows, each of which corresponding to a generator of C_0 for a given vertex $v \in V_0$.
The columns are indexed by the set of squares $\{g,a,b \mid g \in G, a \in A, b \in B\}$, thus there are $|G| \cdot \Delta^2$ columns in the quadripartite version. A row of H_X, indexed by $v \in V_0$ and $\lambda \in \beta_0$, has support $G \times A \times B$ and when restricted to the support $A \times B$, the row corresponds to the generator λ. The matrix H_Z is constructed in a similar manner. This construction implies that $\mathcal{C}_X$ (resp. $\mathcal{C}_Z$) is orthogonal to all Z-generators (resp. X-generators) and every codeword of $\mathcal{C}_X$ (resp. $\mathcal{C}_Z$) are in $C_0^\perp$ (resp. $C_1^\perp$). The quantum Tanner code $\mathcal{Q} = (\mathscr{C}_0, \mathscr{C}_1)$ is the pair of Tanner codes

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

Theorem 8 (Parameters of quantum Tanner codes [LZ22a]). *Suppose a large enough Δ is chosen, together with an infinite family of groups G with generating sets A,B, $|A| = |B| = \Delta$, such that the Cayley graphs $Cay(G,A)$ and $Cay(G,B)$ are Ramanujan.*
Suppose that random classical codes C_A, C_B are chosen to be of length Δ, rates ρ and $1-\rho$ respectively, and distances at least δn so that the dual tensor codes are κ-robust (Theorem 3).
Then, the quantum Tanner code $\mathbf{Q} = (\mathscr{C}_0, \mathscr{C}_1)$ has parameters

$$[\![n = |Q|, k \geq (2\rho-1)^2|Q|, d \geq \frac{\delta^2\kappa^2}{256\Delta} n]\!]$$

Hence, quantum Tanner codes form a family of good quantum LDPC codes.

II From hypergraph product codes to quantum Tanner codes

A Description of hypergraph product code (HGP code)

Introduced in 2009, the hypergraph product code is a CSS code constructed from two linear seed codes $\mathscr{C}_1, \mathscr{C}_2$ [TZ09]. For $i = 1,2$, let $\mathscr{C}_i$ be a $[n_i,k_i,d_i]$ classical code with parity check matrix $H_i \in \mathbb{F}_2^{m_i \times n_i}$, bit set V_i and check set C_i.

In the following definition, a matrix written as $H = (A, B)$ is such that the submatrix A acts on the qubit set $V_1 \times V_2$ and the submatrix B on the qubit set $C_1 \times C_2$.

Definition (Hypergraph product code).
The hypergraph product (HGP) code $\mathcal{Q} = (\mathcal{C}_X, \mathcal{C}_Z)$ *is a CSS code such that*

$$\mathcal{C}_X = ker(H_X) \quad with \quad H_X = (\mathbb{I}^{n_1} \otimes H_2, H_1^T \otimes \mathbb{I}^{m_2})$$

$$\mathcal{C}_Z = ker(H_Z) \quad with \quad H_Z = (H_1 \otimes \mathbb{I}^{n_2}, \mathbb{I}^{m_1} \otimes H_2^T) \, .$$

Thus, $H_X \in \mathbb{F}_2^{M_X \times N}$, $H_Z \in \mathbb{F}_2^{M_Z \times N}$ *with* $N = n_1 n_2 + m_1 m_2$, $M_X = n_1 m_2$ *and* $M_Z = n_2 m_1$.

For $i = 1, 2$, let $\mathcal{T}_i = (V_i \cup C_i, E_i)$ be the Tanner graph of $\mathcal{C}_i$ with V_i the set of qubit vertices and C_i the set of checks. The Tanner graph of $\mathcal{Q}$ is $\mathcal{T} = \mathcal{T}_1 \times \mathcal{T}_2 = (V \cup S_Z \cup S_X, E)$ such that

- the qubit set is $V = (V_1 \times V_2) \cup (C_1 \times C_2)$,
- the X-stabilizer set is $S_X = C_1 \times V_2$
- the Z-stabilizer set is $S_Z = V_1 \times C_2$,
- the edge set is

$$E = \left\{ \{(u_1, u_2), (v_1, v_2)\} \in (V \cup S_Z \cup S_X)^2 \mid (u_1 = v_1 \wedge (u_2, v_2) \in E_2) \vee (u_2 = v_2 \wedge (u_1, v_1) \in E_1) \right\}$$

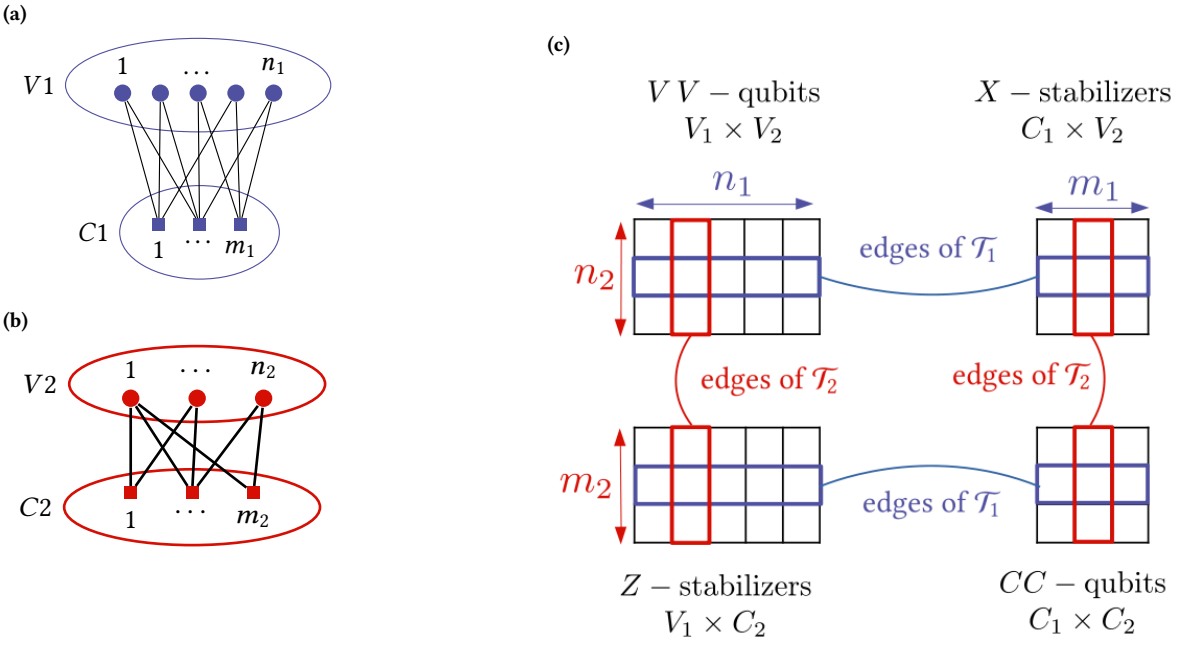

Figure 6: **(a)**: Tanner graph $\mathcal{T}_1$ of $\mathcal{C}_1$. **(b)**: Tanner graph $\mathcal{T}_2$ of $\mathcal{C}_2$. **(c):** Tanner graph $\mathcal{T} = \mathcal{T}_1 \times \mathcal{T}_2$ of the HGP code $\mathcal{Q}$. Each row is a copy of $\mathcal{T}_1$ and each column a copy of $\mathcal{T}_2$

Given a $[n, k, d]$ classical code $\mathcal{C}$ with m parity checks, one can define the transpose code $\mathcal{C}^T$ with parameters $[m, k^T, d^T]$ and n checks. The Tanner graph of $\mathcal{C}^T$ is obtained by inverting the role of the bits node and the parity check nodes in the Tanner graph of $\mathcal{C}$.
Applying the Rank nullity theorem,

$$\text{rank } H + \text{Dim (Ker } H) = \text{Dim } (\mathbb{F}_2^n) \quad \text{and} \quad \text{rank } H^T + \text{Dim (Ker } H^T) = \text{Dim } (\mathbb{F}_2^m),$$

which gives

$$k = n - \text{rank } H \quad \text{and} \quad k^T = m - \text{rank } H^T \, .$$

Since rank H = rank H^T,

$$k = n - m + k^T \, . \tag{4}$$

Property 9 (Parameters of hypergraph product code [TZ09]).
The HGP code $\boldsymbol{Q}$ has parameters $[\![N, K, D]\!]$ where

- $N = n_1 n_2 + m_1 m_2$,
- $K = k_1 k_2 + k_1^T k_2^T$,
- $D \geq \min(d_1, d_2, d_1^T, d_2^T)$.

Proof. See Appendix A. □

B From HGP code to non-lifted quantum Tanner codes

Consider two Tanner codes $\mathscr{C}_A = T_A(\mathscr{G}_A, C_A)$, $\mathscr{C}_B = T_B(\mathscr{G}_B, C_B)$ defined on the bipartite graphs $\mathscr{G}_A = (V_0 \cup V_1, E_A)$, $\mathscr{G}_B = (V_0 \cup V_1, E_B)$ and for local codes $C_A = [n_A, k_A, d_A]$, $C_B = [n_B, k_B, d_B]$. Let $H_A \in \mathbb{F}_2^{M_A \times N_A}$, $G_B \in \mathbb{F}_2^{M_B \times N_B}$ be the respective parity check matrices of $\mathscr{C}_A$, $\mathscr{C}_B$ that can be written as

$$H_A = \begin{pmatrix} H_{A,0} \\ H_{A,1} \end{pmatrix} , H_B = \begin{pmatrix} H_B^0 \\ H_{B,1} \end{pmatrix} ,$$

where $H_{\alpha,i} \in \mathbb{F}_2^{m_\alpha \times N_A}$, $\alpha = A, B$, $i = 0, 1$ is the submatrix of H_α whose rows correspond to the parity-checks associated to vertices in V_i.

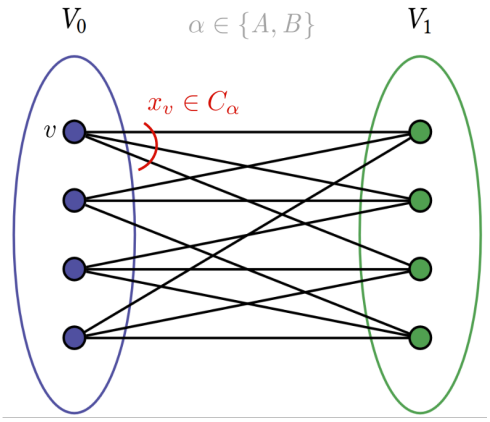

Figure 7: Representation of the Tanner code $T_\alpha(\mathscr{G}_\alpha, C_\alpha)$.

The submatrices $H_{\alpha,0}, H_{\alpha,1}$, $\alpha = A, B$ can be related by

$$H_{\alpha,1} = H_{\alpha,0} \pi_\alpha ,$$

where π_α is a permutation matrix corresponding to the change of point of view between V_0 to V_1. The columns of the matrices H_A, H_B corresponding to the bits are ordered following the basis of edges $E_{01} = \{\{v_0, v_1\}$ for $v_0 \in V_0$, $v_1 \in V_1\}$. The edge neighborhood of $v \in V_1$ is a codeword of $\mathscr{C}_\alpha$ but for the basis of edges ordered as $E_{10} = \{\{v_1, v_0\}$ for $v_1 \in V_1$, $v_0 \in V_0\}$. Therefore, the parity constraints for V_1 in H_α must undergo a change of basis from E_{10} to E_{01} that is described by the permutation π_α.
For $\alpha = A, B$, let $\mathcal{T}_\alpha$ be the Tanner graph associated to $\mathscr{C}_\alpha$ with bits set E_α and check set V'_α. For each $v \in V_0 \cup V_1$, the set of edges $\{e_v\}$ incidents to v must form a codeword of C_A and hence, $\{e_v\}$ must satisfy $n_\alpha - k_\alpha$ checks. Therefore, $|V'_\alpha| \leq (n_\alpha - k_\alpha)(|V_0| + |V_1|)$ considering that some checks might not be linearly independent. In the following, for $\alpha = A, B$ and $i = 0, 1$, we denote $V'_{i,\alpha}$ the checks associated to the set V_i such that $V'_\alpha = V'_{0,\alpha} \cup V'_{1,\alpha}$.
Consider the hypergraph product (HGP) code $\boldsymbol{Q} = (\mathscr{C}_X, \mathscr{C}_Z)$ such that

$$\mathscr{C}_Z = \ker(H_Z) \text{ with } H_Z = (\mathbb{I}^{N_A} \otimes H_B, H_A^T \otimes \mathbb{I}^{M_B}) , \tag{5}$$

$$\mathscr{C}_X = \ker(H_X) \text{ with } H_X = (H_A \otimes \mathbb{I}^{N_B}, \mathbb{I}^{M_A} \otimes H_B^T) . \tag{6}$$

Thus, $H_X \in \mathbb{F}_2^{M_X \times N}$, $H_Z \in \mathbb{F}_2^{M_Z \times N}$ with $N = N_A N_B + M_A M_B$, $M_Z = N_A M_B$ and $M_X = N_B M_A$.

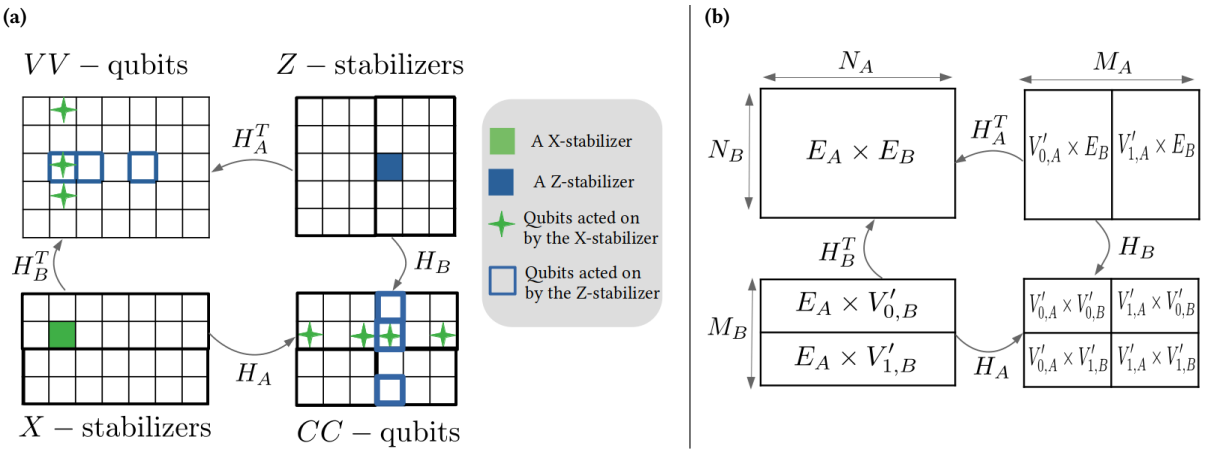

Figure 8: **(a)**: Tanner graph of the hypergraph product code $\mathcal{Q}$. **(b)**: Depiction of the sets associated to the qubits and stabilizers of $\mathcal{Q}$.

The idea behind the quantum Tanner code construction is to transform the matrices H_X, H_Z such that the X-stabilizers and Z-stabilizers never intersect on the CC-qubits. This way, the X-stabilizers and Z-stabilizers always commute on the CC-qubits and these qubits can be discarded. The parts of H_X and H_Z acting on the CC-qubits are respectively

$$\begin{array}{l|cc|cc}
\text{Action on} & V'_{0,A}\times V'_{0,B} & V'_{0,A}\times V'_{1,B} & V'_{1,A}\times V'_{0,B} & V'_{1,A}\times V'_{1,B} \\
\hline
\mathrm{H}_X^{CC} = & \begin{pmatrix} \mathbb{I}^{M_{A,0}}\otimes H_{B,0}^T \\ 0 \end{pmatrix} & \begin{matrix} \mathbb{I}^{M_{A,0}}\otimes H_{B,1}^T \\ 0 \end{matrix} & \begin{matrix} 0 \\ \mathbb{I}^{M_{A,1}}\otimes H_{B,0}^T \end{matrix} & \begin{matrix} 0 \\ \mathbb{I}^{M_{A,1}}\otimes H_{B,1}^T \end{matrix} \\
\mathrm{H}_Z^{CC} = & \begin{pmatrix} H_{A,0}^T\otimes \mathbb{I}^{M_{B,0}} \\ 0 \end{pmatrix} & \begin{matrix} 0 \\ H_{A,0}^T\otimes \mathbb{I}^{M_{B,1}} \end{matrix} & \begin{matrix} H_{A,1}^T\otimes \mathbb{I}^{M_{B,0}} \\ 0 \end{matrix} & \begin{matrix} 0 \\ H_{A,1}^T\otimes \mathbb{I}^{M_{B,1}} \end{matrix}
\end{array}$$

The next step consists in modifying this matrices such that the Z-stabilizers corresponding to the set $E_A \times V'_{0,B}$ undergo a transformation to stabilizers acting only on the CC-qubits defined on the set $V'_{0,A}\times V'_{1,B}$, the Z-stabilizers corresponding to the set $E_A \times V'_{1,B}$ act on the CC-qubits defined on $V'_{1,A}\times V'_{0,B}$, the X-stabilizers corresponding to the set $V'_{0,A}\times E_B$ act on the CC-qubits defined on $V'_{0,A}\times V'_{0,B}$ and the X-stabilizers corresponding to the set $V'_{1,A}\times E_B$ act on the CC-qubits defined on $V'_{1,A}\times V'_{1,B}$. To this aim, we use the fact that for $i = 0, 1$, $\alpha = A, B$, the linear code defined by the parity-check matrix $H_{\alpha,0}$ and the generator matrix $G_{\alpha,i}$ fulfill $G_{\alpha,i}H_{\alpha,i}^T = 0$ by definition. Then, the first part of H_X is multiplied by $\mathbb{I}^{M_{A,0}}\otimes G_{B,0}$, the second part of H_X by $\mathbb{I}^{M_{A,1}}\otimes G_{B,1}$ and similarly, the first part of H_Z is multiplied by $G_{A,1}\otimes \mathbb{I}^{M_{B,0}}$ and the second part of H_Z by $G_{A,0}\otimes \mathbb{I}^{M_{B,1}}$. Hence, the part of H_X and H_Z acting on the CC-qubits are transformed into

$$\widetilde{H}_X^{CC} = \begin{pmatrix} 0 & \mathbb{I}^{M_{A,0}}\otimes H_{B,1}^T G_{B,0} & 0 & 0 \\ 0 & 0 & \mathbb{I}^{M_{A,1}}\otimes H_{B,0}^T G_{B,1} & 0 \end{pmatrix},$$
$$\widetilde{H}_Z^{CC} = \begin{pmatrix} H_{A,0}^T G_{A,1}\otimes \mathbb{I}^{M_{B,0}} & 0 & 0 & 0 \\ 0 & 0 & 0 & H_{A,1}^T G_{A,0}\otimes \mathbb{I}^{M_{B,1}} \end{pmatrix},$$

and can be discarded as all stabilizers now commute on the CC-qubits. Therefore, keeping only the part acting on the VV-qubits, the modified parity-check matrices are

$$\widetilde{H_X} = \begin{pmatrix} H_{A,0}\otimes G_{B,0} \\ H_{A,1}\otimes G_{B,1} \end{pmatrix} \text{ and } \widetilde{H_Z} = \begin{pmatrix} G_{A,1}\otimes H_{B,0} \\ G_{A,0}\otimes H_{B,1} \end{pmatrix}. \tag{7}$$

The code $\mathcal{Q} = (\widetilde{\mathcal{C}_X}, \widetilde{\mathcal{C}_Z})$ associated to these parity-check matrices is a CSS code of length $N_A N_B$ since the orthogonality constraints between the two types of generators are upheld, i.e $\widetilde{H_X}\widetilde{H_Z}^T = 0$.

This code can be depicted as in Figure 9 where the qubits lie on the edges and the parity constraints are imposed at the vertices. Z-stabilizers coming from $H_{A,0} \otimes G_{B,0}$ and $H_{A,1} \otimes G_{B,1}$ lie respectively on the vertices v_{00} and v_{11} and X-stabilizers coming from $G_{A,1} \otimes H_B^0$ and $G_{A,0} \otimes H_B^1$ respectively on v_{01} and v_{10}. Hence, in the edge neighborhoods of v_{00} and v_{11} a codeword of $C_A^\perp \otimes C_B$ must be seen and in the edge neighborhoods of v_{10} and v_{01} a codeword of $C_A \otimes C_B^\perp$. Noticing that the role of C_B and $C_B^\perp$ can be permuted without any modification in the previous proofs, this code is closely related to the quantum Tanner code presented in Section D and actually corresponds to its non-lifted version. The lifting procedure according to a group G is presented in Section A and will make this link clearer.

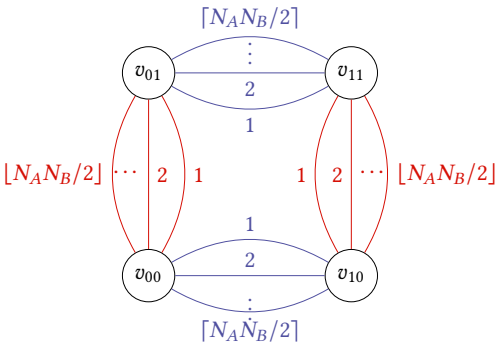

Figure 9: Representation of $\mathcal{Q} = (\widetilde{\mathscr{C}_X}, \widetilde{\mathscr{C}_Z})$ defined by the parity-check matrices in Equation 7.

C Rank of $\widetilde{H_X}$

Since only a lower bound on the dimension K of the quantum Tanner code of length N is known and that, for parity-check matrices $\widetilde{\widetilde{H_X}}, \widetilde{\widetilde{H_Z}}$, we have

$$K = N - \text{rank}\, \widetilde{\widetilde{H_X}} - \text{rank}\, \widetilde{\widetilde{H_Z}}\,,$$

our first step was to try to establish the dimension of the non-lifted version of the quantum Tanner code by evincing rank $\widetilde{H_X}$ and rank $\widetilde{H_Z}$ in the hope to be able to extend it to the lifted version afterwards. In this section, only the steps for $\widetilde{H_X}$ is exposed as the ones for $\widetilde{H_Z}$ are similar.

The first attempt was to use the Rank-Nullity theorem and write

$$\begin{aligned}\text{rank}\, \widetilde{H_X} &= N_A N_B - \text{Dim}\, \left(\text{Ker}\, \widetilde{H_X}\right) \\ &= N_A N_B - \text{Dim}\, \left(\text{Ker}\, (H_{A,0} \otimes G_{B,0}) \cap \text{Ker}\, (H_{A,1} \otimes G_{B,1})\right)\,.\end{aligned}$$

Unfortunately, we did not find any mathematical tools allowing us to express the dimension of the intersection of the two kernels in a simple and useful way. Hence, a more elementary attempt was taken which consists in exploring the kind of relations arising between the lines of $\widetilde{H_X}$ and counting their numbers.

Let $\alpha = A, B$, $i = 0, 1$. Recall that $H_{\alpha,i} \in \mathbb{F}_2^{m_\alpha \times N_\alpha}$ and let the associated generator matrix be $G_{\alpha,i} \in \mathbb{F}_2^{l_\alpha \times N_\alpha}$. Since π_α, $\alpha = A, B$ is invertible, we have

$$\text{rank}\, (H_{\alpha,1}) = \text{rank}\, (H_{\alpha,0}) \;\text{ and }\; \text{rank}\, (G_\alpha^1) = \text{rank}\, (G_{\alpha,0})\,.$$

Suppose there are r_A linear relations between the rows of $H_{A,0}$ and r_B linear relations between the rows of $G_{B,0}$ such that

$$\text{rank}\, (H_{A,0}) = \text{rank}\, (H_{A,1}) = m_A - r_A \;\text{ and }\; \text{rank}\, (G_{B,0}) = \text{rank}\, (G_{B,1}) = l_B - r_B \tag{8}$$

Suppose also there are r_{AA} (resp. r_{BB}) relations between the rows of $H_{A,0}$ and $H_{A,1}$ (resp. $G_{B,0}$ and $G_{B,1}$). Then,

$$\text{rank}\, (H_A) = \text{rank}\, (\begin{bmatrix} H_{A,0} \\ H_{A,1} \end{bmatrix}) = 2m_A - 2r_A - r_{AA} \;\text{ and }\; \text{rank}\, (G_B) = \text{rank}\, (\begin{bmatrix} G_{B,0} \\ G_{B,1} \end{bmatrix}) = 2l_B - 2r_B - r_{BB} \tag{9}$$

Rough bounds can be derived for rank $(\widetilde{H_X})$,

$$\text{rank}\, (H_A)\text{rank}\, (G_B) \leq \text{rank}\, (\widetilde{H_X}) \leq 2\text{rank}\, (H_A)\text{rank}\, (G_B) \tag{10}$$

$$\Leftrightarrow \quad m_A l_B - l_B r_A - m_A r_B + r_A r_B \leq \text{rank}\, (\widetilde{H_X}) \leq 2m_A l_B - 2l_B r_A - 2m_A r_B + 2r_A r_B\,, \tag{11}$$

where the upper bound corresponds to the case in which there is no linear relations between $H_{A,0} \otimes G_{B,0}$ and $H_{A,1} \otimes G_{B,1}$ and the lower bound to the one in which every row of $H_{A,1} \otimes G_{B,1}$ can be written as linear combinations of the rows of $H_{A,0} \otimes G_{B,0}$.
The linear relations between the rows of H_A and those of G_B can be written as matrix equations and are summarized in the two following table.

Matrices	Linear equations	Number of relations
$M_A^0, M_A^1 \in \mathbb{F}_2^{r_{AA} \times m_A}$	$M_A^0 H_{A,0} = M_A^1 H_{A,1}$	r_{AA}
$N_A^0 \in\in \mathbb{F}_2^{r_A \times m_A}$	$N_A^0 H_{A,0} = 0$	r_A
$N_A^1 \in \mathbb{F}_2^{r_A \times m_A}$	$N_A^1 H_{A,1} = 0$	r_A

Matrices	Linear equations	Number of relations
$M_B^0, M_B^1 \in \mathbb{F}_2^{r_{BB} \times l_B}$	$M_B^0 G_{B,0} = M_B^1 G_{B,1}$	r_{BB}
$N_B^0 \in \mathbb{F}_2^{r_B \times l_B}$	$N_B^0 G_{B,0} = 0$	r_B
$N_B^1 \in \mathbb{F}_2^{r_B \times l_B}$	$N_B^1 G_{B,1} = 0$	r_B

The previous linear equations give rise to some linear relations between the rows of $\widetilde{H_X}$:

Equations	Number of relations
$(M_A^0 \otimes M_B^0)(H_{A,0} \otimes G_{B,0}) = (M_A^1 \otimes M_B^1)(H_{A,1} \otimes G_{B,1})$	$r_{AA} \times r_{BB}$
$(N_A^0 \otimes \mathbb{I})(H_{A,0} \otimes G_{B,0}) = 0$	$r_A \times \text{rank } (G_{B,0})$
$(N_A^1 \otimes \mathbb{I})(H_{A,1} \otimes G_{B,1}) = 0$	$r_A \times \text{rank } (G_{B,1})$
$(\mathbb{I} \otimes N_B^0)(H_{A,0} \otimes G_{B,0}) = 0$	$\text{rank } (H_{A,0}) \times r_B$
$(\mathbb{I} \otimes N_B^1)(H_{A,1} \otimes G_{B,1}) = 0$	$\text{rank } (H_{A,1}) \times r_B$
$(N_A^0 \otimes N_B^0)(H_{A,0} \otimes G_{B,0}) = 0$	$r_A \times r_B$
$(N_A^1 \otimes N_B^1)(H_{A,1} \otimes G_{B,1}) = 0$	$r_A \times r_B$

Let r_e be the number of relations existing in $\widetilde{H_X}$ that do not come from the linear relations of H_A and G_B. Then,

$$\begin{aligned} \text{rank } (\widetilde{H_X}) &= 2m_A l_B - \left(r_{AA} r_{BB} + 2r_A r_B + 2r_A \text{rank } (G_{B,0}) + 2r_B \text{rank } (H_{A,0}) + r_e\right) && (12)\\ &= 2m_A l_B - r_{AA} r_{BB} - 2r_A r_B - 2r_A(l_B - r_B) - 2r_B(m_A - r_A) - r_e && (13)\\ &= 2m_A l_B - r_{AA} r_{BB} + 2r_A r_B - 2r_A l_B - 2r_B m_A - r_e && (14) \end{aligned}$$

Numerically, by taking random matrices H_A^0, G_B^0, π_A, π_B, it seems that $r_e = 0$. If this is always the case (?), it would imply

$$\text{rank } (\widetilde{H_X}) = 2m_A l_B - r_{AA} r_{BB} + 2r_A r_B - 2r_A l_B - 2r_B m_A, \tag{15}$$

and the rank would reach its upperbound defined in Equation 11 whenever $r_{AA} = 0$ or $r_{BB} = 0$, i.e whenever there exists no linear dependencies between $H_{A,0}$ and $H_{A,1}$ or $G_{B,0}$ and $G_{B,1}$. Therefore, to increase the dimension of the codespace, one should try to maximize the number of linear relations between $H_{A,0}$ and $H_{A,1}$ and between $G_{B,0}$ and $G_{B,1}$. Nevertheless, we did not succeed in proving that $r_e = 0$ always holds true, i.e that the only relations arising between the rows of $\widetilde{H_X}$ are those listed in the last table and that rank $\widetilde{H_X}$ can always be expressed as in Equation 15.

D Logical operators bases for the non-lifted quantum Tanner codes

Through a different lens, the dimension K of a code can also be derived by expliciting the bases $\mathcal{L}_X$, $\mathcal{L}_Z$ of X and Z logical operators since $K = |\mathcal{L}_X| = |\mathcal{L}_Z|$. Furthermore, the logical operators bases prove valuable for gaining insights into the implementation of fault-tolerant logical quantum gates that can function reliably in the presence of errors.

Property 10 (Logical operators bases for HGP code [QC22])**.** *Considering the HGP code defined by Equation 6 and Equation 5, the bases for logical operators acting on the VV-qubits are*

$$\mathcal{L}_Z^l = \left\{(k \otimes \bar{f}, 0) \mid k \in Ker\ H_A, \bar{f} \in (Im\ H_B^T)^\bullet, |\bar{f}| = 1\right\}, \tag{16}$$

$$\mathcal{L}_X^l = \left\{(\bar{f} \otimes k, 0) \mid k \in Ker\ H_B, \bar{f} \in (Im\ H_A^T)^\bullet, |\bar{f}| = 1\right\}. \tag{17}$$

while the bases for logical operators acting on the CC-qubits are

$$\mathcal{L}_Z^r = \left\{0, \bar{f} \otimes k) \mid k \in Ker\ H_B^T, \bar{f} \in (Im\ H_A)^\bullet, |\bar{f}| = 1\right\}, \tag{18}$$

$$\mathcal{L}_X^r = \left\{(0, (k \otimes \bar{f}) \mid k \in Ker\ H_A^T, \bar{f} \in (Im\ H_B)^\bullet, |\bar{f}| = 1\right\}. \tag{19}$$

The cardinals of these sets are

$$\begin{aligned}|\mathcal{L}_Z^l| &= \text{Dim}\,(\text{Ker}\ H_A)\text{Dim}\left((\text{Im}\ H_B^T)^\bullet\right)\\ &= k_A(N_B - \text{Dim}\,(im H_B^T))\\ &= k_A(N_B - M_B + k_B^T) \quad \text{(Rank-Nullity theorem)}\\ &= k_A k_B \quad \text{(Equation 4)}\end{aligned}$$

$$\begin{aligned}|\mathcal{L}_Z^r| &= \text{Dim}\,(\text{Ker}\ H_B^T)\text{Dim}\,((\text{Im}\ H_A)^\bullet)\\ &= k_B^T(M_A - \text{Dim}\,(\text{Im}\ H_A))\\ &= k_B^T(M_A - N_A + k_A) \quad \text{(Rank-Nullity theorem)}\\ &= k_A^T k_B^T \quad \text{(Equation 4)},\end{aligned}$$

Since these two bases does not act on the qubits, we have $\mathcal{L}_Z = \mathcal{L}_Z^l \cup \mathcal{L}_Z^r$ such that $|\mathcal{L}_Z| = |\mathcal{L}_Z^l| + |\mathcal{L}_Z^r| = K$. The same reasoning apply to $\mathcal{L}_X$.
From these logical operators bases depicted on Figure 10, the logical operators are supported either on a combination of rows of qubits or on a combination of columns of qubits. These logical operators are still valid logical operators for the Quantum Tanner code defined by $\widetilde{H_X}$, $\widetilde{H_Z}$ but additional operators may exist.

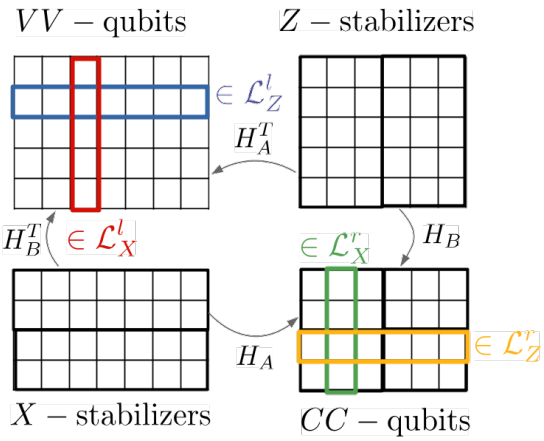

Figure 10: Depiction of the logical operator bases for the HGP codes.

D.1 Basis for logical operators under a tensor form

Looking at $\widetilde{H_X}$, $\widetilde{H_Z}$ (Equation 7), other logical operators can be considered to form a basis, namely

$$\mathcal{L}_Z^{supp} = \{\bar{f} \otimes g \mid \bar{f} \in (\text{Im}\ G_A^T)^\bullet, |\bar{f}| = 1, g \in \text{Ker}\ G_B\} \tag{20}$$
$$\mathcal{L}_X^{supp} = \{g \otimes \bar{f} \mid \bar{f} \in (\text{Im}\ G_B^T)^\bullet, |\bar{f}| = 1, g \in \text{Ker}\ G_A\} \tag{21}$$

In this subsection, we show that $\mathcal{L}_Z^l \cup \mathcal{L}_Z^{supp}$ and $\mathcal{L}_X^l \cup \mathcal{L}_X^{supp}$ form bases for every logical operators v that can be written as a tensor product $v_A \otimes v_B$ with $v_A \in \mathbb{F}_2^{N_A}$ and $v \in \mathbb{F}_2^{N_B}$ as stated in Property 13. For this purpose, some intermediate lemmas are required.

Lemma 11. *For the Quantum Tanner code defined by*

$$\widetilde{H_X} = \begin{pmatrix} H_{A,0} \otimes G_{B,0} \\ H_{A,1} \otimes G_{B,1} \end{pmatrix} \quad \text{and} \quad \widetilde{H_Z} = \begin{pmatrix} G_{A,1} \otimes H_{B,0} \\ G_{A,0} \otimes H_{B,1} \end{pmatrix},$$

the following holds

- $Ker\ H_A \cap (Im\ G_A^T)^\bullet = 0$
- $Ker\ H_B \cap (Im\ G_B^T)^\bullet = 0$
- $Ker\ G_A \cap (Im\ H_A^T)^\bullet = 0$
- $Ker\ G_B \cap (Im\ G_B^T)^\bullet = 0$

Proof. Since $H_{A,i} G_{A,i}^T = 0$ for $i = 0, 1$, we have $\text{Im}\ G_A^T = \text{Im}\ G_{A,0}^T + \text{Im}\ G_{A,1}^T = \text{Ker}\ H_{A,0} + \text{Ker}\ H_{A,1}$.
Combining this fact to the definition of a complemented subspace,

$$\begin{aligned}&\text{Im}\ G_A^T \cap (\text{Im}\ G_A^T)^\bullet = 0\\ \Leftrightarrow\ &\text{Ker}\ H_{A,0} \cap (\text{Im}\ G_A^T)^\bullet + \text{Ker}\ H_{A,1} \cap (\text{Im}\ G_A^T)^\bullet = 0\\ \Leftrightarrow\ &\text{Ker}\ H_{A,i} \cap (\text{Im}\ G_A^T)^\bullet = 0 \text{ for } i = 0, 1\,.\end{aligned}$$

Considering that $\text{Ker}\ H_A = \text{Ker}\ H_{A,0} \cap \text{Ker}\ H_{A,1}$,

$$\text{Ker}\ H_A \cap (\text{Im}\ G_A^T)^\bullet = \text{Ker}\ H_{A,1} \cap \text{Ker}\ H_{A,0} \cap (\text{Im}\ G_A^T)^\bullet = 0\,.$$

The same reasoning applies to the other cases. □

Lemma 12. *For the seed matrices H_A, H_B considered in the HGP construction, the following holds :*

1. *If $Ker\, H_A \cap (Im\, G_A^T)^\bullet = \{0\}$ and $Ker\, G_B \cap (Im\, H_B^T)^\bullet = \{0\}$, then*
$$\left(Ker\ H_A \otimes (Im\, H_B^T)^\bullet\right) \cap \left((Im\, G_A^T)^\bullet \otimes Ker\ G_B\right) = \{0\}\,.$$
2. *If $Ker\, H_B \cap (Im\, G_B^T)^\bullet = \{0\}$ and $Ker\, G_A \cap (Im\, H_A^T)^\bullet = \{0\}$, then*
$$\left(Ker\ G_A \otimes (Im\, G_B^T)^\bullet\right) \cap \left((Im\, H_A^T)^\bullet \otimes Ker\ H_B\right) = \{0\}\,.$$

Proof. Let $\{k_A^i\}$ be a basis of Ker H_A, $\{h_B^j\}$ basis of $(\text{Im } H_B^T)^\bullet$,$\{g_A^k\}$ basis of $(\text{Im } G_A^T)^\bullet$ and $\{k_B^l\}$ basis of Ker G_B.

Let $v \in \left(\text{Ker } H_A \otimes (\text{Im } H_B^T)^\bullet\right) \cap \left((\text{Im } G_A^T)^\bullet \otimes \text{Ker } G_B\right)$.
Then, there exists scalars $\{\lambda_{ij}\}$, $\{\mu_{kl}\}$ such that

$$v = \sum_{ij} \lambda_{ij} k_A^i \otimes h_B^j = \sum_{kl} \mu_{kl} g_A^k \otimes k_B^l\,. \tag{22}$$

Multiplying Equation 22 by $\mathbb{I} \otimes G_B$,

$$\sum_{ij} \lambda_{ij} k_A^i \otimes G_B h_B^j = 0\,.$$

Since Ker $G_B \cap (\text{Im } H_B^T)^\bullet = \{0\}$, $h_B^j \notin \text{Ker } G_B\ \forall\, j$ and hence, for scalars $\{\alpha_j\}$,

$$\sum_j \alpha_j G_B h_B^j = 0 \Rightarrow G_B\left(\sum_j \alpha_j h_B^j\right) = 0 \Rightarrow \sum_j \alpha_j h_B^j = 0 \Rightarrow \alpha_j = 0\ \forall\, j$$

and the set $\{G_B h_B^j\}$ as well as $\{k_A^i\}$ are both linearly independent sets. As the tensor product preserves the linear independence, we get

$$\sum_{ij} \lambda_{ij} k_A^i \otimes G_B h_B^j = 0 \Rightarrow \lambda_{ij} = 0\ \forall i, j\,.$$

Therefore, $v = 0$ and $\left(\text{Ker } H_A \otimes (\text{Im } H_B^T)^\bullet\right) \cap \left((\text{Im } G_A^T)^\bullet \otimes \text{Ker } G_B\right) = \{0\}$ □

Property 13. *Let $\{h_i^\alpha\}$ be a basis of $Ker\, H_\alpha$, $\{e_j^\alpha\}$ a basis of $(Im\, H_\alpha^T)^\bullet$, $\{f_k^\alpha\}$ a basis of $(Im\, G_\alpha^T)^\bullet$ and $\{g_l^\alpha\}$ a basis of $Ker\, G_\alpha$.*
The bases for the X and Z logical operators, that can written as $v = v_A \otimes v_B$ with $v_A \in \mathbb{F}_2^{N_A}$, $v_B \in \mathbb{F}_2^{N_B}$, are

$$\mathcal{L}_Z = \mathcal{L}_Z^l \cup \mathcal{L}_Z^{supp} = \{h_i^A \otimes e_j^B\} \cup \{f_k^A \otimes g_l^B\} \quad \textit{and} \quad \mathcal{L}_X = \mathcal{L}_X^l \cup \mathcal{L}_X^{supp} = \{e_j^A \otimes h_i^B\} \cup \{g_l^A \otimes f_k^B\}$$

Proof. **Linear independence:**
Suppose there exists scalars $\{\lambda_{ij}\}$, $\{\mu_{lk}\}$ such that

$$\sum_{ij} \lambda_{ij} h_i^A \otimes e_j^B + \sum_{l,k} \mu_{lk} f_k^A \otimes g_l^B = 0$$
$$\Leftrightarrow \sum_{ij} \lambda_{ij} h_i^A \otimes e_j^B = \sum_{l,k} \mu_{lk} f_k^A \otimes g_l^B\,.$$

However, from Lemma 12, $\left(\text{Ker } H_A \otimes (\text{Im } H_B^T)^\bullet\right) \cap \left((\text{Im } G_A^T)^\bullet \otimes \text{Ker } G_B\right) = 0$. Hence, $\lambda_{ij} = \mu_{lk} = 0$, $\forall i, j, k, l$ and $\mathcal{L}_Z$ is linearly independent.

spanning property: Let $v = v_A \otimes v_B \in \operatorname{Ker} \widetilde{H_X} \backslash \operatorname{Im} \widetilde{H_Z}^T$.
Then, v must satisfy:

1. $\widetilde{H_X}(v_A \otimes v_B) = 0 \Leftrightarrow \left\{ \begin{array}{rcl} H_{A,0} v_A \otimes G_{B,0} v_B & = & 0 \\ H_{A,1} v_A \otimes G_{B,1} v_B & = & 0 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lll} v_A \in \operatorname{Ker} H_{A,0} & \text{or} & v_B \in \operatorname{Ker} G_{B,0} \\ v_A \in \operatorname{Ker} H_{A,1} & \text{or} & v_B \in \operatorname{Ker} G_{B,1} \end{array} \right.$

2. $v \notin \operatorname{Im} \widetilde{H_Z}^T \Leftrightarrow v \notin \operatorname{Im} (G_{A,1} \otimes H_B^0)^T + \operatorname{Im} (G_{A,0} \otimes H_B^1)^T$.

Case 1: $v_A \in \operatorname{Ker} H_{A,0} \cap \operatorname{Ker} H_{A,1} = \operatorname{Ker} H_A$.
Then $v_A \in \operatorname{Im} G_{A,0}^T \cap \operatorname{Im} G_{A,1}^T$.
To respect condition 2., we must have $v_B \notin \operatorname{Im} H_{B,0}^T + \operatorname{Im} H_{B,1}^T \Leftrightarrow v_B \notin \operatorname{Im} H_B^T \Leftrightarrow v_B \in (\operatorname{Im} H_B^T)^\bullet$.
Therefore, $v \in \operatorname{Ker} H_A \otimes (\operatorname{Im} H_B^T)^\bullet$.
Case 2: $v_B \in \operatorname{Ker} G_{B,0} \cap \operatorname{Ker} G_{B,1} = \operatorname{Ker} G_B$.
Then $v_B \in \operatorname{Im} H_{B,0}^T \cap \operatorname{Im} H_{B,1}^T$.
To respect condition 2., we must have $v_A \notin \operatorname{Im} G_{A,0}^T + \operatorname{Im} G_{A,1}^T \Leftrightarrow v_A \notin \operatorname{Im} G_A^T \Leftrightarrow v_A \in (\operatorname{Im} G_A^T)^\bullet$.
Therefore, $v \in (\operatorname{Im} G_A^T)^\bullet \otimes \operatorname{Ker} G_B$.
Case 3: $v_A \in \operatorname{Ker} H_{A,0}$ and $v_B \in \operatorname{Ker} G_{B,1}$.
Then $v_A \in \operatorname{Im} G_{A,0}^T$ and $v_B \in \operatorname{Im} H_{B,1}^T$.
Hence $v \in \operatorname{Im} \widetilde{H_Z}^T$ which is impossible according to condition 2.
Case 4: $v_A \in \operatorname{Ker} H_{A,1}$ and $v_B \in \operatorname{Ker} G_{B,0}$.
Then $v_A \in \operatorname{Im} G_{A,1}^T$ and $v_B \in \operatorname{Im} H_{B,0}^T$.
Hence $v \in \operatorname{Im} \widetilde{H_Z}^T$ which is impossible according to condition 2.
Therefore, $\mathcal{L}_Z$ is a spanning set of linearly independent vectors for tensor product vectors in $\operatorname{Ker} \widetilde{H_X} \backslash \operatorname{Im} \widetilde{H_Z}^T$, so it is a basis.
The proof for $\mathcal{L}_X$ being a basis follows the same lines. □

D.2 Bases for every logical operators

In Property 13, the proof for the linear independence holds for every logical operators whereas the proof concerning the spanning property holds true only when considering logical operators that can be written as a tensor product. Nonetheless, the numerical calculations performed hints to these bases being bases for all type of logical operators as the cardinal of the bases always matched the dimension of the randomly generated codes. In this subsection, we prove that this always holds true and we then conclude in Property 19 that the bases considered in the last section are in fact bases for all the logical operators of the non-lifted quantum Tanner codes. Since the proofs of this section are lengthy and only confer technical details, the choice has been made to write them in Appendix B.

Before explicitly deriving $\operatorname{rank} \widetilde{H_X} + \operatorname{rank} \widetilde{H_Z}$ in Property 17, intermediate lemmas are necessary.

Lemma 14. *For $\alpha = A, B$,*

- $rank\ H_\alpha = 2 rank\ H_{\alpha,0} + rank\ G_\alpha - N_\alpha$
- $rank\ G_\alpha = 2 rank\ G_{\alpha,0} + rank\ H_\alpha - N_\alpha$

Proof. See Appendix B. □

Lemma 15. *Let A^0, A^1 be vector spaces over $\mathbb{F}_2^{N_A}$ and B^0, B^1 vector spaces over $\mathbb{F}_2^{N_B}$ such that $Dim\ A^0 = Dim\ A^1$ and $Dim\ B^0 = Dim\ B^1$. Let $A = A^0 \cap A^1$ and $B = B^0 \cap B^1$. Then,*

$$Dim\left((A^0 \otimes \mathbb{F}_2^{N_B} + \mathbb{F}_2^{N_A} \otimes B^0) \cap (A^1 \otimes \mathbb{F}_2^{N_B} + \mathbb{F}_2^{N_A} \otimes B^1)\right) = N_B Dim\ A + N_A Dim\ B - 2 Dim\ A^0 Dim\ B^0 + (2 Dim\ B^0 - Dim\ B)(2 Dim\ A^0 - Dim\ A)\ .$$

Proof. See Appendix B. □

Lemma 16. *Let A^0, A^1 be vector spaces over $\mathbb{F}_2^{N_A}$ and B^0, B^1 be vector spaces over $\mathbb{F}_2^{N_B}$.*

$$Ker\,(A^0 \otimes B^0) \cap Ker\,(A^1 \otimes B^1) = (\mathbb{F}_2^{N_A} \otimes Ker\,B^0 + Ker\,A^0 \otimes \mathbb{F}_2^{N_B}) \cap (\mathbb{F}_2^{N_A} \otimes B^1 + Ker\,A^1 \otimes \mathbb{F}_2^{N_B})$$

Proof. A more general proof can be found at http://www.cip.ifi.lmu.de/~grinberg/algebra/tensorext.pdf, in section 0.9. □

Property 17.

$$rank\,\widetilde{H_X} + rank\,\widetilde{H_Z} = -N_A N_B + N_B(rank\,H_A + rank\,G_A) + N_A(rank\,H_B + rank\,G_B) - rank\,G_A\,rank\,G_B - rank\,H_A\,rank\,H_B$$

Proof. See Appendix B □

Property 18.

$$\begin{aligned}|\mathcal{L}_Z| = |\mathcal{L}_X| &= k_A k_B + k_A^\perp k_B^\perp \\ &= (N_A - rank\,H_A)(N_B - rank\,H_B) + (N_A - rank\,G_A)(N_B - rank\,G_B)\end{aligned}$$

Proof. From the complemented subspace definition,

$$\begin{aligned}\mathrm{Dim}\,((\mathrm{Im}\,H_B^T)^\bullet) &= N_B - \mathrm{Dim}\,(\mathrm{Im}\,H_B^T) \\ &= \mathrm{Dim}\,(\mathrm{Ker}\,H_B) = k_B\end{aligned}$$

Similarly, $\mathrm{Dim}\,((\mathrm{Im}\,G_A^T)^\bullet) = \mathrm{Dim}\,(\mathrm{Ker}\,G_A) = k_A^\perp$. According to item 12, $\mathcal{L}_X^l \cap \mathcal{L}_X^{supp} = \{0\}$. Therefore,

$$\begin{aligned}|\mathcal{L}_X| &= \mathrm{Dim}\,(\mathrm{Ker}\,H_A \otimes (\mathrm{Im}\,H_B^T)^\bullet) + \mathrm{Dim}\,((\mathrm{Im}\,G_A^T)^\bullet \otimes \mathrm{Ker}\,G_B) \\ &= k_A k_B + k_A^\perp k_B^\perp \\ &= (N_A - \mathrm{rank}\,H_A)(N_B - \mathrm{rank}\,H_B) + (N_A - \mathrm{rank}\,G_A)(N_B - \mathrm{rank}\,G_B),\end{aligned}$$

where the last equality follows from the rank-nullity theorem. □

Property 19. *Let $\{h_i^\alpha\}$ be a basis of $Ker\,H_\alpha$, $\{e_j^\alpha\}$ a basis of $(Im\,H_\alpha^T)^\bullet$, $\{f_k^\alpha\}$ a basis of $(Im\,G_\alpha^T)^\bullet$ and $\{g_l^\alpha\}$ a basis of $Ker\,G_\alpha$.*
The bases for the X and Z logical operators are

$$\begin{aligned}\mathcal{L}_Z &= \mathcal{L}_Z^l \cup \mathcal{L}_Z^{supp} \\ &= \{h_i^A \otimes e_j^B\} \cup \{f_k^A \otimes g_l^B\}\end{aligned} \quad \textit{and} \quad \begin{aligned}\mathcal{L}_X &= \mathcal{L}_X^l \cup \mathcal{L}_X^{supp} \\ &= \{e_j^A \otimes h_i^B\} \cup \{g_l^A \otimes f_k^B\},\end{aligned} \quad \textit{and}$$

the code has dimension $K = (N_A - rank\,H_A)(N_B - rank\,H_B) + (N_A - rank\,G_A)(N_B - rank\,G_B)$.

Proof. $\mathcal{L}_X$ and $\mathcal{L}_Z$ are sets of linearly independent following the exact same proof as in Property 13.

The number of logical qubits in the considered Quantum Tanner code is $K = N_A N_B - \mathrm{rank}\,\widetilde{H_X} - \mathrm{rank}\,\widetilde{H_Z}$. Hence, from Property 17,

$$K = (N_A - \mathrm{rank}\,H_A)(N_B - \mathrm{rank}\,H_B) + (N_A - \mathrm{rank}\,G_A)(N_B - \mathrm{rank}\,G_B)\,.$$

Then, using Property 18, we trivially obtain

$$|\mathcal{L}_X| = |\mathcal{L}_Z| = K\,.$$

Hence, $\mathcal{L}_Z$ and $\mathcal{L}_Z$ are sets of linearly independent vectors whose cardinals match the dimension K of the logical space. Therefore, $\mathcal{L}_Z$ and $\mathcal{L}_X$ are bases for the logical operators. □

The logical operators bases are depicted on Figure 11. In contrast to the HGP case, the logical X and Z operators for the non-lifted quantum Tanner codes are supported on linear combination of rows and columns of the qubits set $E_A \times E_B$.

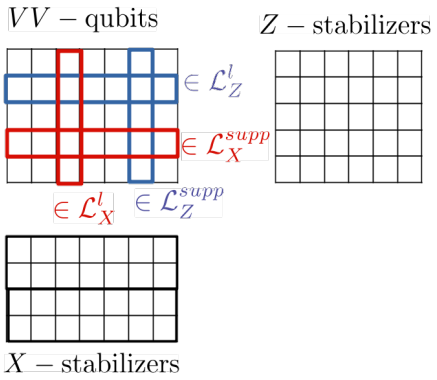

Figure 11: Depiction of the logical operators bases for the non-lifted quantum Tanner codes.

III Lifted quantum Tanner codes

This section aims to study the logical operators of the quantum Tanner codes when a lift is applied.

A Graph lift

Let $\mathcal{G} = (V, E)$ be a graph. A *voltage assignment* for $\mathcal{G}$ with a *voltage group* G is a map $\gamma : E \to G$. The G-*lifted* version of $\mathcal{G}$ is a graph $\hat{\mathcal{G}} = (\hat{V}, \hat{E})$ where $\hat{V} = V \times G$, $\hat{E} = E \times G$. Let $v, w \in V$ and suppose that $e \in E$ connects v and w in $\mathcal{G}$. Then, when G is non-Abelian, for every $g \in G$, the edge $\hat{e} = (e, g)$ connects the vertices $\hat{v} = (v, g)$ and $\hat{w} = (w, \gamma(e)g)$ for a left lift and it connects the vertices $\hat{v} = (v, g)$ and $\hat{w} = (w, g\gamma(e))$ for a right lift. A simple example of this lifting procedure is depicted in Figure 12.

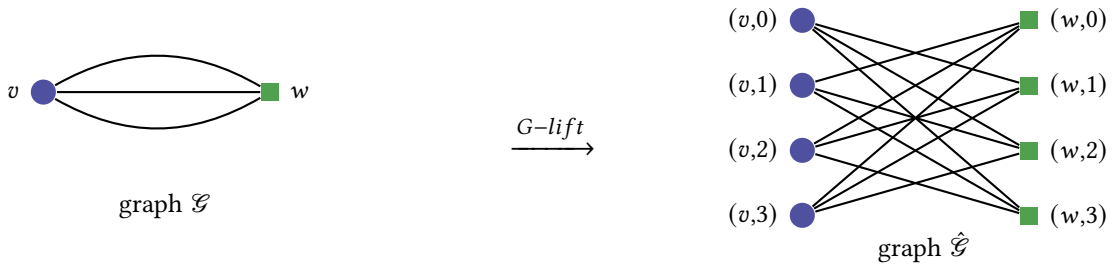

Figure 12: Example of a G-lift of the graph $\mathcal{G}$ with $G = \mathbb{Z}/4\mathbb{Z}$ and voltage assignment $\gamma(e_i) = i$ for $i \in \mathbb{Z}/4\mathbb{Z}$

A G-lifted version of a code can be obtained by applying a G-lift to its Tanner graph. In 2022, Panteleev and Kalachev devised asymptotically good quantum LDPC codes by taking the G-lifted product of two G-lifted Tanner codes where G is a non-Abelian group [PK22]. These codes are closely related to the lifted version of the quantum Tanner codes that are also good quantum LDPC codes [LZ22b].

The lifting procedure can give rise to the double cover of a Cayley graph. To do so, consider the graph $\mathcal{G}_k$ with two vertices $V = 0, 1$ and k multiple edges E_k (Figure 13). Let G be a finite group and a symmetric set of generators $S \subseteq G$ such that $|S| = k$ and for all $s \in S$, $s^{-1} \neq s$. Then, a left G-lift of $\mathcal{G}_k$ with the voltage assignment $\gamma : E_k \to S$ leads to the double cover of the left Cayley graph $Cay_L(G, S)$ with the set vertices $\hat{V} = G \times \{0, 1\}$ and the set of edges $\hat{E} = \{\{(0, g), (1, sg)\} \,|\, g \in G, s \in S\}$. The double cover of the right Cayley graph $Cay_R(G, S)$ can be obtained by taking a right G-lift such that the set of edges is $\hat{E} = \{\{(0, g), (1, gs)\} \,|\, g \in G, s \in S\}$.

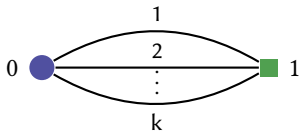

Figure 13: Graph $\mathcal{G}_k$

Going back to the non-lifted version of quantum Tanner codes exposed in Section B, the connection with the quantum Tanner codes described in Section D is now clearer. Consider a non-Abelian group G and two symmetric subsets of generators $A, B \subseteq G$ of size $|A| = \lfloor N_A N_B/2 \rfloor$ and $|B| = \lceil N_A N_B/2 \rceil$ where N_A, N_B are the length of the classical codes $\mathcal{C}_A, \mathcal{C}_B$ of Section B. For $i, j, k, l \in \{0, 1\}$, let E_{ij-kl} denote the set of edges connecting the vertex v_{ij} to v_{kl} in Figure 9. Then, in Figure 9, applying a right G-lift with the voltage assignment $\gamma_{ij-kl} : E_{ij-kl} \to A$ to each of the subgraphs $\mathcal{H}_{00-01}(\{v_{00}, v_{01}\}, E_{00-01})$ and $\mathcal{H}_{10-11}(\{v_{00}, v_{01}\}, E_{00-01})$ as well as a left G-lift with voltage assignment $\gamma_{ij-kl} : E_{ij-kl} \to B$ to each of the subgraphs $\mathcal{H}_{00-10}(\{v_{00}, v_{10}\}, E_{00-10})$ and $\mathcal{H}_{01-11}(\{v_{01}, v_{11}\}, E_{01-11})$ leads to the quadripartite version of the left-right Cayley complex with vertices set $V = \cup_{i,j=0,1} V_{ij}$ where for

all $i,j=0,1$, $V_{ij}=\{v_{ij}\}\times G$. After the lifting procedure, the length of the code is $|G||A||B|$, the bits sit on the squares of the complexes and as expected, the codeword obtained when the square sets is restricted to the squares incident to $v\in V_{00}\cup V_{11}$ (resp.$v\in V_{01}\cup V_{10}$) belongs to $\mathscr{C}_A\otimes\mathscr{C}_B^{\perp}$ (resp. $\mathscr{C}_A^{\perp}\otimes\mathscr{C}_B$).

B Exploration into the basis of logical operators

Recall that the quantum Tanner codes $\mathcal{Q}(H_X,H_Z)$ is such that

$$\widetilde{H_X}=\begin{pmatrix}H_{A,0}\otimes G_{B,0}\\ H_{A,1}\otimes G_{B,1}\end{pmatrix}\equiv\begin{pmatrix}H_X^0\\ H_X^1\end{pmatrix}\ ,\ \widetilde{H_Z}=\begin{pmatrix}G_{A,1}\otimes H_{B,0}\\ G_{A,0}\otimes H_{B,1}\end{pmatrix}\equiv\begin{pmatrix}H_Z^0\\ H_Z^1\end{pmatrix}\ ,$$

where $H_{A,0}$, $H_{B,0}$ are the parity-check matrices describing two classical Tanner codes $\mathscr{C}_A$, $\mathscr{C}_B$ and $H_{\alpha,1}=\mathcal{H}_{\alpha,0}pi_\alpha$ for $\alpha=A,B$ and some permutation matrix π_α.
Since the parity-check matrix of a code corresponds to the adjacency matrix of its Tanner graph, it is equivalent to perform a lift directly on the Tanner graph as exposed previously or to apply a lift to the parity-check matrix as exposed next. Without loss of generality, we consider in the following that the codes $\mathscr{C}_A$, $\mathscr{C}_B$ have both length $N_A=N_B=\Delta$. Consider a group G of order n with generators $\{g_1,\cdots,g_n\}$and let $\widetilde{\widetilde{H}}$ be the G-lifted version of any matrix H or $\widetilde{H}$. Let $\alpha=A,B$, the lifting procedure is the following

$$H_X^0=\begin{pmatrix}1&1&1&\\0&1&0&\dots\\&\vdots&&\end{pmatrix}\xrightarrow{G-lift}\widetilde{\widetilde{H_X^0}}=\begin{pmatrix}\mathbb{I}^{n\times n}&\mathbb{I}^{n\times n}&\mathbb{I}^{n\times n}&\\0^{n\times n}&\mathbb{I}^{n\times n}&0^{n\times n}&\dots\\&\vdots&&\end{pmatrix},$$

$$H_X^1=\begin{pmatrix}1&0&1&\\1&1&0&\dots\\&\vdots&&\end{pmatrix}\xrightarrow{G-lift}\widetilde{\widetilde{H_X^1}}=\begin{pmatrix}\mathbb{I}^{n\times n}&\mathbb{I}^{n\times n}&\mathbb{I}^{n\times n}&\\\mathbb{I}^{n\times n}&0^{n\times n}&0^{n\times n}&\dots\\&\vdots&&\end{pmatrix}\begin{pmatrix}M_{g_1}&0&&\\0&M_{g_2}&&\\&&\ddots&\\&&&M_{g_n}\end{pmatrix}=\begin{pmatrix}M_{g_1}&0&M_{g_3}&\\M_{g_1}&M_{g_2}&0&\dots\\&\vdots&&\end{pmatrix},$$

and for i=0,1,

$$H_Z^i=\begin{pmatrix}1&1&1&\\1&0&0&\dots\\&\vdots&&\end{pmatrix}\xrightarrow{G-lift}\widetilde{\widetilde{H_Z^i}}=\begin{pmatrix}\mathbb{I}^{n\times n}&\mathbb{I}^{n\times n}&\mathbb{I}^{n\times n}&\\\mathbb{I}^{n\times n}&0^{n\times n}&0^{n\times n}&\dots\\&\vdots&&\end{pmatrix}\begin{pmatrix}M_{g_1}&0&&\\0&M_{g_2}&&\\&&\ddots&\\&&&M_{g_n}\end{pmatrix}=\begin{pmatrix}M_{g_1}&M_{g_2}&M_{g_3}&\\M_{g_1}&0&0&\dots\\&\vdots&&\end{pmatrix},$$

where, for $g\in G$, $M_g\in\mathbb{F}_2^{n\times n}$ is the action matrix of g which must satisfies

$$\forall\ h_1,h_2\in G\text{ such that }g\cdot h_1=h_2\ \Leftrightarrow\ M_gM_{h_1}=M_{h_2}\ ,$$

and

$$\forall\ h_1,h_3\in G\text{ such that }h_1\cdot g=h_3\ \Leftrightarrow\ M_{h_1}M_g=M_{h_3}\ .$$

After checking numerically that our lifting procedure applied to the non-lifted quantum Tanner codes parity-check matrices $\widetilde{H_X}$, $\widetilde{H_Z}$ leads to the same parity-check matrices described explicitly in [LZ22b], our goal was to explore the dimension of the lifted code and the logical operator bases as previously with the non-lifted version. The main difficulty we encountered is that the lift is applied to a tensor product of matrices. A first wrong lifting procedure we applied was to first lift the matrices $H_{\alpha,i}$, $G_{\alpha,i}$, for $\alpha=A,B,\ i=0,1$, and then to take their tensor product to form

$$\begin{pmatrix}\widetilde{\widetilde{H_{A,0}}}\otimes\widetilde{\widetilde{G_{B,0}}}\\ \widetilde{\widetilde{H_{A,1}}}\otimes\widetilde{\widetilde{G_{B,1}}}\end{pmatrix}\ ,\ \begin{pmatrix}\widetilde{\widetilde{G_{A,1}}}\otimes\widetilde{\widetilde{H_{B,0}}}\\ \widetilde{\widetilde{G_{A,0}}}\otimes\widetilde{\widetilde{H_{B,1}}}\end{pmatrix}.$$

In this case, the bases of logical operators are simply

$$\widetilde{\widetilde{\mathcal{L}_Z}}=\{\widetilde{\widetilde{h_i^A}}\otimes\widetilde{\widetilde{e_j^B}}\}\cup\{\widetilde{\widetilde{f_k^A}}\otimes\widetilde{\widetilde{g_l^B}}\}$$

and

$$\widetilde{\widetilde{\mathcal{L}_X}}=\{\widetilde{\widetilde{e_j^A}}\otimes\widetilde{\widetilde{h_i^B}}\}\cup\{\widetilde{\widetilde{g_l^A}}\otimes\widetilde{\widetilde{f_k^B}}\}$$

where $\{\widetilde{\widetilde{h_i^\alpha}}\}$ be a basis of Ker $\widetilde{\widetilde{H_\alpha}}$, $\{\widetilde{\widetilde{e_j^\alpha}}\}$ a basis of $(\text{Im }\widetilde{\widetilde{H_\alpha^T}})^\bullet$, $\{\widetilde{\widetilde{f_k^\alpha}}\}$ a basis of $(\text{Im }\widetilde{\widetilde{G_\alpha^T}})^\bullet$ and $\{\widetilde{\widetilde{g_l^\alpha}}\}$ a basis of Ker $\widetilde{\widetilde{G_\alpha}}$.
And the dimension of the lifted code found was simply $\widetilde{\widetilde{K}}=n^2K$. But this lifting procedure does not corresponds to the one leading to a code on a left-right Cayley complex and leads to a code of length $n^2N_AN_B$.
With the correct lifting procedure, the VV-qubits corresponds to $E_A\times E_B\times G$ and can be represented by 3-dimensional matrices of size nN_AN_B. Looking at the logical operators bases obtained for the non-lifted version,

the intuition is that the logical operators might express as a linear combination of vertical and horizontal slices in $E_A \times E_B \times G$. Unfortunately, we did not find a general way to either describe the logical operators bases or the rank of the lifted matrices $\widetilde{\widetilde{H_X}}, \widetilde{\widetilde{H_Z}}$ as new linear relations can arise between the lines depending on the chosen group G and its action matrices. We tried to conjecture the dimension $\widetilde{\widetilde{K}}$ of the lifted code by performing numerical simulation on some examples but did not exhibit any evident relations between the known quantities and $\widetilde{\widetilde{K}}$.

IV Abelian quantum Tanner codes

This section is independent from the previous ones and is dedicated to adapt the proof on the minimal distance of the quantum Tanner codes from [LZ22a] when considering an Abelian group instead of a non-Abelian one. The interest of this study lies in the hope that the minimal distance might be not too low even for Abelian groups opening the road to the construction of a new quantum LDPC code built on a complex that exhibits, in addition to the vertices, edges and squares, a higher dimensional structure such as cubes. Such a complex would necessitate to consider an Abelian group to be able to define the cubes.

A Cayley graphs expanding property for Abelian groups

Let G_0 be an Abelian group. Given a group $G = G_0^m$ for some integer $m > 1$ and $\varepsilon_0 > 0$, $\mathcal{G} = Cay(G,S)$ is an expander with high probability and with normalized spectral gap $1-\varepsilon_0$ by taking uniformly random subset $S \subset G^m$ of size $O\left(\frac{\log(|G|)}{\varepsilon_0^2}\right)$ [JM21].

$\mathcal{G}$ is Δ_n-regular with $\Delta_n = |S|$. The subscript n is a reminder that the graph degree is not a constant anymore and when considering Quantum Tanner code, it will vary with the codelength such as $n = |G|\Delta_n^2$. The expanding property of $\mathcal{G}$ is expected to be poorer than in the Ramanujan case, namely $\lambda(\mathcal{G}) = \Delta^{1-\varepsilon}$ for $\varepsilon \in]0, 1/2[$. Taking this into account and an unnormalised spectral gap, the property from [JM21] can be reformulated as in Property 20.

Property 20 (Expansion in Abelian Cayley graphs)**.** *Let G_0 be an Abelian group. Given a group $G = G_0^m$ for some integer $m > 1$, $\mathcal{G} = Cay(G,S)$ is an expander with high probability and with $\lambda(\mathcal{G}) = \Delta_n^{1-\varepsilon}$, $\varepsilon \in]0, 1/2[$, by taking uniformly random subset $S \subset G^m$ of size $\Delta_n = O\left((\log n)^{\frac{1}{1-2\varepsilon}}\right)$.*

B Minimal distance with Abelian groups

Let G_0 be an Abelian group. Let $G = G_0^m$ for some $m > 1$ and $A, B \subset G$ two self-inverse subsets such that $|A| = |B| = \Delta_n$.
Let $\mathcal{G}_A = Cay(G,A)$ and $\mathcal{G}_B = Cay(G,B)$ such that

$$\lambda(\mathcal{G}_A) = \lambda(\mathcal{G}_B) = \Delta_n^{1-\varepsilon}$$

for some $\varepsilon \in]1/2, 1[$.
As in the non Abelian case, we consider the quantum Tanner code $\mathcal{Q} = (\mathcal{C}_0, \mathcal{C}_1)$ defined by

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

on the quadripartite version of the left-right Cayley complex constructed from G^n, A, B. The expanding property of $\mathcal{G}_i^{\square}$, $i = 0, 1$ is modified as exposed in Lemma 21.

Lemma 21.

$$\lambda(\mathcal{G}_i^{\square}) = \Delta_n^{2-2\varepsilon} \ .$$

Proof. By using similar arguments as in [LZ22b]. □

Recall that to obtain good random linear codes C_A, C_B of length Δ takes time $e^{\Omega(\Delta)}$. This was not too cumbersome previously as Δ was constant but with Abelian groups, we have codelength Δ_n in polylog(n) and hence, to find good random linear codes can take time poly(n).

The support of the codewords is the set of squares Q indexed by (g,a,b), $g \in G$, $a \in A$, $b \in B$. Hence this code has length

$$n = |G|\Delta_n^2. \tag{23}$$

Let $\mathbf{x} \in \mathscr{C}_1 \setminus \mathscr{C}_0^\perp$ and x_v be the local view at $v \in V_1$ that can be written as $x_v = r_v + c_v$ where $r_v \in \mathbb{F}_2^\Delta \otimes C_B$, $c_v \in C_A \otimes \mathbb{F}_2^\Delta$. We define $R_i = \sum_{v \in V_{i\bar{i}}} r_v$ and $C_i = \sum_{v \in V_{i\bar{i}}} c_v$ such that $\mathbf{x} = R_0 + C_1 = R_1 + C_0$. In the following, $||C_i||$ will denote the number of non zero column codewords belonging to C_i and $||R_i||$ the number of non zero row codewords belonging to R_i. The ensuing proof on the minimal distance is established for a codeword in $\mathscr{C}_1 \setminus \mathscr{C}_0^\perp$, however, by symmetry, the arguments are identical for a codeword in $\mathscr{C}_0 \setminus \mathscr{C}_1^\perp$.

Theorem 22 (Minimum distance). *For* $\mathbf{x} \in \mathscr{C}_1 \setminus \mathscr{C}_0^\perp \cup \mathscr{C}_0 \setminus \mathscr{C}_1^\perp$,

$$d_{min} \geq \frac{\kappa \Delta_n}{2} ||\mathbf{x}|| .$$

Proof. Exactly the same as in [LZ22a]. □

In the following, $\mathbf{x}$ is supposed to achieve the minimum of $||\mathbf{x}||$ in $\mathbf{x} + \mathscr{C}_0^\perp$ and (C_0, R_0, C_1, R_1) is its minimum representation. Let $S_{ij} = \{v \in V_{ij} | C_j + R_i \text{ is non zero on } Q(v)\}$. A vertex $v \in S_{ij}$ is said *exceptional* if $||r_v|| + ||c_v|| \geq \alpha\Delta$ with $\alpha = \delta^2/256$, otherwise, it is said *ordinary*. The sets of exceptional vertices are denoted S_{ij}^e and the sets of ordinary vertices $S_{i_j}^{ord}$.

Lemma 23 (Rarity of exceptional vertices). *Let* $i = 0, 1$. *If* $|S_{ij}| \leq \frac{\alpha\kappa}{2}|V_{00}|$, *then*

$$|S_{ii}^e| \leq \left(\frac{2\lambda(\mathcal{G}_0^\square)}{\Delta_n^2 \alpha\kappa}\right)^2 |S_0| = \frac{4}{\alpha^2\kappa^2\Delta^{4\varepsilon}}|S_0| ,$$
$$|S_{i\bar{i}}^e| \leq \left(\frac{2\lambda(\mathcal{G}_1^\square)}{\Delta_n^2 \alpha\kappa}\right)^2 |S_1| = \frac{4}{\alpha^2\kappa^2\Delta^{4\varepsilon}}|S_1| .$$

Proof. Let $v \in S_{00}^e$.
Applying robustness and minimality of the representation,

$$|x_v| = |c_v| + |r_v| \geq \kappa\Delta(||c_v|| + ||r_v||) \geq \kappa\Delta\alpha\Delta.$$

Hence, the degree of each $v \in S_{00}^e$ is at least $\kappa\alpha\Delta^2$. From the Expander Mixing Lemma applied in $\mathcal{G}_0^\square$,

$$|S_{00}^e \alpha\kappa\Delta^2 \leq |E(S_{00}^e, S_{11})| \leq \Delta^2 \frac{|S_{00}^e||S_{11}|}{|V_{00}|} + \lambda(\mathcal{G}_0^\square)\sqrt{|S_{00}^e||S_{11}|} .$$

Using the hypothesis $|S_{11}| \leq \frac{\alpha\kappa}{2}|V_{00}|$, one gets

$$|S_{ii}^e| \leq \left(\frac{2\lambda(\mathcal{G}_0^\square)}{\Delta_n^2 \alpha\kappa}\right)^2 |S_{11}| \leq \left(\frac{2\lambda(\mathcal{G}_0^\square)}{\Delta_n^2 \alpha\kappa}\right)^2 |S_0| .$$

By symmetry, the proofs for the other cases are similar. □

Let T be the set of vertices of V_{ij} whose local views see at least one non zero C_A codeword of C_j that is shared by the local view of an ordinary vertex $w \in V_{\bar{i}j}$.

Lemma 24 (Upper bound on $|T|$). *Let* $\mathcal{G}_A = Cay(G, A)$ *and* $i, j = 0, 1$. *If* $|S_{i\bar{j}}| \leq \frac{\delta|V_{00}|}{4}$, *then*

$$|T| \leq \left(\frac{4\lambda(\mathcal{G}_A)}{\delta\Delta_n}\right)^2 |S_{i\bar{j}}| = \frac{16}{\delta^2\Delta_n^\varepsilon}|S_{i\bar{j}}| .$$

Proof. Let $i = j = 0$ such that the local view of $v \in T \subset V_{00}$ share at least one non zero codeword with the local view of an ordinary vertex $w \in V_{10}$. Keeping only the two sets V_{00} and V_{01}, we obtain a multigraph in which every square became a edge and that corresponds to the double cover of $\mathcal{G}_A$. The subgraph induced by $\mathbf{x}$ is obtain by keeping the edge only when the row view of the local is non zero in $\mathbf{x}$.

Recall that $w \in V_{10}$ is ordinary if it fosters at most $\alpha\Delta_n$ non zero columns and rows, i.e $||c_w|| + ||r_w|| \leq \alpha\Delta_n$. This implies that any column vector in C_0 belonging to the local of an ordinary vertex $w \in V_{10}$ has at most $\alpha\Delta_n$ non-zero coordinates with R_1 as in the worst case, $||c_w|| = 1$ and $||r_w|| = \alpha\Delta_n - 1$, i.e the only column c_w intersects with $\alpha\Delta_n - 1$ rows. These intersections between the column and the row codewords in the local view of an ordinary vertex can be understood as a perturbation of weight at most $\alpha\Delta$, namely, a column (resp. row) codeword will be at distance at most $\alpha\Delta_n$ from a nonzero codeword of C_A (resp. C_B).

As a codeword lying in C_A has weight at least $\delta\Delta_n$ and a column codeword shared between T and an ordinary vertex în V_{10} has at most $\alpha\Delta_n$ disturbed coordinates, the weight of this shared column is at least $\delta\Delta_n - \alpha\Delta_n$. Hence, there is at least $\delta\Delta_n - \alpha\Delta_n$ edges between $v \in T$ and $v' \in S_{01}$, i.e every vertex of T in the subgraph has degree at least $\delta\Delta_n - \alpha\Delta_n$. For the simplicity sake, the degree can be lower bounded by $\delta\Delta_n/2$. Therefore,

$$|T|\frac{\delta\Delta_n}{2} \leq |E(S_0 1, T)|,$$

and the expander mixing Lemma in the double cover of $\mathcal{G}_A$ yields

$$|E(S_{01}, T)| \leq \Delta_n \frac{|S_{01}||T|}{|V_{01}|} + \lambda(\mathcal{G}_A)\sqrt{|S_{01}||T|}.$$

Under the hypothesis $|S_{01}| \leq \delta|V_{01}|/4$,

$$|T| \leq \left(\frac{4\lambda(\mathcal{G}_A)}{\delta\Delta_n}\right)^2 |S_{01}|$$

.
By symmetry, the case $i = j = 1$ is similar as well as the case $i = \bar{j}$, except that in the latter, the codeword considered is $\mathbf{x}^0$ instead of $\mathbf{x}$.

□

Lemma 25 (Lower bound on the codeword norm). *Suppose $\varepsilon \in (\frac{1}{4}, \frac{1}{2})$ and that the fraction β of ordinary vertices in S_{01} or S_{10} is such that $4\beta \leq c' \log(|G|)$.*
Then $\forall \mathbf{x} \in C_1 \setminus C_0^\perp$,

$$||\mathbf{x}|| \geq \frac{\delta^2 \kappa n}{512\Delta_n^2}.$$

Proof. Let $\mathbf{x} \in C_1 \setminus C_0$ such that $||\mathbf{x}|| < \frac{\kappa\delta^2 n}{512\Delta_n^2}$.

$$|S_{ij}| \leq ||C_j|| + ||R_i|| \leq ||\mathbf{x}|| < \frac{\kappa\delta^2}{512}|V_{00}|$$

As $\kappa\alpha/2 \leq \delta/4$, Lemma 11 and Lemma 10 hold.
In the following, suppose $|S_1| > |S_0|$ and $|S_{10}| \geq |S_{01}|$ (if one of these inequalities is not satisfied, invert the roles of the two sets in the argument). From Lemma 10,

$$|S_{10}^e| \leq \left(\frac{2}{\alpha\kappa\Delta^{2\varepsilon}}\right)^2 |S_1|$$

and for Δ large enough, the exceptional vertices are rare in S_1. Therefore, most of the vertices of S_{01} are ordinary, i.e $|S_{10}^{ord}| \geq \beta|S_{01}|$ for $\beta < 1$. Since each vertex has at least one ordinary row or ordinary column in its local view,

$$\sum_{v \in S_{01}^{ord}} ||r_v|| + ||c_v|| \geq \beta|S_{01}|.$$

Therefore either the number of ordinary columns or the number of ordinary rows in the Q-neighborhood of S_{01} exceeds $\beta|S_{01}|/2$. In the following, we suppose

$$\sum_{v \in S_{01}^{ord}} ||c_v|| \geq \frac{\beta|S_{01}|}{2},$$

and Lemma 25 grants that these ordinary columns cluster among the Q-neighborhood of a subset $T \subset S_{00}$ such that

$$|T| \leq \frac{16}{\delta^2 \Delta_n^{\varepsilon}}.$$

If it is the number of ordinary rows that exceeds $\beta|S_01|/2$, the ordinary rows will cluster in $T' \subset S_{11}$ and the following arguments are unchanged. The average number of non zero column of C_0 seen in each $v \in T$ is at least

$$\frac{\frac{\beta|S_{01}|}{2}}{\sup(|T|)} = \frac{\beta}{32}\delta^2\Delta_n^{2\varepsilon} = 8\beta\Delta_n^{2\varepsilon-1}\alpha\Delta_n\,.$$

This corresponds to at least twice the minimum norm $\alpha\Delta_n$ of a local view for an exceptional vertex if $\Delta_n \geq (4\beta)^{\frac{1}{1-2\varepsilon}}$ or equivalently, using **??**, $4\beta \leq c' \log(|G|)$. Alleging that the latter condition is satisfied, a constant proportion of vertices in T must be exceptional.
Each vertex carries at most Δ_n columns in its neighborhood, hence the size of T can be lower bounded by

$$|T| \geq \frac{1}{\Delta_n}\frac{\beta}{2}|S_{01}| \geq \frac{\beta}{4\Delta_n}|S_1| \geq \frac{\beta}{4\Delta_n}|S_0|,$$

using that $|S_1| = |S_{01}| + |S_{10}|$, $|S_{10}| \geq |S_{01}|$ and $|S_1| \geq |S_0|$. Therefore,

$$|S_{00}^e| \geq \frac{\beta}{4\Delta_n}|S_0|\,.$$

However, Lemma 23 settles that

$$|S_{00}^e| \leq \frac{2}{\alpha^2\kappa^2}\frac{1}{\Delta^{4\varepsilon}}\,.$$

This will give rise to a contradiction if

$$\frac{4}{\alpha^2\kappa^2\Delta_n^{4\varepsilon}} < \frac{\beta}{4\Delta_n},$$

which will happen, for Δ_n large enough, whenever $\varepsilon > 1/4$. The contradiction implies $||\mathbf{x}|| \geq \frac{\delta^2\kappa n}{512\Delta_n^2}$.

□

Theorem 26 (Minimal distance for Abelian groups)**.**

$$d_{min} \geq \frac{\kappa^2\delta^2 n}{1024(\log n)^{c''}}$$

with $c'' = \frac{c'}{1-2\varepsilon}$.

Proof. Combining Theorem 9 and Lemma 8,

$$d_{min} \geq \frac{\kappa^2\delta^2 n}{1024\Delta_n},$$

and Property 20 yields

$$d_{min} \geq \frac{\kappa^2\delta^2 n}{1024(\log n)^{c''}} \tag{24}$$

with $c'' = \frac{c'}{1-2\varepsilon}$. □

To conclude, when changing the non-Abelian group to an Abelian one, the minimal distance is lowered from being linear in n to $d_{min} = \Omega\left(n/polylog(n)\right)$. This means that less errors can be detected when considering a Abelian group but even if the Abelian quantum Tanner codes do not form a family of good error correcting codes, they remain interesting as their minimal distance is better than other quantum LDPC codes such that the fiber bundle codes that have a minimal distance $d_{min} = \Omega(n^{0.6}/polylog(n))$ [HHO21].

V Conclusion and perspectives

The first part of this report showed how to construct a non-lifted version of the quantum Tanner codes from the Hypergraph Product codes. The bases for the non-trivial logical operators is then derived as well as the number of logical qubits which was not explicitly known before. Then, the lifting procedure to obtain the quantum Tanner codes of [LZ22b] that achieved asymptotically a constant rate and a linear distance is described. However, the attempt to find the bases for the non-trivial logical operators was unsuccessful which makes the exact dimension

of the codespace as well as the non-trivial logical gates that could be implemented to perform fault-tolerant computation still unveilled.
In the second part, we studied how the minimum distance is modified when constructing a quantum Tanner code on a left-right Cayley complex built from a Abelian group. Since this complex has a less satisfactory expansion, the minimum distance is smaller than in the non-Abelian case. Even though this code has a distance in $\Omega(n/polylog(n))$ instead of a linear distance, its correcting capacity can still be interesting. For now, the good families of quantum codes, namely the quantum Tanner codes [LZ22b] and the lifted product codes [PK22], are not locally testable. It is believed that good LDPC quantum error correcting codes satisfying the property of local testability could solve the quantum PCP conjecture [AE15]. One way to achieve local testability could be to construct a good quantum LDPC code that exhibits, in addition to usual qubits, X checks and Z checks, some X meta-checks and Z meta-checks that can be described informally as checks acting on X checks and Z checks instead of the qubits [PK22]. To do so, a complex similar to the left-right Cayley complex exhibiting higher dimensional elements such as cubes could be considered.

References

[AE15] Dorit Aharonov and Lior Eldar. "Quantum Locally Testable Codes". In: *SIAM Journal on Computing* 44.5 (2015), pp. 1230–1262. DOI: 10.1137/140975498. eprint: https://doi.org/10.1137/140975498.

[BS04] Eli Ben-Sasson and Madhu Sudan. "Robust Locally Testable Codes and Products of Codes". In: *CoRR* cs.IT/0408066 (2004).

[Cob+23] Nolan J. Coble et al. "Local Hamiltonians with No Low-Energy Stabilizer States". en. In: Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. DOI: 10.4230/LIPICS.TQC.2023.14.

[CS96] A. R. Calderbank and Peter W. Shor. "Good quantum error-correcting codes exist". In: *Physical Review A* 54.2 (Aug. 1996), pp. 1098–1105. DOI: 10.1103/PhysRevA.54.1098.

[Din+21] Irit Dinur et al. *Locally Testable Codes with constant rate, distance, and locality*. Tech. rep. arXiv:2111.04808. arXiv, Dec. 2021.

[Gil52] E. N. Gilbert. "A comparison of signalling alphabets". In: *The Bell System Technical Journal* 31.3 (1952), pp. 504–522. DOI: 10.1002/j.1538-7305.1952.tb01393.x.

[Got97] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction*. 1997. arXiv: quant-ph/9705052 [quant-ph].

[HHO21] Matthew B Hastings, Jeongwan Haah, and Ryan O'Donnell. "Fiber bundle codes: breaking the n 1/2 polylog (n) barrier for quantum ldpc codes". In: *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. 2021, pp. 1276–1288.

[JM21] Akhil Jalan and Dana Moshkovitz. "Near-Optimal Cayley Expanders for Abelian Groups". In: *41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2021)*. Leibniz International Proceedings in Informatics (LIPIcs). 2021, 24:1–24:23. ISBN: 978-3-95977-215-0. DOI: 10.4230/LIPIcs.FSTTCS.2021.24.

[KP22] Gleb Kalachev and Pavel Panteleev. *Two-sided Robustly Testable Codes*. 2022. arXiv: 2206.09973 [cs.IT].

[LZ22a] Anthony Leverrier and Gilles Zémor. *Decoding quantum Tanner codes*. 2022. arXiv: 2208.05537.

[LZ22b] Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes*. Tech. rep. arXiv:2202.13641. arXiv, Apr. 2022.

[MS78] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Manual of microsurgery on the laboratory rat / ed. J.J. van Dongen. Elsevier Science, 1978. ISBN: 9780444851932.

[PK22] Pavel Panteleev and Gleb Kalachev. "Asymptotically Good Quantum and Locally Testable Classical LDPC Codes". In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2022. Rome, Italy: Association for Computing Machinery, 2022, 375–388. ISBN: 9781450392648. DOI: 10.1145/3519935.3520017.

[QC22] Armanda O. Quintavalle and Earl T. Campbell. "ReShape: A Decoder for Hypergraph Product Codes". In: *IEEE Transactions on Information Theory* 68.10 (2022), pp. 6569–6584. DOI: 10.1109/TIT.2022.3184108.

[Ste96] A. M. Steane. "Error Correcting Codes in Quantum Theory". en. In: *Physical Review Letters* 77.5 (July 1996), pp. 793–797. DOI: 10.1103/PhysRevLett.77.793.

[Tan81] R. Tanner. "A recursive approach to low complexity codes". In: *IEEE Transactions on Information Theory* 27.5 (Sept. 1981), pp. 533–547. DOI: 10.1109/TIT.1981.1056404.

[TZ09] Jean-Pierre Tillich and Gilles Zemor. "Quantum LDPC codes with positive rate and minimum distance proportional to n½". In: *2009 IEEE International Symposium on Information Theory*. 2009, pp. 799–803. DOI: 10.1109/ISIT.2009.5205648.

[Var57] R. R. Varshamov. “The evaluation of signals in codes with correction of errors”. Russian. In: *Dokl. Akad. Nauk SSSR* 117 (1957), pp. 739–741.

Appendices

A Parameters of the hypergraph product code

The proof for the number of physical qubits is trivial from the definition of the HGP code.
Applying Equation 4 to $\mathscr{C}_X, \mathscr{C}_Z, \mathscr{C}_1, \mathscr{C}_2$,

$$\begin{aligned} k_1 &= n_1 - m_1 + k_1^T \\ k_2 &= n_2 - m_2 + k_2^T \\ k_X &= n_1 n_2 + m_1 m_2 - n_1 m_2 + k_X^T \\ k_Z &= n_1 n_2 + m_1 m_2 - m_1 n_2 + k_Z^T \end{aligned}$$

For a CSS code, $K = k_X + k_Z - N$ and thus $K = k_X + k_Z - n_1 n_2 - m_1 m_2$.
For $\mathscr{C}_X^T = \mathscr{C}_1 \otimes \mathscr{C}_2^T$ and $\mathscr{C}_Z^T = \mathscr{C}_1^T \otimes \mathscr{C}_2$, we have

$$k_X^T = k_1 k_2^T \text{ and } k_Z^T = k_1^T k_2 \ .$$

Hence,

$$\begin{aligned} K &= k_X + k_Z - n_1 n_2 - m_1 m_2 \\ &= k_1 k_2^T + k_1^T k_2 + n_1 n_2 + m_1 m_2 - n_1 m_2 - m_1 n_2 \\ &= n_1 \underbrace{(n_2 - m2)}_{k_2 - k_2^T} + m_1 \underbrace{(m_2 - n_2)}_{k_2^T - k_2} + k_1 k_2^T + k_1^T k_2 \\ &= k_2(n_1 - m_1 + k_1^T) + k_2^T(m_1 - n_1 + k_1) \\ &= k_2 k_1 + k_2^T k_1^T \end{aligned}$$

The proof for the minimal distance can be found in [TZ09].

B Proofs of Section III-D

Recall that we consider the non lifted quantum Tanner code defined by the parity matrices

$$\widetilde{H_X} = \begin{pmatrix} H_A^0 \otimes G_B^0 \\ H_A^1 \otimes G_B^1 \end{pmatrix} \text{ and } \widetilde{H_Z} = \begin{pmatrix} G_A^1 \otimes H_B^0 \\ G_A^0 \otimes H_B^1 \end{pmatrix} .$$

A Proof of Lemma 14

Lemma 14.
- $rank\ H_A = 2 rank\ H_A^0 + rank\ G_A - N_A$
- $rank\ G_A = 2 rank\ G_A^0 + rank\ H_A - N_A$

Proof. Applying the rank-nullity theorem,

$$\begin{aligned} \text{rank } H_A &= N_A - \text{Dim } (\text{Ker } H_A) \\ &= N_A - \text{Dim } (\text{Ker } H_A^0 \cap \text{Ker } H_A^1) \\ &= N_A - \text{Dim } (\text{Ker } H_A^0) - \text{Dim } (\text{Ker } H_A^1) + \text{Dim } (\text{Ker } (H_A^0) + \text{Ker } (H_A^1)) \\ &= N_A - 2\,\text{Dim } (\text{Ker } H_A^0) + \text{Dim } (\text{Im } G_A^{0T} + \text{Im } G_A^{1T}) \\ &= N_A - 2\,\text{Dim } (\text{Ker } H_A^0) + \text{Dim } (\text{Im } G_A) \\ &= N_A - 2\,\text{Dim } (\text{Ker } H_A^0) + \text{rank } G_A \end{aligned}$$

□

B Proof of Lemma 15

Lemma 15. *Let A^0, A^1, B^0, B^1 be vector spaces such that $Dim\ A^0 = Dim\ A^1$ and $Dim\ B^0 = Dim\ B^1$. Let $A = A^0 \cap A^1$ and $B = B^0 \cap B^1$. Then,*

$$Dim\left((A^0 \otimes \mathbb{F}_2^{N_B} + \mathbb{F}_2^{N_A} \otimes B^0) \cap (A^1 \otimes \mathbb{F}_2^{N_B} + \mathbb{F}_2^{N_A} \otimes B^1)\right) = N_B Dim\ A + N_A Dim\ B - 2Dim\ A^0 Dim\ B^0 + (2Dim\ B^0 - Dim\ B)(2Dim\ A^0 - Dim\ A)\ .$$

Proof. Let $X = A^0 \otimes \mathbb{F}_2^{N_B} + \mathbb{F}_2^{N_A} \otimes B^0$ and $Z = A^1 \otimes \mathbb{F}_2^{N_B} + \mathbb{F}_2^{N_A} \otimes B^1$. We have

$$\mathrm{Dim}\ (X \cap Z) = \mathrm{Dim}\ X + \mathrm{Dim}\ Z - \mathrm{Dim}\ (X + Z),$$

where

$$\begin{aligned}
\mathrm{Dim}\ X &= \mathrm{Dim}\ A^0 \otimes \mathbb{F}_2^{N_B} + \mathrm{Dim}\ \mathbb{F}_2^{N_A} \otimes B^0 - \mathrm{Dim}\left((A^0 \otimes \mathbb{F}_2^{N_B}) \cap (\mathbb{F}_2^{N_A} \otimes B^0)\right) \\
&= \mathrm{Dim}\ A^0 \mathrm{Dim}\ \mathbb{F}_2^{N_B} + \mathrm{Dim}\ \mathbb{F}_2^{N_A} \mathrm{Dim}\ B^0 - \mathrm{Dim}\ (A^0 \otimes B^0) \\
&= N_B \mathrm{Dim}\ A^0 + N_A \mathrm{Dim}\ B^0 - \mathrm{Dim}\ A^0 \mathrm{Dim}\ B^0\ ,
\end{aligned}$$

$$\begin{aligned}
\mathrm{Dim}\ Z &= \mathrm{Dim}\ A^1 \otimes \mathbb{F}_2^{N_B} + \mathrm{Dim}\ \mathbb{F}_2^{N_A} \otimes B^1 - \mathrm{Dim}\left((A^1 \otimes \mathbb{F}_2^{N_B}) \cap (\mathbb{F}_2^{N_A} \otimes B^1)\right) \\
&= N_B \mathrm{Dim}\ A^1 + N_A \mathrm{Dim}\ B^1 - \mathrm{Dim}\ A^1 \mathrm{Dim}\ B^1\ ,
\end{aligned}$$

$$\begin{aligned}
\mathrm{Dim}\ (X + Z) &= \mathrm{Dim}\left((A^0 + A^1) \otimes \mathbb{F}_2^{N_B} + \mathbb{F}_2^{N_A} \otimes (B^0 + B^1)\right) \\
&= \mathrm{Dim}\left((A^0 + A^1) \otimes \mathbb{F}_2^{N_B}\right) + \mathrm{Dim}\left(\mathbb{F}_2^{N_A} \otimes (B^0 + B^1)\right) - \mathrm{Dim}\left((A^0 + A^1) \otimes \mathbb{F}_2^{N_B} \cap \mathbb{F}_2^{N_A} \otimes (B^0 + B^1)\right) \\
&= N_B \mathrm{Dim}\ (A^0 + A^1) + N_A \mathrm{Dim}\ (B^0 + B^1) - \mathrm{Dim}\left((A^0 + A^1) \otimes (B^0 + B^1)\right) \\
&= N_B \left(\mathrm{Dim}\ A^0 + \mathrm{Dim}\ A^1 - \mathrm{Dim}\ A\right) + N_A \left(\mathrm{Dim}\ B^0 + \mathrm{Dim}\ B^1 - \mathrm{Dim}\ B\right) - \mathrm{Dim}\ (A^0 + A^1) \mathrm{Dim}\ (B^0 + B^1) \\
&= N_B \left(\mathrm{Dim}\ A^0 + \mathrm{Dim}\ A^1 - \mathrm{Dim}\ A\right) + N_A \left(\mathrm{Dim}\ B^0 + \mathrm{Dim}\ B^1 - \mathrm{Dim}\ B\right) \\
&\quad - \left(\mathrm{Dim}\ A^0 + \mathrm{Dim}\ A^1 - \mathrm{Dim}\ A\right)\left(\mathrm{Dim}\ B^0 + \mathrm{Dim}\ B^1 - \mathrm{Dim}\ B\right)\ .
\end{aligned}$$

Hence,

$$\begin{aligned}
\mathrm{Dim}\ (X \cap Z) &= -\mathrm{Dim}\ A^0 \mathrm{Dim}\ B^0 - \mathrm{Dim}\ A^1 \mathrm{Dim}\ B^1 + N_B \mathrm{Dim}\ A + N_A \mathrm{Dim}\ B \\
&\quad + \left(\mathrm{Dim}\ A^0 + \mathrm{Dim}\ A^1 - \mathrm{Dim}\ A\right)\left(\mathrm{Dim}\ B^0 + \mathrm{Dim}\ B^1 - \mathrm{Dim}\ B\right) \\
&= N_B \mathrm{Dim}\ A + N_A \mathrm{Dim}\ B + \mathrm{Dim}\ A^0 \mathrm{Dim}\ B^1 + \mathrm{Dim}\ A^1 \mathrm{Dim}\ B^0 - \mathrm{Dim}\ B\left(\mathrm{Dim}\ A^0 + \mathrm{Dim}\ A^1\right) - \mathrm{Dim}\ A\left(\mathrm{Dim}\ (B^0 + B^1)\right) \\
&= N_B \mathrm{Dim}\ A + N_A \mathrm{Dim}\ B + \overbrace{2\mathrm{Dim}\ A^0 (2\mathrm{Dim}\ B^0 - \mathrm{Dim}\ B) - 2\mathrm{Dim}\ A^0 \mathrm{Dim}\ B^0}^{} \\
&\quad = N_B \mathrm{Dim}\ A + N_A \mathrm{Dim}\ B + 2\mathrm{Dim}\ A^0 \mathrm{Dim}\ B^0 - 2\mathrm{Dim}\ A^0 \mathrm{Dim}\ B - \left(2\mathrm{Dim}\ B^0 - \mathrm{Dim}\ B\right)\left(2\mathrm{Dim}\ A^0 - \mathrm{Dim}\ (A^0 + A^1)\right) \\
&= N_B \mathrm{Dim}\ A + N_A \mathrm{Dim}\ B - 2\mathrm{Dim}\ A^0 \mathrm{Dim}\ B^0 + \left(2\mathrm{Dim}\ B^0 - \mathrm{Dim}\ B\right)\left(\mathrm{Dim}\ (A^0 + A^1)\right) \\
&= N_B \mathrm{Dim}\ A + N_A \mathrm{Dim}\ B - 2\mathrm{Dim}\ A^0 \mathrm{Dim}\ B^0 + \left(2\mathrm{Dim}\ B^0 - \mathrm{Dim}\ B\right)\left(2\mathrm{Dim}\ A^0 - \mathrm{Dim}\ A\right)
\end{aligned}$$

□

C Proof of Property 17

Property 17.

$$rank\ \widetilde{H_X} + rank\ \widetilde{H_Z} = -N_A N_B + N_B(rank\ H_A + rank\ G_A) + N_A(rank\ H_B + rank\ G_B) - rank\ G_A rank\ G_B - rank\ H_A rank\ H_B$$

Using the Rank-Nullity theorem,

$$\begin{aligned}
\mathrm{rank}\ \widetilde{H_X} + \mathrm{rank}\ \widetilde{H_Z} &= 2N_A N_B - \mathrm{Dim\ Ker}\ \widetilde{H_X} - \mathrm{Dim\ Ker}\ \widetilde{H_Z} \\
&= 2N_A N_B - \mathrm{Dim}\left(\mathrm{Ker}\ (H_A^0 \otimes G_B^0) \cap \mathrm{Ker}\ (H_A^1 \otimes G_B^1)\right) - \mathrm{Dim}\left(\mathrm{Ker}\ (G_A^1 \otimes H_B^0) \cap \mathrm{Ker}\ (G_A^0 \otimes H_B^1)\right)
\end{aligned}$$

By dint of Lemma 16 and Lemma 15,

$$\begin{aligned}\operatorname{rank}\widetilde{H_X}+\operatorname{rank}\widetilde{H_Z} &= 2N_AN_B-\operatorname{Dim}\left((H_A^0\otimes\mathbb{F}_2^{N_B}+\mathbb{F}_2^{N_A}\otimes G_B^0)\cap(H_A^1\otimes\mathbb{F}_2^{N_B}+\mathbb{F}_2^{N_A}\otimes G_B^1)\right)\\ &\quad-\operatorname{Dim}\left((G_A^0\otimes\mathbb{F}_2^{N_B}+\mathbb{F}_2^{N_A}\otimes H_B^0)\cap(G_A^1\otimes\mathbb{F}_2^{N_B}+\mathbb{F}_2^{N_A}\otimes H_B^1)\right)\\ &= 2N_AN_B-N_B\operatorname{Dim}(\operatorname{Ker}H_A)-N_A\operatorname{Dim}(\operatorname{Ker}G_B)-(2\operatorname{Dim}(\operatorname{Ker}G_B^0)-\operatorname{Dim}(\operatorname{Ker}G_B))(2\operatorname{Dim}(\operatorname{Ker}H_A^0)\\ &\quad-\operatorname{Dim}(\operatorname{Ker}H_A))+2\operatorname{Dim}(\operatorname{Ker}H_A^0)\operatorname{Dim}(\operatorname{Ker}G_B^0)-N_B\operatorname{Dim}(\operatorname{Ker}G_A)-N_A\operatorname{Dim}(\operatorname{Ker}H_B)\\ &\quad-(2\operatorname{Dim}(\operatorname{Ker}H_B^0)-\operatorname{Dim}(\operatorname{Ker}H_B))(2\operatorname{Dim}(\operatorname{Ker}G_A^0)-\operatorname{Dim}(\operatorname{Ker}G_A))+2\operatorname{Dim}(\operatorname{Ker}G_A^0)\operatorname{Dim}(\operatorname{Ker}H_B^0)\end{aligned}$$

Employing again the Rank-Nullity theorem several times,

$$\begin{aligned}\operatorname{rank}\widetilde{H_X}+\operatorname{rank}\widetilde{H_Z} = &-2N_AN_B+N_B\operatorname{rank}H_A+N_A\operatorname{rank}G_B+N_B\operatorname{rank}G_A+N_A\operatorname{rank}H_B+2\operatorname{rank}G_A^0(N_B-\operatorname{rank}G_B^0)\\ &+2\operatorname{rank}G_B^0(N_A-\operatorname{rank}G_A^0)-(N_B-2\operatorname{rank}G_B^0+\operatorname{rank}G_B)(N_A-2\operatorname{rank}H_A^0+\operatorname{rank}H_A)\\ &-(N_B-2\operatorname{rank}H_B^0+\operatorname{rank}H_B)(N_A-2\operatorname{rank}G_A^0+\operatorname{rank}G_A)\end{aligned}$$

All the remaining steps consist in applying Lemma 14 several times in order to simplify the expression.

$$\begin{aligned}\operatorname{rank}\widetilde{H_X}+\operatorname{rank}\widetilde{H_Z} = &-2N_AN_B+N_B\operatorname{rank}H_A+N_A\operatorname{rank}G_B+N_B\operatorname{rank}G_A+N_A\operatorname{rank}H_B+\overbrace{2\operatorname{rank}G_A^0}^{\operatorname{rank}G_A-\operatorname{rank}H_A+N_A}\overbrace{(N_B-\operatorname{rank}G_B^0)}^{\operatorname{rank}H_B-\operatorname{rank}G_B+\operatorname{rank}G_B^0}\\ &+\overbrace{2\operatorname{rank}G_B^0}^{\operatorname{rank}G_B-\operatorname{rank}H_B+N_B}\overbrace{(N_A-\operatorname{rank}G_A^0)}^{\operatorname{rank}H_A-\operatorname{rank}G_A+\operatorname{rank}G_A^0}\overbrace{-(N_B-2\operatorname{rank}G_B^0+\operatorname{rank}G_B)}^{\operatorname{rank}H_B}\overbrace{(N_A-2\operatorname{rank}H_A^0+\operatorname{rank}H_A)}^{\operatorname{rank}G_A}\\ &\overbrace{-(N_B-2\operatorname{rank}H_B^0+\operatorname{rank}H_B)}^{\operatorname{rank}G_B}\overbrace{(N_A-2\operatorname{rank}G_A^0+\operatorname{rank}G_A)}^{\operatorname{rank}H_A}\\ = &-2N_AN_B+N_B\operatorname{rank}H_A+N_A\operatorname{rank}G_B+N_B\operatorname{rank}G_A+N_A\operatorname{rank}H_B\\ &+(\operatorname{rank}G_A-\operatorname{rank}H_A+N_A)(\operatorname{rank}H_B-\operatorname{rank}G_B+\operatorname{rank}G_B^0)\\ &+\overbrace{(\operatorname{rank}G_B-\operatorname{rank}H_B+N_B)(\operatorname{rank}H_A-\operatorname{rank}G_A+\operatorname{rank}G_A^0)}^{\cancel{\operatorname{rank}G_B\operatorname{rank}H_A}+\cancel{\operatorname{rank}H_B\operatorname{rank}G_A}-\operatorname{rank}G_B\operatorname{rank}G_A+\operatorname{rank}G_B\operatorname{rank}G_A^0-\operatorname{rank}H_B\operatorname{rank}H_A+\operatorname{rank}H_B\operatorname{rank}G_A^0+N_B\operatorname{rank}H_A-N_B\operatorname{rank}G_A+N_B\operatorname{rank}G_A^0}\\ &-\cancel{\operatorname{rank}H_B\operatorname{rank}G_A}-\cancel{\operatorname{rank}G_B\operatorname{rank}H_A}\\ = &-2N_AN_B+N_B\operatorname{rank}H_A+N_A\operatorname{rank}G_B+N_B\operatorname{rank}G_A+N_A\operatorname{rank}H_B\\ &\operatorname{rank}G_A\operatorname{rank}H_B-2\operatorname{rank}G_A\operatorname{rank}G_B+\operatorname{rank}G_A\operatorname{rank}G_B^0-2\operatorname{rank}H_A\operatorname{rank}H_B+\operatorname{rank}H_A\operatorname{rank}G_B-\operatorname{rank}H_A\operatorname{rank}G_B^0+\\ &N_A\overbrace{(\operatorname{rank}H_B-\operatorname{rank}G_B+\operatorname{rank}G_B^0)}^{N_B-\operatorname{rank}G_B^0}+\operatorname{rank}G_B\operatorname{rank}G_A^0-\operatorname{rank}H_B\operatorname{rank}G_A^0+N_B\overbrace{(\operatorname{rank}H_A-\operatorname{rank}G_A+\operatorname{rank}G_A^0)}^{N_A-\operatorname{rank}G_A^0}\\ = &-N_AN_B+N_B\operatorname{rank}H_A+N_A\operatorname{rank}G_B+N_B\operatorname{rank}G_A+N_A\operatorname{rank}H_B-\operatorname{rank}G_A\operatorname{rank}G_B-\operatorname{rank}H_A\operatorname{rank}H_B\\ &\operatorname{rank}G_A\operatorname{rank}H_B-\operatorname{rank}G_A\operatorname{rank}G_B+\operatorname{rank}G_A\operatorname{rank}G_B^0-\operatorname{rank}H_A\operatorname{rank}H_B+\operatorname{rank}H_A\operatorname{rank}G_B-\operatorname{rank}H_A\operatorname{rank}G_B^0+\\ &N_A\operatorname{rank}G_B^0+\operatorname{rank}G_B\operatorname{rank}G_A^0-\operatorname{rank}H_B\operatorname{rank}G_A^0+N_BN_A-N_B\operatorname{rank}G_A^0\\ = &-N_AN_B+N_B\operatorname{rank}H_A+N_A\operatorname{rank}G_B+N_B\operatorname{rank}G_A+N_A\operatorname{rank}H_B-\operatorname{rank}G_A\operatorname{rank}G_B-\operatorname{rank}H_A\operatorname{rank}H_B\\ &\operatorname{rank}G_A\operatorname{rank}H_B-\operatorname{rank}G_A\operatorname{rank}G_B+\operatorname{rank}G_A\operatorname{rank}G_B^0-\operatorname{rank}H_A\operatorname{rank}H_B+\operatorname{rank}H_A\operatorname{rank}G_B-\operatorname{rank}H_A\operatorname{rank}G_B^0+\\ &N_A(N_B-\operatorname{rank}G_B^0)+\operatorname{rank}G_B\operatorname{rank}G_A^0-\operatorname{rank}H_B\operatorname{rank}G_A^0+N_B\operatorname{rank}G_A^0\\ = &-N_AN_B+N_B\operatorname{rank}H_A+N_A\operatorname{rank}G_B+N_B\operatorname{rank}G_A+N_A\operatorname{rank}H_B-\operatorname{rank}G_A\operatorname{rank}G_B-\operatorname{rank}H_A\operatorname{rank}H_B\\ &\operatorname{rank}G_A\overbrace{(\operatorname{rank}H_B-\operatorname{rank}G_B+\operatorname{rank}G_B^0)}^{N_B-\operatorname{rank}G_B^0}+\operatorname{rank}H_A\overbrace{(\operatorname{rank}G_B-\operatorname{rank}H_B-\operatorname{rank}G_B^0)}^{\operatorname{rank}G_B^0-N_B}\\ &+N_A(N_B-\operatorname{rank}G_B^0)+2\operatorname{rank}G_B^0\operatorname{rank}G_A^0-2N_B\operatorname{rank}G_A^0\\ = &-N_AN_B+N_B\operatorname{rank}H_A+N_A\operatorname{rank}G_B+N_B\operatorname{rank}G_A+N_A\operatorname{rank}H_B-\operatorname{rank}G_A\operatorname{rank}G_B-\operatorname{rank}H_A\operatorname{rank}H_B\\ &+(N_B-\operatorname{rank}G_B^0)\overbrace{(\operatorname{rank}G_A-\operatorname{rank}H_A)}^{2\operatorname{rank}G_A^0-N_A}+N_A(N_B-\operatorname{rank}G_B^0)+2\operatorname{rank}G_B^0\operatorname{rank}G_A^0-2N_B\operatorname{rank}G_A^0\\ = &-N_AN_B+N_B\operatorname{rank}H_A+N_A\operatorname{rank}G_B+N_B\operatorname{rank}G_A+N_A\operatorname{rank}H_B-\operatorname{rank}G_A\operatorname{rank}G_B-\operatorname{rank}H_A\operatorname{rank}H_B\\ &\cancel{2N_B\operatorname{rank}G_A^0}-\cancel{2\operatorname{rank}G_B^0\operatorname{rank}G_A^0}+\cancel{N_A\operatorname{rank}G_B^0}-\cancel{N_A\operatorname{rank}G_B^0}+\cancel{2\operatorname{rank}G_B^0\operatorname{rank}G_A^0}-\cancel{2N_B\operatorname{rank}G_A^0}\end{aligned}$$