A construction of quantum LDPC codes from Cayley graphs

Alain Couvreur, Nicolas Delfosse, Gilles Zemor

A construction of quantum LDPC codes from Cayley graphs

Alain Couvreur, Nicolas Delfosse and Gilles Zémor
{Alain.Couvreur, Nicolas.Delfosse, Gilles.Zemor}@math.u-bordeaux1.fr
Institut de Mathématiques de Bordeaux, Université Bordeaux 1, France

February 10, 2011

Abstract

We study a construction of Quantum LDPC codes proposed by MacKay, Mitchison and Shokrollahi in the draft [6]. It is based on the Cayley graph of $\mathbb{F}_2^n$ together with a set of generators regarded as the columns of the parity–check matrix of a classical code. We give a general lower bound on the minimum distance of the quantum code in $\mathcal{O}(dn^2)$ where d is the minimum distance of the classical code. When the classical code is the $[n, 1, n]$ repetition code, we are able to compute the exact parameters of the associated quantum code which are $[[2^{n-1}, 2^{\frac{n}{2}}, 2^{\frac{n}{2}-1}]]$.

1 Introduction

Classical LDPC codes, it hardly needs to be recalled, come together with very efficient and fast decoding algorithms and overall display extremely good performance for a variety of channels. Quantum error-correcting codes on the other hand, under the guise of the CSS [2, 7] scheme, are in some ways strikingly similar to classical codes, and in particular can be decoded with purely classical means. It is therefore natural to try to import the classical LDPC know-how to the quantum setting. There is however a structural obstacle. A quantum CSS code is defined by two binary parity-check matrices whose row-spaces must be orthogonal to each other. To have a quantum LDPC code decodable by message-passing these two matrices should be sparse, as in the classical case. Therefore randomly choosing these matrices, the generic method which works very well in the classical case, is simply not an option in the quantum case, because the probability of finding two

sparse row-orthogonal matrices is extremely small. A number of constructions have been suggested by classical coding theorists nevertheless (see the list of references quoted in the introduction of [8]) but they do not produce families of quantum LDPC codes with a minimum distance growing with the blocklength. While this may be tolerable for practical constructions of fixed size, this is clearly an undesirable feature of any asymptotic construction and it raises the intriguing theoretical question of how large can the minimum distance of sparse (or LDPC) CSS codes be. Families of sparse CSS codes with a growing minimum distance do exist, the most well-known of these being Kitaev's toric code [4], which has been generalised to codes based on tesselations of surfaces (see *e.g.* [1]) and higher-dimensional objects. These constructions exhibit minimum distances that scale at most as a square root of the blocklength N (to be precise, $N^{1/2} \log N$ is achieved in [3]) though this often comes at the cost of a very low dimension (recall that the dimension of the toric code is 2). It is an open question as to whether families of sparse CSS codes exist with a minimum distance that grows at least as N^α for $\alpha > 1/2$, even for quantum codes with dimension 1. The recent construction [8] manages to reconcile a minimum distance of the order of $N^{1/2}$ with a dimension linear in the blocklength. All these constructions borrow ideas from topology and can be seen as some generalisation of Kitaev's toric code.

In a follow-up to the paper [5] MacKay, Mitchison and Shokrollahi [6] proposed a construction that seemingly owes very little to the topological approach. They noticed that the adjacency matrix of any Cayley graph over $\mathbb{F}_2^r$ with an even set of generators is self-dual and can therefore be used to define a sparse CSS code. Experiments with some Cayley graphs were encouraging. In the present work we take up the theoretical study of the parameters of these CSS codes which was left open by MacKay *et al.* The quantum code in the construction is defined by a classical $[n, k, d]$ linear binary code where n must be even. Its length is $N = 2^{n-k}$, and the row-weight of the parity-check matrix is n. The dimension and the minimum distance of the quantum code does not depend solely on the classical code's parameters, but depend more subtly on its structure. We solve the problem in the first non-trivial case, which was an explicit question of MacKay *et al.*, namely the case when the classical code is the $[n, 1, n]$ repetition code. Computing the parameters of the associated quantum code turns out to be not easy, even in this apparently simple case. Our main result, Theorem 10, gives the exact parameters for this quantum code, namely:

$$[[N = 2^{n-1}, K = 2^{\frac{n}{2}}, D = 2^{\frac{n}{2}-1}]].$$

The construction therefore hits the $N^{1/2}$ barrier for the minimum distance,

but it is quite noteworthy that it does so using a construction that breaks significantly with the topological connection. For quantum codes based on more complicated classical $[n, k, d]$ structures, similarly precise results seem quite difficult to obtain, but we managed to prove a lower bound on the quantum minimum distance of the form $D \geq adn^2$ for some constant a (Theorem 9).

2 Quantum codes from Cayley graphs

A quantum CSS code is defined by two binary parity–check matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ with the same number of columns N and such that the rows of $\mathbf{H}_X$ are orthogonal to the rows of $\mathbf{H}_Z$. Denote by C_X the classical code of parity–check matrix $\mathbf{H}_X$ and by C_Z the code of parity–check matrix $\mathbf{H}_Z$. We obtain a quantum code of length N which encodes K quantum bits or qubits in N qubits with:

$$K = N - \mathrm{Rank}(\mathbf{H}_X) - \mathrm{Rank}(\mathbf{H}_Z),$$

and with minimum distance:

$$D = \inf\{w(x) : x \in C_X \backslash C_Z^{\perp} \cup C_Z \backslash C_X^{\perp}\}.$$

Notation and construction. In what follows, r, n denote two integers with n even. Denote by e_i the i-th vector of the canonical basis of $\mathbb{F}_2^r$. Let H be a full-rank $r \times n$ binary matrix that can be considered as the parity–check matrix of a classical code C of length n and dimension $k = n - r$. Denote by S the set of columns of H. Let $G(C) = G(H)$ be the Cayley graph over $\mathbb{F}_2^r$ with set of generators S. In other words this graph has $\mathbb{F}_2^r$ as vertex set and its edges are $\{x, x + s\}$ for all $x \in \mathbb{F}_2^r$ and all $s \in S$. This graph depends only on C and is often known as the coset graph of C. Let $A(H)$ be the adjacency matrix of $G(H)$. When no confusion is possible we denote $A(H)$ simply by A.

Proposition 1. *The matrix $A(H)$ defines a quantum code Q_H of length $N = 2^r$ with $\mathbf{H}_X = \mathbf{H}_Z = A(H)$.*

Proof. It is sufficient to prove that A satisfies the orthogonality relations. Since n is even, the rows of A have even weight and hence are self-orthogonal. If $x, y \in \mathbb{F}_2^r$, denote by A_x the row indexed by $x \in \mathbb{F}_2^r$ and by $A_{x,y}$ the entry indexed by (x, y). Now, let x, x' be two distinct elements of $\mathbb{F}_2^r$. That $\langle A_x, A_{x'} \rangle = 0$ means that the cardinality of the set:

$$\{y \in \mathbb{F}_2^r \mid A_{x,y} = A_{x',y} = 1\} = (x + S) \cap (x' + S)$$

is even. The subgroup $\{0, x+x'\}$ acts by translation on the set $x+S \cap x'+S$ and the action is free. Thus, $x + S \cap x' + S$ is a disjoint union of classes of cardinality 2 and hence has an even number of elements. This concludes the proof. □

This proposition is present in [6]. In this construction $C_X = C_Z = \operatorname{Ker} A$, it is the space of vectors $\mathbf{c} \in \mathbb{F}_2^{2r}$ such that $A^t\mathbf{c} = 0$. A codeword $\mathbf{c} \in \operatorname{Ker} A$ is the characteristic vector of a set of vertices of the graph $G(H)$. It will be convenient in the sequel to think of a vector $\mathbf{c}$ as a set of vertices, or as a subgraph of $G(H)$, and we will freely apply set and graph-theoretic operations to vectors $\mathbf{c}$, meaning that they apply to the underlying subgraph. The reader should also not confuse indices of the rows of the matrix A, denoted by x or y, which are elements of $\mathbb{F}_2^r$, with the vectors of the space $\mathbb{F}_2^{2r}$, denoted by boldface letters $\mathbf{c}$, which support the code $\operatorname{Ker} A$.

3 The n-cube cover

To begin we study the example of the identity matrix $H = I_n$. The classical code C and the quantum code Q_H are trivial, but the code $\operatorname{Ker} A(I_n) \subset \mathbb{F}_2^{2^r}$ is not and will be of use. We will show that there is a morphism from the Cayley graph $G(I_n)$ to $G(H)$ for every $r \times n$ matrix. This gives us a morphism from $\operatorname{Ker} A(I_n)$ to $\operatorname{Ker} A(H)$.

Proposition 2. *If n is an even integer, then the matrix $A(I_n)$ has rank 2^{n-1}.*

Proof. Since the row–space of A is (weakly) self-dual, its rank is at most 2^{n-1}. It is straightforward to see that if one sorts the the elements of $\mathbb{F}_2^n$ by the lexicographic order, the matrix $A(I_n)$ has the following block-representation.

$$A(I_n) = \begin{pmatrix} A(I_{n-1}) & I_{2^{n-1}} \\ I_{2^{n-1}} & A(I_{n-1}) \end{pmatrix}.$$

Thus, this matrix has rank at least 2^{n-1}. □

This example is useful because it provides a cover (or lift) of the general Cayley graph $G(H)$ for arbitrary H. The following proposition states that the graphs $G(I_n)$ and $G(H)$, when restricted to small enough balls, look exactly the same.

Proposition 3. *If the classical code C of parity–check matrix H has minimum distance d, then we have a graph isomorphism between the balls of radius $\lceil d/2 \rceil - 1$ of $G(H)$ and $G(I_n)$:*

$$\pi : \mathbb{B}_{I_n}(y, \lceil d/2 \rceil - 1) \xrightarrow{\sim} \mathbb{B}_H(x, \lceil d/2 \rceil - 1)$$

for all x in $\mathbb{F}_2^r$ and for all y in $\mathbb{F}_2^n$.

Proof. It is sufficient to show that the balls of centre 0 and radius $\lceil d/2 \rceil - 1$ are isomorphic because Cayley graphs are vertex transitive. Consider the natural map from the vertex set of $G(I_n)$ to that of $G(H)$, namely the syndrome function:

$$\begin{array}{rcl} \pi : \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^r \\ x & \longmapsto & H^t x \end{array}$$

Now consider the restriction of this map to the ball of radius $\lceil d/2 \rceil - 1$ centred at 0. This is a graph morphism and it is injective by definition of the minimum distance. Therefore, π induces an isomorphism between the balls. □

We say that $\mathbf{c}$ is included in a ball if the corresponding vertices are. We denote by $\mathbb{S}(x)$ the sphere of centre x and radius 1 in the Cayley graph. These spheres play an important role because they correspond to the rows of A. In particular we will say that a vector in $\mathbb{F}_2^{2^r}$ is a sum a spheres to mean that it belongs to the row–space of A. The following lemma is obvious but we state it for reference.

Lemma 4. *A word $\mathbf{c} \in \mathbb{F}_2^{2^r}$ is in $\operatorname{Ker} A(H)$ if and only if it contains an even number of vertices of $\mathbb{S}(x)$ for all $x \in \mathbb{F}_2^r$.*

Lemma 5. *Let $\mathbf{c}$ be a codeword of $\operatorname{Ker} A(I_n)$ such that $\mathbf{c}$ is included in $\mathbb{B}(0,t)$ with $0 < t < n$. If $\partial\mathbf{c} := \mathbf{c} \cap \mathbb{S}(0,t)$ is non-empty, then for all $i \in \{1, \ldots, n\}$, there exists $x \in \partial\mathbf{c}$ such that $x_i \neq 0$.*

Proof. Suppose that $\partial\mathbf{c}$ is non-empty and that there exists an index i such that $x_i = 0$ for all x in $\partial\mathbf{c}$. Let x be an element of $\partial\mathbf{c}$. We consider the sphere of centre $x + e_i$. We have:

$$\mathbb{S}(x + e_i) \cap \mathbf{c} = \{x + e_i + e_j, 1 \leq j \leq n\} \cap \partial\mathbf{c} = \{x\}.$$

The last equality comes from the hypothesis $x_i = 0$ for all x in $\partial\mathbf{c}$. This is impossible because $\mathbf{c}$ must satisfy Lemma 4. □

Proposition 6. *Let* $\mathbf{c}$ *be a codeword of* $\operatorname{Ker} A(I_n)$ *such that* $\mathbf{c}$ *is included in a ball of radius* $\lceil d/2 \rceil - 1$. *Then* $\mathbf{c}$ *is a sum of spheres of radius 1 which are included in this ball.*

Proof. By vertex–transitivity we can assume that $\mathbf{c}$ is included in the ball centred at 0. Let us prove the result by induction on the radius t of the ball.

If $t = 0$, then from Lemma 4, $\mathbf{c}$ is the zero codeword and hence the empty sum of spheres.

Assume the property to be true for $t-1 \geq 0$. If $\partial\mathbf{c} := \mathbf{c} \cap \mathbb{S}(0,t)$ is empty, then $\mathbf{c} \subset \mathbb{B}(0, t-1)$ and the result is obtained by induction. Thus, suppose that $\partial\mathbf{c} \neq \emptyset$. Set

$$T = \mathbb{S}(0,t) \cap \{x \in \mathbb{F}_2^r \mid x_r = 1\}.$$

From Lemma 5, we have $T \cap \partial\mathbf{c} \neq \emptyset$. Let $u_1 + e_r, \ldots, u_s + e_r$ be the elements of $T \cap \partial\mathbf{c}$, where u_i is in $\mathbb{S}(0, t-1)$ and hence $\mathbb{S}(u_i) \subset \mathbb{B}(0,t)$. Moreover, the only neighbour of u_i in T is $u_i + e_r$. Thus when we add $\mathbb{S}(u_i)$ to $\mathbf{c}$ this deletes $u_i + e_i$ of T without other modification of T. Thus, the word

$$\mathbf{c}' := \mathbf{c} - \sum_{i=1}^{s} \mathbb{S}(u_i)$$

has no elements in T. From Lemma 5, we get $\partial\mathbf{c}' = \emptyset$ and, from the induction hypothesis, $\mathbf{c}'$ is a sum of spheres contained in $\mathbb{B}(0, t-1)$. Consequently, $\mathbf{c}$ is a sum of spheres contained in $\mathbb{B}(0,t)$. □

4 Lower bound on the minimum distance of the quantum code Q_H

To bound the minimum distance of the quantum code, we examine the weight of the vectors of $\operatorname{Ker} A \setminus \operatorname{Ker} A^{\perp}$. By the following lemma, this set is exactly the set $\operatorname{Ker} A \setminus \operatorname{Im} A$.

By symmetry of A we have:

Lemma 7. $(\operatorname{Ker} A(H))^{\perp} = \operatorname{Im} A(H)$.

The following lemma concerns the weight of words in $\operatorname{Ker} A(I_n)$. Using the local isomorphism described in Proposition 3 it will yield a lower bound for the minimum distance of any quantum code Q_H associated to $A(H)$.

Lemma 8. *Let* $\mathbf{c}$ *be a codeword of* $\operatorname{Ker} A(I_n)$. *Then, for all* x *in* $\mathbf{c}$ *such that* $\mathbf{c} \not\subseteq \mathbb{B}(x,2)$ *we have:*

$$w(\mathbf{c} \cap \mathbb{B}(x,4)) \geq an^2,$$

for some constant $a > 0$.

Sketch of proof: By transitivity, one can assume that $x = 0$.

Claim 1. For all $i \in \{1 \dots n\}$, there is at least one vertex $e_i + e_j$ in $\mathbf{c}$. Indeed, the word $\mathbf{c}$ contains the vertex 0. By Lemma 4, it must contain at least another vertex of each sphere $\mathbb{S}(e_i)$, *i.e.* a vertex of the form $e_i + e_j$. Such a vertex can satisfy the orthogonality relations for at most two such spheres: $\mathbb{S}(e_i)$ and $\mathbb{S}(e_j)$. This gives us at least $n/2$ vertices.

We want to use this idea with spheres of the form $\mathbb{S}(e_i+e_j+e_k)$ to obtain others vertices in the ball of radius 4.

Let κ be the maximum number of elements of $\mathbf{c} \cap \mathbb{S}(0, 2)$ such that any two of them have disjoint supports. By transitivity, these κ elements can be assumed to be $V = \{e_1 + e_2, \dots, e_{k-1} + e_k\}$, where $k := 2\kappa$.

Step 1. When $k \geq n/4$, we use the spheres $\mathbb{S}(e_i + e_{i+1} + e_s)$ for $s \leq k$ and $s \notin \{i, i + 1\}$. Such a sphere contains exactly one vertex of V. Thus it must contain a vertex which is not in V. This vertex is at most in four such spheres. This gives us at least an^2 vertices for some constant a.

Step 2. Assume $k < n/4$. By maximality of κ, for all $l > k$, if $e_i + e_l \in \mathbf{c}$, then $i \leq k$. Moreover, by Claim 1, there exists $n - k$ elements $e_{i_l} + e_l \in \mathbf{c}$ with $l = k + 1, \dots, n$ and $i_l \leq k$. Using the spheres $\mathbb{S}(e_{i_l} + e_l + e_m)$ where m is such that $i_m \neq i_l$, we obtain the lemma. Be careful, this uses a word $\mathbf{c}$ of minimum weight. ∎

Applying the local isomorphism π now yields the following:

Theorem 9. *Assume that the classical code of parity–check matrix H has minimum distance d. Then the minimum distance D of the quantum code of matrix $A(H)$ is bounded from below as:*

$$D \geq adn^2,$$

for some constant $a > 0$.

Sketch of proof: What needs to be done is to bound from below the minimum weight of a codeword $\mathbf{c}$ of $\operatorname{Ker} A \setminus \operatorname{Im} A$ for $A = A(H)$. By Propositions 3 and 6, we have that if a codeword of $\operatorname{Ker} A$ is included in a ball of radius $\lceil d/2 \rceil$ in $G(H)$, then it is a sum of spheres and therefore lies in $\operatorname{Im} A$. Therefore if $\mathbf{c}$ contains vertex x, it must have non-zero intersection with all spheres centred on x of even radii $i < \lceil d/2 \rceil$. To cover $\mathbf{c}$ by disjoint balls of radius 4 one needs Md balls for some $M > 0$. Using Lemma 8, we get the result. ∎

5 The quantum code associated to the repetition code

Now we look at an open question proposed by Mackay *et al.* in [6]. What are the parameters of the quantum code constructed from the repetition code?

In what follows, $n \geq 4$ is an even integer and H_n is the $(n-1) \times n$ parity–check matrix of the $[n, 1, n]$ repetition code whose columns consist of the elements of $\mathbb{F}_2^{n-1}$, $\{e_1, e_2, \ldots, e_{n-1}, \sum_1^{n-1} e_i\}$. Denote by A_n the adjacency matrix $A(H_n)$.

Our goal is to prove the following theorem.

Theorem 10. *The quantum code associated to the repetition code has parameters:*

$$[[N = 2^{n-1}, K = 2^{\frac{n}{2}}, D = 2^{\frac{n}{2}-1}]].$$

In fact we can improve the parameters of this family of quantum codes using the fact that the Tanner graph can be decomposed into two disjoint isomorphic graphs. We obtain the same rate and the same distance but for a length divided by 2:

$$[[N = 2^{n-2}, K = 2^{\frac{n}{2}-1}, D = 2^{\frac{n}{2}-1}]].$$

5.1 The matrices A_n

We sort the vectors of $\mathbb{F}_2^{n-1}$ in the lexicographic order, we obtain in particular:

$$A_4 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

To pass from the matrix A_n to the matrix A_{n+1} the following formula is proved straightforwardly enough:

Lemma 11. *For all integer $n \geq 4$, we have:*

$$A_{n+1} = \begin{pmatrix} A_n + J_n & I_n + J_n \\ I_n + J_n & A_n + J_n \end{pmatrix},$$

where J_n is the binary anti-diagonal matrix of size 2^{n-1}. To lighten notation, I_n denotes the $2^{n-1} \times 2^{n-1}$ identity matrix (rather than an $n \times n$ matrix).

5.2 Computation of the dimension

To compute the dimension of the quantum code, it suffices to find the rank of A_n. We will determine the dimension of the classical code $\operatorname{Ker} A_n$.

Lemma 12. $J_n^2 = I_n$.

Using the symmetries of the matrix A_n we obtain the following Lemmas.

Lemma 13. *We have:*

- $\mathbf{x} \in \operatorname{Ker} A_n \Leftrightarrow J_n\mathbf{x} \in \operatorname{Ker} A_n$,
- $\mathbf{x} \in \operatorname{Im} A_n \Leftrightarrow J_n\mathbf{x} \in \operatorname{Im} A_n$,
- $\operatorname{Im} A_n \subset \operatorname{Ker} A_n$.

Lemma 14. *Let* $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4) \in \mathbb{F}_2^{2^{n+1}}$ *where* $\mathbf{x}_i$ *are vectors of* $\mathbb{F}_2^{2^{n-1}}$. *Then we have* $\mathbf{x} \in \operatorname{Ker} A_{n+2}$ *if and only if:*

$$\begin{cases} \mathbf{x}_4 = \mathbf{x}_1 + \mathbf{c}_1 \text{ where } \mathbf{c}_1 \in \operatorname{Ker} A_n \\ \mathbf{x}_3 = \mathbf{x}_2 + \mathbf{c}_2 \text{ where } \mathbf{c}_2 \in \operatorname{Ker} A_n \\ A_n\mathbf{x}_1 = \mathbf{c}_2 + J_n\mathbf{c}_1 \\ A_n\mathbf{x}_2 = \mathbf{c}_1 + J_n\mathbf{c}_2 \end{cases}.$$

Proof. By the recursion formula of Lemma 11, we have:

$$A_{n+2} = \left(\begin{array}{cc|cc} A_n + J_n & I_n & I_n & J_n \\ I_n & A_n + J_n & J_n & I_n \\ \hline I_n & J_n & A_n + J_n & I_n \\ J_n & I_n & I_n & A_n + J_n \end{array}\right).$$

This gives a characterisation of the vectors of the kernel A_{n+2} in function of A_n. We have $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4) \in \operatorname{Ker} A_{n+2}$ if and only if

$$\Leftrightarrow \begin{cases} A_n\mathbf{x}_1 = (\mathbf{x}_2 + \mathbf{x}_3) + J_n(\mathbf{x}_1 + \mathbf{x}_4) \\ A_n\mathbf{x}_2 = (\mathbf{x}_1 + \mathbf{x}_4) + J_n(\mathbf{x}_2 + \mathbf{x}_3) \\ A_n\mathbf{x}_3 = A_n\mathbf{x}_2 \\ A_n\mathbf{x}_4 = A_n\mathbf{x}_1 \end{cases}$$

$$\Leftrightarrow \begin{cases} \mathbf{x}_4 = \mathbf{x}_1 + \mathbf{c}_1 \text{ where } \mathbf{c}_1 \in \operatorname{Ker} A_n \\ \mathbf{x}_3 = \mathbf{x}_2 + \mathbf{c}_2 \text{ where } \mathbf{c}_2 \in \operatorname{Ker} A_n \\ A_n\mathbf{x}_1 = \mathbf{c}_2 + J_n\mathbf{c}_1 \\ A_n\mathbf{x}_2 = \mathbf{c}_1 + J_n\mathbf{c}_2 \end{cases}$$

□

Proposition 15. $\dim \operatorname{Ker} A_n = 2^{n-2} + 2^{\frac{n}{2}-1}$.

Proof. The case of A_4 is clear. We will show that the dimension of the kernel of A_n satisfies $\dim \operatorname{Ker} A_{n+2} = 2 \dim \operatorname{Ker} A_n + 2^{n-1}$.

If $\mathbf{x} \in \operatorname{Ker} A_{n+2}$ then by the characterisation of Lemma 14, $\mathbf{c}_1 + J_n\mathbf{c}_2$ and $\mathbf{c}_2 + J_n\mathbf{c}_1$ are in the image of the matrix A_n. To study these couples $(\mathbf{c}_1, \mathbf{c}_2)$, let us introduce:

$$\begin{array}{rcl} \varphi : \operatorname{Ker} A_n \times \operatorname{Ker} A_n & \longrightarrow & \operatorname{Ker} A_n / \operatorname{Im} A_n \\ (\mathbf{c}_1, \mathbf{c}_2) & \longmapsto & \mathbf{c}_1 + J_n\mathbf{c}_2 \end{array}$$

From Lemma 13, $\mathbf{c}_1 + J_n\mathbf{c}_2$ and $\mathbf{c}_2 + J_n\mathbf{c}_1$ are both in $\operatorname{Im} A_n$ if and only if $(\mathbf{c}_1, \mathbf{c}_2)$ is in the kernel of φ.

Given such a couple $(\mathbf{c}_1, \mathbf{c}_2)$, we can construct a codeword in $\operatorname{Ker} A_{n+2}$ by choosing $\mathbf{x}_1$ and $\mathbf{x}_2$ pre-images of $\mathbf{c}_1 + J_n\mathbf{c}_2$ and $\mathbf{c}_2 + J_n\mathbf{c}_1$. From this we deduce a bijection onto the code $\operatorname{Ker} A_{n+2}$. Let L_n be a map from $\operatorname{Im} A_n$ to $\mathbb{F}_2^{2^{n-1}}$ such that $L_n(\mathbf{y})$ is a pre-image of $\mathbf{y}$ by A_n, *i.e.* $A_n(L_n(\mathbf{y})) = \mathbf{y}$. Let us introduce the map Ψ:

$$\begin{array}{rcl} \operatorname{Ker} \varphi \times (\operatorname{Ker} A_n)^2 & \to & \operatorname{Ker} A_{n+2} \\ (\mathbf{c}_1, \mathbf{c}_2, \mathbf{s}_1, \mathbf{s}_2) & \mapsto & \left(\begin{array}{l} \mathbf{x}_1 = L_n(\mathbf{c}_2 + J_n\mathbf{c}_1) + \mathbf{s}_1 \\ \mathbf{x}_2 = L_n(\mathbf{c}_1 + J_n\mathbf{c}_2) + \mathbf{s}_2 \\ \mathbf{x}_3 = \mathbf{x}_2 + \mathbf{c}_2 \\ \mathbf{x}_4 = \mathbf{x}_1 + \mathbf{c}_1 \end{array} \right) \end{array}$$

This map is injective because $\Psi(\mathbf{c}, \mathbf{s}) = \Psi(\mathbf{c}', \mathbf{s}')$ implies $\mathbf{x}_1 + \mathbf{x}_4 = \mathbf{x}'_1 + \mathbf{x}'_4$. That is $\mathbf{c}_1 = \mathbf{c}'_1$, by the same way $\mathbf{c}_2 = \mathbf{c}'_2$. By definition of L_n, we obtain $\mathbf{s} = \mathbf{s}'$. To see that Ψ is surjective, we use the characterisation of Lemma 14 of the words of the code $\operatorname{Ker} A_{n+2}$. We can write these vectors $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)$ with:

$$\left\{ \begin{array}{l} \mathbf{x}_4 = \mathbf{x}_1 + \mathbf{c}_1 \\ \mathbf{x}_3 = \mathbf{x}_2 + \mathbf{c}_2 \\ A_n\mathbf{x}_1 = \mathbf{c}_2 + J_n\mathbf{c}_1 \\ A_n\mathbf{x}_2 = \mathbf{c}_1 + J_n\mathbf{c}_2 \end{array} \right.$$

where $\mathbf{c}_1, \mathbf{c}_2 \in \operatorname{Ker} A_n$. The vectors $\mathbf{c}_1$ and $\mathbf{c}_2$ appear clearly and we can see that $A_n\mathbf{x}_1 = A_n(L_n(\mathbf{c}_2 + J_n\mathbf{c}_1))$ so $\mathbf{x}_1$ and $L_n(\mathbf{c}_2 + J_n\mathbf{c}_1)$ are equal modulo a codeword $\mathbf{s}_1$ of $\operatorname{Ker} A_n$. We define $\mathbf{s}_2$ similarly. This gives an pre-image of $\mathbf{x}$. We proved that Ψ is a bijection. So the cardinality of $\operatorname{Ker} A_{n+2}$ is exactly $|\operatorname{Ker} A_n|^2 . |\operatorname{Ker} \varphi|$. We deduce the dimension equality:

$\dim \operatorname{Ker} A_{n+2} = 2 \dim \operatorname{Ker} A_n + \dim \operatorname{Ker} \varphi$. By the rank-nullity theorem, we get $\dim \operatorname{Ker} \varphi = 2^{n-1}$, because φ is surjective. Finally we have:

$$\dim \operatorname{Ker} A_{n+2} = 2 \dim \operatorname{Ker} A_n + 2^{n-1}.$$

We conclude using the case $n = 4$. □

We know that that the number of encoded qubits is $N - 2 \operatorname{Rank} A_n$. From the above proposition, we deduce the dimension of the quantum code.

Corollary 16. *The quantum code Q_n associated to the matrix A_n has parameters:* $[[N = 2^{n-1}, K = 2^{\frac{n}{2}}]]$.

5.3 Computation of the distance

To compute the minimum distance of the quantum code, we examine the weight of the vectors of $\operatorname{Ker} A_n \setminus \operatorname{Ker} A_n^{\perp}$. By Lemma 7 this set is exactly the set $\operatorname{Ker} A_n \setminus \operatorname{Im} A_n$.

Lemma 17. *Every word of* $\operatorname{Ker} A_{n+2} / \operatorname{Im} A_{n+2}$ *has a representative either of the form* $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_2 + \mathbf{c}_2, \mathbf{x}_1 + \mathbf{c}_1)$ *with* $\mathbf{c}_1, \mathbf{c}_2 \notin \operatorname{Im} A_n$ *or of the form* $(\mathbf{x}_1, 0, 0, \mathbf{x}_1)$ *with* $\mathbf{x}_1 \in \operatorname{Ker} A_n$.

Proof. The vectors of $\operatorname{Im} A_{n+2}$ are of the form:

$$\begin{pmatrix} A_n\mathbf{y}_1 + J_n(\mathbf{y}_1 + \mathbf{y}_4) + (\mathbf{y}_2 + \mathbf{y}_3) \\ A_n\mathbf{y}_2 + J_n(\mathbf{y}_2 + \mathbf{y}_3) + (\mathbf{y}_1 + \mathbf{y}_4) \\ A_n\mathbf{y}_3 + J_n(\mathbf{y}_2 + \mathbf{y}_3) + (\mathbf{y}_1 + \mathbf{y}_4) \\ A_n\mathbf{y}_4 + J_n(\mathbf{y}_1 + \mathbf{y}_4) + (\mathbf{y}_2 + \mathbf{y}_3) \end{pmatrix},$$

where $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3, \mathbf{y}_4 \in \mathbb{F}_2^{2^{n-1}}$. Let $\mathbf{x}$ be a vector of $\operatorname{Ker} A_{n+2}$. The first case of the statement is Lemma 14 when $\mathbf{c}_1, \mathbf{c}_2 \notin \operatorname{Im} A_n$.

Now, assume that $\mathbf{c}_1 \in \operatorname{Im} A_n$. Then $\mathbf{c}_2$ is also in the image of A_n because $A_n\mathbf{x}_1 = \mathbf{c}_2 + J_n\mathbf{c}_1$. By symmetry this is the only case that remains to study. Let $\mathbf{b}_1$ and $\mathbf{b}_2$ be pre-images of $\mathbf{c}_1, \mathbf{c}_2$. Set $\mathbf{y}_1 = \mathbf{y}_2 = 0$, $\mathbf{y}_3 = \mathbf{b}_2$ and $\mathbf{y}_4 = \mathbf{b}_1$. We obtain the vector $(\mathbf{v}, J_n\mathbf{v}, J_n\mathbf{v} + \mathbf{c}_2, \mathbf{v} + \mathbf{c}_1) \in \operatorname{Im} A_{n+2}$ where $\mathbf{v} := \mathbf{b}_2 + J_n\mathbf{b}_1$. Thus, modulo the image, $\mathbf{x}$ can be written with $\mathbf{c}_1 = \mathbf{c}_2 = 0$. This yields $A_n\mathbf{x}_2 = \mathbf{c}_1 + J_n\mathbf{c}_2 = 0$. Afterwards, with $\mathbf{y}_2 = J_n\mathbf{x}_2$ and $\mathbf{y}_1 = \mathbf{y}_3 = \mathbf{y}_4 = 0$, we get the vector of the image $(J_n\mathbf{x}_2, \mathbf{x}_2, \mathbf{x}_2, J_n\mathbf{x}_2)$. Consequently, we can assume $\mathbf{x}_2 = \mathbf{x}_3 = 0$ and $\mathbf{x}_1 = \mathbf{x}_4$, which yields a representative of the form $\mathbf{x} = (\mathbf{x}_1, 0, 0, \mathbf{x}_1)$ with $\mathbf{x}_1 \in \operatorname{Ker} A_n$. □

Proposition 18. *The minimum distance of the quantum code Q_n is:*

$$D_n = 2^{\frac{n}{2}-1}.$$

Proof. For $n = 4$ we can see that the distance of the quantum code is 2. Indeed every non zero codeword has weight at least 2 and for example the word $e_2 + e_3 = (01100000)$ is in the kernel of A_4 although it is not a sum of rows.

We will show that the minimum distance is at least multiplied by 2 when n increases of 2. Let $\mathbf{x} \in \operatorname{Ker} A_{n+2}$. Assume that we are in the first case of Lemma 17. The word $\mathbf{x}$ has a representative of the form $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_2+\mathbf{c}_2, \mathbf{x}_1+\mathbf{c}_1)$, where $\mathbf{c}_1$ and $\mathbf{c}_2$ are in $\operatorname{Ker} A_n$ but are not sums of rows. By definition of the distance, we have $w(\mathbf{c}_i) \geq D_n$. Using the triangle inequality for the Hamming distance, we get:

$$\begin{aligned} w(\mathbf{x}_1) + w(\mathbf{x}_1 + \mathbf{c}_1) &= d(0, \mathbf{x}_1) + d(\mathbf{x}_1, \mathbf{c}_1) \\ &\geq d(0, \mathbf{c}_1) \\ &\geq D_n. \end{aligned}$$

We can apply the same reasoning with $\mathbf{c}_2$, so the weight of $\mathbf{x}$ is at least $2D_n$.

Now, assume that we are in the second case of Lemma 17. We know that $\mathbf{x}$ has a representative of the form $\mathbf{x} = (\mathbf{x}_1, 0, 0, \mathbf{x}_1)$ with $\mathbf{x}_1 \in \operatorname{Ker} A_n$. Assume that $\mathbf{x}_1 \in \operatorname{Im} A_n$. Let $\mathbf{w_1}$ be a pre-image of $\mathbf{x}_1$. Take $\mathbf{y}_1 = \mathbf{y}_4 = \mathbf{w_1}$ and $\mathbf{y}_2 = \mathbf{y}_3 = 0$, this shows that $\mathbf{x}$ is in the image of A_{n+2} so its weight does not appear in the computation of the minimum distance. Otherwise $\mathbf{x}_1 \in \operatorname{Ker} A_n \setminus \operatorname{Im} A_n$, so by definition of the distance, the weight of $\mathbf{x}$ is at least $2D_n$.

It remains to see that the bound holds after adding to $\mathbf{x}$ a vector of the image. Let $\mathbf{y}$ be a vector of the image, we know that:

$$\mathbf{y} = \begin{pmatrix} A_n\mathbf{y}_1 + \mathbf{v} \\ A_n\mathbf{y}_2 + J_n\mathbf{v} \\ A_n\mathbf{y}_3 + J_n\mathbf{v} \\ A_n\mathbf{y}_4 + \mathbf{v} \end{pmatrix}$$

where $\mathbf{v}$ is a vector of $\mathbb{F}_2^{2^{n-1}}$ depending on $\mathbf{y}$. Look at the weight of the two first components of $\mathbf{x} + \mathbf{y}$. Using the triangle inequality for the Hamming

distance we find:

$$\begin{aligned} & w(\mathbf{x}_1 + A_n\mathbf{y}_1 + \mathbf{v}) + w(A_n\mathbf{y}_2 + J_n\mathbf{v}) \\ = \;& d(\mathbf{x}_1 + \mathbf{v}, A_n\mathbf{y}_1) + d(J_n\mathbf{v}, A_n\mathbf{y}_2) \\ \geq \;& d(\mathbf{x}_1 + \mathbf{v}, \operatorname{Im} A_n) + d(J_n\mathbf{v}, \operatorname{Im} A_n) \\ = \;& d(\mathbf{x}_1 + \mathbf{v}, \operatorname{Im} A_n) + d(\mathbf{v}, \operatorname{Im} A_n) \\ \geq \;& d(\mathbf{x}_1, \operatorname{Im} A_n) \\ \geq \;& D_n. \end{aligned}$$

The equality $d(J_n\mathbf{v}, \operatorname{Im} A_n) = d(\mathbf{v}, \operatorname{Im} A_n)$ comes from the fact that J_n is an isometry which stabilises $\operatorname{Im} A_n$. We have the same result for the last two components of $\mathbf{x} + \mathbf{y}$ so the weight of every representative of $\mathbf{x}$ is at least $2D_n$.

We have a lower bound for the minimum distance. Actually, the distance of Q_{n+2} is exactly $2D_n$. Indeed the vector $(0, 0, \mathbf{c}_2, \mathbf{c}_1)$ is in the code $\operatorname{Ker} A_n$ and its weight is exactly $2D_n$ when the words $\mathbf{c}_i$ are words of minimum weight in the set $\operatorname{Ker} A_n \backslash \operatorname{Im} A_n$. This vector is not in the image otherwise we should have $\mathbf{c}_1 = A_n(\mathbf{y}_1 + \mathbf{y}_4)$. □

Acknowledgement

This work was supported by the French ANR Defis program under contract ANR-08-EMER-003 (COCQ project).

References

[1] H. Bombin and M. A. Martin-Delgado. Homological error correction: classical and quantum codes. *J. Math. Phys.*, 48, 052105 (2007).

[2] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996.

[3] M. H. Freedman, D. A. Meyer, and F. Luo. $\mathbb{Z}_2$-systolic freedom and quantum codes. In *Mathematics of quantum computation*, Chapman & Hall/CRC, pages 287–320, Boca Raton, FL, 2002.

[4] A. Y. Kitaev. Fault-tolerant quantum computation by anyons. *Ann. Phys.*, 303:2, 2003.

[5] D. J. C. MacKay, G. Mitchison, and P. L. McFadden. Sparse graph codes for quantum error-correction. *IEEE Trans. Info. Theory*, 50(10):2315–2330, 2004.

[6] D. MacKay, G. Mitchison, A. Shokrollahi. More Sparse-Graph Codes for Quantum Error-Correction, 2007. `www.inference.phy.cam.ac.uk/mackay/cayley.pdf`

[7] A. M. Steane. Multiple particle interference and quantum error correction. *Proc. R. Soc. Lond. A*, 452:2551–2577, 1996.

[8] J.P. Tillich, G. Zémor, Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$ Proceedings of the *IEEE Symposium on Information Theory, ISIT 2009*, pp.799-804.