MASTER'S THESIS

Master of Science in Advanced Mathematics and Mathematical Engineering

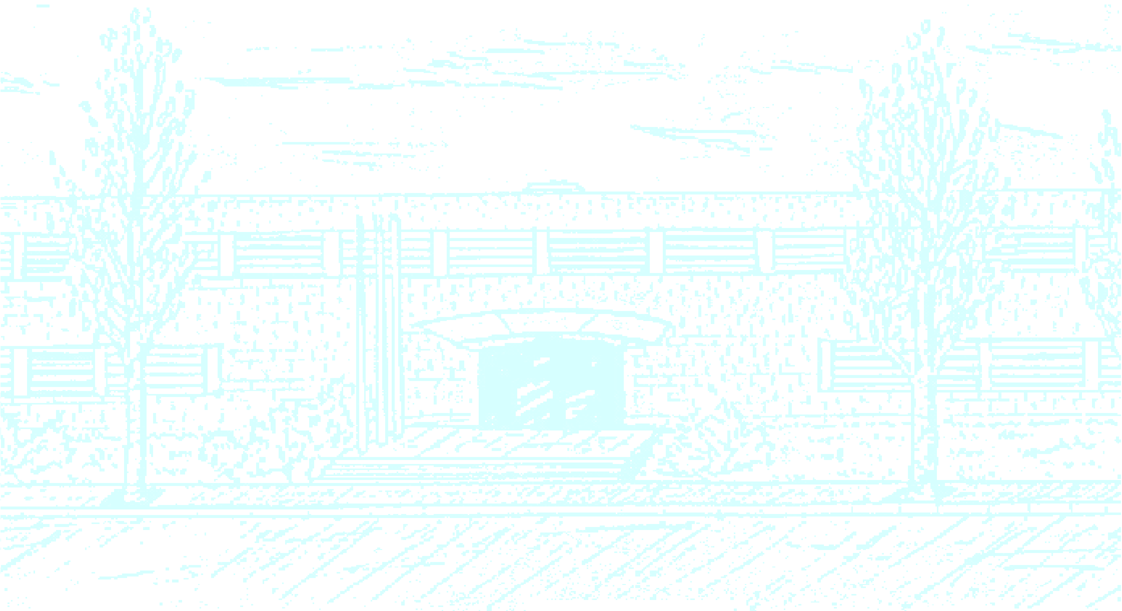
Title: The Geometry of Quantum Codes

Author: Pablo Puig pericas

Advisor: Simeon Ball

Department: Mathematics Department (749)

Academic year: 2020 - 2021



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Strongly grateful to professor Simeon Ball who introduced me in the fascinating and quite new world of quantum codes and their geometries.

Abstract

Quantum particles are continuously interacting with the environment hence quantum information is always susceptible to errors. Consequently when encoding information into quantum bits a special treatment is required such that there is a recovery map between the information sent and the information received capable to correct certain class of errors. We allow the quantum bits to take two orthogonal values (qubits) and we encode k logical qubits on n physical qubits. We first present the already well known class of quantum codes called stabiliser codes and its geometry from which one can deduce the code parameters. Finally we shall study the much less known class of quantum codes called non additive codes, result of direct sums of stabilizer codes, and for which we provide a geometric framework which appears to be new.

Keywords

Error Correcting Quantum Codes, Qubits, Stabilizer Codes, Non Additive Quantum Codes, Pauli Group, Projective Space.

Contents

The first two chapters, devoted to introduce quantum codes and study quantum stabilizer codes, are based on chapters 2 and 10 from Nielsen & Chuang [1] while the third chapter, devoted to the geometry of stabilizer codes, is based on Glynn et al [2] despite the $\mathbb{F}_4$ trick presented there is not used here. Actually for the first three chapters we have followed the expository paper [3] which also uses the above main sources as guidance. Finally the most original part is chapter 4 where we present non additive quantum codes together with a geometric framework which fully characterizes them and which appears to be new.

1. Quantum Codes

1.1 Qubits and Hilbert Space

Analogous to a bit in classical information theory, a quantum bit or *qubit* is the basic unit of quantum information consisting in a two-state quantum-mechanical system: typically the intrinsic angular momentum (spin) of an electron where the spin can be "up" or "down" or the polarization of a single photon where the polarization can be "vertical" or "horizontal". We shall focus on the first example but the main idea is the same for both electrons and photons. Electrons can take a continuum of possible spin-directions while, surprisingly, when measuring we only obtain two discrete values. The measurement indicates in which of two mutually exclusive states the qubit is found after the measurement. Qubits are the states of quantum particles described as the superposition of two mutually exclusive states together with the probabilities p and $(1-p)$ to obtain these two values when measuring. We will not go deeper in the theory behind the counter-intuitive behaviour of quantum particles but we refer the interested reader to the book of Sakurai [6].

Mathematically a qubit is defined as a unit vector in the Hilbert space $\mathbb{C}^2$ equipped with the *inner product*

$$(z, w) := \overline{z} \cdot w = \overline{z_1}w_1 + \overline{z_2}w_2$$

where $z, w \in \mathbb{C}^2$ and $\overline{z}$ denotes the complex conjugation. In quantum mechanics the columns vectors are denoted by $|\ \rangle$ and called *ket* while the row vectors are denoted by $\langle\ |$ and called *bra*. To switch form one to another we simply must transpose and and apply complex conjugation. Then given two vectors $|\alpha\rangle, |\beta\rangle \in \mathbb{C}^2$ the inner product, denoted by $\langle\alpha|\beta\rangle$ and called *braket*, is

$$\langle\alpha|\beta\rangle = (\overline{\alpha_1}, \overline{\alpha_2})\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix} = \overline{\alpha_1}\beta_1 + \overline{\alpha_2}\beta_2$$

The inner product $\mathbb{C}^n \times \mathbb{C}^n \longrightarrow \mathbb{C}$ satisfies:

1. Conjugate-linear on the first argument: $\langle\sum_i \lambda_i v_i|w\rangle = \sum_i \overline{\lambda_i}\langle v_i|w\rangle$
2. Linear on the second argument: $\langle v|\sum_i \lambda_i|w_i\rangle = \sum_i \lambda_i \langle v|w_i\rangle$
3. $\langle v|w\rangle = \overline{\langle w|v\rangle}$
4. $\langle v|v\rangle \geq 0$ with equality if and only if $|v\rangle = 0$

We can use the inner product to represent linear operators with what is known as the *outer product* representation. Let $|v\rangle \in V$ and $|w\rangle \in W$ where V and W are Hilbert spaces. We define $|v\rangle\langle w|$ to be the linear operator from V to W whose action is ruled by

$$(|v\rangle\langle w|)(|v'\rangle) \equiv |w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle$$

The above action can be interpreted as the result of multiplying $|w\rangle$ by the complex number $\langle v|v'\rangle$ or as the (much more interesting) result of the operator $|v\rangle\langle w|$ acting over $|v'\rangle$. Indeed the two potential meanings coincide as the second one is defined in terms of the first one.

Let $|i\rangle$ be any orthonormal basis for the Hilbert space V. Then for any $|v\rangle \in V$ we have $|v\rangle = \sum_i v_i |i\rangle$. Recall that $\langle i|v\rangle = v_i$ hence

$$\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i |i\rangle\langle i|v\rangle = \sum_i v_i|i\rangle = |v\rangle$$

which it is true for all $|v\rangle \in V$ hence we end up with what is known ad the *completeness relation*

$$\sum_i |i\rangle\langle i| = \mathbb{I}$$

The completeness relation let represent any linear operator in outer product notation as follows: Let A be a linear operator from V to W and let $\{|v_i\rangle\}$ and $\{|w_i\rangle\}$ be the orthonormal basis for V and W respectively. Then

$$A = I_W A I_V = \sum_{i,j} |w_j\rangle\langle w_j| A |v_i\rangle\langle v_i| = \sum_{i,j} \langle w_j| A |v_i\rangle |w_j\rangle\langle v_i|$$

where $A|v_i\rangle$ is a ket hence $\langle w_j| A|v_i\rangle$ is a complex number. Thus, the above expression is the outer product representation of A. Observe that the entry of A in the i-th column and j-th row, with respect to the input basis $\{|v_i\rangle\}$ and and output basis $\{|w_i\rangle\}$, is precisely $\langle w_j| A|v_i\rangle$.

Coming back to qubits, the mutually exclusive states spin up and spin down are represented by an orthonormal basis of $\mathbb{C}^2$. By convention we assign the spin up state to the column vector $|0\rangle$ while the spin down state is assigned to the column vector $|1\rangle$ where

$$|0\rangle := \begin{pmatrix}1\\0\end{pmatrix} \quad ; \quad |1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$$

Clearly $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 0|1\rangle = 0$ therefore effectively $\{|0\rangle, |1\rangle\}$ forms an orthonormal basis.

An arbitrary qubit state $|\psi\rangle \in \mathbb{C}^2$ is described as the linear combination of the spin up and down states. Thus

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \text{ with } \alpha_0, \alpha_1 \in \mathbb{C}$$

We say the qubit is in *superposition* of both states. After measuring, the probability to find the qubit on state $|0\rangle$ is $\overline{\alpha_0}\alpha_0$ while the the probability to find the qubit on state $|1\rangle$ is $\overline{\alpha_1}\alpha_1$. The sum of the above probabilities must be 1 hence

$$\langle\psi|\psi\rangle = \overline{\alpha_0}\alpha_0 + \overline{\alpha_1}\alpha_1 = 1$$

which implies the normalization of $|\psi\rangle$, namely, $|\psi\rangle$ must be a unit vector.

A system of n qubits is mathematically described as a unit vector in the n-fold tensor product of the one-qubit spaces, namely, the 2^n-dimensional Hilbert space $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ (n times). For example for $n = 2$ a basis of $\mathbb{C}^4$ is:

$$|0\rangle \otimes |0\rangle := |00\rangle \quad ; \quad |0\rangle \otimes |1\rangle := |01\rangle \quad ; \quad |1\rangle \otimes |0\rangle := |10\rangle \quad ; \quad |1\rangle \otimes |1\rangle := |11\rangle$$

where we use the short hand notation $|\psi\rangle \otimes |\theta\rangle \equiv |\psi\ \theta\rangle$.

1.2 Observables and Pauli Group

Through this section we briefly present some well known results of linear algebra. We also show the basics of quantum mechanics notation which should be more than enough to follow the whole text. Anyway, we refer the interested reader to chapter 2 of [1] or any standard book of linear algebra to go deeper on these topics.

A unitary transformation of $\mathbb{C}^2$ is represented by a non singular 2×2 matrix U which preserves the inner product. Thus

$$\langle U\alpha | U\beta \rangle = \langle \alpha | \beta \rangle$$

The set of unitary transformations in $\mathbb{C}^2$ forms the special unitary group $SU(2)$ and their matrix representations take all eigenvalues modulo 1, namely, of the form $e^{i\theta}$ for some $\theta \in \mathbb{R}$.

Let the set $\{|v_i\rangle\}$ be an orthonormal basis and define $|w_i\rangle = U\, |\psi\rangle\, v_i$ where U is an unitarian operator. Then U can be written in terms of an outer product as

$$U = \sum_i |w_i\rangle \langle v_i|$$

The *hermitian conjugate* $M^\dagger$ of a linear operator M is defined as the operator which satisfies

$$\langle M\psi | \theta \rangle = \langle \psi | M^\dagger \theta \rangle$$

Observe that the above shows how to move an operator between the two elements of the inner product.

A linear operator M is called *Hermitian* if

$$M = M^\dagger \text{ which implies } \langle M\psi | \theta \rangle = \langle \psi | M\theta \rangle$$

For a matrix representation A of M the above condition is equivalent to $A^{*^T} = A$. Hermitian operators have the property that their eigenvalues are real and that the eigenvectors belonging to different eigenvalues are all orthogonal.

Observe that a unitary operator can be defined in terms of the hermitian conjugate as those operators fulfilling $U^\dagger U = \mathbb{I}$:

$$\langle U\alpha | U\beta \rangle = \langle \alpha | U^\dagger U\beta \rangle = \langle \alpha | \beta \rangle$$

An operator N is called *normal* if

$$NN^\dagger = N^\dagger N$$

The *spectral decomposition theorem* states that any normal operator N on a Hilbert space V is diagonal with respect to some orthonormal basis for V. Conversely, any diagonalizable operator is normal. Note that both unitarian operators ($U^\dagger U = \mathbb{I}$) and hermitian operators ($M = M^\dagger$) are normal and hence by spectral decomposition theorem they are diagonalizable.

Let M be a linear operator over a Hilbert Space with orthonormal basis $\{|i\rangle\}$. The *trace* of M is defined as

$$tr(M) := \sum_i \langle i|M|i \rangle$$

In matrix terms $tr(M)$ is equal to the sum of the elements on the principal diagonal.

Using the completeness relation we can easily check that the trace is invariant under a change of basis. Let $\{|j\rangle\}$ be another orthonormal basis, then

$$tr(M) = \sum_i \langle i|M|i\rangle = \sum_j \sum_i \langle i|j\rangle \langle j|M|i\rangle = \sum_j \sum_i \langle j|M|i\rangle \langle i|j\rangle = \sum_j \langle j|M|j\rangle$$

In quantum mechanics the *measurements* or *observables* are represented by hermitian operators: the result of the measurement (eigenvalue) is a real number and the state of the particle after the measurement (eigenvector) has no superposition because the eigenvectors of different eigenvalues are orthogonal.

Let $\widehat{A}$ denote an observable hence represented by an Hermitian matrix A and let $\{m_i\}$ and $\{|m_i\rangle\}$ be its sets of eigenvalues and eigenvectors. When measuring the observable $\widehat{A}$ on a quantum state $|\psi\rangle$ we obtain the eigenvalue m_i with probability

$$p_i = |\langle\psi|m_i\rangle|^2$$

Then, after the measurement the original state $|\psi\rangle$ becomes $|m_i\rangle$. Then intuitively the *expected value* $\langle\widehat{A}\rangle$ is

$$\langle\widehat{A}\rangle = \sum_i p_i m_i$$

which implies

$$\langle\widehat{A}\rangle = \langle\psi|A|\psi\rangle = \sum_i \langle i|A|\psi\rangle \langle\psi|i\rangle = tr(A\,|\psi\rangle\langle\psi|)$$

In the classical framework an error is a bit-flip between 0 and 1. In the quantum framework an error is represented by an non-identity unitary transformation, namely, an element of $SU(n)$. Thus, the errors may vary the probabilities of the superposed states but they preserve the normalisation of qubit states.

Recall that any element of $SU(n)$ decomposes in terms of the matrix basis. We choose the *Pauli group* $\mathcal{P}_n$ as such a basis i.e. the group generated by all possible tensor products of the four *Pauli matrices*

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad ; \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad ; \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad ; \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

together with the phases $\{\pm1, \pm i\}$. The Pauli matrices form a basis for the space of 2 × 2 matrices and any error affecting a single qubit can be written as a linear combination of Pauli matrices. Similarly, any error affecting n qubits can be written as a linear combination of elements of the Pauli group. Below we summarize the main properties of Pauli matrices:

1. Anti-commutation: $\sigma_i\sigma_j = -\sigma_j\sigma_i$ for $i \neq j$ and $i, j \in \{x, y, z\}$
2. Hermitian: $\sigma_i = \sigma_i^\dagger$
3. Unitarian: $\sigma_i^\dagger\sigma_i = \sigma_i^2 = \mathbb{I}$
4. Product rules: $\sigma_x\sigma_y = i\sigma_z$; $\sigma_y\sigma_z = i\sigma_x$; $\sigma_z\sigma_x = i\sigma_y$
5. The eigenvalues of σ_i for $i \in \{x, y, z\}$ are ±1 while σ_0 has eigenvalue 1.
6. They act over $|0\rangle$ and $|1\rangle$ ad follows: σ_0 acts as the identity, σ_0 flips the probabilities of the superposed states, σ_z indicates if the spin is up or down and $\sigma_y = -i\sigma_z\sigma_x$ adds a phase i, change the sign and flips the states.

$$\begin{array}{ccccccc} \sigma_0|0\rangle = |0\rangle & ; & \sigma_x|0\rangle = |1\rangle & ; & \sigma_z|0\rangle = |0\rangle & ; & \sigma_y|0\rangle = i\,|1\rangle \\ \sigma_0|1\rangle = |1\rangle & ; & \sigma_x|1\rangle = |0\rangle & ; & \sigma_z|1\rangle = -|1\rangle & ; & \sigma_y|1\rangle = -i\,|0\rangle \end{array}$$

Thus, $\mathcal{P}_n$ is a non abelian group formed by 4^n tensor products of the Pauli matrices together with 4 phases $\{\pm 1, \pm i\}$ hence it has size 4^{n+1}.

Example 1.1. Let $|\psi\rangle \in \mathbb{C}^2$ be a qubit described by

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

We want to measure the spin up/down expected value of a particle. The individual measurement σ_z can only take two values ± 1, namely, the eigenvalues of σ_z. After the measurement the original state $|\psi\rangle$ becomes $|0\rangle$ if the value obtained is 0 and $|1\rangle$ if the value obtained is 1. The probabilities p_0 and p_1 of each event are

$$p_0 = |\langle\psi|0\rangle|^2 = |\alpha_0|^2 = \overline{\alpha_0}\alpha_0 \quad ; \quad p_1 = |\langle\psi|1\rangle|^2 = |\alpha_1|^2 = \overline{\alpha_1}\alpha_1$$

The expected value $\widehat{\sigma}_z$ obtained by the repeated measurement of identically prepared spin particles is

$$\langle\widehat{\sigma}_z\rangle = \langle\psi|\sigma_z|\psi\rangle = tr(\sigma_z |\psi\rangle\langle\psi|) = \alpha_0^2 - \alpha_1^2$$

Alternatively, we can compute the expected value in the usual way, namely, as the sum of the possible values multiplied by their probabilities:

$$\langle\widehat{\sigma}_z\rangle = p_0(+1) + p_1(-1) = \alpha_0^2 - \alpha_1^2$$

A *quantum correcting error code* is a linear subspace Q of $(\mathbb{C}^2)^{\otimes n}$ into which a number of logical qubits are encoded into n physical qubits with a special treatment such that all errors of certain type can be detected and corrected. Thus, given a noisy channel which propagates errors of certain type over the quantum information sent through it, we must find a recovery map such that the original information can be restored.

In classical code theory the simplest way to equip a code with error-correcting capabilities is to add redundancy to the bits. For example, we can encode 0 as 000 and 1 as 111. Then we can correct up to one error by majority decision. For example the codewords 001 and 010 decode as 0 while the codewords 110 and 101 decode as 1.

In quantum code theory this is no longer possible due to the *no-cloning theorem* which states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state.

Theorem 1.2. *(no-cloning). There is no linear operator from $|\psi\rangle$ to $|\psi\rangle \otimes |\psi\rangle$ for all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$*

Proof. Suppose such an operator exists and let $|\psi\rangle, |\theta\rangle \in (\mathbb{C}^2)^{\otimes n}$. Then there is a map:

$$|\psi\rangle \longrightarrow |\psi\rangle \otimes |\psi\rangle \quad ; \quad |\theta\rangle \longrightarrow |\theta\rangle \otimes |\theta\rangle$$

But this map is not linear since

$$|\psi\rangle + |\theta\rangle \longrightarrow (|\psi\rangle + |\theta\rangle) \otimes (|\psi\rangle + |\theta\rangle) \neq |\psi\rangle \otimes |\psi\rangle + |\theta\rangle \otimes |\theta\rangle$$

□

Example 1.3. (Shor Code). Shor introduced a quantum code in [5] capable to correct any single-qubit error by introducing a majority decision in both bits and sings.

Shor code encodes a single logical qubit into 9 physical qubits such that the given qubit

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

is encoded by a linear map as

$$|\psi_L\rangle = \alpha_0 \, |0\rangle_L + \alpha_1 \, |1\rangle_L$$

where

$$|0\rangle \longrightarrow |0_L\rangle = (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$
$$|1\rangle \longrightarrow |1_L\rangle = (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

Hence we end up with

$$\begin{gathered}|\psi_L\rangle = \alpha_0(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \\ + \\ \alpha_1(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)\end{gathered}$$

Suppose there is a bit-flip error σ_x on the 4-th bit. Since

$$\sigma_x \, |0\rangle = |1\rangle \quad ; \quad \sigma_x \, |1\rangle = |0\rangle$$

the term α_0 changes to

$$(|000\rangle + |111\rangle) \otimes (|\mathbf{1}00\rangle + (|\mathbf{0}11\rangle) \otimes (|000\rangle + |111\rangle)$$

which it is enough to detect the error, identify it as σ_x and correct it by majority decision decoding

$$|100\rangle + |011\rangle \text{ as } |000\rangle + |111\rangle$$

Suppose we have a σ_z error on the 7-th bit. Since

$$\sigma_z \, |0\rangle = |0\rangle \quad ; \quad \sigma_z \, |1\rangle = - \, |1\rangle$$

the term α_0 changes to

$$(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle - |111\rangle)$$

which it is enough to detect the error, identify it as σ_z and correct it by majority decision decoding

$$|000\rangle - |111\rangle \text{ as } |000\rangle + |111\rangle$$

Since $\sigma_y = i\sigma_x\sigma_z$ we can also correct this single error since the majority decisions to correct σ_x and σ_z are independent of each other while the scalar factor i is indifferent when decoding.

1.3 The Orthogonal Projection

As we shall show the measurement operators, which are hermitian, act over a qubit by arising an eigenvalue and projecting the qubit state onto the corresponding eigenspace.

Let Q be a subspace of $(\mathbb{C}^2)^{\otimes n}$. Let $Q^\perp$ be the subspace of $(\mathbb{C}^2)^{\otimes n}$ orthogonal to Q. Thus

$$Q^\perp = \{u : \langle u|v\rangle = 0 \text{ for all } v \in Q\}$$

Any $\psi \in (\mathbb{C}^2)^{\otimes n}$ can be written as a sum of a vector $P\,|\psi\rangle \in Q$ and a vector $P^\perp\,|\psi\rangle \in Q^\perp$. The operator P which maps $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ to $P\,|\psi\rangle \in Q$ is called the *orthogonal projection* onto Q.

Lemma 1.4. *Let $\{\psi_i\}$ be an orthonormal basis of Q. Then*

$$P = \sum_i |\psi_i\rangle \langle\psi_i|$$

Proof. For any $j \leq k$ we have

$$P|\psi_j\rangle = \sum_{i=1}^{k} |\psi_i\rangle \langle\psi_i|\psi_j\rangle = |\psi_j\rangle$$

Hence $P|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in Q$. □

Observe that if $|\psi\rangle \in Q^\perp$ then $P|\psi\rangle = \sum_i |\psi_i\rangle \langle\psi_i|\psi\rangle = 0$. Also recall that

$$P = \sum_i |\psi_i\rangle \langle\psi_i| = \sum_i P_i$$

where $P_i = |\psi_i\rangle \langle\psi_i|$ is the projection onto the subspace spanned by $|\psi_i\rangle$. By definition $P^2 = P$ while by Lemma 1.4 P is hermitian since each P_i is hermitian.

Lemma 1.5. *If P is a linear operator such that*

(i) $P^2 = P$

(ii) *P is hermitian.*

(iii) *The image of P is in Q*

Then P is the orthogonal projection onto Q.

Proof. If P is hermitian then it is normal hence it is diagonalitzable. Also the fact it is hermitian implies it has real eigenvalues. Suppose $P|\psi\rangle = \lambda|\psi\rangle$ for some $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$. Since $P^2 = P$ is idempotent then

$$P^2|\psi\rangle = \lambda P|\psi\rangle = \lambda^2|\psi\rangle \to \lambda = \lambda^2$$

Thus, the eigenvalues of P are 0 and 1.

By the spectral decomposition theorem any normal operator N is diagonalitzable, namely,

$$N = \sum_i \lambda_i |\psi_i\rangle \langle\psi_i|$$

for some orthonormal basis $\{|\psi_i\rangle\}$ where λ_i and $|\psi_i\rangle$ are the eigenvalues and eigenvectors of N. In terms of projectors P_i it yields to

$$N = \sum_i \lambda_i P_i$$

where P_i is the projector onto the λ_i-eigenspace of N.

Since P is hermitian it normal too hence

$$P = \sum_i |\psi_i\rangle \langle\psi_i|$$

where $\{|\psi_i\rangle\}$ is an orthonormal basis for its eigenspace with eigenvalue 1.

Since $P|\psi_i\rangle = |\psi_i\rangle$ for all i then $Im(P) = Q$ is contained on the eigenspace with eigenvalue 1 while the eigenspace with eigenvalue 0 is $Im(P)^\perp$. Thus, P is the orthogonal projection onto Q. □

1.4 Error Weights

A code of length n is a subset $C \subseteq A^n$, where A is a finite set called the alphabet. An element of C is called a codeword.

The *Hamming distance* or simply distance $d(u, v)$ between two codewords $u, v \in C$ is the number of coordinates in which they differ. We denote by d the minimum distance between all codewords of C.

Lemma 1.6. *Let $u, v, w \in A^n$. The Hamming distance satisfies the triangle inequality*

$$d(u, v) = d(u, w) + d(w, v)$$

Proof. If u and v differ in the i-th coordinate then w must differ from u or v in the i-th coordinate too. □

The *nearest neighbour decoding* is the decoding map such that a received codeword v is decoded as u where u is the closest codeword to v with respect to the Hamming distance.

Lemma 1.7. *Using nearest neighbour decoding, a block code of minimum distance d can correct up to $\lfloor (d-1)/2 \rfloor$ errors*

Proof. By lemma 1.6 any codewords $w, u, v \in A^n$ and codewords u and v satisfy

$$d \leq d(u, v) = d(u, w) + d(w, v)$$

Hence, there is at most one codeword at distance at most $\lfloor (d-1)/2 \rfloor$ from w. □

A *linear code* C is a subspace of A^n where A is a finite field and for all $u, v \in C$ and $\lambda, \mu \in A$ we have

$$\lambda u + \mu v \in C$$

The *weight* $w(u)$ of a codeword $u \in C$ is defined as the number of non-zero coordinates of u. Linear codes are subspaces hence $0 \in C$, thus

$$w(u) = d(u, 0)$$

Lemma 1.8. *Let C be a linear code over a finite field. Then the minimum distance d of C is equal to its minimum weight.*

Proof. Suppose that u is a codeword the codeword of C with minimum weight which we denote by w. Then since C is linear $0 \in C$ hence $d(u, 0) = w \geq d$.

Next let $u, v \in C$ be two codewords which differ in exactly d coordinates. Since C is linear $u - v \in C$ and has weight d and since w is the minimum weight of C we have $d \geq w$. □

In the quantum case the *weight* of an element $M \in \mathcal{P}_n$ is defined as the number of tensor components different to σ_0. For example, the following element has weight 3:

$$M = \sigma_x \otimes \sigma_x \otimes \sigma_0 \otimes \sigma_0 \otimes \sigma_y \otimes \sigma_0$$

Let $\mathcal{E}_d$ denote the set of elements of $\mathcal{P}_n$ with weight at most $\lfloor (d-1)/2 \rfloor$

$$\mathcal{E}_d = \{E \in \mathcal{P}_n \mid wt(E) \leq \lfloor (d-1)/2 \rfloor\}$$

Conceptually similar to its classic analog, the *minimum distance* of a quantum code is defined as the positive integer d such that all errors in $\mathcal{E}_d$ are correctable. We shall see in later sections which is the syndrome of a quantum error and how to correct it.

1.5 Error-Correcting Conditions

Quantum particles are continuously interacting with the environment hence quantum information is always susceptible to errors. When sending (unknown) quantum information through a noisy channel there are three major problems to take into account:

1. The quantum system is in superposition of states and any measurement fixes it to one of the basis states. Thus, if we measure to obtain an error syndrome we may modify the quantum system.
2. The set of errors is continuous rather than discrete hence a first sight it seems that we can not delimit the errors.
3. The no-cloning theorem states that unknown quantum states can not be copied therefore we can not add redundancy when encoding as in the classical case.

Which can be solved by the following three approaches:

1. The error syndrome measurements are chosen such that the code states are not modified while erroneous states are modified in a reversible way.
2. Quantum mechanics are linear hence if a set of discrete errors is correctable then their span is correctable too. In other words, there are infinite unitary operators representing errors but all of them can be written in terms of the Pauli group.
3. The quantum information (k logical qubits) is encoded through many systems (n physical qubits) where $k \leq n$ and thus "hidden" from errors of certain type while avoiding to add redundancy by cloning.

The following theorem provides a necessary and sufficient condition for the existence of a recovery map between the information sent and the information received capable to correct all errors in the set $\mathcal{E}$. It is taken from Nielsen and Chuang [1], theorem [10.1], and is due to Bennett, DiVincenzo, Smolin and Wootters [8] and Knill and Laflamme [13]. For the proof, which it is quite long and technical, we redirect to [1].

Theorem 1.9. *(Knill-Laflamme Conditions). Let Q be a quantum code and let P be the orthogonal projector onto Q. Suppose $\mathcal{E}$ is a quantum operation with operation elements $\{E_i\}$. A necessary and sufficient condition for the existence of an error-correction map (recovery map) correcting $\mathcal{E}$ on Q is that*

$$PE_i^\dagger E_j P = \alpha_{ij} P$$

for some Hermitian matrix α of complex numbers.

Remark. By multiplying both sides of the equality by $\langle\theta|$ and $|\psi\rangle$ where $|\theta\rangle$ and $|\psi\rangle$ are elements of an orthonormal basis of Q the above necessary and sufficient condition is equivalent

$$\langle\theta|E_i^\dagger E_j|\psi\rangle = \alpha_{ij}\langle\theta|\psi\rangle$$

for all elements $|\theta\rangle$ and $|\psi\rangle$ of an orthonormal basis of Q.

A set of errors $\mathcal{E}$ *detectable* if and only if all errors $E_i^\dagger E_j$ with $E_i E_j \in \mathcal{E}$ are correctable.

Theorem 1.9 implies the following major conclusions:

1. Orthogonal states of Q remain orthogonal under the action of errors. Thus, given a pair $|\theta\rangle, |\psi\rangle \in Q$

   $$\text{If } \langle\theta|\psi\rangle = 0 \text{ then } \langle\theta|E_i^\dagger E_j|\psi\rangle = 0 \text{ for all } E_i E_j \in \mathcal{E}.$$

   This implies we can apply a convenient error syndrome measurement such that the codeword $|\psi\rangle$ remains unchanged while an erroneous state $E|\psi\rangle$ where $E \in \mathcal{E}$ is modified in a reversible way. Thus, all errors in $\mathcal{E}$ fulfill the above condition hence they are detectable.

2. The expectation value of $E_i^\dagger E_j$ is the same for all code states of Q. Thus

   $$\widehat{\langle E_i^\dagger E_j\rangle} = tr(E_i^\dagger E_j |\psi\rangle\langle\psi|) = \langle\psi|E_i^\dagger E_j|\psi\rangle = \langle\theta|E_i^\dagger E_j|\theta\rangle = \alpha_{ij} \text{ for all } |\psi\rangle, |\theta\rangle \in Q$$

   which implies the quantum information encoded in Q is "hidden" from the errors in $\mathcal{E}$.

The aim is to construct codes capable to correct all errors of weight at most $\lfloor (d-1)/2 \rfloor$. Thus, all errors in the set

$$\mathcal{E}_d = \{E \in \mathcal{P}_n \mid wt(E) \le \lfloor (d-1)/2 \rfloor\}$$

Any error is represented by a unitary operator hence it can be written in terms of the Pauli group, namely, it can be discretised. Therefore we must focus only on how to correct the errors represented by the elements of the Pauli group. Then the constructed codes will be able to correct any linear combination of the errors in $\mathcal{E}_d$.

Example 1.10. Let $|\psi\rangle \in Q$ describe a system of n qubits and let P be the orthogonal projector onto the quantum code Q. In the proof of Lemma 1.5 we have shown that P has eigenvalues 1 and 0 where the $+1$-eigenspace contains $Im(P) = Q$ while the 0-eigenspace contains $im(P)^\perp$. Also, by Lemma 1.5 the projector P is hermitian hence it can be considered a measurement. Indeed, P can be used as an error syndrome measurement, more precisely, it can be used to check if some error has occurred or not.

Suppose an error E occurs. Then the resulting state is $E|\psi\rangle$. By Theorem 1.9 an error $E \in \mathcal{P}_n$ is detectable for Q if and only if for any $|\theta\rangle \in Q$ such that $\langle\theta|\psi\rangle = 0$ we have

$$\langle\theta|E|\psi\rangle = 0$$

Suppose the measurement P returns 1, namely, $PE|\psi\rangle = +1E|\psi\rangle$. If E is detectable then given $|\theta\rangle \in Q$ such that $\langle\theta|\psi\rangle = 0$ we have

$$\langle\theta|PE|\psi\rangle = \langle\theta|E|\psi\rangle = 0$$

which implies $PE|\psi\rangle$ is a multiple of $|\psi\rangle$ because $\langle\theta|\psi\rangle = 0$ too. Thus, $PE|\psi\rangle \in Q$ hence we can recover the original state $|\psi\rangle$ up to a scalar factor. Indeed, no "effective" error has occurred as the scalar factor is irrelevant when decoding.

Suppose the measurement P returns 0, namely $PE|\psi\rangle = 0|\psi\rangle = 0$. Then

$$E|\psi\rangle \in Q^\perp$$

Which implies the new state $E|\psi\rangle$ no longer belongs to the quantum code Q. Thus, we can ensure some error has occurred. The capability of Q to uniquely identify and correct the error will depend on the weight of the error as we shall see in future sections.

2. Quantum Stabilizer Codes

2.1 Definition

Much of the currently known quantum codes belong to the class of Stabilizer codes. These codes are efficiently described due to their connection to classical linear codes.

A Quantum stabilizer code $Q(S)$ is the joint $+1$-eigenspace of all elements of an abelian subgroup S of the non-abelian Pauli group $\mathcal{P}_n$ where $-\mathbb{I} \notin S$ (details below). Such subgroup S us called the stabilizer.

For convenience, we define S as being generated by $n-k$ commuting independent generators $M_1, \dots, M_{n-k}$ of $\mathcal{P}_n$. By independent we mean that by removing a generator the remaining set no longer generates S. Thus:

$$S = \langle M_1, \dots, M_{n-k} \rangle = \{\prod M_1^{\alpha_1} \dots M_{n-k}^{\alpha_{n-k}} : \alpha_i \in \{0, 1\}\}$$

where S is abelian so $M_i M_j = M_j M_i$ and $\alpha_i \in \{0, 1\}$ because the square of any Pauli matrix is $\mathbb{I}$ and each $M_i \in \mathcal{P}_n$ is a tensor product of Pauli matrices hence $M_i^2 = \mathbb{I}$. Recall that S has size 2^{n-k} as its elements are all possible combinations of $n-k$ generators without taking into account the order as S is abelian.

The definition of $Q(S)$ as the joint $+1$-eigenspace of the elements in S can be equivalently formulated in terms of its generators:

$$|\psi\rangle \in Q(S) \iff M_i |\psi\rangle = +1 |\psi\rangle \text{ for all } i \in \{1, \dots, n-k\}$$

Therefore $Q(S)$ is the intersection of the $+1$-eigenspace of each M_i.

Observe that if $|\psi\rangle \in Q(S)$ then

$$\prod_{i \in J} M_i |\psi\rangle = +1 |\psi\rangle \text{ for all } J \subseteq \{i, \dots, n\}$$

therefore any element of S has any vector $|\psi\rangle \in Q(S)$ as eigenvector of eigenvalue $+1$ and, equivalently, $Q(S)$ is the intersection of the $+1$-eigenspace of each element of S.

Recall that if $|\psi_1\rangle, |\psi_2\rangle \in Q(S)$ then:

$$M_i(\lambda |\psi_1\rangle + \mu |\psi_2\rangle) = \lambda M_i |\psi_1\rangle + \mu M_i |\psi_2\rangle = \lambda |\psi_1\rangle + \mu |\psi_2\rangle \text{ for all } i \in \{1, \dots, n-k\}$$

Hence $\lambda |\psi_1\rangle + \mu |\psi_2\rangle \in Q(S)$ and thus $Q(S)$ is a subspace of $(\mathbb{C}^2)^{\otimes n}$.

We assume that there is no coordinate between the n possible such that all elements of S have a σ_0 on it because then we can simply delete that coordinate while keeping the same error correcting properties of the code.

On the other hand, in the definition of $Q(S)$ we have required $-\mathbb{I} \notin S$. The reason is that if

$$-\mathbb{I} \in S \to -\mathbb{I} |\psi\rangle \neq +1 |\psi\rangle \to Q(S) = \{0\}$$

because the $+1$-eigenspace of $-\mathbb{I}$ is the zero vector and consequently $Q(S)$, defined as the intersection of all elements in S, results on the zero vector too. Also note that the phase of any element in S must be ± 1 and never $\pm i$ because if

$$M = \pm i \sigma_1 \otimes \dots \otimes \sigma_n \to M^2 = -\mathbb{I} \in S$$

hence again $Q(S) = \{0\}$. We will always assume the phase of any element in S to be 1. However, changing the sign of some of M_i has deep implications as detailed in a later section.

We will use many times the following short-hand notation:

$$\begin{array}{rclcrcl} \sigma_0 & = & I & \quad & \sigma_x & = & X \\ \sigma_y & = & Y & & \sigma_z & = & Z \end{array}$$

Observe that, taking into account how the product between Pauli matrices work, we can quickly verify that a given set of generators commute by making sure that different σ_x, σ_y, σ_z coincide in the same position in distinct pairs M_i and M_j an even number of times. For example, consider the following two generators:

$$\begin{array}{rcl} M_1 & = & I \;\; X \;\; Z \\ M_2 & = & I \;\; Y \;\; X \end{array}$$

They have different σ_x, σ_y, σ_z in both the second and the third position, namely, they have different σ_x, σ_y, σ_z in an even number of positions hence they commute.

One can define a basis for $Q(S)$ by analysing the coefficients of an arbitrary vector of $Q(S)$. Let the family $\{\varphi_i\}$ be basis $(\mathbb{C}^2)^{\otimes n}$, namely, all possible vectors $|a_1 a_2 \ldots a_n\rangle$ with $a_i \in \{0,1\}$. Thus, we have 2^n of such vectors. Let $|\psi\rangle$ be an arbitrary vector in $(\mathbb{C}^2)^{\otimes n}$:

$$|\psi\rangle = \sum_{i=1}^{2^n} \alpha_i |\varphi_i\rangle$$

Then

$$|\psi\rangle \in Q(S) \iff M_j |\psi\rangle = +1 |\psi\rangle \iff \quad \forall j \in \{1, \ldots, n-k\}$$

Therefore, we must find the values of the coefficients $\alpha_i \in \mathbb{C}$ such that the above holds. Then the resulting vectors in the linear combination to build $|\psi\rangle$ provide a basis for $Q(S)$. This becomes laborious even for lower n and $n-k$. Luckily, in practise we only need the orthogonal projection P of $Q(S)$ and there is no need to find a basis of $Q(S)$ but we provide the following easy example to illustrate the idea.

Example 2.1. Let $n = 2$ and let S bi an abelian subgroup of $\mathcal{P}_n$ of size 2 generated by $M = I\ Z$.

Let $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ be a basis of $(\mathbb{C}^2)^{\otimes 2}$. For an arbitrary vector $|\psi\rangle \in (\mathbb{C}^2)^{\otimes 2}$ we have:

$$|\psi\rangle = \alpha_{00} |\varphi_{00}\rangle + \alpha_{01} |\varphi_{01}\rangle + \alpha_{10} |\varphi_{10}\rangle + \alpha_{11} |\varphi_{11}\rangle$$

As commented in previous sections we have

$$\sigma_x |0\rangle = |1\rangle, \sigma_x |1\rangle = |0\rangle, \sigma_z |0\rangle = |0\rangle, \sigma_z |1\rangle = -|1\rangle$$

Therefore

$$M |\psi\rangle = \alpha_{00} |\varphi_{10}\rangle - \alpha_{01} |\varphi_{11}\rangle + \alpha_{10} |\varphi_{00}\rangle - \alpha_{11} |\varphi_{01}\rangle$$

Finally we request $M |\psi\rangle = |\psi\rangle$ which it is fulfilled if and only if $\alpha_{00} = \alpha_{10}$ and $\alpha_{01} = -\alpha_{11}$.

Therefore any vector in $Q(S)$ must have the form:

$$|\psi\rangle = \alpha_{00}(|00\rangle + |10\rangle) + \alpha_{01}(|01\rangle + |11\rangle)$$

Thus, a basis of $Q(S)$ is $\{|00\rangle + |10\rangle, |01\rangle + |11\rangle\}$ and so $dim\, Q(S) = 2$.

2.2 Dimension

By Lemma 1.4 given an orthonormal basis $\{|\psi_i\rangle\}$ of the subspace $Q(S)$ the orthogonal projection P onto $Q(S)$ is

$$P = \sum_i |\psi_i\rangle \langle\psi_i|$$

and by Lemma 1.5 any linear hermitian operator P fulfilling

$$P^2 = P \text{ and } P|\psi\rangle \in Q \text{ for all } |\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$$

is the orthogonal projection onto $Q(S)$

Lemma 2.2. *Let E be an arbitrary element of S. The orthogonal projection $P = P(S)$ onto $Q(S)$ is*

$$P = \frac{1}{|S|}\sum_{E\in S} E$$

Proof. Let M be an arbitrary element of S. Then:

$$MP = PM = \frac{1}{|S|}\sum_{E\in S} EM = \frac{1}{|S|}\sum_{M\in S} M = P$$

where we use the fact that EM is another arbitrary element of S so we relabel it as M.

Suppose that $|\psi\rangle \in Q(S)$. Then $P|\psi\rangle = |\psi\rangle$ and therefore $|\psi\rangle \in Im(P)$.

Now the backward implication, if $P|\theta\rangle = |\psi\rangle$, namely, $|\psi\rangle \in Im(P)$, then for all $M \in S$

$$M|\psi\rangle = MP|\theta\rangle = P|\theta\rangle = |\psi\rangle$$

hence $|\psi\rangle \in Q(S)$ and therefore $Q(S) = Im(P)$.

The Pauli matrices are hermitian ($\sigma_i^\dagger = \sigma_i$) and $E = \prod \otimes\sigma_i$ hence $E^\dagger = E$ for all $E \in \mathcal{P}_n$ which implies $P^\dagger = P$. Furthermore

$$P^2 = P\frac{1}{|S|}\sum_{E\in S} E = \frac{1}{|S|}\sum_{E\in S} PE = \frac{1}{|S|}\sum_{E\in S} E = P$$

Therefore, by Lemma 1.5 $P = P(S)$ is the orthogonal projector onto $Q(S)$. □

Theorem 2.3. *Let $S\mathcal{P}_n$ be an abelian group of size 2^{n-k}. Then the subspace $Q(S)$ has dimension 2^k.*

Proof. By Lemma 2.2 the orthogonal projection onto $Q(S)$ is

$$P = \frac{1}{|S|}\sum_{M\in S} M$$

Then $P|\psi\rangle \in Q(S)$ for all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, namely, the image of P is its $+1$-eigenspace and also $Q(S)$.

P is hermitian hence diagonalitzable. Since P is idempotent ($P^2 = P$) its eigenvalues are 0 and/or 1 because if $P|\psi\rangle = \lambda|\psi\rangle$ then

$$P^2|\psi\rangle = P(P|\psi\rangle) = \lambda P|\psi\rangle = \lambda^2|\psi\rangle$$

The trace of P is equal to the sum of its eigenvalues which in the case of P is the dimension of the $+1$-eigenspace hence

$$Dim\ Q(S) = Tr\ P(S)$$

Observe that

$$tr(\sigma_1 \otimes ... \otimes \sigma_n) = tr(\sigma_1) ... \sigma_n)$$

hence for all $M \in \mathcal{P}_n \setminus \pm\mathbb{I}$ with phase ± 1 we have $tr(M) = 0$ because $tr(\sigma_x) = tr(\sigma_y) = tr(\sigma_z) = 0$ while $tr(\mathbb{I}) = 2^n$ because $tr(\sigma_0) = 2$.

Finally,

$$Dim\ Q(S) = Tr\ P(S) = \frac{1}{|S|} \sum_{M \in S} tr(M) = \frac{1}{2^{n-k}} 2^n = 2^k$$

□

2.3 Minimum Distance

Let Cent(S) denote the centralizer of S, namely, all elements of $\mathcal{P}_n$ which commute with all elements of S. Thus

$$\text{Cent}(S) = \{x \in \mathcal{P}_n : xy = yx\ ,\ \forall y \in S\}$$

Note that $S \subseteq \text{Cent}(S) \subset \mathcal{P}_n$.

Lemma 2.4. *If we encode with $Q(S)$ then $E \in \mathcal{P}_n$ is an undetectable error if and only if $E \in Cent(S) \setminus S$.*

Proof. We seek for contradiction.

($\Rightarrow$) Suppose $E \in \mathcal{P}_n$ is undetectable but $E \notin \text{Cent}(S) \setminus S$. $EM = \pm ME$ for any pair of elements $E, M \in \mathcal{P}_n$ hence $E \notin \text{Cent}(S)$ then $EM = -ME$ for some $M \in S$.

Let $|\psi\rangle, |\theta\rangle \in Q(S)$. Then $M|\psi\rangle = |\psi\rangle$ and $M|\theta\rangle = |\theta\rangle$ for all $M \in S$. Also let $\langle\psi|\theta\rangle = 0$. Then

$$\langle\psi|E|\theta\rangle = \langle\psi|ME|\theta\rangle = -\langle\psi|EM|\theta\rangle = -\langle\psi|E|\theta\rangle$$

Therefore $\langle\psi|E|\theta\rangle = 0$ which implies that the error E preserves the orthogonality between states, namely, $|\psi\rangle \perp E|\theta\rangle$. Finally, by Theorem 1.9 E is detectable which contradicts the initial assumption.

($\Leftarrow$) Suppose $E \in \mathcal{P}_n$ is detectable but $E \in \text{Cent}(S) \setminus S$. Then for any $|\psi\rangle \in Q(S)$ and $M \in S$ we have $M|\psi\rangle = |\psi\rangle$ and

$$ME|\psi\rangle = EM|\psi\rangle = E|\psi\rangle$$

hence $E|\psi\rangle \in Q(S)$.

We extend $|\psi\rangle$ to an orthonormal basis B of $Q(S)$. The error E is detectable hence

$$\langle\theta|E|\psi\rangle = 0$$

for all $|\theta\rangle \in B \setminus \{\psi\}$. Then $E|\psi\rangle \in (B\{\psi\})^\perp$. The subspace $B\{\psi\})^\perp$ has basis $\{\psi\}$ ($\langle\psi|\theta\rangle = 0$) therefore:

$$E|\psi\rangle = \lambda_\psi |\psi\rangle$$

for some $\lambda_\psi \in \mathbb{C}$ hence $|\psi\rangle$ is an eigenvector of E.

By Theorem 1.9

$$\langle\theta|E|\theta\rangle = \lambda_E$$

for all $\theta \in B$. Recall that $\langle\psi|\psi\rangle = \langle\theta|\theta\rangle = 1$ therefore the above implies $\lambda_\psi = \lambda_E$.

We can apply the same argument for $|\psi\rangle$ over all $|\theta\rangle \in Q(S)$. Thus, for all $|\theta\rangle \in Q(S)$, since $E \notin S$ and $\lambda_E \neq 1$, we have

$$E\,|\theta\rangle = \lambda_E\,|\lambda\rangle$$

The subgroup generated by S and $\lambda_E^{-1}E$ defines a smaller stabilizer code hence there is a $|\psi\rangle \in Q(S)$ such that

$$\lambda_E^{-1}E\,|\psi\rangle \neq |\psi\rangle$$

contradicting the above. Hence, E is not detectable. □

Next we wonder which errors are not only detectable but also correctable. The following definition is justified in Theorem 2.6.

Definition 2.5. The minimum distance d of $Q(S)$ is defined as:

(i) $k > 0 \to d := \min\{wt(E) : E \in \text{Cent}(S) \setminus S\}$

(ii) $k = 0 \to d := \min\{wt(E) : E \in S \setminus \mathbb{I}\}$

Thus for $k > 0$ the minimum distance of $Q(S)$ is equal to the minimum weight of the undetectable errors of $Q(S)$. If $k = 0$ then $S = \text{Cent}(S)$ and $Dim\ Q(S) = 1$ hence $Q(S)$ can not store quantum information but the subgroups of S are still of interest.

Let $\mathcal{E}_d$ denote the set of elements of $\mathcal{P}_n$ with weight at most $\lfloor(d-1)/2\rfloor$

$$\mathcal{E}_d = \{E \in \mathcal{P}_n \mid wt(E) \leq \lfloor(d-1)/2\rfloor\}$$

Theorem 2.6. *Let $Q(S)$ be a stabilizer code with $k \geq 1$. The minimum weight of Cent$(S) \setminus S$ is equal to d if and only if there is a recovery map which corrects all errors in $\mathcal{E}_d$ when encoding with $Q(S)$.*

Proof. ($\Rightarrow$) Suppose $E_i, E_j \in \mathcal{E}_d$. Then both E_i and E_j have weight at most $(d-1)/2$ hence $E = E_iE_j$ has weight at most $d-1$. But the elements of Cent$(S) \setminus S$ have weight at least d therefore

$$E \notin \text{Cent}(S) \setminus S$$

Recall that $E \notin \text{Cent}(S) \setminus S$ implies there is an element $M \in S$ such that $ME = -EM$ or $E \in S$ which implies $EM = ME$ for all $M \in S$.

The projector onto $Q(S)$ is

$$P = \sum_{i=1}^{2^k} |\psi_i\rangle\langle\psi_i|$$

where $\{|\psi_i\rangle \mid i = 1, \ldots, 2^k\}$ is an orthonormal basis for $Q(S)$. Recall that $M\,|\psi\rangle = +\,|\psi\rangle$ for all $M \in S$ and all $|\psi\rangle \in Q(S)$.

If $E \notin \text{Cent}(S)$ then

$$PE_iE_jP = PEP = \sum_{r,s=1}^{2^k} |\psi_r\rangle \langle\psi_r| E |\psi_s\rangle \langle\psi_s|$$

$$= \sum_{r,s=1}^{2^k} |\psi_r\rangle \langle\psi_r| EM |\psi_s\rangle \langle\psi_s| = -\sum_{r,s=1}^{2^k} |\psi_r\rangle \langle\psi_r| ME |\psi_s\rangle \langle\psi_s| = -PEP$$

which implies $PEP = 0$.

If $E \in S$ then $E|\psi\rangle = +1|\psi\rangle$ for all $|\psi\rangle \in Q(S)$. Thus

$$PE_iE_jP = PEP = \sum_{r,s=1}^{2^k} |\psi_r\rangle \langle\psi_r| E |\psi_s\rangle \langle\psi_s| = \sum_{r,s=1}^{2^k} |\psi_r\rangle \langle\psi_r|\psi_s\rangle \langle\psi_s| = P$$

Therefore in both cases by Theorem 1.9 there is a recovery map.

($\Leftarrow$) We assume there is a recovery map which corrects all errors in $\mathcal{E}_d$. Let $E \in \mathcal{E}_d$ and suppose $E \in \text{Cent}(S) \setminus S$. We want prove that then E is undetectable.

If E is detectable then by Theorem 1.9 we have

$$PEP = \alpha P$$

By Lemma 2.2 the projector onto $Q(S)$ is $P = \frac{1}{|S|}\sum_{M\in S} M$. Thus

$$PEP = EPP = EP = \alpha P$$

Which implies $E \in \text{Cent}(S)$.

The projector P onto $Q(S)$ fulfils $P|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in Q(S)$ hence

$$EP|\psi\rangle = E|\psi\rangle \to \alpha P|\psi\rangle = E|\psi\rangle$$

and therefore

$$\frac{E|\psi\rangle}{\alpha} = |\psi\rangle$$

Thus, E/α takes eigenvalue $+1$ for all $|\psi\rangle \in Q(S)$ which implies E/α is equal to some multiplication of the generators of S. Therefore $E \in S$ which contradicts the initial assumption hence E is undetectable. □

Definition 2.7. An stabilizer code $Q(S)$ is called *impure* if there are elements of S whose weight is less than the minimum distance of $Q(S)$. Otherwise is called *pure*.

A quantum code in $(\mathbb{C}^2)^{\otimes n}$ of dimension K and minimum distance d is denoted by the shorthand notation $((n, K, d))$ while the notation $[\![n, k, d]\!]$ denotes a quantum code of dimension 2^k.

2.4 Syndrome Decoding

Quantum Information is constantly susceptible to errors hence correcting capabilities are fundamental when encoding with qubits. Let $[\![n,k,d]\!]$ be a stabilizer code and let $E \in \mathcal{P}_n$ be an error such that $E \notin \text{Cent}(S) \backslash S$ and $E \in \mathcal{E}_d$, in other words, let E be a correctable error.

Pauli matrices commute or anticommute hence $EM = \pm ME$ for all elements $M \in S$. Consider the set of $M_1, \dots, M_{n-k}$ generators of S. Then $E \in S$ if and only if $EM_i = M_iE$ for all $i \in \{1, \dots, n-k\}$.

If $E \notin S$ then $EM_i = -M_iE$ for some generator M_i of S. One can define a patron of $n-k$ signs $\pm$ where we write $+$ if $M_iE = M_iE$ and $-$ if $M_iE = -M_iE$ and i runs from 1 to $n-k$.

Lemma 2.8. *The patron of signs of the $n-k$ "measurements" M_i over the errors $E \in \mathcal{E}_d$ are all distinct.*

Proof. Let $E, E' \in \mathcal{E}_d$ be two different errors. Assume they are really errors hence $E, E \notin S$ and suppose they return the same patron of signs, namely, for each generator of S they both commute or anti-commute.

Consider the error EE'. Then for any element $M \in S$:

If $EM = ME$ and $E'M = ME'$ then $EE'M = MEE'$.

If $EM = -ME$ and $E'M = -ME'$ then $EE'M = -EME' = MEE'$.

Hence in both cases EE' commutes with any element $M \in S$,namely, $EE' \in \text{Cent}(S) \setminus S$.

The minimum distance is the minimum weight of the elements in $\text{Cent}(S)$ hence

$$w(EE') \geq d$$

On the other hand both $w(E)$ and $w(E')$ are at most $\lfloor \frac{d-1}{2} \rfloor$ hence

$$w(EE') \leq w(E) + w(E') \leq d - 1$$

which it is a contradiction. □

We can identify which error has occurred by computing the following lookup table:

- Compute all possible errors of weight at most $\lfloor (d-1)/2 \rfloor$
- Compute the characteristic patron of $n-k$ signs $\pm$ for each error E.

By lemma 2.8 the patron of signs for each E, called its *syndrome*, is unique hence we can use the above lookup table to identify which error has occurred and correct it. An important remark is that when we perform the "measurement" M_i over the received state $E|\psi\rangle$ ($|\psi\rangle \in Q(S)$) we obtain

$$M_iE|\psi\rangle = \pm EM_i|\psi\rangle = \pm E|\psi\rangle$$

Therefore we really do not modify the information received when measuring with M_i.

Example 2.9. Consider the code $[\![5,1,3]\!]$ generated by:

$$\begin{array}{rccccc} M_1 = & X & Z & Z & I & X \\ M_2 = & Z & X & I & Z & X \\ M_3 = & I & Z & X & Z & Y \\ M_4 = & Z & I & Z & X & Y \end{array}$$

It can correct all errors $E \in \mathcal{P}_n$ with $wt(E) \leq \lfloor (d-1)/2 \rfloor = 1$ hence its corresponding lookup table is:

	M_1	M_2	M_3	M_4		M_1	M_2	M_3	M_4		M_1	M_2	M_3	M_4
XIIII	+	−	+	−	*ZIIII*	−	+	+	+	*YIIII*	−	−	+	−
IXIII	−	+	−	+	*IZIII*	+	−	+	+	*IYIII*	−	−	−	+
IIXII	−	+	+	−	*IIZII*	+	+	−	+	*IIYII*	−	+	−	−
IIIXI	+	−	−	+	*IIIZI*	+	+	+	−	*IIIYI*	+	−	−	−
IIIIX	+	+	−	−	*IIIIZ*	−	−	−	−	*IIIIY*	−	−	+	+

2.5 Transformation to Linear Codes

As already commented stabilizer codes are efficiently described thanks to their connection with classical linear codes. This section is devoted to such transformation of the subspace $Q(S)$ of $(\mathbb{C}^2)^{\otimes n}$ into classical linear codes $\{0,1\}^{2n}$.

Let τ be a map between Pauli matrices and the finite field of 2 elements:

$$\tau : \ \{\sigma_0, \sigma_x, \sigma_y, \sigma_z\} \longrightarrow \mathbb{F}_2^2$$

such that

$$\tau : \ \sigma_0 \rightarrow (0|0) \quad ; \quad \tau : \ \sigma_x \rightarrow (1|0) \quad ; \quad \tau : \ \sigma_z \rightarrow (0|1) \quad ; \quad \tau : \ \sigma_y \rightarrow (1|1)$$

We extend τ to $\mathcal{P}_n$ by applying τ to each element of $\mathcal{P}_n$ componentwise so the Pauli matrix in the i-th position is mapped to the i-th and $i+n$-th coordinates of the resulting vector. For example:

$$\tau(\sigma_x \otimes \sigma_0 \otimes \sigma_z) \longrightarrow (100|001)$$

where the line $|$ between the n-th and the $n+1$-th coordinates is added only for readability sake.

The function τ is defined as a quotient respect to the possible phases $\lambda = \{\pm 1, \pm i\}$ of the elements in $\mathcal{P}_n$, namely, $\tau(\lambda M) = \tau(M)$.

Lemma 2.10. *for all $M, N \in \mathcal{P}_n$ it holds*

$$\tau(MN) = \tau(M) + \tau(N)$$

Proof. The multiplicative structure, up to phase factor, is isomorphic to the additive structure of $\mathbb{F}_2^2$ and, consequently, there is a bijection between the elements of $\mathcal{P}_n \setminus \{\pm 1, \pm i\}$ and $\mathbb{F}_2^{2n}$. □

An an example of the above proof, consider the product $\sigma_x \sigma_y = i\sigma_z$:

$$\tau(\sigma_x \sigma_y) = \tau(i\sigma_z) = \tau(\sigma_z) = (0|1)$$

$$\tau(\sigma_x) + \tau(\sigma_y) = (1|0) + (1,1) = (2|1) \mod 2 = (0|1)$$

Next we wonder how the fact that $S \subset \mathcal{P}_n$ is abelian affects to the corresponding map $\tau(S)$. Observe that Lemma 2.10 implies that S is an abelian subgroup of $\mathcal{P}_n$ if and only if $\tau(S)$ is a subspace of $\mathbb{F}_2^{2n}$. In the above observation we request S to be abelian because if not there is no bijection between S and $\tau(S)$ as the inverse map of $\tau(M) + \tau(N)$ has as image both MN or NM.

Definition 2.11. We define the alternating form of a pair $u, w \in \mathbb{F}_n^{2n}$ as

$$(u, w)_a = \sum_{j=1}^{n} (u_j w_{j+n} - u_{j+n} w_j)$$

Lemma 2.12. *Let $M, N \in \mathcal{P}_n \setminus \{\pm 1, \pm i\}$. Then $MN = NM$ if and only if $(\tau(M), \tau(N))_a = 0$*

Proof. Let $u = \tau(M)$ and $v = \tau(N)$. One can check directly that

$$u_j w_{j+n} - u_{j+n} w_j = 0$$

if and only if the Pauli matrices in the j-th position of both M and N commute. Otherwise

$$u_j w_{j+n} - u_{j+n} w_j = \pm 1$$

Observe that, taking into account how the product between Pauli matrices work, $NM = MN$ if and only if there are an even number of positions such that the Pauli matrices do not commute. This happens if and only if there is an even number of coordinates j such that $u_j w_{j+n} - u_{j+n} w_j = 1$ which implies $(\tau(M), \tau(N))_a = 0$. □

Definition 2.13. Given a subspace C of $\mathbb{F}_2^{2n}$ we define its orthogonal subspace $C^{\perp_a}$ as

$$C^{\perp_a} = \{u \in \mathbb{F}_2^{2n} : (u, w)_a = 0, \forall w \in C\}$$

By Lemmas 2.10 and 2.12 one can easily deduce that $C = \tau(S)$ is always contained in $C^{\perp_a}$. Furthermore

$$C^{\perp_a} = \tau(\mathrm{Cent}(S))$$

Definition 2.14. We define the symplectic weight of a vector $v \in \mathbb{F}_n^{2n}$ as the number of pairs of coordinates i and $i + n$ such that not both are zero. Thus:

$$|\{i \in \{1, \dots, n\} \ : \ (v_i, v_{i+n}) \neq (0, 0)\}|$$

Observe that the weight of any element $M \in S$ is equal to the symplectic weight of $\tau(M)$ because the symplectic weight of $\tau(M)$ is equal to n minus the number σ_0's in M, namely, $w(E)$.

Theorem 2.15. *S is an abelian subgroup of $\mathcal{P}_n$ of size 2^{n-k} if and only if $C = \tau(S)$ is a $(n-k)$-dimensional subspace of $\mathbb{F}_2^{2n}$.*

(i) If $k \geq 1$ then the minimum distance of $Q(S)$ is equal to the minimum symplectic weight of the elements of $C^{\perp_a} \setminus C$.

(ii) If $k = 0$ then the minimum distance of $Q(S)$ is equal to the minimum symplectic weight of the non-zero elements of $C = C^{\perp_a}$.

Proof. By theorem 2.6 for $k \geq 1$ the minimum distance is equal to the minimum weight of the elements in $\mathrm{Cent}(S) \setminus S$. As the minim weight of an element $M \in S$ is equal to the minimum symplectic weight of $\tau(M)$ the theorem follows. For $k = 0$ the minimum distance is defined as the minimum weight of the elements in $S \setminus \mathbb{I}$ and, again, applying τ the theorem follows. □

Given a linear code $C = \tau(S)$ we define its $(n-k) \times 2n$ generator matrix $G(S)$ whose i-th row is $\tau(M_i)$.

Lemma 2.16. *S is an abelian subgroup of $\mathcal{P}_n$ of size 2^{n-k} if and only if the generator matrix $G(S)$ has rank $n - k$.*

Proof. Consider the linear combination of a set of rows G defined by

$$\sum_{j \in J} \alpha_j \tau(M_j)$$

where $\alpha_j = \{0, 1\}$ and $J \subseteq \{1, \dots, n-k\}$. Then

$$\sum_{j \in J} \alpha_j \tau(M_j) = 0;$$

where not all $\alpha_j = 0$ if and only if the rank of G is not $n-k$ which, by Lemma 2.10 this happens if and only if

$$\prod_{j \in J} M_j = \mathbb{I}$$

□

3. The Geometry of Stabilizer Codes

This section is devoted to the equivalence between the group setting $Q(S)$ and some geometric features in an associated projective space. We first briefly present the projective geometry formalism and we summarize the basic results needed. Next we present the geometric equivalence for classical linear codes and finally we extend a similar approach to stabilizer codes.

3.1 Projective Geometry

The aim of projective geometry is to remove the anomaly of the zero vector which it is different from the other vectors since it is contained in any linear subspace. The zero vector is naturally removed by "projecting" from it which results in a quotient of all scalar multiple vectors, namely, two vectors in the same direction become equivalent.

We define the projective space $PG(k-1, q)$ of the vector space $\mathbb{F}_q^k$ by identifying the points of $PG(k-1, q)$ with the lines of $\mathbb{F}_q^k$, the lines of $PG(k-1, q)$ with the planes of $\mathbb{F}_q^k$ and, in general, the $(d-1)$-dimensional subspaces of $PG(k-1, q)$ with the d-dimensional subspaces of $\mathbb{F}_q^k$.

Subspaces in finite projective geometry are understood as the collection of points they contain and their intersection is determined by their corresponding intersection in the vector space. By the shift in the dimension usual geometric properties still hold, for example, two points are joined by a line the intersection of two plains is a line etc. If the intersection of two subspaces is empty then we say they are *skew*, otherwise we say they are *incident*.

The number of set of r linear independent vectors in $\mathbb{F}_q^k$ is

$$(q^k - 1)(q^k - q) \dots (q^k - q^{r-1})$$

This can be easily deduced as follows: Consider all q^k points of $\mathbb{F}_q^k$. We first have freedom to choose any point except 0. Next we can choose any point expect those q multiples of the first point chosen and so on.

The number of $(r-1)$-dimensional subspaces in $PG(k-1,q)$ is

$$\binom{k}{r}_q = \frac{(q^k-1)(q^k-q)\dots(q^k-q^{r-1})}{(q^r-1)(q^r-q)\dots(q^r-q^{r-1})}$$

because the number of $(r-1)$-dimensional subspaces in $PG(k-1,q)$ is precisely the number of r-dimensional subspaces of $\mathbb{F}_q^k$ which can be computed as the number of choices of r linearly independent vectors of $\mathbb{F}_q^k$ divided by the number of sets of r linearly independent vectors of $\mathbb{F}_q^r$.

Applying the q-analog binomial it follows that the that the number of points in $PG(k-1,q)$ is

$$\binom{k}{1}_q = \frac{q^k-1}{q-1} = q^{k-1}+q^{k-2}+\dots+q+1$$

Similar to the standard binomial, its q-analog is also symmetric hence the number of hyperplanes in $PG(k-1,q)$ is, again,

$$\binom{k}{k-1}_q = \binom{k}{1}_q = q^{k-1}+q^{k-2}+\dots+q+1$$

Indeed there is a natural duality between the set of points and the set of hyperplanes by mapping each point $(a_1,\dots,a_k)$ to the hyperplane $a_1X_1+\dots+a_kX_k=0$ and vice versa.

The number of $(r-1)$-dimensional subspaces of $PG(k-1,q)$ containing a fixed $(s-1)$-dimensional subspace is

$$\binom{k-s}{r-s}_q$$

because the quotient $\mathbb{F}_q^k/U$ where U is a s-dimensional subspace of $\mathbb{F}_q^k$ is a $(k-s)$-dimensional vector space. Then a r-dimensional subspace containing U is a $(r-s)$-dimensional subspace in the quotient space and by taking into account the dimension shift of the projective space the result follows.

Setting $s=1$ and $r=2$ we obtain that each point in $PG(k-1,q)$ is incident to $\binom{k-1}{1}_q$ lines. On the other hand, setting $k=2$ and $r=1$ in the binomial q-analog formula we obtain that each line is incident to $\binom{2}{1}_q = q+1$ points. In our particular case of interest, $PG(k-1,2)$, each line is incident to 3 points.

3.2 Classical Linear Codes

A linear code of length n over a finite field $\mathbb{F}_q$ ($q=p^h$,p prime) is a subset $C\subseteq\mathbb{F}_q^n$ such that if $v,w\in C$ and $\lambda,\mu\in\mathbb{F}_q$ then

$$\lambda v+\mu w\in C$$

Thus, C is a subspace of dimension at most n.

The elements of C are called *codewords*. The distance between two codewords in C is defined as the number of coordinates in which they differ and the minimum value between all pairs $u,v\in C$ is called the *minimum distance* of the code C. The *weight* of a codeword of C is defined as its number of non-zero coordinates.

Lemma 1.8 states that if C is a linear code over a finite field $\mathbb{F}_q$ then the minimum distance d of C is equal to its minimum weight.

A k-dimensional linear code C over $\mathbb{F}_q$ of length n and minimum distance d is denoted by $[n,k,d]_q$.

Let G be the $k \times n$ generator matrix of C, namely, a matrix whose k rows form a basis of C. Then for any codeword $u \in C$ there is a row vector $a^t \in \mathbb{F}_q^k$ such that

$$u = a^t G$$

which is nothing else than express $u \in C$ as a linear combination elements of the basis of C. The above expression can be regarded as the encoding through G of the message a into the codeword u of C such that u is ready to be sent over a noisy channel.

The columns of G, which we denote by $\mathcal{X}$, are a multi-set (the columns can be repeated) of n vectors of $\mathbb{F}_q^k$. Let $u = (u_1, \dots u_n) = a^t G$ and let z be the i-th column of G. Then

$$u_i = a \cdot z = a_1 z_1 + \dots + a_k z_k$$

The above implies that the i-th coordinate of u is 0 if and only if z is incident to the kernel of the linear form

$$a_1 X_1 + \dots + a_k X_k$$

This property is unaffected if we replace z by λz where $\lambda \in \mathbb{F}_q \setminus \{0\}$ hence it is natural to consider $\mathcal{X}$ as a multi-set of n points of $PG(k-1,q)$ instead of n vectors in $\mathbb{F}_q^k$.

Theorem 3.1. *An $[n,k,d]_q$ linear code over $\mathbb{F}_q$ is equivalent to a multi-set of points $\mathcal{X}$ in $PG(k-1,q)$ such that:*

(i) Every hyperplane of $PG(k-1,q)$ contains at most $n-d$ points of $\mathcal{X}$.

(ii) Some hyperplane of $PG(k-1,q)$ contains exactly $n-d$ points of $\mathcal{X}$.

Proof. Let G be the generator matrix of the $[n,k,d]_q$ linear code and let $\mathcal{X}$ be the multi-set of columns of G regarded as points in $PG(k-1,q)$.

Let $u = (u_1, \dots, u_n) = a^t G$ and let z be the i-t column of G. Then

$$u_i = 0 \iff \sum_{j=1}^{k} a_j z_j = 0.$$

The above implies that i-th coordinate of u is null if and only if the point $z \in \mathcal{X}$ is incident to the hyperplane π_a (codimension one) in $PG(k-1,q)$

$$a_1 X_1 + \dots + a_k X_k = 0$$

hence the codeword $u = a^t G$ has weight w if and only if $n-w$ coordinates of u are 0, namely, if and only if $n-w$ points of $\mathcal{X}$ are incident to π_a.

By Lemma 1.8 the minimum distance d of a linear code is equal to the minimum weight. Then by the previous argument there is an hyperplane which contains exactly $n-d$ points of $\mathcal{X}$ (his proves (ii)) while all hyperplanes contain at most $n-d$ points of $\mathcal{X}$ (this proves (i)).

□

3.3 The Geometry of Stabilizer Codes

Thanks to their connection to linear codes, quantum stabilizer codes can also be described in geometric terms. We shall show the equivalence between the group setting $Q(S)$ and the geometrical setting $\mathcal{X}$ where $\mathcal{X}$ is a multi-set of lines in $PG(n-k-1,2)$ fulfilling certain condition.

By Theorem 2.15 a stabilizer code $Q(S)$ where $S \subset \mathcal{P}_n$ is an abelian group of size 2^{n-k} is fully equivalent to the $(n-k)-$ dimensional linear code $C = \tau(S)$ of length $2n$ which it is contained in $C^{\perp_a} = \tau(\text{Cent}(S))$.

Given the $(n-k) \times 2n$ generator matrix G of C we construct a multi-set $\mathcal{X}$ of n lines (possibly points) as follows: for each $i \in \{1, \dots, n-k\}$ we span the i-th and $(i+n)$-th column of G in $PG(n-k-1,2)$. Each span results in a point in $PG(n-k-1,2)$ if and only if the i-th and $(i+n)$-th column are either the same vector or at least one is the zero vector. Otherwise the span results in a line in $PG(n-k-1,2)$.

On the other hand, given $\mathcal{X}$, one can identify two points incident to each line (or point) in $\mathcal{X}$ and consider them as the i-th and the $(i+n)$-th column of the Generator matrix G of C. As commented before, each line in $PG(k-1,q)$ is incident to $q+1$ points. In our case $q=2$ hence each line is incident to 3 points and we must choose two points of each line when building G. Indeed this choice is equivalent to invoking an arbitrary permutation between σ_x, σ_y, and σ_z on the i-th component of each $M_1, \dots, M_{n-k}$. Recall that after such a permutation S is still abelian. Therefore we consider equivalent all quantum codes obtained by applying such permutation or, analogous, by choosing different points of the lines to construct G.

Example 3.2. Consider the code $[\![5,0,3]\!]$ generated by

$$\begin{array}{rccccc}
M_1 = & X & Z & I & I & Z \\
M_2 = & Z & X & Z & I & I \\
M_3 = & I & Z & X & Z & I \\
M_4 = & I & I & Z & X & Z \\
M_5 = & Z & I & I & Z & X
\end{array}$$

Its generator matrix

$$G = \left(\begin{array}{ccccc|ccccc}
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0
\end{array}\right)$$

Next we apply the permutation $X \to Z$, $Z \to Y$, $Y \to X$ over the first, second and fourth components of $M_1, \dots, M_5$ so we get the generators:

$$\begin{array}{rccccc}
M_1' = & Z & Y & I & I & Z \\
M_2' = & Y & Z & Z & I & I \\
M_3' = & I & Y & X & Y & I \\
M_4' = & I & I & Z & Z & Z \\
M_5' = & Y & I & I & Y & X
\end{array}$$

Applying τ to M_i' we construct the generator matrix

$$G' = \left(\begin{array}{ccccc|ccccc}
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0
\end{array}\right)$$

Let e_i be the i-th element of the canonical basis of $\mathbb{F}_2^5$ and regard the columns of G an G' in terms of such basis. Then the quantum set of lines $\mathcal{X}$ and $\mathcal{X}'$ is

$$\mathcal{X} = \{\langle e_1, e_2 + e_5\rangle, \langle e_2, e_1 + e_3\rangle, \langle e_3, e_2 + e_4\rangle, \langle e_4, e_3 + e_5, \rangle, \langle e_5, e_1 + e_4\rangle\}$$

$$\mathcal{X}' = \{\langle e_2 + e_5, e_1 + e_2 + e_5\rangle, \langle e_1 + e_3, e_1 + e_2 + e_3\rangle, \langle e_3, e_2 + e_4, \rangle, \langle e_3 + e_5, e_3 + e_4 + e_5\rangle, \langle e_5, e_1 + e_4\rangle\}$$

where $\langle e_i, e_j\rangle$ denote the line incident to the points e_i and e_j. One can check that the rows of G span the same subspace C as the rows G'. Thus, they represent the same stabilizer code and the quantum set of lines remains unchanged.

It is also possible to choose the phase ± 1 of M. We set up the phase be always 1 however when building non additive quantum codes the freedom on the phase will become crucial.

Lemma 3.3. *The i-th and $i + n$-th columns of the generator matrix G span a line (instead of a point) of $PG(n - k - 1, 2)$ for all $i \in \{1, \dots, n\}$ if and only if the minimum weight of $Cent(S)$ is at least 2.*

Proof. The span of the i-th and $(i + n)$-th column of G results on a point in $PG(n - k - 1, 2)$ if and only if the i-th and $(i + n)$-th column are either the same vector or at least one is the zero vector. This occurs if and only if the i-th component of all generators of S are the same Pauli matrix: if the i-th component of all generators of S is $\sigma = \sigma_0$ then the columns C_i and C_{i+n} of G are both the zero vector. If $\sigma = \sigma_x$ or $\sigma = \sigma_z$ then one the two columns C_i and C_{i+n} is the zero vector. If $\sigma = \sigma_y$ then both columns C_i and C_{i+n} are the vector with all entries equal to 1.

Suppose that the i-th component of all generators of S is the same Pauli matrix . If $\sigma_0 = \sigma_0$ we can delete that component such that the length of the code decreases to $n - 1$ without affecting its error correcting properties. Consider $\sigma \in \{\sigma_x, \sigma_y, \sigma_z\}$. Then there is an element $E \in \mathcal{P}_n$ such that all its components are equal to σ_0 except the i-th component which it is σ. Clearly this element is in Cent(S) and has weight 1. □

Let d be the minimum distance of $Q(S)$, namely, equal to the minimum weight of Cent$(S) \setminus S$. If the code is pure $(min\{w(S)\} \geq d)$ then the condition $min\{w(\text{Cent}(S))\} \geq 2$ in Lemma 3.3 can be replaced by $d \geq 2$. If the code is impure this replacement is not necessarily true.

The following theorem states the equivalence between the group setting $Q(S)$ and the geometrical setting $\mathcal{X}$ where $\mathcal{X}$ is a multi-set of lines in $PG(n - k - 1, 2)$ fulfilling certain conditions.

Theorem 3.4. *There is an $[\![n, k, d]\!]$ stabilizer code $Q(S)$ where S is an abelian subgroup of $\mathcal{P}_n$ of size 2^{n-k} such that $min\{w(Cent(S))\} \geq 2$ if and only if there is a multi-set of n lines (not points) $\mathcal{X}$ spanning $PG(n - k - 1, 2)$ such that every codimension 2 subspace is skew to an even number of lines in $\mathcal{X}$.*

Proof. (⇒)

$C^{\perp_a}$ is defined in 2.13 as

$$C^{\perp_a} = \{u \in \mathbb{F}_2^{2n} : (u, w)_a = 0, \forall w \in C\}$$

By Lemmas 2.10 and 2.12 one can easily deduce that $C = \tau(S)$ is always contained in $C^{\perp_a} = \tau(\text{Cent}(S))$.

Let $u, w \in C$. Then $u = a^t G$ and $w = b^t G$ for some $a, b \in \mathbb{F}_2^{n-k}$ and

$$(u, w)_a = \sum_{j=1}^{n} (u_j w_{j+n} - u_{j+n} w_j) = 0$$

Consider a single term j in the above sum. Let $x, y \in \mathbb{F}_2^{n-k}$ be the j-th and the $(j+n)$-th column of G respectively. Since $u, w \in C$ we have

$$u_j = a \cdot x \ ; \ u_{j+n} = a \cdot y \ ; \ w_j = b \cdot x \ ; \ w_{j+n} = b \cdot y$$

Thus,

$$u_j w_{j+n} - u_{j+n} w_j = (a \cdot x)(b \cdot y) - (a \cdot y)(b \cdot x)$$

which it is 0 if and only if the determinant of

$$\begin{pmatrix} a \cdot x & a \cdot y \\ b \cdot x & b \cdot y \end{pmatrix}$$

is null, namely, the above matrix has rank 1. This implies its rows and columns are not linearly independent and span subspaces of dimension lower than 2 hence there is a pair $\lambda, \mu \in \mathbb{F}_2$ such that

$$\begin{cases} a \cdot (\lambda x + \mu y) = 0 \\ b \cdot (\lambda x + \mu y) = 0 \end{cases}$$

Let π_a denote the hyperplane

$$a \cdot X = a_1 X_1 + ... + a_{n-k} X_{n-k} = 0$$

Recall that all hyperplanes in $PG(n-k-1, 2)$ can be defined as above hence any codimension 2 subspace of $PG(n-k-1, 2)$ can be defined as $\pi_a \cap \pi_b$ for some pair of hyperplanes π_a and π_b.

The above two conditions are equivalent to request that the point $(\lambda x + \mu y) \in \mathbb{F}_2^{n-k}$, which belongs to the line of $\mathcal{X}$ spanned by x and y, is incident to $\pi_a \cap \pi_b$.

Summarizing,

$$(u, w)_a = \sum_{j=1}^{n} (u_j w_{j+n} - u_{j+n} w_j) = 0$$

if and only if there is an even number of terms 1 in the above sum. On the other hand, each line of $\mathcal{X}$ is skew to $\pi_a \cap \pi_b$ for some $a, b \in \mathbb{F}_2^{n-k}$ contribute to the sum with a term 1. Thus, for any codimension 2 subspace $\pi_a \cap \pi_b$ of $PG(n-k-1, 2)$ the number of lines of $\mathcal{X}$ skew to it must be even.

($\Leftarrow$) Let $\mathcal{X}$ be a multi-set of n lines (not points) $\mathcal{X}$ spanning $PG(n-k-1, 2)$ such that every codimension 2 subspace is skew to an even number of lines in $\mathcal{X}$. Let G be the $(n-k) \otimes 2n$ matrix whose i-th and $(i+n)$-th columns are two distinct points spanning the i-th line of $\mathcal{X}$. Let $C = \tau(S)$ be the $(n-k)$-dimensional linear code generated by G.

As proved in the forward implication, if every codimension 2 subspace of $PG(n-k-1, 2)$ is skew to an even number of lines of $\mathcal{X}$ then $(u, w)_a = 0$ for any pair $u, w \in C$. Then $C = \tau(S)$ is contained in $C^{\perp_a} = \tau(\text{Cent}(S))$ and by Lemma 2.16 this implies S is an abelian subgroup of $\mathcal{P}_n$ of size 2^{n-k}.

□

Definition 3.5. A *quantum set of lines* is defined as a multi-set of n lines (not points) $\mathcal{X}$ spanning $PG(n-k-1, 2)$ such that every codimension 2 subspace is skew to an even number of lines in $\mathcal{X}$.

Remark. By Lemma 3.3 and Theorem 3.4 $\mathcal{X}$ the condition $min\{w(\text{Cent}(S))\} \geq 2$ grants there is a quantum set of lines characterizing a stabilizer code $Q(S)$.

A set of r points are called *independent* if they span a $(r-1)$- dimensional subspace, otherwise they are called *dependent*. For example, 4 points on a plane are dependent while if we remove one point the remaining 3 become independent. The following geometric definition of the minimum distance $d(\mathcal{X})$ together with its remark is justified in Theorem 3.7.

Definition 3.6. The minimum distance $d(\mathcal{X})$ of the code characterized by the quantum set of lines $\mathcal{X}$ is defined as the minimum number of dependent points that can be found in distinct lines of $\mathcal{X}$.

Remark. If $k \geq 0$ we must not taken into account the dependencies for which there is an hyperplane of $PG(n-k-1,2)$ which both contains all dependent points and also all lines of $\mathcal{X}$ not incident to the dependent points. If $k=0$ then $d(\mathcal{X})$ can be equivalently defined as the minimum positive integer d such that there is an hyperplane of $PG(n-k-1,2)$ which contains $n-d$ lines of $\mathcal{X}$.

If two lines of $\mathcal{X}$ are incident in the same point p (or even they are the same line) then p is considered "dependent with itself". Thus, the minimum set of dependent points in distinct lines is p two times because the set has size two while spans a 0-dimensional subspace. If $k=0$ then $d(\mathcal{X})=2$. If $k \geq 1$ we first must check the exceptions in the dependencies noted on the above remark.

Theorem 3.7. *There is an* $[\![n,k,d]\!]$ *stabilizer code* $Q(S)$ *where* $min\{w(Cent(S))\} \geq 2$ *if and only if there is a quantum set of lines* $\mathcal{X}$ *spanning* $PG(n-k-1,2)$ *and such that* $d = d(\mathcal{X})$.

Proof. By Theorem 3.4 the equivalence between $Q(S)$ with $min\{w(\text{Cent}(S))\} \geq 2$ and the quantum set of lines $\mathcal{X}$ spanning $PG(n-k-1,2)$ is already granted hence it only remains to prove that the minimum distance d of $Q(S)$ follows the definition 3.6 and its remark. Let G be the generator matrix of $C=\tau(S)$ and let $\mathcal{X}$ be the set of n lines where the line l_j is spanned by the j-th and $(j+n)$-th column of G.

$\underline{\underline{k \geq 1}}$:

By Theorem 2.15 the minimum distance d is equal to the minimum symplectic weight of $C^{\perp_a} \setminus C$. Let $v \in C^{\perp_a}$ be a vector of $\mathbb{F}_2^{2n}$ of symplectic weight w and let W be the set of coordinates which contribute to its weight. Thus,

$$W = \{j \in \{1,\dots,n\} : (v_j, v_{j+n}) \neq (0,0)\} \; ; \; |W| = w$$

Let $u=(u_1,\dots,u_{2n})$ be an arbitrary vector of C. Then $u=a^tG$ for some $a \in \mathbb{F}_2^{n-k}$ and $u_j = a \cdot x_j$ where $x_j \in \mathbb{F}_2^{n-k}$ is the j-th column of G and $j \in \{1,\dots,2n\}$. Since $v=(v_1,\dots,v_{2n}) \in C^{\perp_a}$ then $(v,u)_a = 0$ for all $u \in C$ hence

$$\sum_{j \in W} (x_j v_{j+n} - x_{j+n} v_j) = 0$$

Each term in the above sum correspond to some point of the line l_j therefore there are $w=|W|$ points on distinct lines $\{l_j : j \in W\}$ which are dependent which are dependent. But the minimum distance d is equal to the minimum symplectic weight of $C^{\perp_a} \setminus C$ hence if $v \in C$ we must disregard this dependency. Observe that $v \in C$ if and only if $v = a^tG$ for some $a \in \mathbb{F}_2^{n-k}$ hence $v_j = a \cdot x_j$ for all $j \in \{1,\dots,2n\}$.

Consider the coordinates $j \notin W$ of v, namely, the coordinates which do not contribute to the symplectic weight. For each $j \notin W$ we have

$$v_j = a \cdot x_j = 0 \text{ and } v_{n+j} = a \cdot x_{n+j} = 0$$

if and only if the line l_j is contained in the hyperplane π_a defined by $a \cdot X = 0$. Thus, the lines $\{l_j : j \notin W\}$ are contained in π_a.

Next Consider the coordinates $j \in W$ of v, namely, the coordinates which do contribute to the symplectic weight. Then since $v_j = a \cdot x_j$ and $v_{j+n} = a \cdot x_{j+n}$ we have

$$a \cdot (v_{n+j}x_j - x_{n+j}v_j) = v_{n+j}(a_j) - v_j(a \cdot x_{n+j}) = v_{n+j}v_j - v_jv_{n+j} = 0$$

therefore the dependent points are also contained in π_a.

Thus, the definition of the minimum distance $d(\mathcal{X})$ in 3.6 is justified through the light of this proof.

$\underline{\underline{k = 0}}$:

By Theorem 2.15 the minimum distance d is equal to the minimum symplectic weight of $C = C^{\perp_a}$. Let $v \in C$, then $v = a^tG$ for some $a^t \in \mathbb{F}_2^{n-k}$ hence $v_j = a \cdot x_j$ where x_j is the j-th column of G and $j \in \{1, \dots, 2n\}$.

Suppose v is the element of C with minimum weight and let W be the set of coordinates that contribute to the symplectic weight of v. Thus,

$$W = \{j \in \{1, \dots, n\} : (v_j, v_{j+n}) \neq (0,0)\} \ ; \ |W| = d$$

Then for all $j \notin W$ we have

$$a \cdot x_j = 0 \text{ and } a \cdot x_{n+j} = 0$$

which it is equivalent to the line $l_j \in \mathcal{X}$ being contained in π_a. Therefore there is a hyperplane of $PG(n-k-1, 2)$ containing $n-d$ lines of $\mathcal{X}$ which coincides with the definition of $d(\mathcal{X})$ in 3.6. Equivalently, similar to the case $k \geq 0$ a vector $v \in C^{\perp_a}$ of symplectic weight d implies a dependency of d points of distinct lines of $\mathcal{X}$, which coincides with the definition of $d(\mathcal{X})$ in 3.6. □

Example 3.8. Consider the $[\![9, 1, 3]\!]$ code (Shor Code) which has generator matrix

$$G_{\,8\times18} = \left(\begin{array}{ccccccccc|ccccccccc}
0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0
\end{array}\right)$$

Observe that S contains elements of weight 2, for example, the first row $\tau(M_1)$ of G has symplectic weight 2 hence $M_1 \in S$ has weight 2. Since the minimum distance is 3 the shore code is impure.

Let e_i be the i-th element of the canonical basis of $\mathbb{F}_2^8$. The i-th and $(i+n)$-th columns of G with $i \in \{1, \dots, 2n\}$ span the 9 quantum set of lines

$$\mathcal{X} = \{\langle e_1, e_7\rangle, \langle e_1{+}e_2, e_7\rangle, \langle e_2, e_7\rangle, \langle e_3, e_7{+}e_8\rangle, \langle e_3{+}e_4, e_7{+}e_8\rangle, \langle e_4, e_7{+}e_8\rangle, \langle e_5, e_8\rangle, \langle e_5{+}e_6, e_8\rangle, \langle e_6, e_8\rangle\}$$

where $\langle e_i, e_j\rangle$ denotes the line incident to the points e_i and e_j.

The point e_7 is incident to the first two lines hence, as detailed previously, e_7 is "dependent with itself". It seems that $d(\mathcal{X}) = 2$ but as $k \geq 1$ we first must check the exceptions in the dependencies of the definition of $d(\mathcal{X})$.

Observe that the remaining 7 lines span a six dimensional subspace since the two planes $\langle e_3, e_4, e_7 + e_8\rangle$ and $\langle e_5, e_6, e_8\rangle$ span a five dimensional subspace while the line $\langle e_2, e_7\rangle$ spans an independent one dimensional subspace. Recall that e_7 belongs to this line $\langle e_2, e_7 \rangle$ hence this 6 dimensional subspace is an hyperplane of $PG(7,2)$ both containing all dependent points (e_7) and containing all lines not incident to the dependent points (the 7 lines commented above). Thus, we do not count this dependency on e_7. Finally, the dependency of the points $\{e_1, e_2, e_1 + e_2\}$ imply $d(\mathcal{X}) = 3$.

4. Non additive quantum codes

In this section we present a new kind of codes called non additive quantum codes which are constructed as direct sums of subspaces representing stabilizer codes. We provide a general geometric framework for such constructions which appears to be new and, similar to stabilizer codes, we provide an equivalence between the group setting and the geometric setting. Furthermore, we show how stabilizer codes can be regarded themselves as direct sums under certain conditions. Finally, we explore some examples and concrete results.

4.1 Construction

As previously detailed a $[\![n,k,d]\!]$ stabilizer code is characterized by an abelian group $S = \langle M_1, \dots, M_{n-k} \rangle \subset P_n$ of size 2^{n-k} where the subspace $Q(S)$ is defined as the joint $+1$-eigenspace of all elements of S. Thus,

$$M_i \left|\psi\right\rangle = +1 \left|\psi\right\rangle \text{ for all } \left|\psi\right\rangle \in Q(S) \text{ and } i \in \{1, \dots, n-k\}$$

Two major results are that $\mathrm{Dim}(Q(S)) = 2^k$ (Theorem 2.3) and that the undetectable errors for $Q(S)$ belong to $\mathrm{Cent}(S) \setminus S$ (Lemma 2.4). Finally, Theorem 2.6 states that the minimum distance d of $Q(S)$ is equal to the minimum weight of $\mathrm{Cent}(S) \setminus S$ for $k \neq 0$ while it is equal to the minimum weight of S for $k = 0$. Summarizing, an $[\![n,k,d]\!]$ stabilizer code encodes k logical qubits in n physical qubits such that there is a recovery map which is able to correct all errors in

$$\mathcal{E}_d = \{E_i \in \mathcal{P}_n \mid wt(E_i) \leq \lfloor (d-1)/2 \rfloor\}$$

As commented previously, when working with stabilizer codes we always request $-\mathbb{I} \notin S$ because $-\mathbb{I}\left|v\right\rangle = +1\left|v\right\rangle$ implies $\left|v\right\rangle = 0$ hence the resulting joint $(+1)$-eigenspace $Q(S)$ the zero vector. Also if $M_i = \pm i\sigma_1 \otimes \cdots \otimes \sigma_n$ then $M_i^2 = -\mathbb{I} \in S$ and again $Q(S) = \{0\}$. Hence each generator M_i must have overall phase ± 1 and never $\pm i$.

We define the element $t = (t_1, \dots, t_{n-k}) \in \mathbb{F}_2^{n-k}$. Different from stabilizer codes where we assume all elements of S have phase 1 we now let the generators of S have overall phase ± 1 or, equivalently, to take eigenvalues ± 1. We fix the eigenvalues of $(-1)^{t_i} M_i$ to $+1$ as follows:

- If $t_i = 0$ then $M_i \left|v_i\right\rangle = +1 \left|v_i\right\rangle$ hence $(-1)^{t_i} M_i \left|v_i\right\rangle = +1 \left|v_i\right\rangle$.
- If $t_i = 1$ then $M_i \left|v_i\right\rangle = -1 \left|v_i\right\rangle$ hence $(-1)^{t_i} M_i \left|v_i\right\rangle = +1 \left|v_i\right\rangle$.

Definition 4.1. Let $T \subseteq \mathbb{F}_2^{n-k}$. For a given $t \in T$ we define the stabilizer code

$$Q_t(S)$$

as the joint $+1$-eigenspace of $(-1)^{t_i} M_i$ for all $i \in \{1, \dots, n-k\}$.

Effectively, $Q_t(S)$ is a stabilizer code too because despite now the generators can take eigenvalues ± 1 the resulting subspace is still the joint $+1$-eigenspace of $(-1)^{t_i} M_i$ with $i \in \{1, \dots, n-k\}$ hence the proof that $Q_t(S)$ has dimension 2^k is mimetic to the proof of Theorem 2.3 for $Q(S)$.

Lemma 4.2. *Let $Q(S)$ be a stabilizer code and let t and u be two distinct elements of $\mathbb{F}_2^{n-k}$. Then the subspaces $Q_t(S)$ and $Q_u(S)$ are orthogonal.*

Proof. If $t \neq u$ then $t_j \neq u_j$ for at least one $j \in \{1, \dots, n-k\}$. Without lost of generality suppose they differ in the first coordinate hence $t_j = 1$ and $u_j = 0$ which implies $M_j |\psi^t\rangle = -|\psi^t\rangle$ for all $|\psi^t\rangle \in Q_t(S)$ and $M_j |\psi^u\rangle = +|\psi^u\rangle$ for all $|\psi^u\rangle \in Q_u(S)$. Then

$$\langle \psi^t | \psi^u \rangle = \langle \psi^t | M_j | \psi^u \rangle = -\langle \psi^t | \psi^u \rangle = 0$$

Therefore $Q_t(S)$ and $Q_u(S)$ are orthogonal. □

Choosing $u = 0$ in Lemma 4.2 we get $Q_u(S) = Q(S)$ hence note that by simply switching the eigenvalue of at least one M_i we obtain a subspace $Q_t(S)$ orthogonal to $Q(S)$.

Let H and K be subspaces of a vector space V such that $H \cap K = \emptyset$. The direct sum $H \oplus K$, which it is the smallest vector space containing both subspaces H and V, is defined as the componentwise operation:

$$H \oplus K = \{w + v : w \in H; v \in K\}$$

where $H \oplus K \subseteq V$, $Dim(H) + Dim(K) = Dim(H \oplus K)$ and if the vector sets B_H and B_K are basis of H and K respectively then $B_H \cup B_K$ is a basis of $H \oplus K$.

Definition 4.3. Let $T \subset \mathbb{F}_2^{n-k}$. We define

$$Q(S, T) = \bigoplus_{t \in T} Q_t(S)$$

as the direct sum of orthogonal subspaces $Q_t(S)$ for each distinct $t \in T$.

Let $t, u \in T \setminus \{0\}$ with $t \neq u$ and let $A_{t,u}$ be a $(n-k) \times (n-k)$ non-singular matrix whose first two columns are t and u. We don't apply any constrain on the other columns of $A_{t,u}$ rather than the requirement that the whole set of $n-k$ columns must be linearly independent. Thus $A_{t,u}$ is a change of basis operator.

Let G be the generator matrix of the code C whose i-th row is $\tau(M_i)$. Then $A_{t,u}^{-1} G$ is another generator matrix for C i.e. the rows of $A_{t,u}^{-1} G$ are another basis for C and we can find another set

$$\{M_i' : i = 1, \dots, n-k\}$$

of generators of S where $\tau(M_i')$ is the i-th row of $A_{t,u}^{-1} G$.

Lemma 4.4. *Let $t, u \in T \setminus \{0\}$ and let $|\psi^t\rangle \in Q_t(S)$ and $|\psi^u\rangle \in Q_u(S)$. Then:*

(i) $M_1' |\psi^t\rangle = -|\psi^t\rangle$ *and* $M_i' |\psi^t\rangle = +|\psi^t\rangle$ *for* $i = \{2, 3, 4, \dots, n-k\}$

(ii) $M_2' |\psi^u\rangle = -|\psi^u\rangle$ *and* $M_i' |\psi^u\rangle = +|\psi^u\rangle$ *for* $i = \{1, 3, 4, \dots, n-k\}$

Proof. $Q_t(S)$ and $Q_u(S)$ depend on the parameters t and u given and the set of generators M_i of S chosen. By applying the change of basis $A_{t,u}$ where its first and second columns are precisely t and u the set M_i is re-expressed as the set M_i' while t an u are re-expressed as $(1,0,0,\dots,0)$ and $(0,1,0,\dots,0)$. Therefore in the new basis the eigenvalues of M_i' over $Q_t(S)$ and $Q_u(S)$ are parameterized by $(1,0,0,\dots,0)$ and $(0,1,0,\dots,0)$, thus, they follow (i) and (ii). □

Lemma 4.4 requires a moment thought. The i-th row of G is $\tau(M_i)$ and the function τ fulfills

$$\tau(M_i)+\tau(M_j)=\tau(M_iM_j)$$

Thus, to sum rows of G, which are a basis of C, is equivalent to multiply generators of S hence to change the basis of the generator matrix G is nothing else than to find an alternative generator set of S. Therefore Lemma 4.4 simply shows that after applying a convenient change of basis we can find a new generator set $M_1',\dots,M_{n-k}'$ such that t and u become elements of the canonical basis i.e. The M_i' have their eigenvalues parameterized by e_1 and e_2. The latter will be extremely useful in the next section to simplify computations when projecting the quantum set of lines $\mathcal{X}$ through the points t and u.

Example 4.5. We shall explicitly check Lemma 4.4 over the code $[\![5,0,3]\!]$. Its generator matrix is:

$$G=\left(\begin{array}{ccccc|ccccc}1&0&0&1&1&0&0&0&1&1\\0&1&0&0&1&0&0&1&0&1\\0&0&1&1&0&0&0&1&0&1\\0&0&0&0&0&1&0&1&1&0\\0&0&0&0&0&0&1&1&1&1\end{array}\right)$$

Suppose that the eigenvalues of the generators of S are parametrizated by the following two elements of $\mathbb{F}_2^5$:

$$t=(1,0,1,1,1)\ ;\ \ u=(0,0,1,1,0)$$

We construct the non-singular 5×5 matrix $A_{t,u}$ whose first and second columns are t and u and the whole set of columns are linearly independent such that $A_{t,u}$ is a change of basis. Thus, our choice for $A_{t,u}$ is:

$$A_{t,u}=\begin{pmatrix}1&0&0&1&1\\0&0&0&1&1\\1&1&0&0&0\\1&1&0&1&0\\1&0&1&1&1\end{pmatrix}\quad ;\quad A_{t,u}^{-1}=\begin{pmatrix}1&1&0&0&0\\1&1&1&0&0\\1&0&0&0&1\\0&0&1&1&0\\0&1&1&1&0\end{pmatrix}$$

Therefore

$$A_{t,u}^{-1}G=\left(\begin{array}{ccccc|ccccc}1&1&0&1&0&0&0&1&1&0\\1&1&1&0&0&0&0&0&1&1\\1&0&0&1&1&0&1&1&0&0\\0&0&1&1&0&1&0&0&1&1\\0&1&1&1&1&1&0&1&1&0\end{array}\right)$$

where $A_{t,u}^{-1}G$ is another generator matrix of $C=\tau(S)$ whose i-th row is $\tau(M_i')$ and $S=\langle M_1',\dots,M_5'\rangle$.

In order check Lemma 4.4 we must find the relations between both sets of generators M_i and M_i' for $i\in\{1,\dots,5\}$. Recall that when we multiply $A_{t,u}^{-1}$ by G to build the new generator matrix $A_{t,u}^{-1}G$ we are simply making linear combinations of rows of G with coefficients in $A_{t,u}^{-1}$. Thus

$$\tau(M_i')=\sum_{j=1}^{j=5}a_{ij}^{-1}\tau(M_j)$$

Therefore by checking the coefficients a_{ij}^{-1} of $A_{t,u}^{-1}$ we can easily express the rows of $A_{t,u}^{-1}G$ in terms of the rows of G:

$$\begin{aligned}
&\tau(M_1') = \tau(M_1) + \tau(M_2)\\
&\tau(M_2') = \tau(M_1) + \tau(M_2) + \tau(M_3)\\
&\tau(M_3') = \tau(M_1) + \tau(M_5)\\
&\tau(M_4') = \tau(M_3) + \tau(M_4)\\
&\tau(M_5') = \tau(M_2) + \tau(M_3) + \tau(M_4)
\end{aligned}$$

Finally applying $\tau(M_i)+\tau(M_j) = \tau(M_iM_j)$ we end up with the relation between both sets of generators:

$$\begin{array}{lcl}
M_1' & = & M_1M_2\\
M_2' & = & M_1M_2M_3\\
M_3' & = & M_1M_5\\
M_4' & = & M_3M_4\\
M_5' & = & M_2M_3M_4
\end{array}
\qquad
\begin{array}{lcccccc}
M_1 & = & X & I & I & Y & Y\\
M_2 & = & I & X & Z & I & Y\\
M_3 & = & I & I & Y & X & Z\\
M_4 & = & Z & I & Z & Z & I\\
M_5 & = & I & Z & Z & Z & Z
\end{array}
\qquad
\begin{array}{lcccccc}
M_1' & = & X & X & Z & Y & I\\
M_2' & = & X & X & X & Z & Z\\
M_3' & = & X & Z & Z & X & X\\
M_4' & = & Z & I & X & Y & Z\\
M_5' & = & Z & X & Y & Y & X
\end{array}$$

Observe that we have not taken into account the phases $\{\pm 1, \pm i\}$ when multiplying the Pauli matrices of the generators, for example, $M_1M_2M_3$ indeed is $-M_2'$ and not M_2'. This omission is delivered due to the function τ is a quotient respect to the phases of the generators, namely, the map does not distinguish between phases. Furthermore, as detailed previously all generators of S must have overall phase ± 1 and never $\pm i$ because then $M_i^2 = -\mathbb{I} \in S$ and hence $Q(S) = \{0\}$.

Given $t = (1, 0, 1, 1, 1)$ and $u = (0, 0, 1, 1, 0)$ we already know that:

$M_i \left|\psi^t\right\rangle = -\left|\psi^t\right\rangle$ for $i = \{1, 3, 4, 5\}$ and $M_2 \left|\psi^t\right\rangle = +\left|\psi^t\right\rangle$

$M_i \left|\psi^u\right\rangle = -\left|\psi^u\right\rangle$ for $i = \{3, 4\}$ and $M_i \left|\psi^u\right\rangle = +\left|\psi^u\right\rangle$ for $i = \{1, 2, 5\}$

And by Lemma 4.4 we expect

$M_1' \left|\psi^t\right\rangle = -\left|\psi^t\right\rangle$ and $M_i' \left|\psi^t\right\rangle = +\left|\psi^t\right\rangle$ for $i = \{2, 3, 4, 5\}$

$M_2' \left|\psi^u\right\rangle = -\left|\psi^u\right\rangle$ and $M_i' \left|\psi^u\right\rangle = +\left|\psi^u\right\rangle$ for $i = \{1, 3, 4, 5\}$

Therefore, applying the relations between both sets of generators we check Lemma 4.4 holds:

$$\begin{array}{llll}
M_1' \left|\psi^t\right\rangle = & M_1M_2 \left|\psi^t\right\rangle & = -\left|\psi^t\right\rangle & \quad M_1' \left|\psi^u\right\rangle = & M_1M_2 \left|\psi^u\right\rangle & = +\left|\psi^u\right\rangle\\
M_2' \left|\psi^t\right\rangle = & M_1M_2M_3 \left|\psi^t\right\rangle & = +\left|\psi^t\right\rangle & \quad M_2' \left|\psi^u\right\rangle = & M_1M_2M_3 \left|\psi^u\right\rangle & = -\left|\psi^u\right\rangle\\
M_3' \left|\psi^t\right\rangle = & M_1M_5 \left|\psi^t\right\rangle & = +\left|\psi^t\right\rangle & \quad M_3' \left|\psi^u\right\rangle = & M_1M_5 \left|\psi^u\right\rangle & = +\left|\psi^u\right\rangle\\
M_4' \left|\psi^t\right\rangle = & M_3M_4 \left|\psi^t\right\rangle & = +\left|\psi^t\right\rangle & \quad M_4' \left|\psi^u\right\rangle = & M_3M_4 \left|\psi^u\right\rangle & = +\left|\psi^t\right\rangle\\
M_5' \left|\psi^t\right\rangle = & M_2M_3M_4 \left|\psi^t\right\rangle & = +\left|\psi^t\right\rangle & \quad M_5' \left|\psi^u\right\rangle = & M_2M_3M_4 \left|\psi^u\right\rangle & = +\left|\psi^u\right\rangle
\end{array}$$

By the example above it becomes clear what Lemma 4.4 implies, namely, that given any two distinct elements $t, u \in T \setminus \{0\} \subset \mathbb{F}_2^{n-k}$ and a set of $n-k$ generators M_i of S we can always apply a convenient change of basis $A_{t,u}$ such that we obtain an alternative set of generators M_i' of S with eigenvalues in $Q_t(S)$ and $Q_u(S)$ parameterized by $(1, 0, \dots 0), (0, 1, 0, \dots, 0) \in \mathbb{F}_2^{n-k}$ instead of the original $t, u \in \mathbb{F}_2^{n-k}$.

Let $\{M_1', \dots, M_{n-k}'\}$ generate S and fulfill Lemma 4.4. Let $S_{t,u}$ denote the group generated by $\{M_3', \dots, M_{n-k}'\}$. Observe that the $n-k-2$ generators of $S_{t,u}$ take eigenvalue $+1$ in $Q(S)$. When deleting an element of the generator set of a group what it remains is a subgroup of it hence

$$S_{t,u} = \langle M'_3, \dots, M'_{n-k} \rangle \subset S = \langle M'_1, \dots, M'_{n-k} \rangle = \langle M_1, \dots, M_{n-k} \rangle \subseteq \mathcal{P}_n$$

In stabilizer codes the minimum distance is equal to the minimum weight of $\mathrm{Cent}(S) \setminus S$ for $k \neq 0$ while equal to the minimum weight of S for $k = 0$. We look for an analogous version for non-additive codes.

Definition 4.6. The minimum distance of $Q(S, T)$ is the minimum weight of $Cent(S_{t,u}) \setminus S_{t,u}$ where the minimum is taken over all possible pairs $t, u \in T \setminus \{0\}$. Thus

$$d_{Q(S,T)} = min\{\, d_{t,u} : t, u \in T \setminus \{0\}\}$$

where $d_{t,u} = min\{\, wt(E) : E \in Cent(S_{t,u}) \setminus S_{t,u}\}$

The following theorem justifies the above definition of $d_{Q(S,T)}$.

Theorem 4.7. *Let $T \subset \mathbb{F}_2^{n-k}$ and let d be the minimum weight of $\mathrm{Cent}(S_{t,u}) \setminus S_{t,u}$ where the minimum is taken over all pairs $t, u \in T \setminus \{0\}$. If we encode with $Q(S, T)$ then there is a recovery map which corrects all errors in $\mathcal{E}_d$.*

Proof. Suppose $E_i, E_j \in \mathcal{E}_d$. Then both E_i and E_j have weight at most $(d-1)/2$ hence $E = E_iE_j$ has weight at most $d-1$. But the elements of $Cent(S_{t,u}) \setminus S_{t,u}$ have weight at least d therefore

$$E = E_iE_j \notin Cent(S_{t,u}) \setminus S_{t,u}$$

for any $t, u \in T$, since the elements of $Cent(S_{t,u}) \setminus S_{t,u}$ have weight at least d. Thus there are two cases to analyse:

1. For all $t, u \in T \setminus \{0\}$ there is an element $M_{t,u} \in S_{t,u}$ such that $M_{t,u}E_iE_j = -E_iE_jM_{t,u}$ and by Lemma 4.4
$$M_{t,u} |\psi^u_s\rangle = |\psi^u_s\rangle \text{ and } M_{t,u} |\psi^t_r\rangle = |\psi^t_r\rangle$$
for all $r, s \in \{1, \dots, 2^k\}$ where $\{|\psi^t_r\rangle\}$ and $\{|\psi^u_s\rangle\}$ are orthonormal basis for $Q(S_t)$ and $Q(S_u)$ respectively.

2. $E \in S$ hence $E|\psi\rangle = +1|\psi\rangle$ for any $|\psi\rangle \in Q(S)$.

The projector onto $Q(S, T)$ is

$$P = \sum_{t\in T}\sum_{i=1}^{2^k} |\psi^t_i\rangle \langle\psi^t_i|$$

where $\{|\psi^t_i\rangle \mid i = 1, \dots, 2^k\}$ is an orthonormal basis for $Q(S_t)$.

Case 1

$$PE_iE_jP = PEP = \sum_{t,u\in T}\sum_{r,s=1}^{2^k} |\psi^t_r\rangle \langle\psi^t_r| E |\psi^u_s\rangle \langle\psi^u_s|$$

$$= \sum_{t,u\in T}\sum_{r,s=1}^{2^k} |\psi^t_r\rangle \langle\psi^t_r| EM_{t,u} |\psi^u_s\rangle \langle\psi^u_s| = -\sum_{t,u\in T}\sum_{r,s=1}^{2^k} |\psi^t_r\rangle \langle\psi^t_r| M_{t,u}E |\psi^u_s\rangle \langle\psi^u_s| = -PEP$$

From which it follows that $PEP = 0$.

Case 2

$$PE_iE_jP = PEP = \sum_{r,s=1}^{2^k} |\psi_r\rangle \langle\psi_r| E |\psi_s\rangle \langle\psi_s| = \sum_{r,s=1}^{2^k} |\psi_r\rangle \langle\psi_r|\psi_s\rangle \langle\psi_s| = P$$

Hence by Theorem 1.9 in both cases there is a recovery map. □

Recall that $[\![n,k,d]\!]$ denotes a 2^k-dimensional code while $((n,k,d))$ denotes a k-dimensional code.

Theorem 4.8. *Let S be an abelian group which characterise an $[\![n,k,d]\!]$ stabilizer code. Then $Q(S,T)$ is a $((n,|T|2^k,d_{Q(S,T)}))$ code.*

Proof. The parameter n is the number of physical qubits, which conform a quantum entanglement-system described in $(\mathbb{C}^2)^{\otimes n}$, therefore n does not depend on the mathematical code used to encode. Also, $d_{Q(S,T)}$ follows from Definition 4.6 so it only remains to prove the dimension parameter. $Q_t(S)$ is a stabilizer code too hence by Theorem 2.3 $Q_t(S)$ has dimension 2^k and by Lemma 4.2 the subspaces $Q_t(S)$ with $t \in T$ are all orthogonal therefore

$$Dim\, Q(S,T) = \sum_{t\in T} Dim\, Q_t(S) = |T|2^k$$

□

Theorem 4.8 shows that non-additive quantum codes are no longer constricted to have dimension a power of 2. Also observe that a stabilizer code encodes $\log_2(2^k) = k$ logical qubits in n physical qubits while a non additive quantum code encodes $\log_2(|T|2^k) = k + \lfloor\log_2(|T|)\rfloor$ in n qubits hence they have "more space "available to encode.

4.2 The Geometry of Non Additive Quantum Codes

An stabilizer code is fully characterized by an abelian group $S \subset \mathcal{P}_n$ of size 2^{n-k}. Theorem 3.4 states that if Cent(S) contains no elements of weight 1 then the stabilizer code is also fully characterised by a quantum set of lines $\mathcal{X}$, namely, a set of lines in $PG(n-k-1,2)$ with the property that any co-dimension two subspace is skew to an even number of the lines in X. The equivalence between the group setting $Q(S)$ and the geometric setting $\mathcal{X}$ is due to the fact that the quantum set of lines $\mathcal{X}$ in $PG(n-k-1,2)$ are spanned precisely by the the i-th and $(i+n)$-th columns of the generator matrix of $C = \tau(S)$. Finally, if the code is pure then the minimum distance d can be obtained from the geometry as the size of the minimum set of dependent points on distinct lines of $\mathcal{X}$. If the code is impure we must discount the dependencies in which the lines of $\mathcal{X}$ which do not contain dependent points are contained in a hyperplane which also contains all the dependent points.

In this section we look for an analogous equivalence between the group setting $Q(S,T)$ where Cent(S) contains no elements of weight 1 and the geometric setting $\mathcal{X}$ together with $T \subset \mathbb{F}_2^{n-k}$ such that the resulting $d_{Q(S,T)}$ is the desired one.

Let $T \subset \mathbb{F}_2^{n-k}$ and pick $t,u \in T \setminus \{0\}$. As detailed previously $A_{t,u}^{-1}G$ is another generator matrix for $C = \tau(S)$ whose i-th row is $\tau(M_i')$ and such that $S = \langle M_1', \dots, M_{n-k}'\rangle$. Then the $n-k-2$ generators of the subgroup

$$S_{t,u} = \langle M_3', \dots, M_{n-k}'\rangle \subset S$$

all take eigenvalue $+1$ in $Q(S)$. We construct the $(n-k-2)\times 2n$ matrix $G_{t,u}$ whose i-th row is $\tau(M'_i)$ and which generates $C_{t,u}=\tau(S_{t,u})$. Then the i-th and the $(i+n)$-th columns of $G_{t,u}$ with $i\in\{1,\dots,n-k-2\}$ span a quantum set of lines of $PG(n-k-3,2)$. The fact that this set of lines is a quantum set of lines is justified below.

Definition 4.9. We define

$$\mathcal{X}_{t,u}$$

as the quantum set of lines in $PG(n-k-3,2)$ obtained from the subgroup $S_{t,u}=\langle M'_3,\dots,M'_{n-k}\rangle$.

In the group setting we obtain $\mathcal{X}_{t,u}$ from $\mathcal{X}$ by carrying out a change of basis $A_{t,u}$ such that the eigenvalues of the new set of generators of S are parameterized by $(1,0,\dots,0)$ and $(0,1,0,\dots,0)$ instead of the original t,u. Then we proceed to delete the first and second rows $\tau(M'_1)$ and $\tau(M'_2)$ of $A^{-1}_{t,u}G$ so we obtain $G_{t,u}$ whose i-th and $(i+n)$-th columns for $i\in\{1,\dots,n-k-2\}$ span $X_{t,u}$ in $PG(n-k-3,2)$. Recall that in order to project from the i-th canonical basis element we simply must delete the i-th coordinate. Thus, in the geometric setting we equivalently obtain $\mathcal{X}_{t,u}$ from $\mathcal{X}$ by simply projecting the quantum set of lines $\mathcal{X}$ from the points t and u into $PG(n-k-3,2)$.

$\mathcal{X}$ is a quantum set of lines if and only if every codimension 2 subspace of $PG(n-k-1,2)$ is skew to an even number of the lines of $\mathcal{X}$. Actually two skew subspaces can intersect after a projection but projections preserve the codimension, namely, the projection of a codimension 2 subspace of $PG(n-k-1,2)$ results on a codimension 2 subspace in $PG(n-k-3,2)$. Therefore the projection $\mathcal{X}_{t,u}$ is only a quantum set of lines if it is a set of lines. We have to choose T so that the projection from t and u is onto a set of lines.

Definition 4.10. The minimum distance of $Q(S,T)$ is defined as

$$d_{Q(S,T)}=min\{\,d(\mathcal{X}_{t,u}):t,u\in T\setminus\{0\}\}$$

where $d(\mathcal{X}_{t,u})$ is the size of the minimum set of dependent points on distinct lines of $\mathcal{X}_{t,u}$ for all pairs $t,u\in T\setminus\{0\}$.

The following theorem justifies the above definition of $d_{Q(S,T)}$ and its equivalence with the definition in 4.6. Furthermore, it provides the equivalence between the group setting $Q(S,T)$ and the geometric setting $\mathcal{X}$ together with certain subset $T\subset\mathbb{F}_2^{n-k}$.

Theorem 4.11. *Let $T\subset\mathbb{F}_2^{n-k}$ and let $\mathcal{X}$ be a quantum set of lines given by the abelian subgroup S such that $Cent(S)$ contains no elements of weight 1. The code $Q(S,T)$ is a $((n,|T|2^k,d))$ code, where d is the minimum over all possible $d(\mathcal{X}_{t,u})$ with $t,u\in T\setminus\{0\}$.*

Proof. We have seen that the geometric way to obtain $\mathcal{X}_{t,u}$ from $\mathcal{X}$ is to project $\mathcal{X}$ onto a quantum set of lines in $PG(n-k-3,2)$ from the points t and u. By changing the basis through $A_{t,u}$ the points t and u become the points e_1 and e_2. Then to project $\mathcal{X}$ from e_1 and e_2 we simply must delete the first and second coordinates of $\mathcal{X}$ to obtain $\mathcal{X}_{t,u}$ or, equivalently, delete M'_1 and M'_2 from S to obtain $S_{t,u}$ and then construct $\mathcal{X}_{t,u}$.

By Theorem 4.7 the minimum distance of $Q(S,T)$ is the minimum weight of $Cent(S_{t,u})\setminus S_{t,u}$ where the minimum is taken over all possible pairs $t,u\in T\setminus\{0\}$. On the other hand the the minimum weight of each $Cent(S_{t,u})\setminus S_{t,u}$ is equal to the minimum distance of each $\mathcal{X}_{t,u}$ hence we can define d as in definition 4.10 and we are done. □

Thus, the geometry of a non-additive quantum code $Q(S, T)$ is given by a quantum set of lines $\mathcal{X}$ of $PG(n-k-1, 2)$, together with a set of points $T \setminus \{0\}$, such that the projection of $\mathcal{X}$ from any pair of points $t, u \in T \setminus \{0\}$ is onto a quantum set of lines of $PG(n-k-3, 2)$. The minimum distance of $Q(S, T)$ is the minimum of $d(\mathcal{X}_{t,u})$, where the minimum is taken over all $t, u \in T \setminus \{0\}$.

4.3 Stabilizer Codes as Direct Sums

In this section we show how to construct stabilizer codes as the direct sum of stabilizer codes for some subset T fulfilling certain conditions.

Let $T \subset \mathbb{F}_2^n$ be the set of all elements of the form

$$\overbrace{(0, \dots, 0)}^{\text{n-k times}} \cup \langle e_{n-k+1}, \dots, e_n \rangle$$

where $\langle e_{n-k+1}, \dots, e_n \rangle$ means all possible sums modulo 2 of the i-th elements of the canonical basis with $i \in \{n-k+1, \dots, n\}$. For example, for $n = 5$ and $k = 3$ the elements of $T \subset F_2^5$ are

$$\begin{array}{cccc} (0,0,1,0,0) & (0,0,0,1,0) & (0,0,0,0,1) & (0,0,1,1,0) \\ (0,0,0,1,1) & (0,0,1,0,1) & (0,0,1,1,1) & (0,0,0,0,0) \end{array}$$

Observe that $T \subset \mathbb{F}_2^n$ is a k-dimensional subspace because it is spanned by k elements of the canonical basis and if $t, u \in T$ then $t + u \in T$. Also recall that a k-dimensional vector space over $\mathbb{F}_q$ has q^k points because there are k positions to fill with q possible values hence $|T| = 2^k$.

Theorem 4.12. *Let $S \subset \mathcal{P}_n$ be an abelian group of size 2^{n-k}. Then $Q(S) = Q(S', T)$ for some group $S' \supseteq S$ of size 2^n and some k-dimensional subspace $T \subset \mathbb{F}_2^n$.*

Remark. In other words, any $[\![n, k]\!]$ stabiliser code can be constructed as the direct sum of a stabiliser code $[\![n, 0]\!]$ for some k-dimensional subspace T.

Proof. Suppose $T \subset \mathbb{F}_2^n$ is a k-dimensional subspace. Then $|T| = 2^k$ and by applying a change of basis the elements of T are of the form

$$\overbrace{(0, \dots, 0)}^{\text{n-k times}} \cup \langle e_{n-k+1}, \dots, e_n \rangle$$

Let $S = \langle M_1, \dots, M_{n-k} \rangle$ be an abelian subgroup of $\mathcal{P}_n$ of size 2^{n-k} which characterises a stabilizer code $[\![n, k]\!]$. Observe that to decrease k in one unit is equivalent to move an element from $\text{Cent}(S)$ to S. Then by moving k independent elements $\{M_{n-k+1}, \dots, M_n\}$ from $\text{Cent}(S)$ to S we construct a bigger abelian group $S' \supset S$ of size 2^n. Note that these elements have to be added to S one by one, namely, we move an element from $\text{Cent}(S)$ to S, we compute the new centralizer, next we move another element and so on until we have added k independent elements to S obtaining the bigger abelian group S' of size 2^n which characterises a $[\![n, 0]\!]$ stabilizer code.

Then for each $t = (0, \dots, 0, t_{n-k+1}, \dots, t_n) \in T$ there is a subspace $Q_t(S')$ defined as the joint $+1$-eigenspace of the operators

$$M_1, \dots, M_{n-k}, (-1)^{t_{n-k+1}} M_{n-k+1}, \dots, (-1)^{t_n} M_n$$

Observe that $S' = S \cup \langle M_{n-k+1}, \dots, M_n \rangle$ where $S = \langle M_1, \dots, M_{n-k} \rangle$ and

$$M_i \left|\psi^t\right\rangle = +1 \left|\psi^t\right\rangle$$

for all $i \in \{1, \ldots, n-k\}$, all $|\psi^t\rangle \in Q_t(S')$ and all $t \in T$. Thus, the joint $+1$-eigenspace of all elements of S defines $Q(S)$.

Summarizing, there are $|T| = 2^k$ of such subspaces $Q_t(S')$, all of them orthogonal, all 1-dimensional and each of them represents a $[\![n, 0]\!]$ stabilizer code where the eigenvalues of the n generators of S' are parameterized by the corresponding $t \in T$.

Finally we construct the $((n, 2^k))$ code

$$Q(S', T) = \bigoplus_{t \in T} Q_t(S')$$

and it follows that $Q(S', T) = Q(S)$. Thus, a $[\![n, k]\!]$ stabilizer code is equivalent to the direct sum of 2^k $[\![n, 0]\!]$ stabilizer codes through some k-dimensional subspace T of $\mathbb{F}_2^n$. □

Example 4.13. Consider the abelian group $S_2 = \langle M_1, M_2 \rangle$ of size 4 which characterises a $[\![4, 2]\!]$ stabilizer code. By Theorem 4.12 this code is equivalent to the direct sum of $2^2 = 4$ stabilizer codes $[\![4, 0]\!]$ through a 2-dimensional subspace $T \subset \mathbb{F}_2^4$. The code $[\![4, 0]\!]$ is characterised by an abelian group $S_4 \supset S_2$ of size 16 generated by M_1, M_2, M_3, M_4 while the 2-dimensional subspace T is chosen such that each subspace $Q_t(S_4)$ is the joint $+1$-eigenspace of

$$M_1, M_2, (-1)^{t_3} M_3, (-1)^{t_4} M_4$$

for each of the four points $t = (0, 0, t_3, t_4) \in T$ with $t_i \in \{0, 1\}$.

We define

$$\begin{aligned} M_1 &= \; X \quad X \quad X \quad X \\ M_2 &= \; Z \quad Z \quad Z \quad Z \end{aligned}$$

Actually they are are the generators of $[\![4, 2, 2]\!]$. We must move two independent elements, one by one, from $Cent(S_2)$ to $S_2 = \langle M_1, M_2 \rangle$ in order to obtain a larger group S_4 of size $2^4 = 16$· Since Pauli matrices fulfill

$$\sigma_i \sigma_j = -\sigma_j \sigma_i \text{ for } i \neq j \text{ and } i, j \in \{x, y, z\}$$

$$\sigma_x \sigma_y = i\sigma_z \; ; \; \sigma_y \sigma_z = i\sigma_x \; ; \; \sigma_z \sigma_x = i\sigma_y \; ; \; \sigma_i^2 = 1$$

we propose the element $M_3 = X\ X\ Z\ Z$. Observe that $M_3 M_1 = M_1 M_3$ and $M_3 M_2 = M_2 M_3$ while clearly $M_3 \notin S_2$ hence $M_2 \in Cent(S_2) \setminus S_2$. We add M_3 to S_2 to obtain a larger group

$$S_3 = \langle M_1, M_2, M_3 \rangle \; ; \; |S_3| = 2^3 = 8$$

We now propose the element $M_4 = Z\ Z\ X\ X$. Recall that $M_4 M_i = M_i M_4$ for $i \in \{1, 2, 3\}$ while $M_4 \notin S_3$ hence $M_3 \in Cent(S_3) \setminus S_3$. We add M_3 to S_3 to obtain the desired group of of size $2^4 = 16$:

$$S_4 = \langle M_1, M_2, M_3, M_4 \rangle = S_2 \cup \langle M_3, M_4 \rangle$$

Regarding the elements of $T \subset \mathbb{F}_2^4$, actually any 4 points, as long as they form a 2-dimensional subspace, would work to construct a $[\![4, 2]\!]$ as the direct sum of $[\![4, 0]\!]$ because due to T is 2-dimensional subspace we can always apply a change of basis such that T is written as $(0, 0) \cup \langle e_3, e_4 \rangle$. We may construct the specific $[\![4, 2, 2]\!]$ as the direct sum of $[\![4, 0, 2]\!]$. With the help of a program in GAP (see section 4.4) we find the following points of T resulting on a minimum distance 2, namely, $d(\mathcal{X}_{t,u}) \geq 2$ for all pairs $t, u \in T \setminus \{0\}$ and $d(\mathcal{X}_{t,u}) = 2$ for at least one pair:

$$t_0 = (0, 0, 0, 0) \quad t_1 = (0, 0, 1, 1) \quad t_2 = (1, 1, 0, 0) \quad t_3 = (1, 1, 1, 1)$$

Observe that for any pair $t, u \in T$ we have $t + u \in T$ and the matrix whose rows are the points of T has rank 2 therefore, as expected by Theorem 4.12, T is a 2-dimensional subspace of $\mathbb{F}_2^4$. We choose the two linearly independent elements t_1 and t_2 as basis for T and we apply the change of basis defined by the map $t_1 \to e_3$ and $t_2 \to e_4$ hence T is written as $(0, 0) \cup \langle e_3, e_4\rangle$:

$$\begin{array}{rcccl} t_0 = (0,0,0,0) & \to & \overline{0} & = (0,0,0,0) \\ t_1 = (0,0,1,1) & \to & e_3 & = (0,0,1,0) \\ t_2 = (1,1,0,0) & \to & e_4 & = (0,0,0,1) \\ t_3 = (1,1,1,1) & \to & e_3 + e_4 & = (0,0,1,1) \end{array}$$

Coming back to the group S_4 found previously observe that

$$S_4 = \langle \widehat{M}_1, \widehat{M}_2, \widehat{M}_3, \widehat{M}_4 \rangle = S_2 \cup \langle \widehat{M}_3, \widehat{M}_4 \rangle$$

Where now the set $\widehat{M}_i$ are the transformation of the original set M_i under the change of basis which expresses T as $(0, 0) \cup \langle e_3, e_4\rangle$. Recall that now the generators of S_2 take all eigenvalue $+1$ in each subspace $Q_t(S_4)$ for all $t \in T$, namely,

$Q_{(0,0,0,0)}$ is the joint $+1$-eigenspace of $\widehat{M}_1, \widehat{M}_2, \widehat{M}_3, \widehat{M}_4$.
$Q_{(0,0,1,0)}$ is the joint $+1$-eigenspace of $\widehat{M}_1, \widehat{M}_2, -\widehat{M}_3, \widehat{M}_4$.
$Q_{(0,0,0,1)}$ is the joint $+1$-eigenspace of $\widehat{M}_1, \widehat{M}_2, \widehat{M}_3, -\widehat{M}_4$.
$Q_{(0,0,1,1)}$ is the joint $+1$-eigenspace of $\widehat{M}_1, \widehat{M}_2, -\widehat{M}_3, -\widehat{M}_4$.

Finally, we construct

$$Q(S_4, T) = \bigoplus_{t \in T} Q_t(S_4)$$

which results on a $((4, 4, 2))$ code. By Theorem 4.12 we conclude the $Q(S_4, T)$ is, indeed, the $[\![4, 2, 2]\!]$ stabilizer code characterized by S_2.

Theorem 4.14. *Let $S' \subset \mathcal{P}_n$ be an abelian group of size 2^{n-r} and let T be a k-dimensional subspace. Then $Q(S', T) = Q(S)$ for some subgroup $S \subset S'$ of size 2^{n-r-k}.*

Remark. In other words, any $[\![n, r]\!]$ stabilizer code can be constructed as the direct sum of a stabilizer code $[\![n, k + r]\!]$ for some k-dimensional subspace T. Note that if T is not a subspace this does not imply that $Q(S', T)$ is not a stabiliser code.

Proof. Let $S' \subset \mathcal{P}_n$ be an abelian group of size 2^{n-r} and let T be a k-dimensional subspace. By applying a change of basis the elements of T are of the form

$$T = (0, \dots, 0) \cup \langle e_{n-k-r+1}, \dots, e_{n-r}\rangle.$$

Let $\{M_1, \dots, M_{n-r}\}$ generate S'. Then for all $|\psi\rangle \in Q(S', T)$ we have

$$M_i |\psi\rangle = |\psi\rangle .$$

Hence,

$$Q(S', T) \leq Q(S),$$

where the subgroup $S \subset S'$ is generated generated by $\{M_1, \dots, M_{n-r-k}\}$.

Since $\dim Q(S', T) = \dim Q(S) = 2^{r+k}$, we have $Q(S', T) = Q(S)$. □

Example 4.15. The stabilizer code $[\![7, 1, 3]\!]$ is called Steane code. We want to construct a stabilizer code as the direct sum of the Steane Code. With the help of a program in GAP (see section 4.4) we look for the subset $T \subset \mathbb{F}_2^6$ of biggest size (hence the resulting dimension is maximised) such that $d_{Q(S,T)}$ does not decrease too much (equal or one unit less). We find the following subset T of size 8 such that the resulting non additive code $((n, |T|2^r, d_{Q(S,T)}))$ has parameters $((7, 16, 2))$:

$$\begin{array}{cccc} (0,0,0,0,0,0) & (1,1,1,1,0,1) & (0,0,1,0,1,0) & (0,1,0,1,0,0) \\ (0,1,1,1,1,0) & (1,0,0,0,1,1) & (1,0,1,0,0,1) & (1,1,0,1,1,1) \end{array}$$

Observe that the sum of any pair of points $t, u \in T$ also belongs to T and the matrix whose rows are the points of T has rank 3. Thus, the subset T is indeed a 3-dimensional subspace of $\mathbb{F}_2^6$. Finally we apply Theorem 4.14 to conclude that the code $((7, 16, 2))$ found is, indeed, the stabilizer code $[\![7, 4, 2]\!]$.

4.4 Examples and Results

Given a $[\![n, k, d]\!]$ stabilizer code we look for the biggest subset $T \subset \mathbb{F}_2^{n-k}$ such that $d(\mathcal{X}_{t,u}) \geq d'$ (usually $d' = d - 1$) for the $\binom{|T|-1}{2}$ possible pairs $t, u \in T \setminus \{0\}$ while $d(\mathcal{X}_{t,u}) = d'$ for at least one pair where $\mathcal{X}_{t,u}$ is the projection of $\mathcal{X}$ through the points $t, u \in T \setminus \{0\}$. If such a maximized subset T exists then there is a non additive quantum code $Q(S, T)$ with parameters $((n, |T|2^k, d'))$. Therefore the above presents an algorithm to find out non additive quantum codes as the direct sum of a stabilizer codes through T such that, despite we decrease the minimum distance in one unit (the new code is able to correct less errors), we increase the dimension in a factor $|T|$ hence the resulting code is able to encode $k + \lfloor \log_2 |T| \rfloor$ logical qubits in n physical qubits. We shall always add the zero vector to T because to include $Q(S)$ in the direct sum does not affect $d_{Q(S,T)}$ while it increases the size of $|T|$ hence the dimension of $Q(S, T)$ grows too. The generator matrices needed as input can be obtained from the web page "codetables.markus-grassl.de".

We carry out all the computations with a program in GAP. The aim is to maximise the size of $T \subset \mathbb{F}_2^{n-k}$ while d' does not decrease too much (usually $d' = d-1$). Recall that we do not know the size of $T \subset \mathbb{F}_2^{n-k}$ in advance. Therefore for each possible subset T of $\mathbb{F}_2^{n-k}$ we look for the biggest "clique" in the graph with vertices $T \subset \mathbb{F}_2^{n-k}$ such that $t, u \in T \setminus \{0\}$ is an edge of the clique if and only if $d(\mathcal{X}_{t,u}) \geq d'$ and at least one edge fulfills $d(\mathcal{X}_{t,u}) = d'$. Computing cliques is a NP-hard problem and the vector space $\mathbb{F}_2^{n-k}$ has 2^{n-k} points hence we are computationally restricted to use as input stabilizer codes with a small $n - k$ (around ≤ 7).

Lastly, take into account our algorithm assumes $\mathrm{Cent}(S)$ has no elements of weight one which, by Lemma 3.3, it is equivalent to assume that the i-th and $(i + n)$ columns of the generator matrix span a line (not a point) in $PG(n - k - 1, 2)$ for all $i \in \{1, \dots, n\}$. This assumption is required in Theorem 3.7 which states the equivalence between the group setting $Q(S)$ and the geometric setting $\mathcal{X}$. Recall that this is precisely how our algorithm computes $d(\mathcal{X}_{t,u})$ for each pair $t, u \in T \setminus \{0\}$. Many generator matrices in "codetables.markus-grassl.de" have a column of 0 which it is a clear indication that the above assumption is not holding. In these cases we must look for a $[\![n, k', d']\!]$ stabilizer code with $k' < k$ and $d' \geq d$ and a generator matrix with no column of 0. Then we project it from a point of $\mathbb{F}_2^{n-k}$ which does not belong to any of the quantum set of lines $\mathcal{X}$ of $[\![n, k', d']\!]$. Each projection increases k' in one unit and may decreases d'. We keep projecting until we obtain a code with the desired parameters but now we have made sure its centralizer contains no elements of weight one hence we can use it as input in our algorithm.

The Rains, Hardin, Shor and Sloane code $((5, 6, 2))$

This code first appeared in an article of 1997 by Rains, Hardin, Shor and Sloane [14]. We want to fit this code into our own approach to non additive codes as directs sums of stabilizer codes and the geometric framework involved.

First recall that clearly $((5,6,2))$ can not be a stabilizer code as its dimension is not a power of 2. We want to show that $((5,6,2))$ is constructed by the direct sum of 6 stabilizer codes $[\![5,0,3]\!]$.

Let $S = \langle M_1, \dots, M_5\rangle$ be an abelian group of size 2^5 which characterises the code $[\![5,0,3]\!]$ and let

$$G = \left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

be the 5×10 generator matrix of $[\![5,0,3]\!]$ whose i-th row is $\tau(M_i)$. Then the i-th and $(i+n)$-th columns of G span a quantum set of lines $\mathcal{X}$ in $PG(4,2)$. Note that the elements of $\mathcal{X}$ are all lines, not points. Then by Lemma 3.3 Cent(S) has no elements of weight 1 hence by Theorem 3.4 $\mathcal{X}$ uniquely characterises the code too. Let $T \subset \mathbb{F}_2^5$ with $|T| = 6$. We look for 6 points $t_0, \dots, t_5$ such that the resulting non additive quantum code has minimum distance 2. Thus,

$$min\{\, d(\mathcal{X}_{t_i,t_j}) : \forall t_i, t_j \in T \setminus \{0\}\} = 2$$

Observe that we can set up $t_0 = 0$ because to include the subspace $Q(S)$ in the direct sum does not modify the minimum distance of $Q(S,T)$ while increases its dimension. Assume we already know the 6 points which conform T such that $d_{Q(S,T)} = 2$. We construct $\binom{5}{2} = 10$ non-singular 5×5 matrices A_{t_i,t_j}, one for each pair $t_i, t_j \in T \setminus \{0\}$. Then $A^{-1}_{t_i t_j} G$ is another generator matrix from which we extract a new set of generators of S such that their eigenvalues are parametrizated by $(1,0,0,0,0)$ and $(0,1,0,0,0)$ instead of t_i and t_j.

Now to project from t_i and t_j we simply remove the first and second rows of $A^{-1}_{t_i t_j} G$ to end up with the 3×10 matrix $G_{t_i t_j}$. The rows of $G_{t_i t_j}$ define the generators of the group $S_{t_i t_j}$ of size $2^3 = 8$ while its columns span the quantum set of lines $\mathcal{X}_{t_i t_j}$ in $PG(2,2)$. Finally, the minimum distance $d_{Q(S,T)}$ is equal to the minimum weight of $Cent(S_{t_i t_j}) \setminus S_{t_i t_j}$ where t_i and t_j run over all possible pairs in $T \setminus \{0\}$ or, geometrically equivalent, the minimum $d(\mathcal{X}_{t_i,t_j})$ between all pairs $t_i, t_j \in T \setminus \{0\}$ where $d(\mathcal{X}_{t_i,t_j})$ is the minimum number of dependent points that can be found in distinct lines of $\mathcal{X}_{t_i,t_j}$.

The set T of size 6 can be regarded as a complete graph of 6 vertices and $\binom{5}{2} = 10$ edges where $t, u \in T \setminus \{0\}$ is an edge if and only if $d(\mathcal{X}_{t,u}) \geq 2$ and at least one edge fulfills $d(\mathcal{X}_{t,u}) = 2$. Applying the previous algorithm in GAP for $d_{Q(S,T)} = 2$ we obtain a subset T of size 6:

$$\begin{array}{lll} t_0 = (0,0,0,0,0) & t_1 = (0,0,0,1,1) & t_2 = (0,1,1,0,1) \\ t_3 = (1,0,1,1,0) & t_4 = (1,1,0,1,0) & t_5 = (1,1,1,0,0) \end{array}$$

Note that T is not a subspace, for example $t_2 + t_5 \notin T$. Thus, we conclude that the direct sum of $[\![5,0,3]\!]$ through the above subset T found constructs the non additive code $((5,6,2))$.

Finally, recall that the code $((5,6,2))$ is optimal because if we increase $|T|$ (and hence the dimension too) then the minimum distance is no longer 2 and the only stabilizer code with $n = 5$ and $d = 2$ is the $[\![5,2,2]\!]$. To clarify the role of an optimal code respect to the dimension suppose the existence of a $((5,4,2))$ code for $|T| = 4$. Clearly this hypothetical code is not the optimal one because despite it is also described in $(\mathbb{C}^2)^{\otimes 5}$, namely, describes a quantum system of 5 physical qubits, the $((5,6,2))$ code spans a bigger space to encode them. Thus, instead of encoding $|00000\rangle$, $|00001\rangle$, $|00010\rangle$, $|00011\rangle$ as logical bits we may encode $|00000\rangle$, $|00010\rangle$, $|00100\rangle$, $|00110\rangle$, $|00001\rangle$, $|00001\rangle$ as logical bits.

The Non Additive $((9,12,3))$ Quantum Code

The non additive $((9,12,3))$ code has been discovered in 2007 in [15]. Again its dimension is not a power of 2 hence it can not be a stabilizer code. The best comparable stabilizer code has parameters $[[9,3,3]]$ which spans a 8-dimensional subspace instead of a 12-dimensional subspace.

This code is the result of the direct sum of twelve $[\![9,0,3]\!]$ stabilizer codes with $T \subset \mathbb{F}_2^9$ being a subset (not a subspace) of size 12.

$$\begin{array}{llll}
(0,0,0,0,0,0,0,0,0) & (0,1,0,0,0,1,1,0,0) & (0,0,0,1,1,0,0,0,1) & (0,1,1,0,0,1,0,1,0) \\
(0,0,1,0,1,0,0,1,1) & (0,1,1,1,1,1,1,1,1) & (1,0,0,1,0,0,1,0,0) & (1,1,0,1,0,1,0,0,0) \\
(1,0,0,0,1,0,1,0,1) & (1,1,1,1,0,1,1,1,0) & (1,0,1,1,1,0,1,1,1) & (1,1,1,0,1,1,0,1,1)
\end{array}$$

The elements of T has been taken directly from [15] instead of obtained with our algorithm because the difference $n-k=9-0=9$ is too big hence computing all possible cliques takes too much time.

The abelian group S which characterises the $[\![9,0,3]\!]$ code is generated by the nine cyclic permutations of

$$\sigma_z \otimes \sigma_x \otimes \sigma_z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$$

which results on the generator matrix

$$G = \left(\begin{array}{ccccccccc|ccccccccc}
0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1
\end{array}\right)$$

The i-th and $(i+n)$-th column of G with $i \in \{1,\dots,n\}$ span $\mathcal{X}$. Since S is generated by nine cyclic permutations of the above element, which has weight 3, then Cent(S) has no elements of weight 1. Therefore by Lemma 3.3 the elements of $\mathcal{X}$ are all lines (not points) and by Theorem 3.4 $\mathcal{X}$ uniquely characterises the code too.

Next we apply our own geometrical framework for non additive codes. With our algorithm we compute $\mathcal{X}$ (which spans $PG(8,2)$) and $\mathcal{X}_{t_i,t_j}$ (which spans $PG(6,2)$) where $\mathcal{X}_{t_i,t_j}$ is the projection of $\mathcal{X}$ from the pair of points $t_i, t_j \in T \setminus \{0\}$. Recall that for each projection we can apply a change of basis A_{t_i,t_j} to simplify computations. Finally we compute

$$d_{Q(S,T)} = min\{\, d(\mathcal{X}_{t_i,t_j}) : \forall t_i, t_j \in T \setminus \{0\}\}$$

and we obtain that $d(\mathcal{X}_{t_i,t_j}) = 3$ for all $t_i, t_j \in T \setminus \{0\}$ hence $d_{Q(S,T)} = 3$.

Thus, the code

$$Q(S', T) = \bigoplus_{t \in T} Q_t(S')$$

is a $((9, |T|2^0 = 12, 3))$ non additive code which hence our geometrical framework is able to deduce the same code as the one obtained in [15].

In [15] they obtain the subset T applying an approach closely related to graph theory. Indeed, the subset T of any non additive code constructed as the direct sum of $[\![n, 0, d]\!]$ stabilizer codes can be deduced using this approach. This includes the previous example $((5, 6, 2))$. Despite this approach is powerful it is limited to use $[\![n, 0, d]\!]$ stabilizer codes as base codes since it requires a basis of the projective space formed by exactly one point of each line of $\mathcal{X}$ (see Lemma 4.16). Note that our geometrical framework does not have this constrain since we are able to construct non additive codes as direct sums of arbitrary $[\![n, r, d]\!]$ stabilizer codes.

Lemma 4.16. *Let $\mathcal{X}$ be a quantum set of n lines characterizing a stabilizer code where $Cent(S)$ contains no elements of weight one. Let B be a set of points such that each point belongs to a distinct line of $\mathcal{X}$. If B is a basis for the projective space spanned by $\mathcal{X}$ then $k = 0$.*

Proof. First note that $|B| = n$. If $k \geq 1$ then the lines of $\mathcal{X}$, which span $PG(n-k-1, 2)$, are not linearly independent hence B, which has size n, can not be a basis.

Let $k = 0$ an suppose B has only $n - r$ independent points of distinct lines of $\mathcal{X}$. Thus, B is a basis for $PG(n - r - 1, 2)$ and there are r points of B contained in the same subspace.

Since $\mathcal{X}$ spans the whole space $PG(n - 1, 2)$ then for each of the previous r points we can always change it for another point of the same line which it is independent from all other points in B until we end up with a set of n independent points in distinct lines spanning $PG(n - 1, 2)$. □

An *adjacency matrix* of a finite graph with n vertices is a $n \times n$ matrix A whose entries a_{ij} are 1 if the vertices i and j are joined by an edge and 0 otherwise. Recall that $a_{ij} = a_{ji}$, namely, A is symmetric.

Theorem 4.17. *An stabilizer code has parameters $[\![n, 0, d]\!]$ if and only if its generator matrix can be written as $G = (I|A)$ where I is the $n \times n$ identity matrix and A is the $n \times n$ adjacency matrix of a simple graph with n vertices.*

Proof. (⇒) Let $G = (I|A)$ be a $n \times 2n$ generator matrix of a $[\![n, 0, d]\!]$ code $C = \tau(S)$. We must prove that A is symmetric. Since S is abelian by Lemma 2.12 we have

$$(u, v)_a = \sum_{j=1}^{n} (u_j v_{j+n} - u_{j+n} v_j) = 0$$

for all codewords $u, v \in C$.

Since the rows of G are a basis of C clearly they are codewords of C too. Let u and v be the i-th and l-th row of G and let g_{ij} denote the entries of $G = (I|A)$. Then

$$(u, v)_a = \sum_{j=1}^{n} (g_{ij} g_{l,j+n} - g_{lj} g_{i,j+n}) = g_{l,i+n} - g_{i,l+n} = a_{li} - a_{il}$$

where a_{ij} denote the entries of A. Thus, $(u, v)_a = 0$ if and only if A is symmetric.

($\Leftarrow$) Let $C = \tau(S)$ be an stabilizer code with parameters $[\![n, k, d]\!]$. Let $C^{\perp_a}$ denote the orthogonal subspace of C. Thus

$$C^{\perp_a} = \{u \in \mathbb{F}_2^{2n} : (u, w)_a = 0, \forall w \in C\}$$

C is an $(n-k)$-dimensional subspace of $\mathbb{F}_2^{2n}$ hence

$$Dim(C^{\perp_a}) = 2n - (n-k) = n + k$$

By definition $(u, v)_a = 0$ for any pair of codewords $u, v \in C$. Observe that for any $u, v \in C$ it also holds

$$(u, v)_a = \sum_{i=1}^{n}(u_i v_{i+n} - u_{i+n} v_i) = \sum_{i=1}^{n}(u_i(v_i + v_{i+n}) - v_i(u_i + u_{i+n})) = \sum_{i=1}^{n}((u_i + u_{i+n})v_{i+n} - (v_i + v_{i+n})u_{i+n}) = 0$$

Thus, we can replace the i-th and $(i+n)$-th columns of G with linear combinations of these columns without affecting to the relation $(u, v)_a = 0$ between any pair of codewords of C. Recall that we can also apply Gaussian elimination which simply changes the basis of C, namely, finds another generator set of S.

Finally, we can also add independent elements from $C^{\perp_a}$ to C to enlarge the subspace C hence after moving k independent elements we end up with a n-dimensional subspace. The elements have to be added one by one, namely, we move an element from $C^{\perp_a}$ to C, we compute the new $C^{\perp_a}$, then we move another independent element and so on.

Then the resulting n-dimensional subspace $C' = \tau(S')$ where $S' \supset S$ has size 2^n represents a $[\![n, 0, d]\!]$ and, as proved in the forward implication, its generator matrix can be written as $(I|A)$ where A is a symmetric matrix. □

Coming back to the generator matrix G of $[\![9, 0, 3]\!]$, if we move both 1-th and $(1+9)$-th columns eight positions so they become the 9-th and 18-th columns then G takes the from $(I|A)$

$$(I|A) = \left(\begin{array}{ccccccccc|ccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right)$$

where A is the adjacency matrix A of the graph in Figure 1. Each element of T, which parameterises the eigenvalues ±1 of the generators of S, is represented in Figure 1 too.

The argument used in [15] to find out the points of T use some mathematical tools not considered in this work but it comes down to be equivalent to the familiar projection of $\mathcal{X}$ from two points. Before we have seen that $d(\mathcal{X}_{t_i,t_j}) = 3$ for all $t_i, t_j \in T \setminus \{0\}$ where $d(\mathcal{X}_{t_i,t_j})$ is the minimum set of dependent points in distinct lines of $\mathcal{X}_{t_i,t_j}$. Thus, the span of any three points of the quantum set of lines is not equal to the span of any point or two points of $T \setminus \{0\}$. Then due to the graph is cyclic we can assume one of the points comes from the span of the 1-th and the $(n+1)$-th column, namely, it is one the following points:

$$(0, 0, 0, 0, 0, 0, 0, 0, 1)$$
$$(1, 0, 0, 0, 0, 0, 0, 1, 0)$$
$$(1, 0, 0, 0, 0, 0, 0, 1, 1)$$

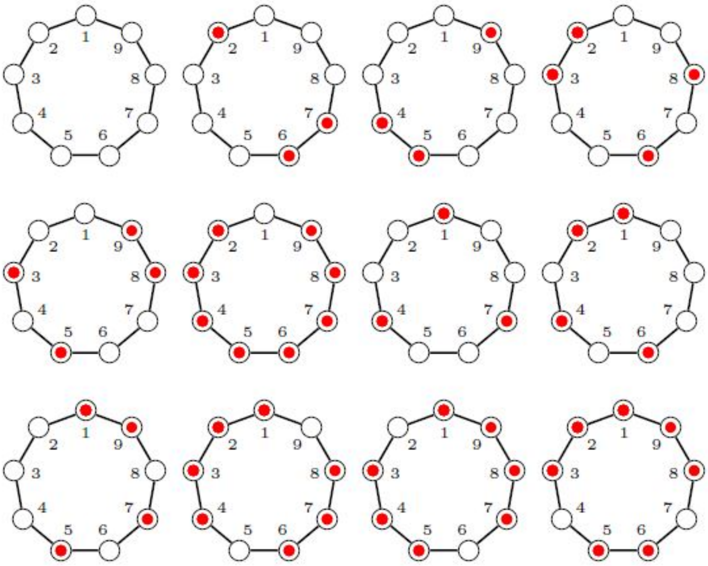


Figure 1: The graph of 9 vertices of $[\![9,0,3]\!]$. Each graph represents a point of T where a coloured vertex v_i indicates the generator M_i takes eigenvalue -1 while an uncolored vertex v_j indicates M_j takes eigenvalue -1. The direct sum of all graphs construct the non additive code $((9,12,3))$. The image has been taken from [15].

Finally we check that adding two further points on the quantum set of lines, we never get a combination of two or one of the points of T.

Ah well, that's only going to be true for pure stabiliser codes. Applying Theorem 4.13 to an impure stab code, we do not get that the [[n,0]] code has minimum distance d. Theorem 4.13 is still fine, because you don't state the min distance.

Nonetheless, the remarkable conclusion is the following: by Theorem 4.12 we can construct any $[\![n,k,d]\!]$ pure stabilizer code as the direct sum of a 2^k stabilizer codes $[\![n,0,d]\!]$ for some k-dimensional subspace $T \subset \mathbb{F}_2^n$ while by Theorem 4.17 any $[\![n,0,d]\!]$ stabilizer code comes from a simple graph in n vertices. Thus, we conclude that, indeed, any pure stabilizer code comes from a graph. Note that we request the code to be pure because applying Theorem 4.12 to an impure stabilizer code, we do not get that the $[\![n,0]\!]$ code has minimum distance d.

References

[1] Michael Nielsen and Isaac Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge, 2011.

[2] D. G. Glynn, T. A. Gulliver, J. G. Maks and M. K. Gupta, *The Geometry of Additive Quantum Codes*, unpublished manuscript. (available online at `https://www.academia.edu/17980449/`)

[3] S. Ball, F. Huber and A. Centelles, Quantum error-correcting codes and their geometries, arXiv:2007.05992.

[4] D. Gottesman, *Stabilizer codes and quantum error correction*, Caltech Ph.D. Thesis, 1997.

[5] P. W. Shor, Scheme for reducing decoherence in quantum memory, *Phys. Rev. Lett.*, **77** (1996) 793-797.

[6] J. J. Sakurai, Modern Quantum Mechanics, Addison-Weyley, 1994.

[7] D. Aharonov and M. Ben-Or, Fault-tolerant quantum computation with constant error, *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pp. 176–188, 1997.

[8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed state entanglement and quantum error correction. *Phys. Rev. A*, **54** (1996) 3824–.

[9] T. A. Brun and D. E. Lidar, *Quantum Error Correction*, Cambridge University Press, 2013.

[10] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inf. Theory*, **44** (1998) 1369–1387.

[11] M. Grassl and M. Rötteler, Quantum Goethals-Preparata codes, *Proceedings of the IEEE International Symposium on Information Theory*, 2008, pp. 300–304.

[12] M. Grassl and M. Rötteler, Nonadditive quantum codes, in: T. A. Brun and D. E. Lidar, *Quantum Error Correction*, Cambridge University Press, pp. 261–278, 2013.

[13] E. Knill and R. Laflamme. A theory of quantum error-correcting codes, *Phys. Rev. A*, **55** (1997).

[14] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, A nonadditive quantum code, *Phys. Rev. Lett.*, **79** 953 (1997).

[15] S. Yu, Q. Chen, C. H. Lai and C. H. Oh, Nonadditive quantum error-correcting code. *Phys. Rev. Lett.*, **101** (2008) 090501, 4 pp. arXiv:0704.2122.

[16] S. Yu, Q. Chen and C. H. Oh, Graphical Quantum Error-Correcting Codes, (2007) arXiv:0709.1780.