

# Introduction to Quantum Error-Correcting Codes

Henry D. Pfister

March 17th, 2025

## 1 Quantum Information

### 1.1 What is it?

A *qubit* is a quantum system with two perfectly distinguishable states (denoted  $|0\rangle$  and  $|1\rangle$ ). This is like a bit but with the key difference that a qubit can be in a superposition of these two states. For example, we will consider the quantum pure state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  with  $\alpha, \beta \in \mathbb{C}$  satisfying  $|\alpha|^2 + |\beta|^2 = 1$ . To make sense of this definition, we treat a qubit as an element of  $|\psi\rangle \in \mathbb{C}^2$  interpret this definition as

$$|\psi\rangle = \alpha \underbrace{|0\rangle}_{\begin{bmatrix} 1 \\ 0 \end{bmatrix}} + \beta \underbrace{|1\rangle}_{\begin{bmatrix} 0 \\ 1 \end{bmatrix}} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

For  $n$  qubits, a quantum pure state is a vector in  $(\mathbb{C}^2)^{\otimes n} \simeq \mathbb{C}^{2^n}$ . The “classical” state associated with the binary string  $x = (x_1, x_2, \dots, x_n) \in \{0, 1\}^n$  is the standard basis vector  $|x\rangle = |x_1 x_2 \dots x_n\rangle \in \mathbb{C}^{2^n}$  whose unit element is in the index  $1 + \sum_{i=1}^n x_i 2^{n-i}$ . Such a vector is part of the *computational basis* and can be defined by

$$|x\rangle := |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle,$$

where  $\otimes$  denotes the Kronecker product matrices (see below for definition). Thus, an arbitrary pure state can be written as

$$|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle.$$

These strange symbols for vectors are known as Dirac (or Bra-Ket) notation. The symbol  $|\psi\rangle$  is read as “ket psi” and represents a column vector. The symbol  $\langle\phi|$  is read as “bra phi” and equals the row vector  $|\phi\rangle^\dagger$  where  $\dagger$  indicates the Hermitian transpose. Using this terminology, the standard inner product in  $\mathbb{C}^{2^n}$  is denoted by  $|\phi\rangle^\dagger |\psi\rangle = \langle\phi| |\psi\rangle$  and called the “bra-ket”  $\langle\phi|\psi\rangle$ . Mapping to standard linear algebra, this implies  $\langle\psi|\psi\rangle = \|\psi\|^2$  and  $|\psi\rangle \langle\psi| = |\psi\rangle \langle\psi|^\dagger$  is the one-dimensional orthogonal projection onto the subspace spanned by  $|\psi\rangle$ .

The Kronecker product of matrices  $A = \{a_{i,j}\}$  and  $B = \{b_{i,j}\}$  is denoted by  $A \otimes B$  and defined by

$$A \otimes B \triangleq \begin{bmatrix} a_{1,1}B & a_{1,2}B & \dots \\ a_{2,1}B & a_{2,2}B & \dots \\ \vdots & \vdots & \ddots \end{bmatrix}.$$

Kronecker powers are defined by  $A^{\otimes n} \triangleq A \otimes A^{\otimes n-1} = A^{\otimes n-1} \otimes A$ . The following well-known multiplication identity for Kronecker products will also be useful

$$(A \otimes B)(C \otimes D) = AC \otimes BD.$$

## 1.2 How can we manipulate it?

In quantum mechanics, there are only two types of operations: unitary evolution and measurement. All of quantum computing is based on these two operations. For  $n$  qubits, unitary evolution takes the form

$$|\psi\rangle \mapsto U |\psi\rangle$$

where  $U \in \mathbb{C}^{2^n \times 2^n}$  is a unitary matrix. For  $n = 1$ , two important unitaries are the Pauli matrices

$$X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

In quantum, a binary measurement of an  $n$ -qubit pure state  $|\psi\rangle$  is defined by a matrix  $\Pi \in \mathbb{C}^{2^n \times 2^n}$  satisfying the orthogonal projection conditions  $\Pi^2 = \Pi$  and  $\Pi^\dagger = \Pi$ . The mathematical process of simulating a measurement consists of first writing the orthogonal decomposition

$$|\psi\rangle = \Pi |\psi\rangle + (\mathbb{I} - \Pi) |\psi\rangle$$

and then computing the energy  $p = \|\Pi |\psi\rangle\|^2 = \langle \psi | \Pi | \psi \rangle$  in the first component. Then, the measurement outcome is determined by a classical Bernoulli- $p$  random bit  $B$  (i.e., where  $B = 1$  with probability  $p$ ) and the resulting quantum state is given by

$$|\psi'\rangle = \begin{cases} \frac{1}{\sqrt{1-p}} (\mathbb{I} - \Pi) |\psi\rangle & \text{if } B = 0 \\ \frac{1}{\sqrt{p}} \Pi |\psi\rangle & \text{if } B = 1. \end{cases}$$

A key point is that  $|\psi'\rangle = |\psi\rangle$  with probability 1 if  $\Pi |\psi\rangle = |\psi\rangle$  or  $\Pi |\psi\rangle = 0$ .

**Example 1.** Consider  $|\psi\rangle = (|01\rangle - |10\rangle) / \sqrt{2}$  and  $\Pi = |00\rangle\langle 00| + |10\rangle\langle 10|$ . Then,  $\Pi |\psi\rangle = -|10\rangle / \sqrt{2}$  and  $p = 1/2$  which makes  $B$  into a uniform random bit. If  $B = 0$ , then the post-measurement state is  $|\psi'\rangle = |01\rangle$  and, if  $B = 1$ , then it is  $|\psi'\rangle = -|10\rangle$ .

This type of measurement generalizes naturally to *projective measurement* where multiple outcomes are defined by a set of  $m$  orthogonal projections  $\{\Pi_i\}$  that sum to the identity (i.e.,  $\sum_i \Pi_i = \mathbb{I}$ ). In that case, the outcome takes one of  $m$  outcomes and the probability of the  $i$ th outcomes is  $p_i = \|\Pi_i |\psi\rangle\|^2$ . Similarly, if the  $i$ th outcome occurs, then the post-measurement state is given by  $|\psi'\rangle = |\psi\rangle / \sqrt{p_i}$ .

## 1.3 How do disturbances affect it?

When transmitting a sequence of classical bits, the most common error is a bit-flip error.

Similarly, for a single qubit, a quantum bit-flip error is defined by the  $X$  operator above because

$$\begin{aligned} X |0\rangle &= |1\rangle \\ X |1\rangle &= |0\rangle. \end{aligned}$$

Another type of error is the quantum phase-flip error. This has no classical equivalent and is defined by the  $Z$  operator above because

$$\begin{aligned} Z |0\rangle &= |0\rangle \\ Z |1\rangle &= -|1\rangle. \end{aligned}$$

Of course, the set of all possible disturbances for a qubit is much larger. One of the surprising parts of quantum error correction (QEC) is that it quantum information can stored and communicated reliably even if we only correct only  $X$  and  $Z$  errors.

For  $n$  qubits, any bit flip or phase flip can affect any qubit. Thus, we let  $X_i$  denote the action of a bit-flip error on the  $i$ th bit. Likewise, we let  $Z_i$  denote the action of a phase-flip error on the  $i$ th bit. Thus, for all  $x \in \{0, 1\}^n$ , these errors are completely defined by action on the computational basis elements

$$\begin{aligned} X_i |x_1 \cdots x_i \cdots x_n\rangle &= |x_1 \cdots \overline{x_i} \cdots x_n\rangle \\ Z_i |x_1 \cdots x_i \cdots x_n\rangle &= (-1)^{x_i} |x_1 \cdots x_i \cdots x_n\rangle, \end{aligned}$$

where  $\overline{x_i}$  denotes the logical negation of  $x_i$ .

## 1.4 How can we mitigate them?

Since quantum operations are defined by unitary evolution and measurement, any  $2^k$ -dimensional subspace of  $\mathbb{C}^{2^n}$  can be treated equivalently as a quantum computer with  $k$  bits. To do this, we can simply have all unitaries and measurements act only on the chosen subspace.

For example, with  $n = 3$  and  $k = 1$ , we can choose the subspace spanned by  $|000\rangle$  and  $|111\rangle$ . This subspace contains a single *logical qubit* in the state

$$|\psi_0\rangle = \alpha |000\rangle + \beta |111\rangle.$$

This representation gives a quantum error correcting code that can correct a single bit-flip error. To see this, observe that

$$\begin{aligned} |\psi_1\rangle &= X_1 |\psi_0\rangle = \alpha |100\rangle + \beta |011\rangle \\ |\psi_2\rangle &= X_2 |\psi_0\rangle = \alpha |010\rangle + \beta |101\rangle \\ |\psi_3\rangle &= X_3 |\psi_0\rangle = \alpha |001\rangle + \beta |110\rangle. \end{aligned}$$

Since all of these states lie in orthogonal subspaces, we can use a projective measurement with 4 outcomes to determine which error occurred:

$$\begin{aligned} \Pi_0 &= |000\rangle\langle 000| + |111\rangle\langle 111| \\ \Pi_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| \\ \Pi_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| \\ \Pi_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|. \end{aligned}$$

A key point is that the outcome of this measurement will be deterministic because each vector is contained in exactly one of these subspaces. In particular, we have

$$\Pi_i |\psi_j\rangle = \begin{cases} |\psi_i\rangle & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

Due to this property, the measurement will also preserve the superposition of logical qubit in the post-measurement state. Specifically, if the  $i$ th error occurs, then the  $i$ th outcome will occur with certainty and the resulting post-measurement will equal the original state because

$$\Pi_i |\psi_i\rangle = |\psi_i\rangle.$$

The final step in error correction is to undo the error by applying  $X_i$  to the post-measurement state if the  $i$ th outcome occurs (with  $X_0 = I$ ). This works because

$$X_i \Pi_i |\psi_i\rangle = X_i X_i |\psi_0\rangle = |\psi_0\rangle.$$

But, what about phase-flip errors? Unfortunately, this quantum code is blind to  $Z$  errors because

$$\Pi_0 Z_i |\psi_0\rangle = Z_i |\psi_0\rangle.$$

For this reason, it cannot correct or even detect any pattern of  $Z$  errors. In these notes, we will describe general approaches to design quantum codes that can correct both  $X$  and  $Z$  errors.

Lastly, it is also good to think about operations on the logical qubit. For example, suppose we want to apply the  $X$  operator to our logical qubit. How can we implement this physically? Denoting the logical  $X$  operator by  $\bar{X}$ , we see that its definition requires that

$$\bar{X} |\psi_0\rangle = \beta |000\rangle + \alpha |111\rangle.$$

Thus, we can choose  $\bar{X} = X_1 X_2 X_3$ . The same idea shows that we can choose logical  $Z$  to be  $\bar{Z} = Z_1$ .

## 1.5 What can we do with it?

To achieve perfectly secure communications of  $n$  bits between two parties, cryptography requires that the two parties have access to a shared random key with entropy greater than  $n$ . Thus, the key challenge (pun intended) occurs in the initial stage where the two parties must agree on a key while keeping it secret from all possible eavesdroppers. Using only classical communication, this cannot be made secure against an eavesdropper who can intercept and forge messages.

But, one can achieve this goal using quantum communication. The technique was first described by Bennett and Brassard in 1984 and is known as the BB84 protocol. In this problem, Alice and Bob want to agree on a secret random string using quantum and classical communication in a way that is robust to the presence of Eve who can intercept and modify the messages sent back and forth. The protocol consists of the following steps:

- Alice generates two sets of  $m$  uniform random bits  $A_1, \dots, A_m$  and  $D_1, \dots, D_m$
- Bob generates one set of  $m$  uniform random bits  $B_1, \dots, B_m$
- Then, for each  $i \in [m]$ , Alice sends to Bob the quantum state

$$|\phi_i\rangle = \begin{cases} |0\rangle & \text{if } A_i = 0, D_i = 0 \\ |1\rangle & \text{if } A_i = 0, D_i = 1 \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \text{if } A_i = 1, D_i = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } A_i = 1, D_i = 1 \end{cases}$$

- Bob receives the state and then applies the projective measurement  $\{\Pi_{B_i}, I - \Pi_{B_i}\}$  where

$$\Pi_b = \begin{cases} |1\rangle\langle 1| & \text{if } b = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } b = 1 \end{cases}$$

- Alice uses classical communication to reveal her sequence  $A_1, \dots, A_m$
- Bob sees Alice's  $A_1, \dots, A_m$  sequence and then compares it to his  $B_1, \dots, B_m$  sequence. For all  $i \in [m]$  where  $A_i = B_i$ , the outcome of Bob's measurement will reveal the value of Alice's  $D_i$  bit. This gives a set of shared random bits between Alice and Bob.
- A very important property from quantum mechanics is that Eve cannot learn the values of too many of these bits without being detected!
- The shared random bits generated by this process allow Alice and Bob to use classical communication to agree on a smaller set of random key bits of which Eve has essentially no knowledge. This process is called privacy amplification.

The quantum process prevents Eve from listening without being detected because, in order to eavesdrop, Eve must measure the quantum state. But, any measurement strategy that can recover a significant amount of information must also disturb the transmitted states in a way that can be detected. One reason is that, if  $A_i \neq B_i$ , then Bob's measurement outcome is independent of  $D_i$ . Eve has the same problem trying to eavesdrop. She doesn't know  $A_i$  but if she measures a state, she must still forward something to Bob to avoid detection. During the reconciliation process, Alice and Bob will discover that there are too many errors in the bits where they chose the same basis for transmission and measurement. This will reveal the presence of Eve.

## 2 Mathematical Background

### 2.1 Basic Quantum Setup

For  $n$  qubits, a quantum pure state is a vector in  $(\mathbb{C}^2)^{\otimes n} \simeq \mathbb{C}^{2^n}$ . The "classical" state associated with the binary string  $x = (x_1, x_2, \dots, x_n) \in \{0, 1\}^n$  is the standard basis vector  $|x\rangle = |x_1 x_2 \dots x_n\rangle \in \mathbb{C}^{2^n}$

whose unit element is in the index  $1 + \sum_{i=1}^n x_i 2^{n-i}$ . Such a vector is part of the *computational basis* and can be defined by

$$|x\rangle := |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle,$$

where  $\otimes$  denotes the Kronecker product matrices (see below for definition). Thus, an arbitrary pure state can be written as

$$|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle.$$

The quantum measurement introduced earlier is called a projective measurement and it is the simplest type of measurement. While there are more general types of measurements, they can be always be implemented by introducing additional *ancilla* qubits and then using a projective measurement. Thus, we restrict our attention to this case. Here, we restate the previous description.

**Definition 2.** A *projective measurement* is defined by a set of  $m$  orthogonal projections  $\{\Pi_i\}$  that sum to the identity (i.e.,  $\sum_i \Pi_i = \mathbb{I}$ ). Each projector represents a possible outcome of the measurement. For a state  $|\psi\rangle$ , the result of the measurement is a classical random variable  $M$  which indicates which outcome occurred and the post-measurement quantum state  $|\psi'\rangle$  of the system. The Born rule states that the probability of the  $i$ th outcome is  $\Pr(M = i) = p_i$ , where

$$p_i = \|\Pi_i |\psi\rangle\|^2.$$

Finally, if the  $i$ th outcome occurs, then the post-measurement state is given by  $|\psi'\rangle = |\psi\rangle / \sqrt{p_i}$ .

In quantum mechanics, the overall (or global) phase of a quantum state does not affect any measurable physical quantity. This is because the probability of a measurement outcome only depends on the energy that state has in the subspace associated with that outcome.

## 2.2 The Pauli Group

The following 4 Hermitian matrices are called the Pauli matrices:

$$I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y := \iota XZ = \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix},$$

where  $\iota = \sqrt{-1}$ . One can verify that these matrices generate the Pauli group on 1 qubit which is given by

$$\mathcal{P}_1 = \{\pm I, \pm X, \pm Y, \pm Z, \pm \iota X, \pm \iota Y, \pm \iota Z\}.$$

This group can also be defined by the relations  $X^2 = Z^2 = I$ ,  $XZ = -ZX$ , and  $Y = \iota XZ$ .

For  $n$  qubits, the Pauli group is formed by taking tensor products of these matrices. Let  $D: \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{C}^{2^n \times 2^n}$  be defined by

$$D(a, b) := X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}.$$

**Definition 3.** The *Pauli group*  $\mathcal{P}_n$  (aka the Heisenberg-Weyl group  $HW_{2^n}$ ) on  $n$  qubits is

$$\mathcal{P}_n := \{\iota^\kappa D(a, b) \mid a, b \in \{0,1\}^n, \kappa \in \{0,1,2,3\}\}.$$

To understand its structure, we can compute

$$\begin{aligned} D(a, b)D(a', b') &= (X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n})(X^{a'_1} Z^{b'_1} \otimes \cdots \otimes X^{a'_n} Z^{b'_n}) \\ &= (X^{a_1} Z^{b_1} X^{a'_1} Z^{b'_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} X^{a'_n} Z^{b'_n}) \\ &= (-1)^{\sum_{i=1}^n b_i a'_i} (X^{a_1+a'_1} Z^{b_1+b'_1} \otimes \cdots \otimes X^{a_n+a'_n} Z^{b_n+b'_n}) \\ &= (-1)^{b \cdot a'} D(a + a', b + b'), \end{aligned}$$

where the dot product  $a \cdot b := \sum_{i=1}^n a_i b_i$  is computed with integer operations and the additions  $a + a'$  and  $b + b'$  are defined via the identification  $\{0,1\}^n \simeq \mathbb{Z}_2^n$ . Using this formula twice, one can verify that any two

Paulis  $D(a, b)$  and  $D(a', b')$  either commute or anti-commute. They commute when  $b \cdot a' \equiv b' \cdot a \pmod{2}$  which is precisely when the symplectic inner product

$$\langle (a, b), (a', b') \rangle_s := (a \cdot b' + a' \cdot b) \pmod{2},$$

equals 0.

Here are some important facts about Paulis:

- A general Pauli  $P = \iota^\kappa D(a, b)$  is Hermitian if and only if  $\kappa = a \cdot b \pmod{2}$  because choosing  $\kappa = a \cdot b$  makes  $P$  into a tensor product of  $I, X, Y, Z$  and choosing  $\kappa = a \cdot b + 2$  only changes the overall sign.
- For the same reason, two Hermitian Paulis  $P, P'$  always commute (i.e.,  $PP' = P'P$ ) or anticommute (i.e.,  $PP' = -P'P$ ).
- An Hermitian Pauli  $P = \pm \iota^{a \cdot b} D(a, b)$  with  $(a, b) \neq (0, 0)$  has an equal number of  $+1$  and  $-1$  eigenvalues. This holds because  $P$  is equal to  $\pm 1$  times a tensor product of  $I, X, Y, Z$  and the matrices  $X, Y, Z$  have an equal number of  $+1$  and  $-1$  eigenvalues. For a tensor product of two matrices, the set of eigenvalues equals the set of all products of the eigenvalues of the component matrices. For Hermitian Paulis, this means that only  $\pm D(0, 0)$  will not have an equal number of  $+1$  and  $-1$  eigenvalues.

### 2.3 Pauli Group Isomorphism

Consider the group  $(G, \star)$  defined by the product set  $G = \mathbb{Z}_2^n \times \mathbb{Z}_2^n \times \mathbb{Z}_4$  equipped with the group operation

$$(a, b, k) \star (a', b', k') = (a + a', b + b', k + k' + 2b \cdot a'),$$

where integer addition is modulo 2 for the first two elements and modulo 4 for the third element. Thus, this is almost a product group except for the twist where the last element is  $k + k' + 2b \cdot a'$  instead of  $k + k'$ . Now, consider the function  $\theta: G \rightarrow \mathcal{P}_n$  defined by

$$\theta(a, b, k) = \iota^k D(a, b).$$

This is a group isomorphism from  $G$  to  $\mathcal{P}_n$  because

$$\begin{aligned} \theta((a, b, k) \star (a', b', k')) &= \theta(a + a', b + b', k + k' + 2b \cdot a') \\ &= \iota^{k+k'+2b \cdot a'} D(a + a', b + b') \\ &= \iota^k D(a, b) \iota^{k'} D(a', b') \\ &= \theta(a, b, k) \theta(a', b', k') \end{aligned}$$

and both groups have exactly  $4^{n+1}$  elements. The main utility of this isomorphism is that we can easily represent all  $n$ -qubit Pauli matrices, which live in  $\mathbb{C}^{2^n \times 2^n}$ , using just  $2n$  bits and 4 phases.

Since the overall phase of a quantum state does not affect any measurable physical quantity, one can effectively ignore the overall phase of the elements of the Pauli group. Mathematically, this is handled by identifying the subgroup  $\langle \iota \mathbb{I} \rangle = \{ \mathbb{I}, \iota \mathbb{I}, -\mathbb{I}, -\iota \mathbb{I} \}$  and constructing the quotient group

$$\mathcal{P}_n^* = \mathcal{P}_n / \langle \iota \mathbb{I} \rangle.$$

This group  $\mathcal{P}_n^*$  represents the Pauli group on  $n$  qubits when overall phase is ignored.

**Lemma 4.** *The group  $\mathcal{P}_n^*$  is isomorphic to the product group  $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ .*

*Proof.* This holds because the twist in the group  $\mathcal{P}_n$  only affects the overall phase factor. To see this, let  $\pi: \mathbb{Z}_2^n \times \mathbb{Z}_2^n \times \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^n \times \mathbb{Z}_2^n$  be the projection defined by  $(a, b, k) \mapsto (a, b)$  which drops the last element. Then,  $\pi \circ \phi^{-1}: \mathcal{P}_n \rightarrow \mathbb{Z}_2^n \times \mathbb{Z}_2^n$  is a group homomorphism from  $\mathcal{P}_n \rightarrow \mathbb{Z}_2^n \times \mathbb{Z}_2^n$  whose kernel is  $\langle \iota \mathbb{I} \rangle$ . By the first isomorphism theorem, the image of  $\mathcal{P}_n$  under  $\pi \circ \theta^{-1}$  is isomorphic to quotient of  $\mathcal{P}_n$  by the kernel of  $\pi \circ \theta^{-1}$  which is  $\mathcal{P}_n / \langle \iota \mathbb{I} \rangle$ .  $\square$

**Lemma 5.** *Let  $\mathcal{S} \subseteq \mathcal{P}_n$  be a commutative Hermitian subgroup of  $\mathcal{P}_n$  such that  $-\mathbb{I} \notin \mathcal{S}$ . Then, for some  $k \in \{0, 1, \dots, n\}$ ,  $\mathcal{S}$  has  $2^k$  elements generated by a subset of  $k$  independent generators.*

*Proof.* Since the image of  $\mathcal{S}$  under  $\pi \circ \theta^{-1}$  is a subgroup of  $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ , it follows that  $|\mathcal{S}|$  divides  $|\mathbb{Z}_2^n \times \mathbb{Z}_2^n| = 2^{2n}$  and thus  $\mathcal{S}$  has  $2^k$  elements for some  $k \in \{0, 1, \dots, n\}$ . For each  $P \in \mathcal{S}$ , we have  $\{\iota P, -P, -\iota P\} \cap \mathcal{S} = \emptyset$  because both  $\iota P$  and  $-\iota P$  are not Hermitian and  $-P \notin \mathcal{S}$  because otherwise  $-\mathbb{I} = P(-P) \in \mathcal{S}$ . Since each  $P \in \mathcal{P}_n$  occurs with only one global phase and the only effect of  $\pi \circ \theta^{-1}$  is to remove this global phase, we have  $|(\pi \circ \theta^{-1})(\mathcal{S})| = |\mathcal{S}|$ . Finally, any size  $2^k$  subgroup of  $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$  is also a subspace. Thus, any minimal set of generators consists contains  $k$  linearly independent elements.  $\square$

## 3 Quantum Error Correction

### 3.1 Warm Up

If one is allowed general quantum operations on  $n$  physical qubits represented by  $\mathbb{C}^{2^n}$ , then any  $2^k$  dimensional subspace can be treated as  $k$  logical qubits. Thus, a quantum error-correcting code (QECC) with  $k$  logical qubits and  $n$  physical qubits is defined to be a  $2^k$  dimensional subspace  $\mathcal{C}$  of  $\mathbb{C}^{2^n}$ . If one has an encoding map  $F: \mathbb{C}^{2^k} \rightarrow \mathcal{C}$  for this code, then one physical implementation of a logical unitary  $U \in \mathbb{C}^{2^k \times 2^k}$  is given by  $FUF^{-1}$  because this maps the code space to the logical space, applies the logical operation, and then maps the logical space back to the code space.

Using this code definition, consider the set of Pauli errors. Each error  $E \in \mathcal{P}_n$  defines a shift of the code subspace  $\mathcal{C} \mapsto EC$ . Thus, two Pauli errors  $E, E' \in \mathcal{P}_n$  can be distinguished and corrected if  $EC \perp E'C$ . The idea is that a projective measurement is first used to distinguish the subspace  $EC$  from the subspace  $E'C$  and then the inverse of the identified error operator can be applied to recover the original state.

It is easy to see that the same argument extends to any subset  $\mathcal{E} \subset \mathcal{P}_n$  such that, for all distinct  $E, E' \in \mathcal{E}$ , we have  $EC \perp E'C$ . Thus, we have a simple condition that is sufficient for general Pauli error correction. What about non-Pauli errors? There was an early worry that quantum error correction was not possible because it requires correcting arbitrarily small errors in the continuous basis coefficients.

Fortunately, this barrier does not exist. As we will see, the measurement process can be used to simultaneously quantize the error into the set of Pauli errors and also identify the resulting Pauli error. This because the error-correction mechanism extends to any unitary error  $U = \sum_i \alpha_i E_i$  which is a linear combination of correctable errors in  $\mathcal{E}$  with  $\sum_i |\alpha_i|^2 = 1$ . For  $|\psi\rangle \in \mathcal{C}$  and

$$U|\psi\rangle = \sum_i \alpha_i E_i |\psi\rangle,$$

we can apply a projective measurement to distinguish between correctable shifts of the code subspace. The outcome results in the Pauli error  $E_i$  with probability  $|\alpha_i|^2$  which is correctable by assumption. Conceptually, the measurement quantizes the unitary error into a Pauli error that can be corrected exactly.

We note that a necessary and sufficient condition for general quantum error correction was given by Knill and LaFlamme [1].

### 3.2 Calderbank-Shor-Steane (CSS) Codes

The first general class of QECCs were constructed in two papers: one by Calderbank and Shor and the other by Steane [2, 3, 4]. They are now called CSS codes. The construction is based on an classical  $[n, k_1]$  binary linear code  $\mathcal{C}_1$  that contains an  $[n, k_2]$  subcode  $\mathcal{C}_2$ . The construction starts by writing the generator matrix of  $\mathcal{C}_1$  in the form

$$G_1 = \begin{bmatrix} G_{1/2} \\ G_2 \end{bmatrix},$$

where  $G_2$  is a  $k_2 \times n$  generator matrix for  $\mathcal{C}_2$  and  $G_{1/2}$  is a  $(k_1 - k_2) \times n$  matrix that generates a set of coset representatives for  $\mathcal{C}_2$  inside  $\mathcal{C}_1$  (e.g.,  $\mathcal{C}_2$  is a subgroup of  $\mathcal{C}_1$ ). The following definition shows how this can be used to define a quantum code with  $n$  physical qubits and  $k = k_1 - k_2$  logical qubits.

**Definition 6.** A CSS quantum error-correcting code is the subspace  $\mathcal{C}$  spanned by the basis elements  $|u\rangle_L$  for  $u \in \{0, 1\}^{k_1 - k_2}$  which are defined by

$$|u\rangle_L := \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |uG_{1/2} + y\rangle.$$

**Lemma 7.** Each element  $|\psi\rangle \in \mathcal{C}$  of the CSS code space satisfies the “stabilizer” conditions,

$$\begin{aligned} D(a, 0) |\psi\rangle &= |\psi\rangle \\ D(0, b) |\psi\rangle &= |\psi\rangle, \end{aligned}$$

for all  $a \in \mathcal{C}_2$  and  $b \in \mathcal{C}_1^\perp$ .

*Proof.* To prove this, it is sufficient to show that the basis elements  $|u\rangle_L$  for  $u \in \{0, 1\}^{k_1 - k_2}$  satisfy

$$\begin{aligned} D(a, 0) |u\rangle_L &= |u\rangle_L \\ D(0, b) |u\rangle_L &= |u\rangle_L \end{aligned}$$

for all  $a \in \mathcal{C}_2$  and  $b \in \mathcal{C}_1^\perp$ . First, we observe the “X-stabilizer” condition

$$\begin{aligned} D(a, 0) |u\rangle_L &= D(a, 0) \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |uG_{1/2} + y\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |uG_{1/2} + y + a\rangle \\ &= |u\rangle_L, \end{aligned}$$

where the last step holds because  $a \in \mathcal{C}_2$  implies  $\mathcal{C}_2 + a = \mathcal{C}_2$ . Next, we observe the “Z-stabilizer” condition

$$\begin{aligned} D(0, b) |u\rangle_L &= D(0, b) \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |uG_{1/2} + y\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} D(0, b) |uG_{1/2} + y\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} (-1)^{b \cdot (uG_{1/2} + y)} |uG_{1/2} + y\rangle \\ &= |u\rangle_L, \end{aligned}$$

where the last step holds because  $b \in \mathcal{C}_1^\perp$  implies  $b \cdot c = 0$  for all  $c \in \mathcal{C}_1$ . □

**Lemma 8.** For  $\bar{a} \in \{0, 1\}^k$ , the logical X operation  $D(\bar{a}, 0) \in \mathbb{C}^{2^k \times 2^k}$  is implemented by the physical X operator  $D(\bar{a}G_{1/2}, 0) \in \mathbb{C}^{2^n \times 2^n}$ . For  $\bar{b} \in \{0, 1\}^k$ , the logical Z operation  $D(0, \bar{b}) \in \mathbb{C}^{2^k \times 2^k}$  is implemented by the physical Z operator  $D(0, \bar{b}F_{1/2}) \in \mathbb{C}^{2^n \times 2^n}$  where  $F_{1/2} \in \mathbb{Z}_2^{(k_1 - k_2) \times n}$  is a matrix satisfying  $G_{1/2}F_{1/2}^T = I_k$  and  $F_{1/2}y = 0$  for all  $y \in \mathcal{C}_2$ .

*Proof.* The first statement follows from applying the proposed logical operator to the logical basis vectors of the CSS code

$$\begin{aligned} D(\bar{a}G_{1/2}, 0) |u\rangle_L &= D(\bar{a}G_{1/2}, 0) \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |uG_{1/2} + y\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |uG_{1/2} + y + \bar{a}G_{1/2}\rangle \\ &= |u + \bar{a}\rangle_L. \end{aligned}$$

Likewise, the second statement follows from applying the proposed logical operator to the logical basis vectors of the CSS code

$$\begin{aligned}
D(0, \bar{b}F_{1/2})|u\rangle_L &= D(0, \bar{b}F_{1/2})\frac{1}{\sqrt{|\mathcal{C}_2|}}\sum_{y\in\mathcal{C}_2}|uG_{1/2}+y\rangle \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}}\sum_{y\in\mathcal{C}_2}(-1)^{\bar{b}F_{1/2}\cdot(uG_{1/2}+y)}|uG_{1/2}+y\rangle \\
&= (-1)^{\bar{b}\cdot u}|u\rangle_L,
\end{aligned}$$

where the last step holds because  $\bar{b}F_{1/2}\cdot(uG_{1/2}+y) = \bar{b}\cdot u$ . This last identity holds because Lemma 20 shows we can choose  $F_{1/2}$  such that  $G_{1/2}F_{1/2}^T = I_k$  and  $F_{1/2}y = 0$  for all  $y \in \mathcal{C}_2$ .  $\square$

The minimum distance of a classical code is the smallest number of coordinates that must be modified to change one codeword into another. Similarly, the minimum distance of a quantum code is the minimum number of qubits that must be disturbed in order to change the logical code state while remaining in the code space. For CSS codes, it also makes sense to distinguish between protection against  $X$  and  $Z$  errors.

**Definition 9.** The *minimum distance of a CSS code* is  $d = \min\{d_X, d_Z\}$ , where  $d_X$  and  $d_Z$  are the minimum Hamming weights of all non-zero binary representations of logical  $X$  and  $Z$  operators. Mathematically, we let  $w_H$  denote the Hamming weight and find that

$$\begin{aligned}
d_X &= \min_{\bar{a}\in\mathbb{Z}_2^{k_1-k_2}\setminus\{0\}} w_H(\bar{a}G_{1/2}) \\
d_Z &= \min_{\bar{b}\in\mathbb{Z}_2^{k_1-k_2}\setminus\{0\}} w_H(\bar{b}F_{1/2}).
\end{aligned}$$

As we will see below, a CSS code is a “stabilizer code” where the stabilizers are generated by subset consisting of only- $X$  operators (e.g., like  $D(a, 0)$ ) and only- $Z$  operators (e.g., like  $D(0, b)$ ). These generators act as quantum parity checks in the following sense. For a Pauli error  $D(e_x, e_z)$ , there is a projective measurement that computes binary syndrome vectors for  $e_x$  (relative to a parity-check matrix for  $\mathcal{C}_1$ ) and  $e_z$  (relative to the parity-check matrix of  $\mathcal{C}_2^\perp$  such as  $G_2$ ). Thus, if we fix a syndrome decoder for  $\mathcal{C}_1$  that corrects all binary errors in the set  $\mathcal{E}_x$  and a syndrome decoder for  $\mathcal{C}_2^\perp$  that corrects all binary errors in the set  $\mathcal{E}_z$ , then the CSS code can correct all Pauli errors of the form  $D(e_x, e_z)$  with  $e_x \in \mathcal{E}_x$  and  $e_z \in \mathcal{E}_z$ . In fact, one can correct more errors than this but that will be discussed later.

This error correction idea is essentially identical to that of the previous section. There is a projective measurement that, without disturbing the logical subspace, reveals the syndrome of the  $X$  error using the binary code  $\mathcal{C}_1$  and the syndrome of the  $Z$  error using the binary code  $\mathcal{C}_2^\perp$ . Then, syndrome decoding is employed for both codes to compute maximum-likelihood (ML) estimates  $\hat{e}_x$  and  $\hat{e}_z$  for the errors. These ML errors are inverted by applying  $D(\hat{e}_x, \hat{e}_z)$  and the original state is recovered (up to a global phase) if  $\hat{e}_x = e_x$  and  $\hat{e}_z = e_z$ . This idea will be described in more detail below in the context of stabilizer codes.

*Remark 10.* One confusing element of CSS codes is that codes and their duals play nonstandard roles relative to classical coding. For example, the  $X$ -stabilizers act as quantum parity checks but they are the codewords of  $\mathcal{C}_2$  (rather than parity checks). Moreover, it is standard to call the generator matrix  $G_2$  for  $\mathcal{C}_2$  a stabilizer generator matrix. In contrast, it is the parity-check matrix of  $\mathcal{C}_1$  that is the stabilizer generator for the  $Z$ -stabilizers.

### 3.3 Stabilizer Codes

The code definition from Section 3.1 is akin to the definition  $\mathcal{C} \subseteq \{0, 1\}^n$  of an unstructured binary error-correcting code. However, in classical coding, it is much easier to work with linear codes. Stabilizer codes are the natural generalization of linear codes to QECC [5, 6, 7]. They are defined by a set of Pauli operators that define “quantum parity-checks” called stabilizers. CSS codes are a special case of stabilizer codes that are somewhat simpler.

**Definition 11.** A Pauli operator  $P \in \mathcal{P}_n$  stabilizes a state  $|\psi\rangle \in \mathbb{C}^{2^n}$  if  $P|\psi\rangle = |\psi\rangle$  (i.e.,  $|\psi\rangle$  is an eigenvector of  $P$  with eigenvalue 1).

**Example 12.** For  $n = 3$  and a state  $|\psi\rangle \in \mathbb{C}^8$ , the Pauli operator  $D(111, 000) = X_1X_2X_3$  stabilizes  $|\psi\rangle$  if and only if the expansion of  $|\psi\rangle$  in the computational basis has equal coefficients on  $|x_1x_2x_3\rangle$  and  $|\bar{x}_1\bar{x}_2\bar{x}_3\rangle$ .

**Example 13.** For  $n = 3$  and a state  $|\psi\rangle \in \mathbb{C}^8$ , the Pauli operator  $D(000, 111) = Z_1Z_2Z_3$  stabilizes  $|\psi\rangle$  if and only if the expansion of  $|\psi\rangle$  in the computational basis has a zero coefficient on all  $|x_1x_2x_3\rangle$  where  $(x_1, x_2, x_3)$  has an odd number of ones.

**Lemma 14.** For any Hermitian unitary matrix  $U$ , the matrix  $\Pi(U) := \frac{1}{2}(\mathbb{I} + U)$  is an orthogonal projection matrix onto the subspace  $V \subseteq \mathbb{C}^{2^n}$  of vectors stabilized by  $U$  and  $\text{Tr}(\Pi(U)) = \dim(V)$ . Similarly, the matrix  $\frac{1}{2}(\mathbb{I} - U)$  is an orthogonal projection matrix onto the orthogonal complement  $V^\perp$ .

*Proof.* Since  $U^\dagger = U$ , we have  $U^2 = \mathbb{I}$  and  $U$  is diagonalizable with all real eigenvalues equal to  $+1$  or  $-1$ . To verify that  $\Pi = \Pi(U)$  is an orthogonal projection, we first observe that  $\Pi$  is Hermitian and idempotent:

$$\begin{aligned}\Pi^\dagger &= \frac{1}{2}(\mathbb{I} + U)^\dagger = \frac{1}{2}(\mathbb{I} + U^H) = \Pi, \\ \Pi^2 &= \frac{1}{4}(\mathbb{I} + 2U + U^2) = \frac{1}{2}(\mathbb{I} + U) = \Pi.\end{aligned}$$

Since  $U|\psi\rangle = |\psi\rangle$  if and only if  $\Pi|\psi\rangle = \frac{1}{2}(\mathbb{I} + U)|\psi\rangle = |\psi\rangle$ , we see that  $\Pi$  projects onto the  $+1$  eigenspace of  $U$  (i.e., the subspace of vectors stabilized by  $U$ ). For the orthogonal projection  $\Pi$ , the  $+1$  eigenvalues can be put into one-to-one correspondence with the elements of an orthogonal basis for  $V$ . This implies that  $\text{Tr}(\Pi) = \dim(V)$ . For  $\frac{1}{2}(\mathbb{I} - U)^\dagger$ , we find that

$$\begin{aligned}\frac{1}{2}(\mathbb{I} - U)^\dagger &= \frac{1}{2}(\mathbb{I} - U^\dagger) = \frac{1}{2}(\mathbb{I} - U)^\dagger, \\ \left(\frac{1}{2}(\mathbb{I} - U)^\dagger\right)^2 &= \frac{1}{4}(\mathbb{I} - 2U + U^2) = \frac{1}{2}(\mathbb{I} - U).\end{aligned}$$

Since  $U|\psi\rangle = -|\psi\rangle$  if and only if  $\frac{1}{2}(\mathbb{I} - U)|\psi\rangle = |\psi\rangle$ , we see that  $\frac{1}{2}(\mathbb{I} - U)^\dagger$  projects onto the  $-1$  eigenspace of  $U$ . Since  $U$  is Hermitian and all eigenvalues are  $+1$  or  $-1$ , the  $\pm 1$  eigenspaces are orthogonal complements of each other and  $\frac{1}{2}(\mathbb{I} - U)^\dagger$  projects onto  $V^\perp$ .  $\square$

**Definition 15.** A subgroup  $\mathcal{S} \subseteq \mathcal{P}_n$  of the Pauli group on  $n$  qubits is called a *stabilizer* subgroup if  $-\mathbb{I} \notin \mathcal{S}$  and all elements in  $\mathcal{S}$  commute with each other and are Hermitian.

By Lemma 5, a stabilizer subgroup with  $|\mathcal{S}| = 2^r$  has an independent set of  $r$  Hermitian generators  $G_1, \dots, G_r$  such that, for any  $P \in \mathcal{S}$ , there is a  $D \subseteq [r]$  such that  $P = \prod_{i \in D} G_i$ . Thus, if  $|\psi\rangle \in \mathbb{C}^{2^n}$  satisfies  $G_i|\psi\rangle = |\psi\rangle$  for all  $i \in [r]$ , then  $P|\psi\rangle = |\psi\rangle$  for all  $P \in \mathcal{S}$ .

Since all Hermitian Paulis take the form  $\delta_i \iota^{a_i \cdot b_i} D(a_i, b_i)$  for some  $a, b \in \mathbb{Z}_2^n$  and  $\delta \in \{\pm 1\}$ , we can choose  $a_i, b_i \in \mathbb{Z}_2^n$  and  $\delta_i \in \{\pm 1\}$  such that  $G_i = \delta_i \iota^{a_i \cdot b_i} D(a_i, b_i)$ . Using this, the orthogonal projection onto the subspace of  $\mathbb{C}^{2^n}$  stabilized by  $G_i$  is given by

$$\Pi_i = \Pi(G_i) = \frac{\mathbb{I} + \delta_i \iota^{a_i \cdot b_i} D(a_i, b_i)}{2}.$$

**Definition 16.** A quantum stabilizer code  $\mathcal{C}$  with  $n$  physical qubits is defined by a stabilizer subgroup  $\mathcal{S} \subseteq \mathcal{P}_n$  with  $|\mathcal{S}| = 2^r$  via

$$\begin{aligned}\mathcal{C} &= \left\{ |\psi\rangle \in \mathbb{C}^{2^n} \mid \text{for all } P \in \mathcal{S}, P|\psi\rangle = |\psi\rangle \right\} \\ &= \left\{ |\psi\rangle \in \mathbb{C}^{2^n} \mid \text{for all } P \in \{G_1, G_2, \dots, G_r\}, P|\psi\rangle = |\psi\rangle \right\}\end{aligned}$$

$$= \text{range}(\Pi_{\mathcal{C}}),$$

where  $\Pi_{\mathcal{C}}$  is the orthogonal projection onto the subspace  $\mathcal{C}$  given by

$$\Pi_{\mathcal{C}} := \prod_{i=1}^r \frac{\mathbb{I} + \delta_i \iota^{a_i \cdot b_i} D(a_i, b_i)}{2}. \quad (1)$$

The implied binary parity-check (or binary stabilizer generator) matrix  $H \in \mathbb{F}_2^{r \times 2n}$  for  $\mathcal{C}$  is defined by

$$H = \left[ \begin{array}{c|c} a_1 & b_1 \\ a_2 & b_2 \\ \vdots & \vdots \\ a_r & b_r \end{array} \right]. \quad (2)$$

**Lemma 17.** *The quantum stabilizer code  $\mathcal{C}$  defined by a stabilizer subgroup  $\mathcal{S} \subseteq \mathcal{P}_n$  with  $|\mathcal{S}| = 2^r$  is called an  $[[n, k]]$  quantum code because it has  $n$  physical qubits and  $k = n - r$  logical qubits. In other words, it defines a  $2^k$ -dimensional subspace of the  $2^n$ -dimensional space  $\mathbb{C}^{2^n}$  defined by  $n$  physical qubits.*

*Proof.* For an orthogonal projection  $\Pi_{\mathcal{C}}$  onto a subspace  $\mathcal{C}$ , the  $+1$  eigenvalues can be put into one-to-one correspondence with the elements of an orthogonal basis for  $\mathcal{C}$ . Thus, the dimension of the range equals the trace of  $\Pi_{\mathcal{C}}$  and we find that

$$\begin{aligned} \dim(\mathcal{C}) &= \text{Tr}(\Pi_{\mathcal{C}}) \\ &= \text{Tr} \left( \prod_{i=1}^r \frac{\mathbb{I} + \delta_i \iota^{a_i \cdot b_i} D(a_i, b_i)}{2} \right) \\ &= 2^{-r} \sum_{A \subseteq [r]} \text{Tr} \left( \prod_{i \in A} \delta_i \iota^{a_i \cdot b_i} D(a_i, b_i) \right) \\ &= 2^{-r} \text{Tr}(\mathbb{I}) \\ &= 2^{n-r}, \end{aligned}$$

because, for all  $A \subseteq [r] \setminus \emptyset$ , we have

$$\text{Tr} \left( \prod_{i \in A} \delta_i \iota^{a_i \cdot b_i} D(a_i, b_i) \right) = 0.$$

This last statement holds because the matrix inside the trace always has an equal number of  $+1$  and  $-1$  eigenvalues. This follows from noticing that, for all  $A \subseteq [r] \setminus \emptyset$ , there exist  $a, b \in \mathbb{Z}_2^n$  such that  $\prod_{i \in A} \delta_i \iota^{a_i \cdot b_i} D(a_i, b_i) = \pm \iota^{a \cdot b} D(a, b)$  and the linear independence established by Lemma 5 implies  $(a, b) \neq (0, 0)$ . Finally,  $\text{Tr}(\delta \iota^{a \cdot b} D(a, b)) = 0$  if  $(a, b) \neq (0, 0)$  because all such matrices have an equal number of  $+1$  and  $-1$  eigenvalues.

For general stabilizer codes, determining the  $X$  and  $Z$  logicals is somewhat more involved and will not be covered in these notes. Also, the minimum distance of a general stabilizer code equals the minimum number of qubits that must be disturbed in order to change the logical code state while remaining in the code space. For more details, see [5, 8].  $\square$

### 3.4 Syndrome Measurement and Decoding

Since the goal of quantum error correction is to preserve the quantum superposition realized by the logical state, the outcomes of measurements used for error correction must not reveal anything about the logical state in order to avoid collapsing the logical state. Instead, the measurements should only provide information about errors. Fortunately, a blueprint of this type of behavior comes naturally from classical linear error-correcting codes. For a linear code, the syndrome vector depends only on the error

vector and has no dependence on which codeword was transmitted. Fortunately, it is possible to design quantum codes with similar properties and to use quantum measurements to simultaneously project the state and compute the syndrome.

For any Hermitian stabilizer  $P = \delta \iota^{a \cdot b} D(a, b)$  with  $a, b \in \mathbb{Z}_2^n$  and  $\delta \in \{\pm 1\}$ , Lemma 14 shows that  $\Pi(P) = \frac{1}{2}(\mathbb{I} + P)$  is a projection matrix that projects onto the subspace

$$\left\{ |\phi\rangle \in \mathbb{C}^{2^n} \mid P|\phi\rangle = |\phi\rangle \right\}.$$

For any state  $|\psi\rangle$ , the projective measurement  $\{\Pi(P), \mathbb{I} - \Pi(P)\}$  tests if the state is fixed by that stabilizer or not. If the  $\Pi(P)$  outcome occurs, then we say that  $|\psi\rangle$  passes the stabilizer test and the associated syndrome bit is 0. In this case, the post-measurement state  $|\psi'\rangle$  is always stabilized by  $P$ . If the  $\mathbb{I} - \Pi(P)$  outcome occurs, then we say that  $|\psi\rangle$  fails the stabilizer test and the associated syndrome bit is 1. In this case, the post-measurement state  $|\psi'\rangle$  always satisfies  $P|\psi'\rangle = -|\psi'\rangle$  because  $\mathbb{I} - \Pi(P) = \frac{1}{2}(\mathbb{I} - P)$ .

For a code state  $|\psi\rangle \in \mathcal{C}$  and a Hermitian Pauli error  $E \in \mathcal{P}_n$ , the question is what happens when to the projective measurement  $\{\Pi(P), \mathbb{I} - \Pi(P)\}$  of  $E|\psi\rangle$ ? Recall that two Hermitian Paulis  $P, E$  either commute or anticommute. If  $P$  and  $E$  commute, then  $\Pi(P)$  and  $E$  commute and we find that

$$\Pi(P)E|\psi\rangle = E\Pi(P)|\psi\rangle = E|\psi\rangle.$$

Since  $\|E|\psi\rangle\|^2 = 1$ , the associated syndrome bit is 0 and the post-measurement state is  $E|\psi\rangle$ . Likewise, if  $P$  and  $E$  anticommute, then we find that

$$\Pi(P)E|\psi\rangle = \frac{1}{2}(\mathbb{I} + P)E|\psi\rangle = 0.$$

In that case, the associated syndrome bit is 1 and the post-measurement state is  $\frac{1}{2}(\mathbb{I} - P)E|\psi\rangle = E|\psi\rangle$ . Since the post-measurement state does not depend on the outcome, we can correct the error  $E$  after measurement as long as we can identify a correction operator  $C$  such that  $CE \in \mathcal{S}$ . If  $C = E^\dagger$ , then correction works because  $CE = \mathbb{I} \in \mathcal{S}$ . But, any correction operator differing only by a stabilizer also correct the error. This phenomenon was mentioned at the end of Section 3.2 is typically attributed to the *degeneracy* of stabilizer codes

Let  $|\psi\rangle$  be the quantum state after some disturbance. Then, its syndrome vector  $s = (s_1, \dots, s_r) \in \{0, 1\}^r$  is defined by letting  $s_i$  be the syndrome bit value associated with stabilizer generator  $G_i$ . Once the syndrome vector is computed, the decoding problem for stabilizer code is essentially classical. As outlined in Section 3.1, the syndrome measurement quantizes the disturbance to a Pauli error. Let  $\mu((e_x, e_z))$  be the probability that the quantized Pauli error is a scalar multiple of  $D(e_x, e_z)$ . Then, the optimal decoder chooses the correction operator  $C = D(\hat{e}_x, \hat{e}_z) \in \mathcal{P}_n$  that maximizes the probability of correcting the error. Since the error is corrected if and only if  $\iota^\kappa C \cdot D(e_x, e_z) \in \mathcal{S}$  for some  $\kappa \in \{0, 1, 2, 3\}$ , the optimal correction is given by choosing

$$(\hat{e}_x, \hat{e}_z) \in \arg \max_{(e_x, e_z) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n} \sum_{u \in \mathbb{Z}_2^r} \mu((e_x, e_z) + uH),$$

where the RHS is a set because the objective (as a function of  $(e_x, e_z)$ ) is invariant under the addition of linear combinations of rows of  $H$ .

### 3.5 Stabilizer Matrix and CSS Codes

Let us define the binary matrix  $\Lambda \in \mathbb{F}_2^{2n \times 2n}$   $2n \times 2n$  via

$$\Lambda := \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}.$$

Using this, the symplectic inner product is given by

$$\langle (a, b), (a', b') \rangle_s = (a \cdot b' + a' \cdot b) \bmod 2$$

$$= (a, b) \underbrace{\begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}}_{\Lambda} (a', b')^T.$$

Thus, the Hermitian Paulis  $\iota^{a \cdot b} D(a, b)$  and  $\iota^{a' \cdot b'} D(a', b')$  commute if and only if  $(a, b) \Lambda (a', b')^T = 0$ .

A binary parity-check (or stabilizer generator) matrix  $H \in \mathbb{F}_2^{r \times 2n}$  (e.g., see 2) defines a set of  $[[n, n-r]]$  stabilizer codes if it is full rank and the stabilizer generators defined by each row commute. Such a matrix only identifies a set of codes because the exact code also depends on the stabilizer signing vector  $\delta \in \{\pm 1\}^n$  (e.g., see 1). The commutativity condition requires that, for all  $i, j \in [r]$ , we have

$$\langle (a_i, b_i), (a_j, b_j) \rangle_s = 0.$$

Grouping these conditions together into a single matrix equation gives the expression

$$H \Lambda H^T = 0.$$

**Definition 18.** A stabilizer code is said to be a *CSS code* if the binary stabilizer generator matrix  $H$  takes the form

$$H = \left[ \begin{array}{c|c} H_X & 0 \\ \hline 0 & H_Z \end{array} \right].$$

This definition is based on the fact that the stabilizers defined by the original CSS construction have this form. Such an  $H$  matrix is full rank if and only if  $H_x$  and  $H_z$  are full rank. By the previous general condition, this  $H$  defines a valid set of stabilizer codes if

$$\begin{aligned} H \Lambda H^T &= \left[ \begin{array}{c|c} H_X & 0 \\ \hline 0 & H_Z \end{array} \right] \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} \left[ \begin{array}{c|c} H_X & 0 \\ \hline 0 & H_Z \end{array} \right]^T \\ &= \left[ \begin{array}{c|c} 0 & H_X H_Z^T \\ \hline H_Z H_X^T & 0 \end{array} \right]. \end{aligned}$$

Thus, a sufficient condition for stabilizer commutativity is  $H_X H_Z^T = 0$ .

*Remark 19.* For the original CSS construction, the  $X$ -stabilizers are the codewords of  $\mathcal{C}_2$  and  $H_X = G_2$ . Similarly, the  $Z$ -stabilizers are the parity-checks of  $\mathcal{C}_1$  and  $H_Z = H_1$ , where  $H_1$  is the parity-check matrix of  $\mathcal{C}_2$ . Fortunately, the original CSS condition is equivalent to the general CSS condition defined above. In particular,  $\mathcal{C}_2 \subseteq \mathcal{C}_1$  is equivalent to  $G_2 H_1^T = 0$  (i.e., all codewords of  $\mathcal{C}_2$  satisfy all parity checks of  $\mathcal{C}_1$ ) and  $H_X H_Z^T = G_2 H_1^T$  by definition.

### 3.6 Hypergraph Product Codes

The *hypergraph product* (HGP) construction generates a CSS code from two classical parity-check matrices. For example, one can think about the matrices as defining the Tanner graphs of the two low-density parity-check (LDPC) codes. Let  $H_1 \in \mathbb{Z}_2^{m_1 \times n_1}$  be the parity-check matrix of an  $[[n_1, k_1, d_1]]$  binary linear code and  $H_2 \in \mathbb{Z}_2^{m_2 \times n_2}$  be the parity-check matrix of an  $[[n_2, k_2, d_2]]$  binary linear code. Then, the resulting hypergraph product code is a CSS code with

$$\begin{aligned} H_X &= [H_1 \otimes I_{n_2} \quad I_{m_1} \otimes H_2^T] \\ H_Z &= [I_{n_1} \otimes H_2 \quad H_1^T \otimes I_{m_2}]. \end{aligned}$$

To verify that this is a valid CSS code, we can easily check that

$$\begin{aligned} H_X H_Z^T &= [H_1 \otimes I_{n_2} \quad I_{m_1} \otimes H_2^T] \begin{bmatrix} I_{n_1} \otimes H_2^T \\ H_1 \otimes I_{m_2} \end{bmatrix} \\ &= H_1 \otimes H_2^T + H_1 \otimes H_2^T \\ &= 0. \end{aligned}$$

If  $H_1$  and  $H_2$  are full rank, then this defines an  $[[n_1 n_2, n_1 n_2 - m_1 n_2 - n_1 m_2, \min\{d_1, d_2\}]]$  quantum stabilizer code.

## A Leftover Lemmas

**Lemma 20.** For the standard CSS construction where  $G_{1/2}$  is a generator matrix for coset representatives of  $\mathcal{C}_2$  in  $\mathcal{C}_1$ , there is a matrix  $F_{1/2} \in \mathbb{Z}_2^{(k_1-k_2) \times n}$  satisfying  $G_{1/2}F_{1/2}^T = I_k$  and  $F_{1/2}y = 0$  for all  $y \in \mathcal{C}_2$ .

*Proof.* To see that there is a  $F_{1/2}$  satisfying the assumed conditions, we first define

$$G = \begin{bmatrix} G_{0/1} \\ G_{1/2} \\ G_2 \end{bmatrix},$$

where  $G_{0/1} \in \mathbb{Z}_2^{(n-k_1) \times n}$  is chosen so that  $G$  is invertible. This works because because  $G_1 = [G_{1/2}^T \ G_2^T]^T$  is full rank. Then, we partition  $G^{-1}$  into  $F_{0/1} \in \mathbb{Z}_2^{(n-k_1) \times n}$ ,  $F_{1/2} \in \mathbb{Z}_2^{(k_1-k_2) \times n}$ , and  $F_2 \in \mathbb{Z}_2^{k_2 \times n}$  so that

$$G^{-1} = \begin{bmatrix} F_{0/1}^T & F_{1/2}^T & F_2^T \end{bmatrix}.$$

Next, we find that

$$GG^{-1} = \begin{bmatrix} G_{0/1} \\ G_{1/2} \\ G_2 \end{bmatrix} \begin{bmatrix} F_{0/1}^T & F_{1/2}^T & F_2^T \end{bmatrix} = \begin{bmatrix} I_{n-k_1} & 0 & 0 \\ 0 & I_{k_1-k_2} & 0 \\ 0 & 0 & I_{k_2} \end{bmatrix}.$$

From this, we see that  $G_{1/2}F_{1/2}^T = I_{k_1-k_2}$  and that  $F_{1/2}y = 0$  for all  $y \in \mathcal{C}_2$  because  $G_2F_{1/2}^T = 0$ .  $\square$

## References

- [1] E. Knill and R. Laflamme, “Theory of quantum error-correcting codes,” *Phys. Rev. A*, vol. 55, no. 2, pp. 900–911, 1997.
- [2] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug 1996.
- [3] A. M. Steane, “Simple quantum error-correcting codes,” *Phys. Rev. A*, vol. 54, no. 6, pp. 4741–4751, 1996.
- [4] A. Steane, “Multiple-particle interference and quantum error correction,” *Proc. Roy. Soc. Lon. A*, vol. 452, no. 1954, pp. 2551–2577, 1996.
- [5] D. Gottesman, *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.
- [6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum Error Correction and Orthogonal Geometry,” *Phys. Rev. Lett.*, vol. 78, no. 3, pp. 405–408, 1997.
- [7] R. Calderbank, E. Rains, P. Shor, and N. Sloane, “Quantum error correction via codes over GF(4),” *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369–1387, Jul 1998.
- [8] M. M. Wilde, “Logical operators of quantum codes,” *Phys. Rev. A*, vol. 79, no. 6, p. 062322, 2009.