Topic: On Error Correction

**Due date:** Tuesday March 25, 2025. Choose a subset of about 7 problems to work on. You can also create your own problem or do problems from the previous problem sets.

#### 1. Identities

- a) Show that HXH = Z.
- b) Show that HZH = X.
- c) Show that HXZH = -XZ.
- d) Find a similar identity for Y.
- Here H is the Hadamard operator and X, Y, Z are the Pauli matrices.
- 2. On Measuring  $X_1X_2X_3X_4X_5X_6$  which is used in Shor's 9-bit code



Figure 1: A circuit that computes the parity of 6 bits using an ancilla qubit.

In Figure 1 we show a circuit that computes the parity of 6 bits. The bottom bit is an ancilla (or ancillary) qubit that is measured at the end. A 1 is measured if there is an odd number of 1s in the 6 qubit state, which are in the top 6 lines in the circuit.

Consider the operator  $Z_1Z_2Z_3Z_4Z_5Z_6$ . Here  $Z_1 = Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$  and the other operators are defined similarly so the index tells you which qubit the Z operates on. The operator  $Z_1 Z_2 Z_3 Z_4 Z_5 Z_6$  has eigenvalues 1, -1.

In the circuit in Figure 1, a 1 is measured if the input in the first 6 qubits is an eigenstate of  $Z_1Z_2Z_3Z_4Z_5Z_6$  with eigenvalue 1. In the circuit a 0 is measured if the input in the first 6 qubits is an eigenstate of  $Z_1Z_2Z_3Z_4Z_5Z_6$  with eigenvalue -1.

Because a different value is measured for each eigenstate of  $Z_1Z_2Z_3Z_4Z_5Z_6$ , the circuit in Figure 1 essentially measures this operator.

a) Design a circuit that measures the operator  $X_1X_2X_3X_4X_5X_6$ .

Hint: The states  $|+\rangle$ ,  $|-\rangle$  are eigenstates of X and you can transfer to the  $|+\rangle$ ,  $|-\rangle$  basis using a Hadamard operator.

b) Design a circuit for a 9 bit system that uses two extra ancilla bits to measure  $X_1X_2X_3X_4X_5X_6$  and  $X_4X_5X_6X_7X_8X_9$ .

#### 3. On correcting errors without measurement and on initializing ancillas

We consider the 3-bit phase-flip error correction code that encodes

$$|0\rangle \rightarrow |+++\rangle$$
 and  $|1\rangle \rightarrow |---\rangle$ .

The encoding subspace consists of states in the form

$$a |+++\rangle + b |---\rangle$$
.

If the state we would like to encode is  $a |0\rangle + b |1\rangle$ , (with complex numbers a, b, normalized so that  $aa^* + bb^* = 1$ ) then the encoded state would be

$$a |+++\rangle + b |---\rangle$$
.

A circuit that performs error detection is shown in Figure 2. Including two ancilla qubits, the initial state (if error free) would be

$$(a |+++\rangle + b |---\rangle) \otimes |00\rangle$$
.

However a phase flip error in one of the first 3 qubits could have affected the initial state. A phase flip error sends  $|+\rangle \rightarrow |-\rangle$  and vice versa and is equivalent to applying the Pauli **Z** to one of the qubits.



Figure 2: Detecting errors in the 3-bit phaseflip error correction code. The bottom two ancilla bits are measured to detect a single **phase** flip error in the top three bits. We can think of the first three Hadamards as a basis change. The CNOTs resemble the syndrome for the 3-bit bit-flip error correcting code. The measurements give the detected errors.

a) Modify the the circuit shown in Figure 2 so that phase flip errors are corrected after the measurement.

b) Design a circuit that corrects the errors without measurement.

c) Consider the possibility that the initial state has not been properly reset and has ancilla qubits in a state other than  $|00\rangle$ , such as  $|01\rangle$ . Show that if no error occurs, the final state, after error correction, is not in the encoding subspace.

This problem illustrates that error correction relies on accurate ancilla initialization.

#### 4. On the Generalized Pauli group $\mathcal{G}_n$

Consider the set of  $2 \times 2$  matrices or operators

$$\{\pm \mathbf{I}, \pm i\mathbf{I}, \pm \mathbf{X}, \pm \mathbf{Y}, \pm \mathbf{Z}, \\\pm i\mathbf{X}, \pm i\mathbf{Y}, \pm i\mathbf{Z}\}$$

where  $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$  are the Pauli spin matrices and  $\mathbf{I}$  is the identity. The set has 16 elements (here  $\pm$  gives pairs of elements).

a) Show that every element in the set has an inverse in the set.

b) Show that any product of two elements in the set gives an element that is also in the set.

This set of operators is known as the Pauli group and it is a discrete subgroup of U(2).

Consider an N qubit system. We denote  $\mathbf{X}_1 = \mathbf{X} \otimes \mathbf{I} \times \mathbf{I}$ ... as the Pauli X operator operating on the first qubit, likewise  $\mathbf{Y}_2$  is a tensor product  $\mathbf{Y}_2 = \mathbf{I} \otimes \mathbf{Y} \otimes \mathbf{I} \otimes \dots$ . We denote  $\mathbf{X}_j$  as a tensor product of identities and a Pauli X operator that operates on the j-th qubit.

A discrete subgroup of  $U(2^n)$  (corresponding to *n* qubits), known as the generalized Pauli group  $\mathcal{G}_n$  is *generated* from the set

$$\langle \mathbf{X}_1, \mathbf{Y}_1, \mathbf{Z}_1, \mathbf{X}_2, \mathbf{Y}_2, \mathbf{Z}_2, ..., \mathbf{X}_n, \mathbf{Y}_n, \mathbf{Z}_n \rangle$$

By generated, we mean that any element in the group can be written as a product of elements in the generating set.

c) How many elements does the generalized Pauli group  $\mathcal{G}_n$  contain? (as a function of n)

# 5. Also on the Generalized Pauli group $\mathcal{G}_n$

Any element in the Generalized Pauli group can be written as

$$g = \mu E_1 E_2 E_3 \dots$$

where  $\mu \in \{1, -1, i, -i\}$  and  $E_1$  is a member of  $\{I, X, Y, Z\}$  and operates on the first

qubit. The index *i* tells you which operator the element operates on. The operator  $E_i$  is similarly a Pauli matrix  $\in \{I, X, Y, Z\}$  working on the *i*-th qubit.

a) Consider two elements  $g, h \in \mathcal{G}_n$  where  $\mathcal{G}_n$  is the Generalized Pauli group. Show that they either commute or anticommute. In other words show that either gh = hg or gh = -hg.

b) Show that elements of  $\mathcal{G}_n$  that are not the identity have order 2 or 4. Give examples for each possibility. An element g of order 4 satisfies  $g^4 = I$ .

c) Show that if S is a subgroup of  $\mathcal{G}_n$  that does not contain  $-\mathbf{I}$ , then S is abelian. An abelian group is one where all pairs of elements commute.

## 6. Creating a projection operator for the encoding space

Consider the stabilizer group S generated by  $\langle X_1 X_2, X_2 X_3 \rangle$  that gives the 3-bit phaseflip quantum error correcting code.

The encoded or stabilized space C contains vectors  $|v\rangle$  such that  $g |v\rangle = |v\rangle$  for all  $g \in S$ . Show that

$$P = \frac{1}{4}(I + X_1 X_2)(I + X_2 X_3) \qquad (1)$$

is a projection operator in the 3 qubit space that projects to the encoding subspace C.

In other words show that

$$P = |+++\rangle \langle +++|+|---\rangle \langle ---|.$$

It may be useful to write

$$X = |+\rangle \langle +| - |-\rangle \langle -|$$
$$I = |+\rangle \langle +| + |-\rangle \langle -|$$

Notice that  $X_1X_2$  has eigenvalues  $\pm 1$  and  $(I + X_1X_2)/2$  has eigenvalues 0, 1.

## 7. Creating a projection operator for the stabilized space

Consider the stabilizer group S generated by k independent generators  $\langle g_1, g_2, ..., g_k \rangle$ . with generators in the generalized Pauli group  $\mathcal{G}_n$ .

Show that a projector giving the stabilized or encoding space C can be constructed by

$$P = \frac{1}{2^k} \prod_{j=1}^k (I+g_j).$$
 (2)

A vector  $|v\rangle$  that is stabilized by stabilizer group S satisfies

$$g |v\rangle = |v\rangle$$
 for all  $g \in S$ .

The coding subspace C is the vector subspace stabilized by S.

A vector  $|w\rangle$  that is perpendicular to subspace C satisfies  $\langle w|v\rangle = 0$  for all  $|v\rangle \in C$ .

This can be done in two parts.

a) Show that for any  $|v\rangle \in C$ , the projection  $P |v\rangle = |v\rangle$ .

b) Show that for any  $|w\rangle \perp C$ , the projection  $P |w\rangle = 0$ .

Stabilizer groups contain operators that are in the generalized Pauli group  $\mathcal{G}_n$ . Stabilizer groups cannot contain -I so all elements commute and all elements are Hermitian. The eigenvalues of any operator in  $\mathcal{G}_n$ has eigenvalues  $\pm 1$ . Consequently, the matrices  $(I + g_j)/2$  have eigenvalues 0, 1. As all members of S must commute, all members of  $\{(I+g_j)\}$  must also commute. A set of matrices that commute are all simultaneously diagonalizable. That means that the eigenvalues of P must be  $\in \{0, 1\}$ .

#### 8. The 5-bit stabilizer code

What is the minimum size for a quantum code which encodes a single qubit so that any error on a single qubit in the encoded state can be detected and corrected? The answer is 5-bits.

The stabilizer group S for the five bit error correcting code is generated by these four operators

$$\langle XZZXI, IXZZX, XIXZZ, ZXIXZ \rangle$$

that are also shown in Table 1. These could also be written as

$$\langle X_1 Z_2 Z_3 X_4, X_2 Z_3 Z_4 X_5, X_1 X_3 Z_4 Z_5, Z_1 X_2 X_4 Z_5 \rangle$$

or as

 $\begin{array}{l} \langle X\otimes Z\otimes Z\otimes X\otimes I, I\otimes X\otimes Z\otimes Z\otimes X, \\ X\otimes I\otimes X\otimes Z\otimes Z, Z\otimes X\otimes I\otimes X\otimes Z \rangle \end{array}$ 

Table 1							
	G	en	era	ato	$\mathbf{rs}$		
$g_1$	X	Z	Z	X	Ι		
$g_2$	I	X	Z	Z	X		
$g_3$	X	Ι	X	Z	Z		
$g_4$	Z	X	Ι	X	Z		

Notice that the generators are cyclic permutations of each other.

Verify that the five qubit code can protect against an arbitrary single qubit error.

In other words check that the set

$$S_E = \{X_1, X_2, X_3, X_4, X_5, Z_1, Z_2, Z_3, Z_4, Z_5\}$$

is a correctible set of errors.

A correctable set of errors satisfies the following: For every pair  $E_i, E_j$  of errors in the set  $S_E$ , the operator  $E_i^{\dagger}E_j$  either is in stabilizer group S or anticommutes with a generator of S. You will need to show that this is true for the set  $S_E$  and using the stabilizer generators in the table.

We don't need to include Y errors as if X and Z errors can be corrected and the product XZ for single qubits can be corrected, then the Y errors can also be corrected. This then means that any single qubit error can be corrected as any unitary transformation for a single qubit can be written as a linear combination of I, X, Y, Z operators.

# 9. The 5-bit stabilizer error correcting code syndrome

Describe a syndrome that allows correction of errors in the set

$$S_E = \{X_1, X_2, X_3, X_4, X_5, Z_1, Z_2, Z_3, Z_4, Z_5\}$$

for the 5 bit stabilizer code generated by the generators in Table 1.

You need to fill in the following table with 1s and -1s that represent measurements of the stabilizer generators. Elements that commute give 1.

	XZZXI	IXZZX	XIXZZ	ZXIXZ
$X_1$				
$X_2$				
$X_3$				
$X_4$				
$X_5$				
$Z_1$				
$Z_2$				
$Z_3$				
$Z_4$				
$Z_5$				

Does the syndrome allow you to also correct for additional errors in the set  $\{Y_1, Y_2, Y_3, Y_4, Y_5\}$ ?

#### 10. The Quantum Hamming Bound

Any non-degenerate quantum [[n, k]] code that corrects all errors with weight t or less must satisfy the quantum Hamming bound

$$\sum_{i=0}^{t} 3^{i} \binom{n}{i} \le 2^{n-k} \tag{3}$$

Suppose the number of qubits you want to encode is k = 1, but you want to be able to correct for all errors with weight t = 2 or less. That means you could correct all errors that affect 1 and 2 qubits. How many qubits n would you need in your error correction code?

You need to compute both sides of the equation 3 for various values of n and see for what n the inequality becomes satisfied.

#### 11. On a stabilizer group

The stabilizer group for Shor's 9-bit code is generated by the following set of operators

$$\langle Z_1 Z_2, Z_2 Z_3, Z_4 Z_5, Z_5 Z_6, Z_7 Z_8, Z_8 Z_9, X_1 X_2 X_3 X_4 X_5 X_6, X_4 X_5 X_6 X_7 X_8 X_9 \rangle$$
(4)

The order of a group is the number of unique elements in a group, including the identity element.

a) What is the order of the group that is generated by the operators  $Z_1Z_2, Z_2Z_3$ ?

b) What is the order of the group that is generated by the operators  $Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6$ ?

c) What is the order of the group that is generated by the operators  $Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9$ ?

d) What is the order of the group that is generated by the operators

$$X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9$$
?

e) What is the order of the stabilizer group for Shor's 9-bit code?

Hints:

The stabilizer group is an abelian group because all the generators commute.

All elements in these groups are their own inverse.

An element in the stabilizer group with m generators can be written  $g = g_1^{i_1} g_2^{i_2} \dots g_m^{i_m}$ 

where  $g_k$  are generators and  $i_k$  are powers which are either 0 or 1.

#### 12. A fault tolerant and transversal phase gate for the 3 bit bit flip error correcting code

The phase gate

$$S = P_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 0\\ 0 & i \end{pmatrix} = \operatorname{diag}(1, i)$$

Consider the 3-bit code with basis for its encoded states

$$\begin{aligned} \left| \tilde{0} \right\rangle &= \left| 000 \right\rangle \\ \left| \tilde{1} \right\rangle &= \left| 111 \right\rangle \end{aligned}$$

We would like to find a way to apply the phase gate transversally so that an operation is performed on each encoded qubit separately. The desired operation would give the same result as the phase gate but would be fault tolerant.

The operation we desire looks like  $Q^1 \otimes Q^2 \otimes Q^3$  where each operation is on a single qubit and it should send  $|000\rangle \rightarrow |000\rangle$  and  $|111\rangle \rightarrow i |111\rangle$ .

a) Show that  $\overline{S} = S \otimes S \otimes S$  in the encoded 3 bit space does not carry out the single qubit phase gate.

b) Find a different gate Q such that  $\overline{Q} = Q \otimes Q \otimes Q$  does give the phase gate.

Hint: Try a different phase.

c) Suppose a single bit flip error occurs prior to applying  $\bar{Q}$  (which effectively implements the phase gate but on the encoded system). Show that the single bit flip error would still be corrected by the syndrome associated with this code, up to a global phase. Note that a phase flip error would be introduced and this would be a problem.

#### 13. The 9-bit surface code - part 1

A 9-qubit surface code (which is also a stabilizer code) is shown in Figure 3.

Each ancilla qubit measures with a stabilizer generator. The blue diamond ancillas (labelled  $A_1$  through  $A_4$ ) are associated with Z gates on neighboring qubits and the red diamond ancillas (labelled  $A_5$  through  $A_8$ ) are associated with X gates. The figure can be used to find the stabilizer generator that is measured with each ancilla qubit.

For example  $A_1$  is associated with  $Z_2Z_3$ . and  $A_7$  is associated with  $X_4X_5X_7X_8$ .



Figure 3: A nine qubit surface code is shown on the right. The code is related to the piece of the lattice on the left.

a) Use Figure 3 to find a generating set of stabilizers. Show that they commute so that they can form a stabilizing group.

b) How many logical qubits does this error correction system encode?

c) Show that any single qubit X or any single qubit Z anticommutes with at least one of the stabilizer generators.

#### 14. A 9-bit surface code - part-2

a) Look to see (in your answer to the previous problem) if there are pairs of two single qubit errors that have the same syndrome. Explain why both errors in the pair are still corrected by the code.

b) Explain why part a and part c of the previous problem imply that all single qubit errors are corrected by this code.

Hint: products of errors either anticommute with at least one member of the stabilizer or have to be in the stabilizer for a set of errors to be correctible.

#### 15. A 9-bit surface code - part-3

a) Show that all two qubit errors are corrected by this code.

Hint: If the errors occur on two qubits that are not nearby, then both errors would be individually detected by separate sets of syndrome operators (or equivalently generators). So you don't need to explicitly check that they anticommute with at least one generator. For two errors on neighboring qubits you can reduce the number of pairs you need to check by exploiting rotational symmetry and the duality between X and Z operators (they are on dual lattices).

A basis for the encoding subspace (the stabilized subspace) is

$$\begin{split} \left| \tilde{0} \right\rangle &= \frac{1}{\sqrt{2^8}} \sum_{g_i \in S} g \left| 00000000 \right\rangle \\ \left| \tilde{1} \right\rangle &= \frac{1}{\sqrt{2^8}} \sum_{g_i \in S} g \left| 11111111 \right\rangle \end{split}$$

where  $g_i$  are elements in the stabilizer group S. The states  $|\tilde{0}\rangle, |\tilde{1}\rangle$  are eigenstates of  $\bar{Z} = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7 Z_8 Z_9$  which commutes with S but is not a member of S.

We similarly define

$$X = X_1 X_2 X_3 X_4 X_5 X_6 X_7 X_8 X_9.$$

b) Show that  $\bar{X} |\tilde{0}\rangle = |\tilde{1}\rangle$  so  $\bar{X}$  can be used to transversally generate the NOT gate. Hint: show that  $\bar{X}$  commutes with S.

### 16. Your Problem here