MATH 3952 (Undergraduate Seminar): Quantum Information Theory **Spring 2024**

Lecture 7, Talk 1: March 18, 2024

Organizer: Patrick Lei; Presenter: Erica Choi *Scribe: Mark Chen*

Chapter 7: Stabilizers

Recall the Pauli matrices:

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Also, recall the following properties of Pauli matrices:

- They form a basis in the $\mathbb{C}_{2\times 2}$ space.
- They all square to the identity (thus they can only have eigenvalues in the set $\{\pm 1\}$]).
- They are all Hermitian and unitary, so they represent both **observables** and **unitary evolutions**.
- They are defined as operators by the commutations relations, without reference to any particular basis. Particularly, we have the following identities:

  $$X^2 = Y^2 = Z^2 = \mathbb{1},$$

  and

  $$XY = iZ, YZ = iX, ZX = iY,$$

  and they are **anti-commutative**.

1 Pauli Group

Notice from the recalled identity above, we see that the set of Pauli operators are closed under multiplications, if we also consider the phase factors. So, with all of them, we actually acquire a group based off of the set, $\{\mathbb{1}, X, Y, Z\}$, called a **single qubit Pauli group**.

Definition 1 (**single qubit Pauli group**, $\mathcal{P}_1$)**.** *A **single qubit Pauli group**, $\mathcal{P}_1$, is the group generated by X, Y, Z. Particularly,*

$$\mathcal{P}_1 = \langle X, Y, Z \rangle = \{\pm\mathbb{1}, \pm i\mathbb{1}, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

Definition 2 (**n-qubit Pauli group**, $\mathcal{P}_n$)**.** *The **n-qubit Pauli group**, $\mathcal{P}_n$ is defined to consist of all n-fold tensor products of Pauli matrices, with possible global phase factors $\pm 1, \pm i$, i.e.*

$$\mathcal{P}_n := \{P_1 \otimes \ldots \otimes P_n \mid P_1, \ldots, P_n \in \mathcal{P}_1\}.$$

Proposition 1 (Properties of $\mathcal{P}_n$)**.** *Some basic ones that are easy to realize are:*

- $|\mathcal{P}_n| = 4 \cdot 4^n = 4^{n+1}$ *(by accounting for the possible global phase factors).*

  Proof. $\mathcal{P}_n$ has two trivial subgroups,

  $$Z_2 = \{\pm 1\}, Z_4 = \{\pm 1, \pm i\},$$

  the quotient group $\mathcal{P}_n/Z_4$ is exactly the n-qubit Pauli group with the phases ignored, which has a size of 4. Then, by Lagrange's theorem and the fact that $|Z_4| = 4$, we have

  $$|\mathcal{P}_n| = 4 \times 4^n.$$

  ■

- *Multiplication, like before for tensor products, are defined component-wise on $\mathcal{P}_n$,*

  $$(ZXX\mathbb{1}) \cdot (XXYY) = (ZX)(XX)(XY)(\mathbb{1}Y) = (iY)(\mathbb{1})(iZ)(Y) = -Y\mathbb{1}ZY.$$

Proposition 2. *Any pair of elements in $\mathcal{P}_n$ either commute or anticommute.*

Proof. Given $P = P_1 \otimes \ldots \otimes P_n$ and $Q = Q_1 \otimes \ldots \otimes Q_n$. Denote k as the number of indices j such that

$$P_j Q_j = -Q_j P_j.$$

Then, the overall global factor is just $(-1)^k$, which means:

- P and Q commute when k is even.
- P and Q anticommute when k is odd.

■

Proposition 3. *Notice that $P^2 = \pm\mathbb{1}, \forall P \in \mathcal{P}_n$, so all elements in $\mathcal{P}_n$ are unitary.*

Proposition 4. *Elements in $\mathcal{P}_n$ either Hermitian (with a ± 1 overall phase and square to $\mathbb{1}$) or anti-Hermitian (with a $\pm i$ overall phase and square to $-\mathbb{1}$).*

Remark 1. *Notice that we are only interested in working with Hermitian elements, and we refer to these elements as the* ***Pauli operators****. That is, an n-**qubit Pauli operator** is a Hermitian element of the n-qubit Pauli group $\mathcal{P}_n$.*

Proposition 5. *Not only do elements of $\mathcal{P}_n$ have eigenvalues of ± 1, these eigenvalues must be of the same degeneracy, and the eigenspaces corresponding to each eigenvalue are of the same dimension, as we can see by taking the trace:*

$$\mathsf{Tr}(P_1 \otimes P_2 \otimes \ldots \otimes P_n) = (\mathsf{Tr}(P_1)) \cdots (\mathsf{Tr}(P_n)) = \begin{cases} 1 \text{ if } P_1 = P_2 = \ldots = P_n = \mathbb{1} \\ 0 \text{ otherwise} \end{cases}$$

Proposition 6. *The n-qubit Pauli group spans the $\mathbb{C}_{2^n \times 2^n}$ space.*

2 Pauli Stabilizers

Recall that, in group theory, a stabilizer G_s is the set of elements of a group G that leaves s fixed. Formally,

$$G_s = \{g \in G : gs = s\}.$$

Example 1. *Here are two examples:*

- *The point of this in the context of QIT is that, given a particular vector in Hilbert space, we can define it by the list of operators that leave it invariant (in contrast to defining it by coordinates based on some basis).*
- *More generally, we can even define a vector subspace by giving a list of operators that fix this subspaces.*

Definition 3 (stabilizers). *The set of operators as given in example 1 are known as* ***stabilizers****.*

*Formally, we say that an operator S **stabilizes** a (non-zero) state $|\psi\rangle$ if $S|\psi\rangle = |\psi\rangle$. In such a case, we say that*

- *$|\psi\rangle$ is a **stabilizer state**.*

- *S stabilizes a subspace V if S stabilizes every state in V, and we call the largest subspace V_S that is stabilized by S the* ***stabilizer subspace****.*

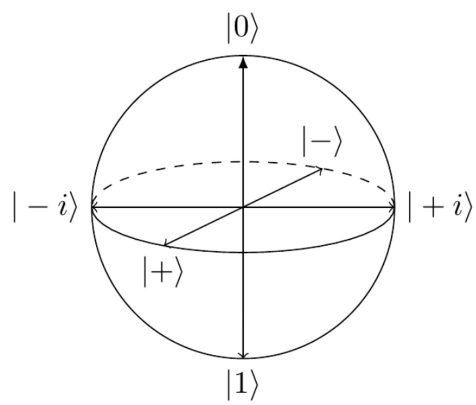
Proposition 7. *The definition is the same as saying that S stabilizes a state $|\psi\rangle$ if $|\psi\rangle$ is an eigenstate of S with eigenvalue 1.*

Specifically, notice that we cannot ignore the global phase factors, here, anymore. Even though

$$S|\psi\rangle = -|\psi\rangle,$$

would have $|\psi\rangle$ and $-|\psi\rangle$ describe the same quantum state, we don't say that S stabilizes $|\psi\rangle$.

Example 2. *Z stabilizes $|0\rangle$, Y stabilizes $|i\rangle$, X stabilizes $|+\rangle$. Similarly, $-Z$ stabilizes $|1\rangle$, $-Y$ stabilizes $|-i\rangle$, $-X$ stabilizes $|-\rangle$. [Recall that $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.] Note that $|0\rangle/|1\rangle, |\pm i\rangle$ and $|\pm\rangle$ denote the intersection of the three axes with the bloch sphere, as eigenvalues of the Pauli opertaors:*



Proposition 8. *In the single-qubit Pauli group, $\mathbb{1}$ stabilizes everything, and $-\mathbb{1}$ stabilizes nothing. More generally, S and $-S$ must generalize different things (recall what was said in the definition that $S|\psi\rangle = -|\psi\rangle$ does not give that S stabilizes $|\psi\rangle$).*

Definition 4 (Stabilizer Group, $\mathcal{S}$)**.** *It is easy to see that the set of stabilizes, V_S, is also a group, which we denote as $\mathcal{S}$, called the* ***stabilizer group****.*

Proof. To show that $\mathcal{S}$ is indeed a group, it suffices to show that the inverse and composition (the binary multiplication) of any $S \in \mathcal{S}$ must be contained in the set. But, it is easy to show:

- (Inverse) If
$$S|\psi\rangle = |\psi\rangle \implies S^{-1}S|\psi\rangle = S^{-1}|\psi\rangle \implies |\psi\rangle = S^{-1}|\psi\rangle.$$
- (Composition as multiplication) Suppose $S, T \in \mathcal{S}$,
$$(ST)|\psi\rangle = S\left(T|\psi\rangle\right) = S|\psi\rangle = |\psi\rangle.$$
- (Identity) Trivially always a stabilizer for any $S \in \mathcal{S}$.

$\blacksquare$

Proposition 9. *It should be clear from the definition how the specific states $|0\rangle/|1\rangle$, $|\pm i\rangle$, and $|\pm\rangle$ are related to the Bloch sphere coordinates, thus related to the non-trivial Pauli operators. In particular, we have:*

- $G_{|1\rangle} = \langle Z\rangle = \{\mathbb{1}, Z\}$.
- $G_{|0\rangle} = \langle -Z\rangle = \{\mathbb{1}, -Z\}$.
- $G_{|+\rangle} = \langle X\rangle = \{\mathbb{1}, X\}$.
- *etc.*

Proposition 10. *It should be clear that, given the tensor product of two states, with stabilizer groups $\mathcal{A}$ and $\mathcal{B}$, respectively, then the resulting tensor product state has stabilizer group given by*
$$\mathcal{A} \times \mathcal{B}.$$
For example, $|1\rangle, |+\rangle$ is stabilized by
$$\langle Z\rangle \times \langle X\rangle = \{\mathbb{1}\mathbb{1}, Z\mathbb{1}, \mathbb{1}X, ZX\} = \langle Z\mathbb{1}, \mathbb{1}X\rangle.$$

Proposition 11. *Generally, say for $|0\rangle^{\otimes n}$, it is stabilized by the group generated by the n elements $\underbrace{Z\mathbb{1}\mathbb{1}\ldots\mathbb{1}}_{n\ places}, \underbrace{\mathbb{1}Z\mathbb{1}\ldots\mathbb{1}}_{n\ places}, \underbrace{\mathbb{1}\mathbb{1}Z\ldots\mathbb{1}}_{n\ places}, \ldots$. For brevity of notation, we usually write such a generating set as an $n\times n$ matrix, labeling the signs on the LHS. For some examples:*

- $$|0000\rangle \equiv \begin{array}{c|cccc|} + & Z & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ + & \mathbb{1} & Z & \mathbb{1} & \mathbb{1} \\ + & \mathbb{1} & \mathbb{1} & Z & \mathbb{1} \\ + & \mathbb{1} & \mathbb{1} & \mathbb{1} & Z \end{array}$$

- $$|0001\rangle \equiv \begin{array}{c} + \\ + \\ + \\ - \end{array}\left|\begin{array}{cccc} Z & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ \mathbb{1} & Z & \mathbb{1} & \mathbb{1} \\ \mathbb{1} & \mathbb{1} & Z & \mathbb{1} \\ \mathbb{1} & \mathbb{1} & \mathbb{1} & Z \end{array}\right|$$

- $$|0101\rangle \equiv \begin{array}{c} + \\ - \\ + \\ - \end{array}\left|\begin{array}{cccc} Z & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ \mathbb{1} & Z & \mathbb{1} & \mathbb{1} \\ \mathbb{1} & \mathbb{1} & Z & \mathbb{1} \\ \mathbb{1} & \mathbb{1} & \mathbb{1} & Z \end{array}\right|$$

For our purposes, we are only interested in **stabilizers that are also elements of the n-qubit Pauli group $\mathcal{P}_n$**, and we shall soon see that this subgroup is an abelian group.

Example 3 (Describe Bell states by stabilizer groups:)**.** *Recall from chapter 5 about Bell states:*

- Φ^+ *can be represented by* $\langle XX, ZZ\rangle$.
- Ψ^+ *can be represented by* $\langle XX, -ZZ\rangle$.
- Φ^- *can be represented by* $\langle -XX, ZZ\rangle$.
- Ψ^- *can be represented by* $\langle -XX, -ZZ\rangle$.

Example 4. *Stabilizer groups can also be used to describe other vector spaces: The subspace of the* 3*-qubit state space spanned by* $|000\rangle, |111\rangle$ *is stabilized by*

$$\{\mathbb{1}\mathbb{1}\mathbb{1}, ZZ\mathbb{1}, Z\mathbb{1}Z, \mathbb{1}ZZ\} = \langle ZZ\mathbb{1}, \mathbb{1}ZZ\rangle.$$

Remark 2. *It is not necessarily guaranteed that the stabilizer group representation is more concise than the component-wise representation, or vice versa. but, in general, the stabilizer group representation is more concise as the number of components increase as should be sensed with example 4.*

2.1 To show that the stabilizer groups that are subgroups of $\mathcal{P}_n$ are abelian

Definition 5 (Alternative definition of an n-qubit Pauli stabilizer group)**.** *An n-qubit Pauli stabilizer group is any subgroup of $\mathcal{P}_n$ that is* ***abelian*** *and does not contain* -1*. Its elements are called* ***Pauli stabilizers****. [To be justified later why this is equivalent.]*

Proof. Recall that all Pauli operators square to the identity, and all pairs of Pauli operators either **commute** or **anticommute**. If we want some Pauli operators to stabilize anything then they must commute. Otherwise, say S_1, S_2 are two Pauli operators that anticommute, then

$$|\psi\rangle = S_1 S_2|\psi\rangle = -S_2 S_1|\psi\rangle = -|\psi\rangle \implies |\psi\rangle = 0.$$

But, $|\psi\rangle \neq 0 \implies$ contradiction. Furthermore, the Pauli stabilizer group as such (i.e. abelian) is exactly the abelian subgroup of Pauli stabilizers. Since the moment that such a subgroup include $-\mathbb{1}$, it must mean that it needs to be a trivial group (because all other Pauli operators square to $\mathbb{1}$, and having $-\mathbb{1}$ means that there exists an anti-commuting element). Therefore, we must have an abelian subgroup of the Pauli group which doesn't contain $-\mathbb{1}$, if non-trivial.

On the other hand, if pick any abelian subgroup of $\mathcal{P}_n$ that doesn't contain -1, it certainly means that it stabilizes some subspace V_S.

So, the two definitions are equivalent. ∎

The size of any Pauli stabilizer $\mathcal{S}$ is $|\mathcal{S}| = 2^r$, where r is some positive integer, since we can always find some choice of generators $G_1, \ldots, G_r$, and then any operator $S \in \mathcal{S}$ can be written as

$$S = G_1^{\epsilon_1} G_2^{\epsilon_2} \ldots G_r^{\epsilon_r},$$

where $r_i \in \{0, 1\}$. But, given any stabilizer group, we can always express its elements using many different set of generators.

Definition 6 (**presentation**)**.** *A specific set of choice of r independent generators of a Pauli stabilizer $\mathcal{S}$ of size 2^r is called the* ***presentation****.*

Proposition 12. *Here is a way to choose a presentation from the set of elements of $\mathcal{S}$:*

1. *We start by picking any non-identity element, so there are $2^r - 1$ choices.*

2. *Inductively, we choose the next generator by picking any element that is not in the subgroup generated by the generators already selected. Thus, there should be a total of*

$$(2^r - 1)(2^r - 2)(2^r - 2^2) \cdots (2^r - 2^{r-1}) \text{ possible generating sets of } \mathcal{S}.$$

Notice that these sets are ordered, as it will consider $G_1, G_2, \dots$ and $G_2, G_1, \dots$ as different sets of generators. So, we need to also divide by $r!$, which gives a total of

$$\boxed{\frac{(2^r-1)(2^r-2)(2^r-2^2)\cdots(2^r-2^{r-1})}{r!} \text{ possible distinct generating sets of } \mathcal{S}}.$$

Example 5. *$\Phi^+ = |00\rangle + |11\rangle$ has $\frac{(2^2-1)(2^2-2)}{2!} = \frac{6}{2} = 3$ presentations, and they are*

$$\langle XX, ZZ\rangle, \langle -YY, XX\rangle, \langle ZZ, -YY\rangle.$$

Now that we know the size of a Pauli stabilizer, but what can we say about the dimension of the subspace that it stabilizes?

Proposition 13. *If $|\mathcal{S}| = 2^r$, then the corresponding stabilizer subspace V_S has dimension 2^{n-r} (where n is the number of qubits, i.e. such that $S \subseteq \mathcal{P}_n$).*

Proof. To see this, we can look at the projector P_S onto V_S, since once we have a projector onto any subspace, we know that the dimension of that subspace is exactly the trace of the projector. In this case, we have

$$\mathsf{Tr}\left(P_S\right) = \frac{1}{2^r}\mathsf{Tr}\left(S_1 + S_2 + \cdots + S_{2^r}\right) \overset{①}{=} \frac{1}{2^r}\mathsf{Tr}\left(\mathbb{1}\right) = 2^{n-r},$$

where ① is because all elements of the stabilizer group (just by inspecting what can be acquired from $X, Y, Z, -\mathbb{1}$ with phase factors) have trace of 0 other than $\mathbb{1}$, and $\mathsf{Tr}\left(\mathbb{1}^{\otimes n}\right) = 2^n$.

■

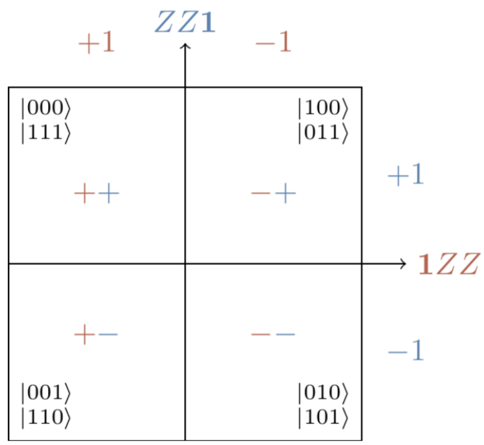
Corollary 1. *If $r = n$, then the stabilized subspace is 1-dimensional, and so we have **stabilizer states**.*

There is a more geometric way of understanding why powers of 2 keep on turning up in these calculations:

Remark 3. *Given independent Pauli operators, we can think of the **state** or **subspace** as they repeated bisecting the Hilbert space.*

Specifically, let $G_1, \dots, G_r$ be a representation of a Pauli stabilizer $\mathcal{S}$. For each operator G_i, half of its eigenvalues are $+1$ and the other half is -1, so each G_i bisects 2^n-dimensional Hilbert space of n qubits into two eigenspaces of equal sizes.

Such an inductive procedure can be visualized as, at each step, we pass from $\{G_1, G_2, \ldots, G_i\}$ *to* $\{G_1, G_2, \ldots, G_{i+1}\}$*: We bisect the subspace into* 2^i *equal parts once more, eventually ending with the* 2^{n-i-1}*-dimensional subspace* $V_{\mathcal{S}}$*. For example, for bisecting a Hilbert space of* 3 *qubits into four equal parts, we can visualize it as:*



NotesL The stabilizer $\mathcal{S} = \langle ZZ\mathbb{1}, \mathbb{1}ZZ\rangle$ *bisects the Hilbert space of* 3 *qubits into four equal parts, with each part representing a subspace spanned by some representations. Notice that labelled sign on each edge (respectively mark which* ***eigenspace*** *it is for* $ZZ\mathbb{1}$ *and* $\mathbb{1}ZZ$*) represents something like a "coordinate" that describes which subspace we should end up in. For example,* $++$ *denotes the upper left subspace that* $|000\rangle$ *and* $|111\rangle$ *span.*

3 Single Stabilizer States

Recall corollary 1, if we are given n independent generators of a stabilizer group $\mathcal{S}$ on a Hilbert space of n qubits, we then specify a 1-dimensional subspace (which means it is spanned by a single basis vector, namely the **stabilizer state**).

Recall from proposition 9 that we have also mentioned that a single-qubit stabilizer state can be fully determined by all possible stabilizers in $\mathcal{P}_1$, namely $|0\rangle$ and $|1\rangle$ for $\langle \pm Z\rangle$, $|\pm\rangle$ for $\langle \pm X\rangle$, and $|\pm i\rangle$ for $\langle \pm Y\rangle$.

We have also talked about some 2-qubit stabilizer states, some **entangled** (like Bells states), and some **separable** (like computational basis states).

Example 6 (Another two-qubit example that is maximally entangled)**.** *Consider* $|00\rangle + |11\rangle$*. This state is stabilized by* $\langle XX, ZZ\rangle$*, and here is how we see it:*

1. *XX splits the 4-dimensional Hilbert space into 2-dimensional subspaces, corresponding to eigenvalues of $\pm\mathbb{1}$. By definition, it stabilizes the one corresponding to eigenvalue $+\mathbb{1}$ ($-\mathbb{1}$ cannot be a stabilizer), and it is spanned by $\underline{|00\rangle + |11\rangle \text{ and } |01\rangle + |10\rangle}$ (or, Φ^+ and Ψ^+).*

2. *ZZ splits, likewise, again corresponding to $\pm\mathbb{1}$. It stabilizes the one corresponding to eigenvalue $+\mathbb{1}$ as well, which is spanned by $\underline{|00\rangle + |11\rangle \text{ and } |00\rangle - |11\rangle}$ (or, Φ^+ and Φ^-).*

3. *So, the only way to achieve $+\mathbb{1}$ for both XX and ZZ is the state Φ^+.*

But, in the process described in example 6, this is just one way to <u>bisect</u> the 4-dimensional Hilbert space, as we have mentioned. Particularly, we can also bisect by $\langle XX, -YY\rangle$ or $\langle -YY, ZZ\rangle$.

$$|00\rangle + |11\rangle \longleftrightarrow \begin{array}{c|cc|} + & X & X \\ + & Z & Z \end{array} \qquad |00\rangle - |11\rangle \longleftrightarrow \begin{array}{c|cc|} - & X & X \\ + & Z & Z \end{array}$$

$$|01\rangle + |10\rangle \longleftrightarrow \begin{array}{c|cc|} + & X & X \\ - & Z & Z \end{array} \qquad |01\rangle - |10\rangle \longleftrightarrow \begin{array}{c|cc|} - & X & X \\ - & Z & Z \end{array}$$

Proposition 14. *So, this brings us to the question: how many n-qubit stabilizer states do we have? The answer is*

$$\boxed{2^n \prod_{k=1}^{n-1} (2^{n-k} + 1)}$$

Proof. We count the number of generating sets with n generators, since this is exactly the right number of generators to specify a 1-dimensional stabilizer subspace. Then, we divide the number of presentations for any given stabilizer.

- There are $\boxed{4^n - 1}$ choices for the first generators G_1 (ignoring all signs), since it can be any n-fold tensor product of the four Pauli matrices, excluding the identity $\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}$. Now, continuing on to the second generator G_2, we have $\boxed{\frac{4^n}{2} - 2}$ (as it must <u>commute with G_1</u> [thus "$\frac{}{2}$"], and it cannot contain $\underline{\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}}$ or $\underline{G_1}$ [thus "-2"]). Continue on, when we consider G_i, we have

$$\frac{4}{2^{n-1}} - 2^{n-1}.$$

So, the total number of possible generating sets is:

$$\boxed{2^n \prod_{i=0}^{n-1} \left(\frac{4^n}{2^i} - 2^i \right)}. \tag{1}$$

- As for the number of presentations that we need to divide, we have already shown:

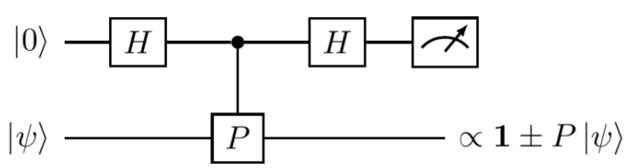
$$\boxed{\prod_{i=0}^{n-1} (2^n - 2^i).} \tag{2}$$

Finally, $\frac{(1)}{(2)}$ gives us the intended total number of n-qubit stabilizer states. ■

4 Measuring Pauli Stabilizers

We bisect Hilbert spaces by measuring stabilizers.

We first measure any single-qubit observable that squares to the identity. An operator P that does this must be both Hermitian and unitary, meaning that they can represent both an observable and a quantum gate.



Notice that this circuit performs a measurement that gives a result of ± 1 and leave the qubit in a post-measurement state (the corresponding eigenvector). Equivalently, this circuit can be written as:

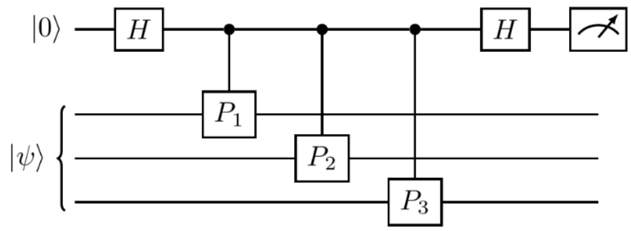
$$|0\rangle|\psi\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle P|\psi\rangle \mapsto |0\rangle\frac{1}{2}(\mathbb{1} + P)|\psi\rangle + |1\rangle\frac{1}{2}(\mathbb{1} - P)|\psi\rangle.$$

The final state of the two qubits indicates that:

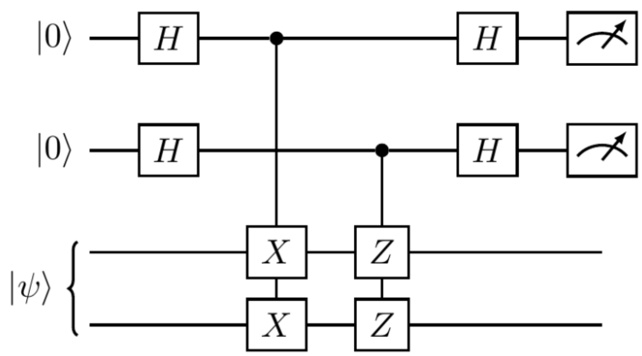
- If the auxiliary (top) qubit is found in state $|0\rangle$, then the state $|\psi\rangle$ was projected onto the $+1$-eigenspace of P.

- If the auxiliary (top) qubit is found in state $|1\rangle$, then the state $|\psi\rangle$ was projected onto the -1-eigenspace of P.

Proposition 15. *Stabilizers help us generalize this concept to any n-qubit Pauli operator, using the stabilizer groups, as it is easy to see that X, Y, and Z observables can be measured using controlled-X, controlled-Y, and controlled-Z gates, respectively and we can use the stabilizer groups based on these gates to measure n-qubit Pauli operator:*



For example, consider the stabilizer group $\mathcal{S} = \langle XX, ZZ\rangle$, we can measure with the following circuit:



hen, the registered bit values from the first and second (counting from the top) auxiliary qubits tell us how we bisect the Hilbert space with XX and ZZ (respectively), recalling that a bit value of 0 corresponds to $+1$ Pauli eigenvalue, and a bit value of 1 to the -1 eigenvalue. So, the first measurement can apply one of two projectors to $|\psi\rangle$:

1. $\frac{1}{2}(\mathbb{1} + XX)$, *in which case the first auxiliary qubit will show 0, corresponding to the $+1$-subspace spanned by $|00\rangle + |11\rangle$ and $|01\rangle + |10\rangle$.*

2. $\frac{1}{2}(\mathbb{1} - XX)$, *in which case the first auxiliary qubit will show 1, corresponding to the -1-subspace spanned by $|00\rangle - |11\rangle$ and $|01\rangle - |10\rangle$.*

Also, the second measurement can further apply one of two projectors to $|\psi\rangle$:

1. $\frac{1}{2}(\mathbb{1} + ZZ)$, *in which case the second auxiliary qubit will show 0, corresponding to the $+1$-subspace spanned by $|00\rangle + |11\rangle$ and $|00\rangle - |11\rangle$.*

2. $\frac{1}{2}(\mathbb{1} - ZZ)$, *in which case the second auxiliary qubit will show* 1, *corresponding to the* -1*-subspace spanned by* $|01\rangle + |10\rangle$ *and* $|01\rangle - |10\rangle$.

Notation 1 (Pauli Notation)**.** *Notice how the bisection is based on the* ± 1 *values of the* XX *and* YY *eigenvalues, respectively. So, for notation, we can denote* $\langle \pm XX, \pm ZZ \rangle$ *by* $(\pm 1, \pm 1)$.

Remark 4. *Even though we have no control over the final state we get, we do know which post-measurement state we have generated, so we can use the circuit to prepare a desired state by applying an appropriate unitary operation to the final state.*

Remark 5. *This is also not the only way of constructing projective measurements of Pauli observables.*