7 - Stabilizers

Erica Choi

March 18, 2024

1 Review

1.1 Pauli matrices

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

These matrices

- span the space of 2×2 complex matrices
- square to the identity
- have eigenvalues {+1,-1}
- Hermitian
- unitary
- either commute or anticommute with each other

The following relations define the Pauli operators:

$$X^2 = Y^2 = Z^2 = I$$

$$XY = iZ \qquad YZ = iX \qquad ZX = iY$$

$$YX == iZ \qquad ZY = -iX \qquad XZ = -iY$$

We can see that when we multiply the Pauli matrices with one another, we get Pauli matrices in return, with possible phase factors ± 1 and $\pm i$. This closure allows us to take advantage of the algebraic structure of a group.

1.2 Group Theory

Definition 1. *A group G is a binary structure $(X, *)$ such that * is associative, there exists an identity element for *, and every $x \in X$ has an inverse for *.*

Remark 2. *G is abelian if * is also commutative.*

Definition 3. *A subgroup H of a group G is a subset $H \subseteq G$ such that*

1. *For all $h_1, h_2 \in H$, $h_1 h_2 \in H$.*
2. *$1 \in H$.*
3. *For all $h \in H$, $h^{-1} \in H$.*

Definition 4. *Given a group G, group generators are the elements $g_1, \ldots, g_n$ of the group that are independent and such that every element of G can be written as a product of elements of $\{g_1, \ldots, g_n\}$. If G is generated by $g_1, \ldots, g_n$, then we write $G = \langle g_1, \ldots, g_n \rangle$.*

2 Pauli Groups

Definition 5. *The single-qubit Pauli group $\mathcal{P}_1$ is defined by*

$$\begin{aligned}\mathcal{P}_1 &:= \langle X, Y, Z \rangle \\ &= \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}\end{aligned}$$

Definition 6. *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 $\pm I$, $\pm i$*

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

$\mathcal{P}_n$ has two trivial subgroups, $Z_2 = \{\pm 1\}$ and $Z_4 = \{\pm 1, \pm i\}$

Notation 7. *We omit the tensor product symbol, writing $XYIZ$ instead of $X \otimes Y \otimes I \otimes Z$. Note that this is different from the product $XYIZ = iI$ inside $\mathcal{P}_1$.*

Now we can discuss the algebraic structure of $\mathcal{P}_n$.

- Multiplication is done component-wise as follows:

$$\begin{aligned}(ZXXI) \cdot (XXYY) &= (ZX)(XX)(XY)(IY) \\ &= (iY)(I)(iZ)(Y) \\ &= -YIZY\end{aligned}$$

- Any pair of elements in $\mathcal{P}_n$ either commute or anticommute:
  $P = P_1 \ldots P_n$ and $Q = Q_1 \ldots Q_n$ commute whenever the number of *anticommuting components*, i.e. incices j such that $P_j Q_j = -Q_j P_j$, is even.

- All elements in the Pauli group are unitary, and either Hermitian or anti-Hermitian. We are interested in Hermitian elements.

Definition 8. *An n-qubit Pauli operator is a Hermitian element of the n-qubit Pauli group $\mathcal{P}_n$.*

3 Pauli Stabilizers

Definition 9. *We say that an operator S stabilizes a (non-zero) state $|\psi\rangle$ if $S|\psi\rangle = |\psi\rangle$, and then call $|\psi\rangle$ a stabilizer state.*

Definition 10. *We say that 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.*

- In other words, S stabilizes $|\psi\rangle$ if $|\psi\rangle$ is an eigenstate of S with eigenvalue 1.
- Note that global phase factor matters; if $S|\psi\rangle = -|\psi\rangle$ then S does not stabilize $|\psi\rangle$.

$$\begin{aligned} Z \text{ stabilizes } |0\rangle \qquad & -Z \text{ stabilizes } |1\rangle \\ Y \text{ stabilizes } |i\rangle \qquad & -Y \text{ stabilizes } |-i\rangle \\ X \text{ stabilizes } |+\rangle \qquad & -X \text{ stabilizes } |-\rangle \end{aligned}$$

where $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

- 1 stabilizes everything
- -1 stabilizes nothing
- if S stabilizes something, then $-S$ cannot stabilize the same thing

Claim 11. *The set of all stabilizers of a given state or given subspace form a group.*

Proof. Need to check: inverse, closure, identity □

7.2. Pauli stabilisers

The stabiliser (or stabilizer, if you like) formalism is an elegant technique that is often used to describe vectors and subspaces. Suppose you want to specify a particular vector in a Hilbert space. The most conventional way to do this would be to pick a basis and then list the coordinate components of the vector. But we could instead list a set of operators that leave this vector invariant. More generally, we can define a vector subspace (rather than just a single vector, which corresponds to a 1-dimensional subspace: its span) by giving a list of operators that fix this subspace. Such operators are called **stabilisers**.

> We say that an operator S **stabilises** a (non-zero) state $|\psi\rangle$ if $S|\psi\rangle = |\psi\rangle$, and we then call $|\psi\rangle$ a **stabiliser state**. We say that S stabilises a subspace V if S stabilises every state in V, and we call the largest subspace V_S that is stabilised by S the **stabiliser subspace**.

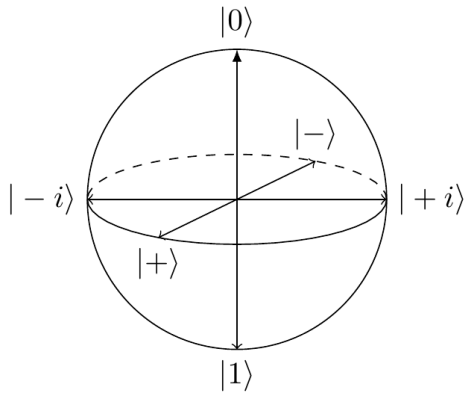
In other words, an operator S stabilises a state $|\psi\rangle$ (or the state is fixed by the operator) if $|\psi\rangle$ is an eigenstate of S with eigenvalue 1. It is very important to note that here we *have* to pay attention to the global phase factor: if $S|\psi\rangle = -|\psi\rangle$ then we do *not* say that S stabilises $|\psi\rangle$, even though $|\psi\rangle$ and $-|\psi\rangle$ describe the same quantum state.

For example, we can look at states stabilised by the Pauli operators with factors ± 1:

$$\begin{aligned} Z \text{ stabilises } |0\rangle \qquad & -Z \text{ stabilises } |1\rangle \\ Y \text{ stabilises } |i\rangle \qquad & -Y \text{ stabilises } |-i\rangle \\ X \text{ stabilises } |+\rangle \qquad & -X \text{ stabilises } |-\rangle \end{aligned}$$

where $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

On the Bloch sphere, these single-qubit stabiliser states lie at the intersection of the three axes with the surface of the sphere.



We can also say something about the remaining two elements of the single-qubit Pauli group: $\mathbf{1}$ stabilises everything, and $-\mathbf{1}$ stabilises nothing (except for the zero state, which we explicitly ignore). More generally, if S stabilises something then $-S$ cannot stabilise the same thing.

The set of all stabilisers of a given state or given subspace form a group: if $S|\psi\rangle = |\psi\rangle$, then multiplying both sides by S^{-1} shows that the inverse of a stabiliser is again a stabiliser; the composition of two stabilisers is again a stabiliser, since $(ST)|\psi\rangle = S(T|\psi\rangle) = S|\psi\rangle = |\psi\rangle$; and as we have just said, the identity is always a stabiliser. This group is called the **stabiliser group** $\mathcal{S}$ of the given state or subspace.

Using this language, we can rephrase the previous example by saying that the stabiliser group of the state $|1\rangle$ is $\{\mathbf{1}, Z\} = \langle Z\rangle$, the stabiliser group of the state $|0\rangle$ is $\{\mathbf{1}, -Z\} = \langle -Z\rangle$, the stabiliser group of the state $|+\rangle$ is $\{\mathbf{1}, X\} = \langle X\rangle$, and so on. If we take the tensor product of a two states, with stabiliser groups $\mathcal{A}$ and $\mathcal{B}$ (respectively), then the resulting tensor product state has stabiliser group given by the cartesian product $\mathcal{A} \times \mathcal{B}$. For example, the state $|1\rangle|+\rangle$ is stabilised by the group

$$\begin{aligned}\{\mathbf{1}, Z\} \times \{\mathbf{1}, X\} &= \{\mathbf{11}, \mathbf{1}X, Z\mathbf{1}, ZX\} \\ &= \langle Z\mathbf{1}, \mathbf{1}X\rangle.\end{aligned}$$

As for the state $|0\rangle^{\otimes n}$, this is stabilised by the group generated by the n elements $Z\mathbf{11}\ldots\mathbf{1}$, $\mathbf{1}Z\mathbf{1}\ldots\mathbf{1}$, ..., $\mathbf{11}\ldots, Z$, so we often simply stack the generators and write such generating sets as $(n \times n)$ matrices, labelling the left-hand side with the relevant signs:

$$|0000\rangle \longleftrightarrow \left|\begin{array}{c|cccc} + & Z & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ + & \mathbf{1} & Z & \mathbf{1} & \mathbf{1} \\ + & \mathbf{1} & \mathbf{1} & Z & \mathbf{1} \\ + & \mathbf{1} & \mathbf{1} & \mathbf{1} & Z \end{array}\right|$$

and we can see that the signs determine the bit value in the computational basis state, if we look at the generators of the stabiliser groups for some other states:

$$|0001\rangle \longleftrightarrow \left|\begin{array}{c|cccc} + & Z & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ + & \mathbf{1} & Z & \mathbf{1} & \mathbf{1} \\ + & \mathbf{1} & \mathbf{1} & Z & \mathbf{1} \\ - & \mathbf{1} & \mathbf{1} & \mathbf{1} & Z \end{array}\right| \qquad |0101\rangle \longleftrightarrow \left|\begin{array}{c|cccc} + & Z & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ - & \mathbf{1} & Z & \mathbf{1} & \mathbf{1} \\ + & \mathbf{1} & \mathbf{1} & Z & \mathbf{1} \\ - & \mathbf{1} & \mathbf{1} & \mathbf{1} & Z \end{array}\right|$$

For our purposes, we are only really interested in stabilisers that are also elements of the n-qubit Pauli group $\mathcal{P}_n$, and we shall soon see that these form an *abelian* group. It turns out that such stabilisers can describe highly entangled states. In particular, the four Bell states (which we first talked about in Section 5.7) can be defined rather succinctly by their stabiliser groups:

Bell state	Stabiliser group
$\Phi^+ = \|00\rangle + \|11\rangle$	$\langle XX, ZZ\rangle$
$\Psi^+ = \|01\rangle + \|10\rangle$	$\langle XX, -ZZ\rangle$
$\Phi^- = \|00\rangle - \|11\rangle$	$\langle -XX, ZZ\rangle$
$\Psi^- = \|01\rangle - \|10\rangle$	$\langle -XX, -ZZ\rangle$

Not only this, but some vector spaces are also rather easily defined: the subspace of the three-qubit state space spanned by $|000\rangle$ and $|111\rangle$ is stabilised by

$$\{\mathbf{111}, ZZ\mathbf{1}, Z\mathbf{1}Z, \mathbf{1}ZZ\} = \langle ZZ\mathbf{1}, \mathbf{1}ZZ\rangle.$$

Right now, it might seem more complicated to use stabilisers to define vectors or subspaces, but when we start looking at states with a larger and larger number of components we will see how this approach ends up being very tidy indeed! It is not be true that the stabiliser description of states

and subspaces will *always* be the most concise, but it is true in a lot of cases that are of interest to us.

Returning to our claim that stabiliser groups that are subgroups of $\mathcal{P}_n$ are abelian, let us start with a definition, and then justify it afterwards.

> An n**-qubit Pauli stabiliser group** is any subgroup of $\mathcal{P}_n$ that is abelian and does not contain $-\mathbf{1}$. Its elements are called **Pauli stabilisers**.

Recall that, in order for the subspace $V_\mathcal{S}$ stabilised by some group $\mathcal{S}$ to be non-trivial, we need $-\mathbf{1} \notin \mathcal{S}$. Given that all Pauli operators square to the identity, and all pairs of Pauli operators either commute or anticommute, this implies that if we want some Pauli operators to stabilise anything then they must *commute*. Indeed, if S_1 and S_2 are two Pauli operators that anticommute, and $|\psi\rangle$ is any vector stabilised by both of them, then

$$\begin{aligned} |\psi\rangle &= S_1 S_2 |\psi\rangle \\ &= -S_2 S_1 |\psi\rangle \\ &= -|\psi\rangle \end{aligned}$$

which means that $|\psi\rangle = 0$. But saying that we are looking at a stabiliser group consisting of Pauli stabilisers that all commute with one another (as opposed to anticommuting) is exactly saying that we have an abelian subgroup of $\mathcal{P}_n$; if we want it to be non-trivial, then we need it to not contain $-\mathbf{1}$. Conversely, if we pick any abelian subgroup of $\mathcal{P}_n$ that does not contain $-\mathbf{1}$, this stabilises *some* subspace $V_\mathcal{S}$.

The size of any Pauli stabiliser $\mathcal{S}$ 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 stabiliser group, we can always express its elements using many different sets of generators; a specific choice of r independent generators of a Pauli stabiliser $\mathcal{S}$ of size 2^r is called a **presentation**. In order to choose a presentation from the set of elements of $\mathcal{S}$, we have to start by picking any non-identity element, of which there are $2^r - 1$. Inductively then, we pick the next generator by picking any element which is not in the subgroup generated by the previously selected generators, which means that there are

$$(2^r - 1)(2^r - 2)(2^r - 2^2) \ldots (2^r - 2^{r-1})$$

possible generating sets of $\mathcal{S}$. But these are *ordered* sets (i.e. we are keeping track of the order in which we pick the elements, so $G_1, G_2, \ldots$ is a "different" choice than $G_2, G_1, \ldots$), so if we want to know the number of presentations then we can simply divide the expression above by $r!$.

An interesting si
to explain why
independent Pau
be equal to the i

For example, the Bell state $\Phi^+ = |00\rangle + |11\rangle$ is stabilised by the group $\{\mathbf{11}, XX, -YY, ZZ\}$. This stabiliser group has $(2^2 - 1)(2^2 - 2)/2! = 3$ presentations, namely $\langle XX, ZZ\rangle$, $\langle -YY, XX\rangle$, and $\langle ZZ, -YY\rangle$.

So now we know the size of a Pauli stabiliser, but what can we say about the dimension of the subspace that it stabilises? If $|\mathcal{S}| = 2^r$ then the corresponding stabiliser subspace $V_\mathcal{S}$ has dimension 2^{n-r} (where n is the number of qubits, i.e. such that $\mathcal{S} \subseteq \mathcal{P}_n$). To see this, we can look at the projector P_S onto $V_\mathcal{S}$, since once we have a projector onto any subspace we know that the dimension of that subspace is exactly the trace of the projector (we can prove this by thinking

about the matrix of the projector in the diagonal form). In our case (using the result of Exercise 7.8.5) we calculate that

$$\begin{aligned}\operatorname{tr} P_S &= \operatorname{tr} \frac{1}{2^r}(S_1 + S_2 + \ldots + S_{2^r}) \\ &= \frac{1}{2^r}(\operatorname{tr} \mathbf{1}) \\ &= 2^{n-r}\end{aligned}$$

since any non-identity element of the stabiliser group has trace equal to zero, and $\operatorname{tr} \mathbf{1}^{\otimes n} = 2^n$, whence $\dim V_s = 2^{n-r}$. If $r = n$ then the stabilised subspace is 1-dimensional, and so we have stabiliser states.

There is a more geometric way of understanding why powers of 2 keep on turning up in these calculations. Given independent Pauli generators, it is convenient to think about the state or subspace that they stabilise as being the result of repeatedly bisecting the Hilbert space. Let $G_1, \ldots, G_r$ be a presentation of a Pauli stabiliser $\mathcal{S}$. For each operator G_i, half its eigenvalues are $+1$ and another half are -1, so each G_i bisects the 2^n-dimensional Hilbert space of n qubits into two eigenspaces of equal size. So G_1 gives two 2^{n-1}-dimensional subspaces: one for the $+1$ eigenvalue and one for the -1 eigenvalue. Forgetting about the -1 part and just focusing on the $+1$ part, G_2 then splits this 2^{n-1}-dimensional subspace into two 2^{n-2}-dimensional subspaces, since it is independent from G_1 (as we justify in Exercise 7.8.5). Repeating this procedure, forgetting about the -1 subspace each time, leads us to consider the simultaneous $+1$-eigenspace of $G_1, \ldots, G_r$, where each time we pass from $\{G_1, G_2, \ldots, G_i\}$ to $\{G_1, G_2, \ldots, G_i, G_{i+1}\}$ we bisect the subspace into two equal parts once more, eventually ending with the 2^{n-2}-dimensional subspace $V_{\mathcal{S}}$, as above. We can show this pictorially, as in Figure 7.1.

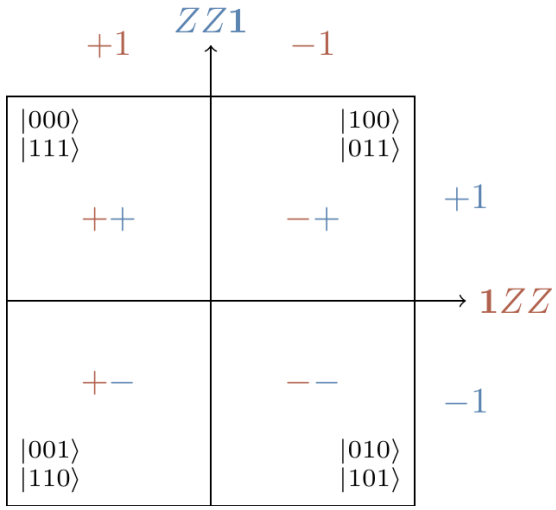


Figure 7.1: The stabiliser group $\mathcal{S} = \langle ZZ\mathbf{1}, \mathbf{1}ZZ \rangle$ bisects the Hilbert space of three qubits into four equal parts, and gives the stabilised subspace $V_{\mathcal{S}}$ which is spanned by $|000\rangle$ and $|111\rangle$. Think of the labels $ZZ\mathbf{1}$ and $\mathbf{1}ZZ$ as the x- and y-axes, and the sign labels on each square as (x, y)-coordinates. So the two squares on the left together make the $+1$-eigenspace of $\mathbf{1}ZZ$, and the two squares on the top make the $+1$-eigenspace of $ZZ\mathbf{1}$.

This diagram will make a reappearance in Sections 13 and 14.

7.3. Single stabiliser states

Given n independent generators of a stabiliser group $\mathcal{S}$ on a Hilbert space of n-qubits, we end up specifying a 1-dimensional subspace, meaning it is spanned by a single basis vector, namely the stabiliser state. We have already talked about the single-qubit stabiliser states determined by all possible stabilisers 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 mentioned some of the two-qubit stabilisers states, some of which are highly entangled, such as the Bell states, and some of which are separable, such as the computational basis states (whose stabilisers groups we described by block matrices with Z on the diagonal, $\mathbf{1}$ everywhere else, and signs labelling each row depending on the binary description of the state).

Here's another two-qubit example: that of the maximally entangled state $|00\rangle + |11\rangle$. This is stabilised by $\langle XX, ZZ\rangle$, but let's explain how we can see this. If we look first at the operator XX, we see that it splits the 4-dimensional Hilbert space into two 2-dimensional subspaces, corresponding to eigenvalues ± 1; by definition, it stabilises the one corresponding to eigenvalue $+1$, which is spanned by $|00\rangle + |11\rangle$ and $|01\rangle + |10\rangle$. Now the operator ZZ also splits the 4-dimensional Hilbert space into two 2-dimensional subspaces, again corresponding to eigenvalues ± 1; it stabilises the one corresponding to eigenvalue $+1$, which is spanned by $|00\rangle + |11\rangle$ and $|00\rangle - |11\rangle$. Note that $|01\rangle + |10\rangle$ is in the -1-eigenspace of ZZ, even though it is in the $+1$-eigenspace of XX (and vice versa for $|00\rangle - |11\rangle$). So the simultaneous $+1$-eigenspace of XX and ZZ is exactly the state $|00\rangle + |11\rangle$.

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

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

As we have already mentioned when discussing presentations of a stabiliser group, there can be multiple different generating sets, which corresponds to the fact that there are multiple different ways of bisecting the Hilbert space. For example, the stabiliser state $|00\rangle + |11\rangle$ is completely specified by $\langle XX, ZZ\rangle$, as shown above, but also by $\langle XX, -YY\rangle$ or $\langle -YY, ZZ\rangle$. But, as we should expect, these three generating sets all generate the same group, namely $\mathcal{S} = \{\mathbf{11}, XX, -YY, ZZ\}$.

How many n-qubit stabiliser states do we have? The answer is

$$
2^n \prod_{k=0}^{n-1} (2^{n-k} + 1)
$$

This is a com
combinatorial
*over*count, and t
by accounting fc

as we can show with a counting argument: we will count the number of generating sets with n generators (since this is exactly the right number of generators to specify a 1-dimensional stabiliser subspace) and then divide by the number of presentations for any given stabiliser. There are 4^{n-1} choices for the first generator G_1 (ignoring overall sign), since it can be any n-fold tensor product of the four Pauli matrices, excluding the identity $\mathbf{1111}$. For the second generator G_2, we have $(4^n/2) - 2$ possibilities, since it must commute with the first generator (and we know that exactly half of the operators commute with any given operator, as shown in Exercise 7.8.3, whence $4^n/2$) and it cannot be $\mathbf{1111}$ or G_1 (whence -2). Similarly, G_3 must commute with both G_1 and

G_2, but it cannot be in the group generated by them, so there are $(4^n/4) - 4$ possible choices, and so on. This means that we have

$$2^n(4^n-1)\left(\frac{4^n}{2}-2\right)\left(\frac{4^n}{4}-4\right)\dots\left(\frac{4^n}{2^{n-1}}-2^{n-1}\right)$$

possible generating sets in total. Now we need to divide by the number of presentations, but we have already calculated this in Section 7.2: it's exactly

$$(2^n-1)(2^n-2)(2^n-2^2)\dots(2^n-2^{n-1}).$$

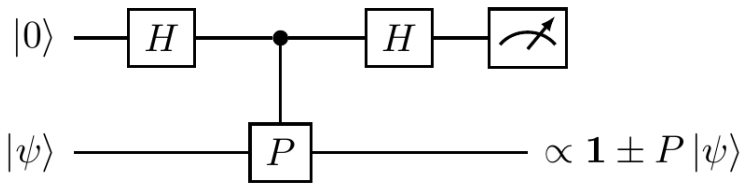
It is a fun algebra exercise to show that this division indeed gives the number we claimed.

As we will see, stabiliser states are ubiquitous in quantum information theory due to their versatility and relative simplicity. They play a crucial role in areas such as quantum error correction, measurement-based quantum computation, and entanglement classification.

7.4. Measuring Pauli stabilisers

How do we bisect Hilbert spaces in practice? By measuring stabilisers.

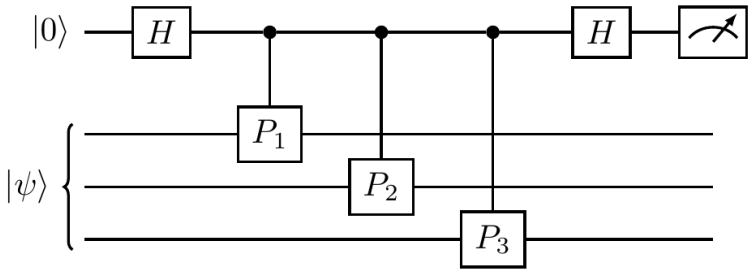
Let's start by measuring any single-qubit observable that squares to the identity. The corresponding operator P with eigenvalues ± 1 is both Hermitian and unitary, and can thus represent both an observable and a quantum gate. If we prepare a qubit in some state $|\psi\rangle$ and then wish to perform a measurement that will give us a result of ± 1 and leave the qubit in a post-measurement state, namely the corresponding eigenvector, then we can use the following circuit (where $\propto$ denotes that two states are multiples of one another).



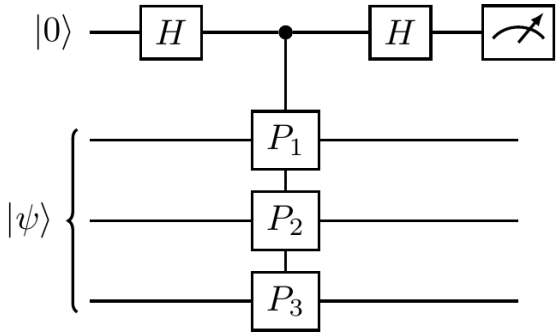
This construction requires an auxiliary qubit (in the top register), two Hadamard gates, and the tacit assumption that we can construct a controlled-P operator. Stepping through the execution of this circuit, we get

$$\begin{aligned}
|0\rangle|\psi\rangle &\overset{H\otimes\mathbf{1}}{\longmapsto} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle \\
&\overset{\text{c-}P}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle P|\psi\rangle \\
&\overset{H\otimes\mathbf{1}}{\longmapsto} |0\rangle\frac{1}{2}(\mathbf{1}+P)|\psi\rangle + |1\rangle\frac{1}{2}(\mathbf{1}-P)|\psi\rangle.
\end{aligned}$$

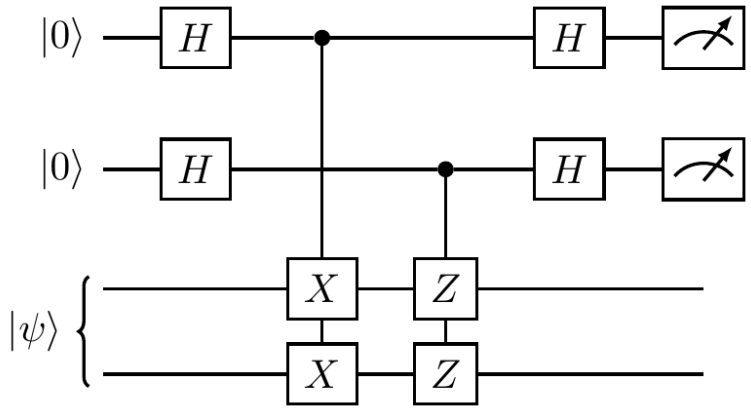
The final state of the two qubits indicates that, when the auxiliary (top) qubit is found in state $|0\rangle$ then we projected the state $|\psi\rangle$ onto the $+1$-eigenspace of P (via the projector $\frac{1}{2}(\mathbf{1}+P)$), and when it is found in state $|1\rangle$ then we projected $|\psi\rangle$ onto the -1-eigenspace (via the projector $\frac{1}{2}(\mathbf{1}-P)$). In particular, the X, Y, and Z observables can be measured using controlled-X, controlled-Y, and controlled-Z gates (respectively). This pattern can easily be extended to an n-qubit Pauli operator. For example, for $n=3$, a generic circuit that implements a projective measurement onto the ± 1-eigenspaces of $S = P_1 \otimes P_2 \otimes P_3$ has the form



and is usually drawn more compactly as



In this way, we can measure stabilisers and project onto the subspaces that they stabilise. For example, take the stabiliser group $\mathcal{S} = \langle XX, ZZ \rangle$, and consider the circuit below:



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 the $+1$ Pauli eigenvalue, and a bit value of 1 to the -1 eigenvalue. The first measurement can apply one of two projectors to $|\psi\rangle$:

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

The second measurement can further project the resulting post-measurement state of the two qubits in one of two ways:

a. $\frac{1}{2}(\mathbf{1} + ZZ)$, in which case the second auxiliary qubit will show 0, corresponding to the eigenvalue $+1$, and the subspace spanned by $|00\rangle + |11\rangle$ and $|00\rangle - |11\rangle$
b. $\frac{1}{2}(\mathbf{1} - ZZ)$, in which case the second auxiliary qubit will show 1, corresponding to the eigenvalue -1, and the subspace spanned by $|01\rangle + |10\rangle$ and $|01\rangle - |10\rangle$.

So if both auxiliary qubits show bit value outcome 0 (corresponding to the **Pauli outcome** $(+1, +1)$ of eigenvalues), then we have successfully projected onto the state stabilised by XX and ZZ, which is exactly $|00\rangle + |11\rangle$. More generally, in **Pauli notation**, the outcome $(\pm 1, \pm 1)$ corresponds to the projection onto the stabiliser state stabilised by $\langle \pm XX, \pm ZZ \rangle$.

Needless to say, we do not have any control over the actual outcomes of the measurement, but we do now know *which* post-measurement state we have generated. This means that we can use the circuit to prepare a desired state by applying an appropriate unitary operation to the final state. For example, if we want to generate the state $|00\rangle + |11\rangle$ but actually end up with the state $|00\rangle - |11\rangle$, then we can simply apply the Z operation to any of the two qubits to get the desired result. This generic method is not the only way of constructing projective measurements of Pauli observables, however — see Exercise 7.8.7