Dr. Nicolai Lang
Institute for Theoretical Physics III, University of Stuttgart

June 26th, 2025
SS 2025

Problem 9.1: Braid group representations from the Majorana algebra [**Oral** | 12 pt(s)]

ID: ex_braid_group_representation:tqp25

Learning objective

Anyons are localized particles in two-dimensional systems that obey neither fermionic nor bosonic statistics. In general, their statistics is described by representations of the *braid group*. In this exercise, you familiarize yourself with the braid group and then use the Majorana modes introduced in the lecture to construct a non-Abelian representation which describes the braiding statistics of so called *Ising anyons*. This construction motivates the concept of so called Majorana-based *topological quantum computing*[a], and can – in principle – be realized with vortices in two-dimensional p-wave superconductors or at the ends of one-dimensional Majorana chains (or generalized *wire networks*[b]).

[a] T. Karzig *et al.*, Scalable designs for quasiparticle-poisoning-protected topological quantum computation with Majorana zero modes, Physical Review B 95, 235305 (2017)

[b] J. Alicea *et al.*, Non-abelian statistics and topological quantum information processing in 1D wire networks, Nature Physics 7, 412 (2011)

A brief[1] introduction to particle statistics

Consider a set of N indistinguishable particles described by positions $\boldsymbol{x} \in \mathbb{R}^{dN}$ in d-dimensional space. A *path integral* is the (formal) sum of all possible paths in *configuration space* $\mathcal{C}$ from a fixed initial point $(\boldsymbol{x}_i, t_i)$ to a fixed finial point $(\boldsymbol{x}_f, t_f)$, weighted by a phase given by the classical action S:

$$\underbrace{\langle \boldsymbol{x}_f | \hat{U}(t_f, t_i) | \boldsymbol{x}_i \rangle}_{\text{Amplitude of configuration } \boldsymbol{x}_i \text{ evolving into configuration } \boldsymbol{x}_f} \sim \underbrace{\sum_{g \in G} \rho(g)}_{\text{Sum over equivalence classes of paths that cannot be continuously deformed into each other}} \underbrace{\int_{\substack{\text{Path}\in g \\ \boldsymbol{x}_i \mapsto \boldsymbol{x}_f}} \mathcal{D}(\text{Path})\, e^{iS[\text{Path}]}}_{\text{Integral over paths in class } g \text{ that can be continuously deformed into each other}} . \tag{1}$$

A key insight is that the *path space* (i.e., the space of all continuous paths through $\mathcal{C}$ with fixed endpoints $\boldsymbol{x}_i$ and $\boldsymbol{x}_f$) splits into topologically inequivalent components. That is, certain paths cannot be continuously deformed into other paths (because we assume the particles cannot occupy the same point in space at the same time). Naturally, paths through $\mathcal{C}$ can be concatenated, which induces a multiplication on path space. The set of (equivalence classes of) topologically inequivalent paths through $\mathcal{C}$ then forms a group known as the *fundamental group* $G := \pi_1(\mathcal{C})$.

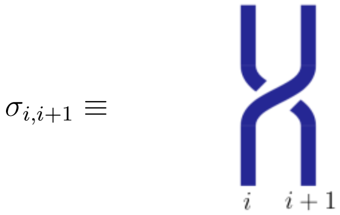
Because one can only define integrals over continuous components, this forces us to split the path integral (1) into separate path integrals over the different classes $g \in G$. This opens the possibility to weight the different contributions with a *class functions* ρ that is independent of the action that determines the local dynamics of the particles.

[1] For more details have a look at Chapter 3 of Topological Quantum by Steven Simon.

Mathematically, one finds that ρ must be *unitary* to conserve probabilities. Furthermore, one can show that ρ must be a *representation* of G to ensure that the composition law for paths remains valid. Beyond these requirements, the laws of quantum mechanics do not tell us which prefactors for the path integral we should use. It is a matter of experiment to determine these representations for different types of particles. The representation ρ of G is what determines the *statistics* of the particles! Thus, to understand which types of statistics are possible, one must understand the possible representations of G:

In $d \geq 3$ spatial dimensions, it turns out that $G \simeq S_N$ is the symmetric group. This means that the different components in the space of paths on $\mathcal{C}$ are labeled by the way the N particles are *permuted*. Focusing on one-dimensional[2] representations of S_N, one finds two of them: the trivial one (where exchanging two particles does nothing) and the sign representation (where exchanging yields a minus sign). These two representations correspond to *bosonic* and *fermionic* statistics, respectively.

Something remarkable happens in $d = 2$ dimensions[3]: Then, $G \simeq B_N$ turns out to be the so called *braid group*. The elements of this group can be visualized as braids of N strings that start and end on fixed positions $i = 1, \ldots, N$ (figure to the right). Physically, the strings correspond to the *world lines* of the N particles through $2+1$-dimensional spacetime.



It is convenient to lay out the strings in parallel and label their horizontal position by an integer $i = 1, \ldots, N$. One then defines the counterclockwise exchange of the two adjacent strands at i and $i+1$ as $\sigma_{i,i+1} \in B_N$ (depicted in the figure). It is easy to see [subtask a)] that all possible braids can be decomposed into such elementary exchanges of adjacent string, hence the set of all $\sigma_{i,i+1}$ *generates* the braid group B_N.

Note that – in contrast to the $3+1$-dimensional case with the symmetric group[4] S_N – exchanging two adjacent braids *twice* knots their paths so that $\sigma_{i,i+1}^2 \neq 1$.

a) Argue that the braid group B_N can be generated by $\sigma_{1,2}, \sigma_{2,3}, \ldots \sigma_{N-1,N}$ and their inverses. **2**pt(s)

What is the order $|B_N|$ of the braid group?
Compare this to the order $|S_N|$ of the symmetric group.

Convince yourself *geometrically* that the defining relations of the braid group B_N are

$$\sigma_{i,i+1}\,\sigma_{i+1,i+2}\,\sigma_{i,i+1} = \sigma_{i+1,i+2}\,\sigma_{i,i+1}\,\sigma_{i+1,i+2}\,, \tag{2a}$$

$$\sigma_{i,i+1}\,\sigma_{j,j+1} = \sigma_{j,j+1}\,\sigma_{i,i+1} \tag{2b}$$

for $i \in \{1, \ldots, N-2\}$, $j \in \{3, \ldots, N-1\}$ and $|j - i| > 1$.

Note: We read a "braid word" like $\sigma_{i,i+1}\sigma_{j,j+1}^{-1}$ from right to left (do the right-most operation first).

This allows us to define the Braid group

$$B_N := \langle\, \sigma_{1,2}, \ldots, \sigma_{N-1,N} \mid \text{Eq. (2a)} \wedge \text{Eq. (2b) fulfilled} \,\rangle \tag{3}$$

[2] Higher-dimensional representations lead to particles with so called *parastatistics*.

[3] Mathematically, the distinction between $2+1$-dimensional spacetime and $3+1$-dimensional spacetime (and higher dimensions) is that there are non-trivial *knots* in *three* dimensions but none in higher dimensions (can you see why?).

[4] This sets the *braid group* B_N apart from the *symmetric group* S_N: The symmetric group can be interpreted as a "truncated" braid group characterized by setting $\sigma_{i,i+1}^2 = 1$. Conversely, the Braid group can be interpreted as a non-Abelian "extension" of the symmetric group which accounts for the direction in which two strands are exchanged.

as the free group of the $N-1$ generators, modulo the relations Eq. (2a) and Eq. (2b).

Particles that live in $2+1$ dimensions and transform via a (non-trivial) braid group representation ρ are known as an *anyons*. If the representation is non-Abelian (and therefore necessarily not one-dimensional), such particles are called *non-Abelian anyons*. This means that in $2+1$ dimensions, indistinguishable particles can behave differently from bosons and fermions!

A particularly simple type of anyon (= statistics) are called *Ising anyons*[5]. Ising anyons can be physically realized (up to phases) in the low-energy sector of models that carry Majorana zero modes; for example, in the vortices of p-wave superconductors or at the ends of one-dimensional Majorana chains (as you have seen in the lecture). Thus, the non-Abelian braiding statistics of Ising anyons can be described in terms of Majorana fermions (by associating a Majorana mode with each anyon).

The goal of this exercise is to derive and study a (non-Abelian) *Braid group representation* that can be constructed from Majorana modes.

To this end, we consider some system with in total $N=2M$ Majorana zero modes

$$\{\gamma_i,\gamma_j\} = 2\delta_{i,j} \quad \text{with} \quad \gamma_i = \gamma_i^\dagger \quad \text{for} \quad i,j \in \{1,\dots,2M\}\,. \tag{4}$$

Note that it is in particular $\gamma_i^2 = \mathbb{1}$. (Think of M Majorana chains in the topological phase.)

Remember that every *pair* of Majorana modes γ_{2i-1} and γ_{2i} can be combined into one fermion mode $c_i = \frac{1}{2}(\gamma_{2i-1}+i\gamma_{2i})$ to each of which we can associate the number operator $n_i = c_i^\dagger c_i$. Since we assume the $2M$ Majorana modes to be zero modes (= not show up in the Hamiltonian), the ground state space of our system must be 2^M-fold degenerate and we can label ground states by the occupation numbers n_i. (Hence we can store M *qubits* in the ground state space.)

In the following, we identify the Majoranas γ_i with the i-th "strand" on which the Braid group B_{2M} ($N=2M$) operates. Our goal is to find a unitary representation ρ built from Majorana zero modes (this representation acts on fermionic Fock space, and in particular the degenerate ground state space of our system). Note that we can completely define a representation of B_{2M} by defining it on the generators $\sigma_{1,2}, \sigma_{2,3}, \dots, \sigma_{2M-1,2M}$.

Physically, we want admissible representations to act *locally*, i.e., the representation $\rho(\sigma_{i,i+1})$ that exchanges the i-th and the $i+1$-th strand (= Majorana mode) should be generated by γ_i and γ_{i+1} only. Furthermore, we require *translational invariance*, i.e., the coefficients in $\rho(\sigma_{i,i+1})$ should be independent of the strand indices i and $i+1$. Finally, since our representation operates on quantum states, it should be *unitary* to conserve probabilities.

b) Use locality and translational invariance to show that a representation of the generators must be of the form **1**pt(s)

$$\rho(\sigma_{i,i+1}) = a\,\mathbb{1} + b\,\gamma_i\gamma_{i+1} \tag{5}$$

for (still unknown) parameters $a, b \in \mathbb{C}$.

Hint: Use the braid group relation Eq. (2b).

c) Show that a *unitary* representation of the form (5) that satisfies the braid group relation Eq. (2a) **2**pt(s)

[5] The name "Ising" hints at a relation to the Ising model, this is not important for us here.

must have the form

$$\rho(\sigma_{i,i+1}) = \frac{e^{i\varphi}}{\sqrt{1+|s|}}(\mathbb{1} + s\gamma_i\gamma_{i+1})\,, \tag{6}$$

with $s \in \{-1, 0, 1\}$ and an arbitrary phase $\varphi \in [0, 2\pi)$.

In which case is this representation Abelian? In which case is it non-Abelian?

What happens when flipping the sign $s \mapsto -s$?

d) Show that the representation (6) can be rewritten as an exponential 1pt(s)

$$\rho(\sigma_{i,i+1}) = e^{i\varphi} \exp\left[s\frac{\pi}{4}\gamma_i\gamma_{i+1}\right] \tag{7}$$

in terms of the anti-Hermitian generator $s\frac{\pi}{4}\gamma_i\gamma_{i+1}$.

Note: In the literature, both expression (6) and expression (7) can be found. For “true” (i.e. non-projective) *Ising anyons*, it is $s = 1$ and the phase would be fixed to $\varphi = \frac{\pi}{8}$.

In the following, we consider the parity $P_i \equiv i\gamma_{2i-1}\gamma_{2i}$ of the fermion mode c_i and the total parity $P = \prod_{i=1}^{M} P_i$ of the zero modes.

e) Show that $P_i = \exp\left[i\pi(1 - n_i)\right]$ and $P = \exp\left[i\pi(M - n)\right]$. 1pt(s)

What are the eigenvalues of P? Interpret these eigenvalues.

f) Show that the eigenvalue of P remains unchanged under every braiding operation. 1pt(s)

Use this to argue that the representation (7) reduces to two 2^{M-1}-dimensional representations.

Naturally, the representation (6) [or (7)] acts on the Majorana zero modes via conjugation:

$$\rho(\sigma_{i,i+1}) \circ \gamma_j \equiv \rho(\sigma_{i,i+1})\,\gamma_j\,\rho(\sigma_{i,i+1})^\dagger\,. \tag{8}$$

g) Compute the group action of $\rho(\sigma_{i,i+1})$ on the Majorana modes $\gamma_1, \ldots, \gamma_{2M}$. 1pt(s)

Does this reflect the interpretation of γ_j as “strands” that are swapped by $\rho(\sigma_{i,i+1})$?

As remarked earlier, for the braid group, the double-exchange $\sigma_{i,i+1}^2 \neq 1$ is *not* the identity. Instead, this describes the *braiding* of one mode γ_i around another mode γ_{i+1}. In the last part of this exercise, we study the effect of such a braiding operation on the degenerate ground state space.

h) First, let us consider the braiding of two Majorana modes γ_{2i-1} and γ_{2i} that belong to the *same* Fermion mode $c_i = \frac{1}{2}(\gamma_{2i-1} + i\gamma_{2i})$. 2pt(s)

As a preparation, show that the exchange of the two modes

$$\rho(\sigma_{2i-1,2i}) = \frac{e^{i\varphi}}{\sqrt{1+|s|}}(\mathbb{1} - isP_i) = e^{i\varphi}\exp\left[-is\frac{\pi}{4}P_i\right] \tag{9}$$

can be expressed in terms of the parity operator of the fermion mode P_i.

What is the representation $\rho(\sigma_{2i-1,2i}^2)$ for *braiding* of two modes?

Use this result to compute the group action on the fermion modes $c_1^{(\dagger)}, \ldots, c_M^{(\dagger)}$.

Since the fermion mode c_i is composed of the two Majoranas γ_{2i-1} and γ_{2i} that we braid around each other, we can interpret this operation as *rotation* of the fermion mode by $360°$. The phase that is picked up due to this operation is therefore called *topological spin*.

Does the topological spin of the fermion mode (for $s \neq 0$) match your expectations for a fermion?

i) Finally, consider the two adjacent fermion modes $c_i = \frac{1}{2}(\gamma_{2i-1}+i\gamma_{2i})$ and $c_{i+1} = \frac{1}{2}(\gamma_{2i+1}+i\gamma_{2i+2})$ that comprise the four Majorana modes $\gamma_{2i-1}, \gamma_{2i}, \gamma_{2i+1}, \gamma_{2i+2}$. 1pt(s)

How does the braiding (= double exchange) of γ_{2i} and γ_{2i+1} act on the two fermion modes?

How can you populate two *non-adjacent* fermion modes by braiding?

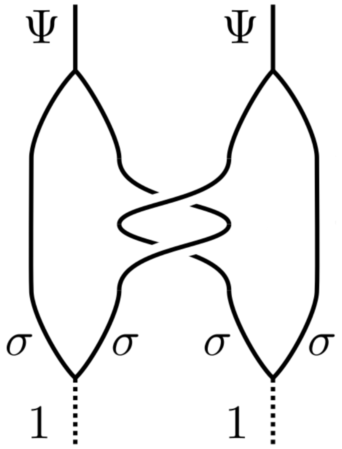
Can you populate only a single fermion mode by braiding?

An **Ising anyons theory** knows two types of particles (plus the trivial particle 1 which means "no particle"): The *Ising anyon* itself (often called σ) and a *fermion* (called Ψ). A characteristic feature of this type of statistics is that when one brings two Ising anyons together (called *fusion*), the outcome is either 1 (no particle) or Ψ (a fermion). Formally, one writes

$$\sigma \otimes \sigma = 1 \oplus \Psi \,. \tag{10}$$

This abstract structure is realized in the Majorana framework considered here by identifying the Ising anyons with Majorana zero modes. Their fusion is then described by measuring the occupation of the Fermion mode that can be constructed from them. Naturally, this process has two outcomes: Either the mode is empty (1) or it is occupied by a fermion (Ψ). The fact that there is more than one possible outcome for fusion makes Ising anyons *non-Abelian*.

This non-Abelian nature also becomes evident in their *braiding rules*, one of which can be pictorially described as shown on the right (time flows from bottom to top).
You start with two pairs of Ising anyons (= Majorana modes) that fuse to 1 (= their fermion modes are empty). Then you braid the two inner Majorana modes (which belong to different pairs) around each other. When you know fuse the two pairs again, you find a fermion in each of them. This is your result from subtask i) reformulated in the abstract language of anyons theories. Operations like this are at the heart of *topological quantum computation*, where unitary gates are implemented by such braiding procedures.



Problem 9.2: Stabilizer formalism

[**Written** | 9 (+3 bonus) pt(s)]

ID: ex_stabilizer_formalism:tqp25

Learning objective

In the lecture, we used the degenerate ground state manifold of the Majorana chain as a quantum error correction code. To this end, we used the *stabilizer formalism*, where the stabilizer operators where constructed from Majorana modes. This is a rather niche application of the stabilizer formalism[a].

The stabilizer formalism itself is much more versatile, and an important tool in quantum information theory. Conventionally, stabilizer codes are *not* constructed from fermionic systems but used to describe systems of *qubits*. Here you study the stabilizer formalism from this more general point of view. In particular, you show how the famous *Shor code* can be expressed within this formalism.

[a] S. Bravyi *et al.*, Majorana fermion codes, New Journal of Physics 12(8), 083039 (2010)

We consider a system of N qubits, described by a Hilbert space $\mathcal{H} = (\mathbb{C}^2)^{\otimes N}$. The *Pauli group* on this Hilbert space is defined as the span

$$\mathcal{P}_N := \langle\, \mathbb{1},\ X_i,\ Y_i,\ Z_i \mid i \in \{1, \dots, N\}\,\rangle \tag{11}$$

of the Pauli matrices X_i, Y_i and Z_i for each qubit $i \in \{1, \dots, N\}$, where the group operation is their multiplication. The Pauli group includes all products of Pauli matrices with multiplicative factors ± 1 and $\pm i$.

We are interested in a subgroup $\mathcal{S} = \langle\, S_1, \dots, S_K\,\rangle \leq \mathcal{P}_N$ spanned by K *independent generators* $\{S_1, \dots, S_K\} \subset \mathcal{P}_N$. (Meaning: $\mathcal{S}$ is the set of products of the generators and no generator is a product of the other generators.) $K = \mathrm{rank}(\mathcal{S})$ is called the *rank* of $\mathcal{S}$.

The choice of generators is not arbitrary. In the following, we require that

$$-\mathbb{1} \notin \mathcal{S} \qquad \text{and} \qquad \forall_{i,j\in\{1,\dots,K\}}\ :\ [S_i, S_j] = 0\,. \tag{12}$$

Note: You show in subtask c) why these assumptions are necessary; here they are simply part of the definition.

With the group $\mathcal{S}$, we can define the linear subspace of states

$$\mathcal{H}_\mathcal{S} := \mathrm{span}\,\{\, |\psi\rangle \in \mathcal{H} \mid \forall_{S\in\mathcal{S}}\ :\ S\,|\psi\rangle = |\psi\rangle\,\} \tag{13}$$

that are invariant under every element of $\mathcal{S}$.
We say that $\mathcal{H}_\mathcal{S}$ is *stabilized* by $\mathcal{S}$ and $\mathcal{S}$ is the *stabilizer* of $\mathcal{H}_\mathcal{S}$.

Note: Convince yourself that Eq. (13) is a linear subspace of $\mathcal{H}$.

The rationale of the *stabilizer formalism* is to describe the quantum state(s) in $\mathcal{H}_\mathcal{S}$ *not* by writing down their amplitudes (which requires an exponential amount of resources), but by tracking (and transforming) their stabilizer group $\mathcal{S}$ (given by its generators S_i) instead. Since this requires only storing $\mathcal{O}(N)$ generators, this approach is much more efficient. Beyond this efficiency gain, the stabilizer formalism is also a versatile tool to describe a variety of quantum error correction codes and protocols.

In the following, you prove crucial properties of the stabilizer formalism and apply it to simple states, including the famous Shor quantum error correction code:

a) Our first goal is to determine the dimension of the stabilizer subspace $\mathcal{H}_\mathcal{S}$ as a function of the number of qubits N and the number of generators K. **2**pt(s)

As a preliminary step, show that for every fixed $i \in \{1, \dots, K\}$, there exists $P_i \in \mathcal{P}_N$ such that

$$\{S_i, P_i\} = 0 \qquad \text{and} \qquad \forall_{j\in\{1,\dots,K\}\setminus\{i\}} \ : \ [S_j, P_i] = 0\,. \tag{14}$$

Hint: Choose a suitable set of basis vectors.

Note: This shows that you can think of the generators S_i as generalized Pauli Z-matrices with the P_i as their associated Pauli X-matrices.

b) Use your result from a) to show that the dimension of the stabilized subspace is **2**pt(s)

$$\dim \mathcal{H}_\mathcal{S} = 2^{N-K}\,. \tag{15}$$

Note: This means, for instance, that to describe a single quantum state uniquely, you need as many stabilizer generators as qubits: $\dim \mathcal{H}_\mathcal{S} = 2^{N-N} = 1$.

Hint: Consider some vector $\boldsymbol{x} \in \mathbb{Z}_2^K$ and show that

$$P_\mathcal{S}^{\boldsymbol{x}} := \prod_{j=1}^{K} \frac{\mathbb{1} + (-1)^{x_j} S_j}{2} \tag{16}$$

is the projector onto the eigenspace $\mathcal{H}_\mathcal{S}^{\boldsymbol{x}}$ with eigenvalues $(-1)^{x_j}$ of S_j. Then use the result from a).

*c) In the definition of a stabilizer, the conditions Eq. (12) seem ad hoc. **+2**pt(s)

Show that $\mathcal{H}_\mathcal{S}$ is only a non-trivial subspace ($\dim \mathcal{H}_\mathcal{S} \neq 0$) if the conditions (12) are satisfied.

d) As a simple example, consider the $N = 2$-qubit *Greenberger–Horne–Zeilinger* state **1**pt(s)

$$|\mathrm{GHZ}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,. \tag{17}$$

What are the stabilizers $\mathcal{S}$ such that $\mathcal{H}_\mathcal{S} = \operatorname{span}\{|\mathrm{GHZ}\rangle\}$?

Write down a suitable set of generators.

Note: This example demonstrates what makes the stabilizer formalism so powerful: It can describe strongly entangled states!

e) Consider again $N = 2$ qubits and delete one generator from your GHZ-stabilizer to obtain the new stabilizer group $\mathcal{S} = \langle\, Z_1 Z_2 \,\rangle$. **1**pt(s)

Write down the full set of stabilizers $\mathcal{S}$.

What is the Hilbert space $\mathcal{H}_\mathcal{S}$ stabilized by $\mathcal{S}$? What is its dimension?

Write down a suitable basis.

Note that not every linear subspace (or state) can be described in terms of stabilizers. A simple counterexample is the space spanned by the W-state on $N = 3$ qubits (named after **W**olfgang Dür)

$$|\mathrm{W}\rangle = \frac{|100\rangle + |010\rangle + |001\rangle}{\sqrt{3}}\,. \tag{18}$$

Note: A proof of this statement requires additional knowledge about measurement outcomes of stabilizer states – otherwise it is not obvious.

As demonstrated in the lecture, the stabilizer formalism is extremely useful to describe *quantum error correction codes*. In this context, the stabilized subspace $\mathcal{H}_\mathcal{S}$ is the *code space* in which one wants to store the *logical qubits* to be protected from noise. Measuring stabilizer operators then yields information on errors that occurred (the so called *error syndrome*) *without affecting the amplitudes in the code space*. Note that this scenario requires $\dim \mathcal{H}_\mathcal{S} > 1$ so that $K < N$.

Suppose we have $N = 9$ qubits and $K = 8$ stabilizer generators which leaves us with a $2^{9-8} = 2$-dimensional Hilbert space $\mathcal{H}_\mathcal{S}$ (→ one logical qubit). The 8 generators are given by

$$S = \langle\, Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9, X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9 \,\rangle\,. \tag{19}$$

This stabilizer describes the famous *Shor code*[6]. Historically, it was the first quantum error correction code that allows for the correction of an arbitrary single qubit error (i.e., one accidental/unknown X_i, Y_i, or Z_i gate applied to any of the 9 qubits).

Note: To think about the Shor code stabilizer, it is convenient to arrange the qubits in a 3×3 array like so:

$$\begin{matrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{matrix} \tag{20}$$

f) Show that by measuring the 8 stabilizers (the error syndrome) one can *detect* whether a single qubit error occurred. **2**pt(s)

Hint: Why is it sufficient to study the effects of X_i and Z_i errors only?

Then show that (and how) by applying a single gate conditioned on the error syndrome, one can *correct* for any single qubit error.

Hint: Start with a state $|\psi\rangle \in \mathcal{H}_\mathcal{S}$ in the code space, such that for all generators $S_i\,|\psi\rangle = |\psi\rangle$, and apply a single qubit error, e.g., $|\psi'\rangle = X_1\,|\psi\rangle$. Then determine the measurement outcomes of all 8 stabilizers and try to come up with an algorithm to reverse the error.

*g) Construct the *logical Pauli matrices* Σ^x and Σ^z that operate on the logical qubit stored in $\mathcal{H}_\mathcal{S}$. **+1**pt(s)

Hint: These operators must satisfy $\{\Sigma^x, \Sigma^z\} = 0$ and $[\Sigma^\alpha, S_i] = 0$ for all $i = 1, \dots, 8$.

So far, you have shown that stabilizers can be used to *describe* states or vector spaces. However, the stabilizer formalism can also be used to describe *operations* acting on these quantum states.

Again, consider a state $|\psi\rangle$ that is uniquely stabilized by the stabilizer $\mathcal{S}$. It is easy to check (do so!) that a state $|\psi'\rangle = U\,|\psi\rangle$ transformed by some unitary U is stabilized by the new generators $S'_i = US_iU^\dagger$. This means that instead of keeping track of the *state* $|\psi\rangle$, we can keep track of the *stabilizer* $\mathcal{S}$ which describes the state.

In order for this to be an efficient encoding, it is necessary that all stabilizers can be described by N generators $S_i, S'_i \in \mathcal{P}_N$ *from the Pauli group*. (Do you see why storing N of such operators does not require an exponential amount of storage?)

Consequently, we can only keep track of unitary gates U that have the property that all new generators $S'_i = US_iU^\dagger$ are still elements of the Pauli group $\mathcal{P}_N$. The subgroup $\mathcal{C}_N \subset \mathrm{U}(2^N)$ of unitaries that maps elements of the Pauli group onto (potentially other) elements of the Pauli group is called the *Clifford group*.

h) Show that the Hadamard gate **1**pt(s)

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{21}$$

and the Phase gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{22}$$

(applied to any of the N qubits) belong to the Clifford group $\mathcal{C}_N$.

Can you write down other single-qubit gates that belong to $\mathcal{C}_N$?

One can show that the Hadamard and phase gate (on every qubit), together with the Controlled-NOT (CNOT) gate (applied between any pair of qubits) generate the complete Clifford group $\mathcal{C}_N$.

For this reason, any quantum circuit that only uses gates from the Clifford group (Hadamard-, Phase-, CNOT- and all Pauli-gates), can be efficiently simulated on a *classical computer* using the stabilizer formalism. This is an important result in quantum information theory known as the *Gottesman-Knill theorem*[7].

Crucially, the Clifford group does not contain all unitary operations. In particular, the T-gate $T = \sqrt{S}$ (which is a phase gate with a $\frac{\pi}{4}$ phase rotation) is *not* part of the Clifford group. It is because of these gates that we need a quantum computer!

[6] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, Physical Review A 52, R2493 (1995)

[7] See Chapter 10.5.4 in Quantum Computation and Quantum Information by Nielsen and Chuang for more details.