Basics for quantum magic

Yi-Ming Ding, Westlake University

Updated: Jan 7, 2025

Contents

1 Introduction 3

2 Stabilizer protocols 4

2.1 Stabilizer 4

2.2 Pauli group and generators of stabilizer group 5

2.3 Stabilizer formalism and Hadamard gate 6

2.4 CNOT gate, Phase gate, and the Clifford group 6

2.5 Normalizer of the Pauli group 8

2.6 Measurements and the Gottesman-Knill theorem 9

2.7 Non-stabilizerness or magic 10

3 Non-stabilizerness monotones 11

3.1 Stabilizer entropy 11

3.2 Mana 12

Notations

We use the following notations throughout the note:

- n denotes the number of qubits, and the dimension of a n-qubit quantum state is then 2^n.
- For a qubit or spin-$1/2$ system, we identify

$$|0\rangle \equiv |{\uparrow}\rangle\ , \ |1\rangle \equiv |{\downarrow}\rangle \tag{1}$$

- Unless otherwise specified, we assume the matrix representations of all the states and operators in this note are under the Pauli-z basis, i.e.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2}$$

  and

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{3}$$

  where X, Y, Z are the three Pauli matrices.

  In addition, we define the identity matrix

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{4}$$

- For each n-qubit state, we label the qubits with numbers from 1 to n, from left to right. For example, in the 2-qubit quantum state $|\phi\rangle = |01\rangle$, the first qubit is in the state of $|0\rangle$, and the second qubit is in the state of $|1\rangle$.

  When considering unitary transformation, we use the subscript to signify which qubit the operator is acting on. For example, X_1 means we act the Pauli-x operator on the first qubit, and it is easy to check that $X_1|\phi\rangle = X_1|01\rangle = |11\rangle$.

1 Introduction

- For a quantum state, which part of it can represent its *quantumness* that a classical system does not possess?

We may come up with few concepts in quantum mechanics to say that they can represent some quantumness such as **entanglement** (it is absolutely true that if and only if a quantum state can be entangled). However, the candidate for quantumness is not unique from the perspective of **quantum resource theory**.

For a set of objects, we identify the **free objects** and **resource objects** and the corresponding **free operations** and **resource operations** to generate these objects. For example, if we consider milk as the resource, the drinks (the set of objects) without milk are free drinks (e.g. lemon tea), and the others are resource drinks (e.g. Latte). Adding water to a cup of espresso requires no milk, thus this is a free operation. Similarly, adding milk to a cup of espresso is a resource operation.

If we bring the view of resource to the Hilbert space, which is basically a set of quantum states, we can divide it into two classes: **free states** and **resource states**. Starting from a free state on a quantum computer, any quantum operation that generates the resource (e.g. entanglement) to the state is a resource operation. Then by looking at how many resource we need to prepare a quantum state, we can tell how quantum it is given some specific resource. Another important question is what are the structures/properties of the resouece embbed in a quantum state since these structures can be responsible for some specific quantum behaviors of the quantum state (e.g. the area law of entanglement for ground states).

The subject of this note is about **magic**, also known as the **non-stabilizerness**. Briefly speaking, it is also some quantum resource, but from an utterly different perspective: **computational complexity**.

- If a classical system **C** can simulate all the behaviors of a quantum system **Q** within polynomial complexity, can we say **Q** is quantum or quantum enough?

The question above is the motivation for studying magic in the context of many-body systems, which alighs with the argument that *entanglement is not enough* [L. Susskind (2014)]. This is further highlighted in [Z.-W. Liu and A. Winter (2022)].

I will introduce what is magic later and provide some conclusions for those who do not like too much maths (there will be some maths since the next section). With magic to be the resource, we have two classes of states: **magic states** and **free states**, where the later one is also called **stabilizer states**. Based on the celebrated **Gottesman-Knill theorem**, the stabilizer states can be efficiently (polynomially) simulated and prepared on a classical Turing machine without any quantum computer. The remarkable thing here is: *a stabilizer state can be entangled, even highly entangled*. Therefore I would like to remark that magic is quite different from entanglement.

Before we step into the magical world, we have to first look at what is **stabilizerness**, which relates to an important theory in quantum information: the **stabilizer formalism**. Please note that it might be a little dull from here on since I will present you some math. To make them more understandable, I will provide as many examples as possible. The main reference of this note is the book *Quantum Computation and Quantum Information*, written by Michael A. Nielsen and Isaac L. Chuang, which I highly recommend to readers as well.

2 Stabilizer protocols

2.1 Stabilizer

Given a quantum state $|\psi\rangle$ and a unitary operation U, we say $|\psi\rangle$ is *stabilized by* U iff

$$U|\psi\rangle = |\psi\rangle \tag{5}$$

The notion that $|\psi\rangle$ is stabilized means it is unchanged after the operation of U. In other words, the state is stable under U. Accordingly, we call U the **stabilizer** of $|\psi\rangle$. (Of course, $|\psi\rangle$ is just an eigenstate of U with eigenvalue one! As we will see later, the introduction of stabilizer is useful!)

As an example, we consider an EPR pair

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{6}$$

which is stabilized by both X_1X_2 and Z_1Z_2 (easy to check this). This example also indicates that a state can have more than one stabilizer. On another hand, a stabilizer can also stabilize more than one state. For example, both $|00\rangle$ and $|11\rangle$ are stabilized by Z_1Z_2.

It is easy to prove that the the multiplication of different stabilizers is still a stabilizer, and diffferent stabilizers then can constitute a group, making it natural for us to consider the group theory. Therefore let us generalize the concept of stabilizer to the case of a set of unitaries.

Given a unitary group $\mathcal{S}$, and some n-qubit state (vector) space V_s, we say V_s is *stabilized by* $\mathcal{S}$ iff

$$\forall\, U \in \mathcal{S},\ |\psi\rangle \in V_s \Rightarrow U|\psi\rangle = |\psi\rangle \tag{7}$$

Similarly, we call $\mathcal{S}$ a **stabilizer group** (also abbriviated as **stabilizer**) of the state space V_s.

Equivalently (easy to check), given a unitary group $\mathcal{S}$, we can define its associated state space V_s as

$$V_s := \bigcap_{U \in \mathcal{U}} \left\{ |\psi\rangle \,\middle|\, U|\psi\rangle = |\psi\rangle \right\} \tag{8}$$

Notice that a $\mathcal{S}$ can have a trivial state space, which means there is no element in V_s.

For example, suppose $\mathcal{S} = \{\pm I, \pm X\}$, and $|\psi\rangle$ is some state stabilized by it, then

$$-I|\psi\rangle = -|\psi\rangle \Leftrightarrow |\psi\rangle = 0 \tag{9}$$

which means the V_s must be trivial.

2.2 Pauli group and generators of stabilizer group

We now define an important unitary group called the **Pauli group**. Given an n-qubit system, the Pauli group $\mathcal{P}_n$ is defined as

$$\mathcal{P}_n := \left\{ \xi \otimes_j \sigma_j \middle| \sigma_j \in \{I, X, Y, Z\}, \xi \in \{\pm 1, \pm i\} \right\} \tag{10}$$

The example for $n = 1$ is then

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \tag{11}$$

and the factors ± 1 and $\pm i$ are to ensure the closure.

Pauli group is a very interesting group, and in stabilizer formalism, *when we are discussing a stabilizer group, we would assume it to be a subgroup of the Pauli group.*

In the last subsection, we have provided such an example $\mathcal{S} = \{\pm I, \pm X\} \in \mathcal{P}_1$, which has a trivial state space. For an arbitary $\mathcal{S} \in \mathcal{P}_n$, it can be proved that a necessary and sufficient condition for V_s to be non-trivial is: $-I \notin \mathcal{S}$ and $\forall\, U_1, U_2 \in \mathcal{S}$, we have $[U_1, U_2] = 0$.

Here we additionally provide a non-trivial example for $n = 3$:

$$\mathcal{S} = \{I, Z_1 Z_2, Z_2 Z_3, Z_1 Z_3\}, \quad V_s = \{\alpha|000\rangle + \beta|111\rangle \mid \alpha, \beta \in \mathbb{C}\} \tag{12}$$

Apparently, we can generates all elements in $\mathcal{S}$ only with $Z_1 Z_2$ and $Z_2 Z_3$, therefore we call them the **generators** of $\mathcal{S}$. For simplicity, we write

$$\mathcal{S} = \langle Z_1 Z_2, Z_2 Z_3 \rangle \tag{13}$$

Generally, for a stabilizer group

$$\mathcal{S} = \langle g_1, \ldots, g_l \rangle \tag{14}$$

removing any g_i would make $\mathcal{S}$ changes, since different g_i are independent.

2.3 Stabilizer formalism and Hadamard gate

Suppose we have a unitary operation U acting on a vector space V_s stabilized by $\mathcal{S}$ (note that U is not necessarily in $\mathcal{S}$), then $\forall g \in \mathcal{S}$, we have

$$U|\psi\rangle = Ug|\psi\rangle = UgU^{\dagger}U|\psi\rangle \tag{15}$$

which means $U|\psi\rangle$ is stabilized by $UgU^{\dagger}$. This result is important if we shift our focus to the Heisenberg picture: the dynamics of V_s can be equivalently achieved by tracking the dynamics of $\mathcal{S}$. This is what we call the **stabilizer formalism**.

For example, suppose $U = H$, where H is the **Hadamard gate** defined as

$$H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{16}$$

then since $HZH^{\dagger} = X$ (it is easy to check this), after acting H on thie input state $|\phi\rangle_{\text{in}} = |0\rangle$ that is stabilized by Z, the output state $|\phi_{\text{out}}\rangle$ will be stabilized by X:

$$Z\,|\phi_{\text{in}}\rangle = Z\,|0\rangle = |\phi_{\text{in}}\rangle \tag{17}$$

$$|\phi_{\text{out}}\rangle = H\,|\phi_{\text{in}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{18}$$

$$X\,|\phi_{\text{out}}\rangle = |\phi_{\text{out}}\rangle \tag{19}$$

In general, for an n-qubit system, if the input stabilizer group is

$$\mathcal{S}_{\text{in}} = \langle Z_1, \dots Z_n \rangle \tag{20}$$

then after applying H to each qubit of the corresponding input state, the output state is stabilized by

$$\mathcal{S}_{\text{out}} = \langle X_1, \dots X_n \rangle \tag{21}$$

The power of the stabilizer formalism is that, rather than specifying 2^n amplitudes of a quantum state, it is equivalent to save the information of its stabilizer group, the element number of which is linear with n, since the number of generators of a group $\mathcal{G}$ is at most $\log|\mathcal{G}|$.

2.4 CNOT gate, Phase gate, and the Clifford group

The result about the Hadamard gate is actually not that surprising as H generates no entanglement. If the input state is a product state, then the output state is still a product state, which of course can be described with linear resources.

However, next I will tell you something incredible! We can show that similar thing also happens on the **CNOT gate**, which is able to generate entanglement in quantum circuits!

We first introduce the CNOT gate for those who are not familiar with quantum computation. CNOT gate is a two-qubit unitary which acts on a **controlled qubit** and a **target qubit**. If the controlled qubit is in $|1\rangle$, apply X operation to the target qubit, otherwise it does nothing. For $|q_1 q_2\rangle$, if the first qubit is the controlled qubit, then the matrix form of the gate is where the matrix form of $\text{CNOT}_{1\to 2}$ is

$$\text{CNOT}_{1\to 2}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \tag{22}$$

Suppose the input state is

$$|\phi_{\text{in}}\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle \tag{23}$$

which is a product state. Apparently it is stabilized by X_1. The output state under CNOT gate (assume the first qubit to be the controlled qubit) is then

$$|\phi_{\text{out}}\rangle = \text{CNOT}_{1\to 2}\,|\phi_{\text{in}}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{24}$$

which is entangled.

On another hand,

$$\text{CNOT}_{1\to 2}(X_1 \otimes I_2)(\text{CNOT}_{1\to 2})^\dagger = X_1 \otimes X_2 \tag{25}$$

which stabilizes $|\psi_{\text{out}}\rangle$. Therefore, the maximally entangled state $|\psi_{\text{out}}\rangle$ (its entanglement entropy is $2\log 2$) can still be described with polynomial resources under the stabilizer formalism.

Similarly, we can derive

Input	$X_1 \otimes I_2$	$I_1 \otimes X_2$	$Z_1 \otimes I_2$	$I_1 \otimes Z_2$
Output	$X_1 \otimes X_2$	$I_1 \otimes X_2$	$Z_1 \otimes I_2$	$Z_1 \otimes Z_2$

Is there any other gates that can be described with the stabilizer formalism? The answer is obviously yes since the Pauli matrices naturally satisfy our requirements.

For the X gate,

$$XXX^\dagger = X \tag{26}$$

$$XZX^\dagger = -Z \tag{27}$$

for the Y gate

$$YXY^\dagger = -X \tag{28}$$

$$YZY^\dagger = -Z \tag{29}$$

$$\tag{30}$$

and for the Z gate

$$ZXZ^\dagger = -X \tag{31}$$

$$ZZZ^\dagger = Z \tag{32}$$

Practically, instead of considering the Pauli gates, we consider the termed **phase gate**, which is defined by

$$S := \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{33}$$

It is also within the stabilizer formalism since

$$SXS^\dagger = Y \tag{34}$$

$$SZS^\dagger = Z \tag{35}$$

With some calculations, you can prove that

$$Z = S^2, \quad X = HZH, \quad Y = iZX \tag{36}$$

Therefore, the Pauli gates can be equivalently performed with H and S gates.

So far, we have obtained three gates: H, CNOT, and S. Taking them as the generators, we can define the termed **Clifford group**:

$$\mathcal{C} := \langle H, \mathrm{CNOT}, S \rangle \tag{37}$$

and the elements in the Clifford group are called the **Clifford gates** or **Clifford unitaries**. The reason why we define this will be clarified in the next subsection.

2.5 Normalizer of the Pauli group

Remember that the notion of stabilizer is defined on the state space, and using the stabilizer formalism, there is no need of considering the state space anymore. Therefore, we have to define a similar concept for a stabilizer group. This is called a **normalizer**. Since all the stabilizer groups are subgroups of the Pauli group in our context, it is straightforward to look at the normalizer of the Pauli group directly.

We say a unitary operator U is a normalizer of the Pauli group $\mathcal{P}_n$ iff

$$UgU^\dagger \in \mathcal{P}_n,\ \forall g \in \mathcal{P}_n \tag{38}$$

A theorem (we do not prove it here) follows is:

- Up to a global phase, ANY normalizer U defined above can be composed with only gates in $\{H, \mathrm{CNOT}, S\}$, with $\mathcal{O}(n^2)$ complexity.

In other words, all normalizers of the Pauli group form the Clifford group. Thus we also say the Clifford group is a normalizer of the Pauli group. Without the knowledge of H, CNOT, and S gates, you can also define the Clifford group by such a normalizer. They are equivalent.

2.6 Measurements and the Gottesman-Knill theorem

What we have so far? Since the Clifford group is the normalizer of the Pauli group, and under the stabilizer formalism, we are able to unitarily evolve those stabilized states (including maximally entangled states) on a classical computer with polynomial complexity. This is quite remarkable because it means entanglement is not the reason that prevents us from simulating quantum systems classically. Wait a minute. What about measurements? To perform quantum computing, we also needs measurements!

Suppose our observable is some Pauli string $P \in \mathcal{P}_n$ (an observable can always be expanded with Pauli strings), which is Hermitian and with phase one without loss of generality. Then there are two cases: P either commutes with all generators in the stabilizer $\langle g_1, \cdots, g_n \rangle$ or anticommutes with at least one generator g_1.

In the first case, $g_j P |\psi\rangle = P g_j |\psi\rangle = P |\psi\rangle$, which means $P |\psi\rangle \in V_s$ holds for any g_j. Then $P |\psi\rangle$ is multiples of $|\psi\rangle$, i.e. $P |\psi\rangle = \lambda |\psi\rangle$ with some number λ. Since P is a Pauli string, then $P^2 = 1$ gives $\lambda = \pm 1$ and P or $-P$ is in the stabilizer. Consequently, such a measurement will not change the state and yields ± 1 with probability one.

For the second case, if P also anticommutes with some g_j, then it is easy to prove that P commutes with $g_1 g_j$. Then we can equivalently consider $\langle g_1, \cdots, g_1 g_j, \cdots g_n \rangle$ as the stabilizer.

On aonther hand, the observable P has eigenvalues ± 1, then after the measurement, we would obtain the two collpased states with probabilities

$$\begin{aligned} p(+) &= \mathrm{Tr}\left(\frac{I+P}{2} |\psi\rangle \langle\psi|\right) \\ p(-) &= \mathrm{Tr}\left(\frac{I-P}{2} |\psi\rangle \langle\psi|\right) \end{aligned} \tag{39}$$

repsectively. Since $\{P, g_1\} = 0$, we have

$$p(+) = \mathrm{Tr}\left(\frac{I+P}{2} g_1 \left|\psi\right\rangle \left\langle\psi\right|\right) = \mathrm{Tr}\left(g_1 \frac{I-P}{2} \left|\psi\right\rangle \left\langle\psi\right|\right) = p(-) \tag{40}$$

which means the probabilities to collapse to both sides are equal. Suppose we obtain $+1$ after the measurement yielding the new state

$$\left|\psi^+\right\rangle = \frac{I+g}{\sqrt{2}} \left|\psi\right\rangle \tag{41}$$

it is easy to check that this state is stabilized by $\langle P, g_2, \cdots, g_n \rangle$. Similarly, if we obtain -1, then the collapsed state is stabilized by $\langle -P, g_2, \cdots, g_n \rangle$.

In addition, before each measurement, a commutativity check obviously costs polynomial complexity. Therefore, the measurements on this computational basis can also be performed within polynomial complexity on a classical computer in the stabilizer formalism.

What we have achieved here is summarized by the celebrated **Gottesman-Knill theorem**: *Given state $\left|00\cdots00\right\rangle$ as the input, if we only consider Clifford unitaries, measurements of observables in the Pauli group (which includes measurement in the computational basis as a special case), the possibility of classical control conditioned on the outcome of such measurements, and any other related operations if necessary, then only polynomial resources are sufficient on classical computers.* Such a special quantum circuit is called a **Clifford circuit**, or more general, a **Clifford protocol**.

2.7 Non-stabilizerness or magic

For convenience, we call the states that are stabilized by the Clifford unitaries the **stabilizer states**, denoted by STAB as their convex hull (the extreme points are exactly the stabilizer states), and those states that are not stabilizer states in the Hilbert space are called the **non-stabilizer states** or **magic states**.

Please note that Gottesman-Knill theorem only says that stabilizer states can be efficiently simulated classically, but we have no idea about the non-stabilizer states. Maybe some of them can, or maybe all of them can (if P=NP=BQP is proved someday).

As we discussed above, the Clifford circuit cannot enable universal quantum computations. To achieve that, we must add some unitaries outside the Clifford group. Such kind of unitaries are called **magic gates**.

In this note, we introduce the T gate, which is defined as

$$T := \begin{bmatrix} 1 & 0 \\ 0 & e^{\pi/4} \end{bmatrix} \tag{42}$$

It is easy to verify that

$$TXT^\dagger = \frac{X+Y}{\sqrt{2}} \notin \mathcal{P}_n \tag{43}$$

thus it is not in the Clifford group. In addition, it can be proved that $\{H, \mathrm{CNOT}, S, T\}$ is a universal set of quantum computation. Therefore, theoretically, we can build a quantum computer composed of Clifford circuit and magic gates to achieve universal quantum computation.

Intuitively, to simulate a quantum state, more magic gates we need, more quantum it is. Roughly speaking, the amount of required magic gates for a quantum state is what we call the **non-stabilizerness** or **magic** of a state. Just like we quantify entanglement, we can also quantify magic. We will introduce some measures of magic in the next section.

3 Non-stabilizerness monotones

3.1 Stabilizer entropy

The stabilizer entropy (SE) is a magic measure proposed in [L. Lenone, S. Oliviero, and A. Hamma 2022], which has recently been proved to be a non-stabilizerness monotone for $\alpha \geq 2 \in \mathbf{Z}$ in [L. Leone and L. Bittel (2024)].

Consider $\tilde{P}_n := P_n/\langle \pm i\mathbf{1}\rangle$, a quotient group of the Pauli group, which includes the Pauli strings with phase factor 1. Since all $P \in \tilde{P}_n$ form a complete and orthogonal set of basis for expanding an arbitary pure state $\rho = |\psi\rangle\langle\psi|$, then we have

$$\rho = \frac{1}{2^n}\sum_P c_P P \tag{44}$$

with $c_P = \mathrm{Tr}(\rho P) = \langle\psi|P|\psi\rangle$. On another hand, the purity of ρ ensures $\mathrm{Tr}(\rho^2) = 1$, which means

$$\begin{aligned} &\mathrm{Tr}\left[\left(\frac{1}{2^n}\sum_P \langle\psi|P|\psi\rangle P\right)^2\right] \\ =&\frac{1}{2^{2n}}\sum_{P,Q}\langle\psi|P|\psi\rangle\langle\psi|Q|\psi\rangle\,\mathrm{Tr}(PQ) \\ =&\frac{1}{2^n}\sum_P \langle\psi|P|\psi\rangle^2 = 1 \end{aligned} \tag{45}$$

Eq. (45) is an interesting result because it enables us to interpret $\Xi_P(|\psi\rangle) := \langle\psi|P|\psi\rangle^2 \geq 0$ as some unnormalized probability distribution of P. Taking the α-Rényi entropy of $\Xi_P(|\psi\rangle)$, we define the stabilizer entropy as

$$M_\alpha(|\psi\rangle) := \frac{1}{1-\alpha}\log\left[\frac{1}{2^n}\sum_{P\in\tilde{\mathcal{P}}_n} \Xi_P^\alpha(|\psi\rangle)\right] \tag{46}$$

For the stabilizer state $|0\cdots0\rangle$, apparently, $\sum_P \Xi_P^\alpha(|\psi\rangle) = 2^n$, where only those P composed of I and Z survive. In addition, for any other stabilizer state $|\psi\rangle = C\,|0\cdots0\rangle$ with $C \in \mathcal{C}$, the normalizer property of $\mathcal{C}$ also ensures the summation to be 2^n as well. For the stabilizer states, the distribution of $\Xi_P(|\psi\rangle)$ is uniform for totally 2^n Pauli strings, thus maximizing the entropy. Therefore, the magic states, on another hand, will make the summation smaller than 2^n, resulting in $M_\alpha(|\psi\rangle) > 0$.

As a measure of non-stabilizerness, SE satisfies

- faithfulness: $M_\alpha(|\psi\rangle) = 0$ iff $|\psi\rangle \in$ STAB;
- stability: $\forall C \in \mathcal{C}$, $M_\alpha(|\psi\rangle) = M_\alpha(C\,|\psi\rangle)$ holds;
- additivity: $M_\alpha(|\psi\rangle \otimes |\phi\rangle) = M_\alpha(C\,|\psi\rangle) + M_\alpha(C\,|\phi\rangle)$.

3.2 Mana