Stabilizer formalism and fault-tolerant quantum computing

Othmane Benhayoune Khadraoui
othmane.benhayounkhadraoui@epfl.ch

Physics Department
Ecole polytechnique federale de Lausanne

January 19, 2022

Overview of the presentation

Stabilizer formalism

- Gottesman-Knill theorem
- Stabilizer codes
- The repetition code as an example

Fault Tolerant quantum computing

- Threshold theorem
- Fault tolerant implementation of an universal set of gates in a stabilizer code?

Stabilizer formalism

For any subgroup $\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle \subset \mathcal{P}_n$, one can define the vector space $\mathcal{T}(\mathcal{S})$ as the space stabilized by S :

$$\mathcal{T}(\mathcal{S}) = \{|\psi\rangle \mid g\,|\psi\rangle = |\psi\rangle\, \forall g \in \mathcal{S}\}$$

There are three possibilities :

1. $-\mathcal{I} \in \mathcal{S}$ then $\mathcal{T}(\mathcal{S}) = \{0\}$.
2. S is not abelian then $\mathcal{T}(\mathcal{S}) = \{0\}$.
3. $-\mathcal{I} \notin \mathcal{S}$ and S is abelian then $\dim(\mathcal{T}(\mathcal{S})) = 2^k$.

Stabilizer formalism

The first non trivial example :

$$\mathcal{T}(\mathcal{S}) = \text{Span}\{|\psi\rangle\}$$

Up to a global phase, there is a one a one correspondence between $\mathcal{S} = \langle g_1, g_2, \ldots, g_n \rangle$ and $|\psi\rangle$.
Then there are two possible way that could change the generators as the state evolves in a quantum circuit :

1. Unitary gate : if $|\psi\rangle$ is stabilized by $\langle g_1, \ldots, g_n \rangle$. Then $U|\psi\rangle$ is stabilized by $\langle U g_1 U^\dagger, \ldots, U g_n U^\dagger \rangle$.
   Particular case : if U is an elementary Clifford gate $\in \{H, S, \text{C-NOT}\}$. Then it takes only $\mathcal{O}(n^2)$ to simulate classically this quantum gate.
2. Measurement of some observable M $\in \mathcal{P}_n$: Two possibilities
   - $[M, g_i] = 0 \ \forall i \Rightarrow$ The stabilizer does not change.
   - $[M, g_1] \neq 0 \Rightarrow$ The stabilizer became $\langle \pm g_1, \ldots, g_n \rangle$

Stabilizer formalism

Gottesman-Knill theorem : If a quantum computation is performed by involving only :

- State preparation in the computational basis
- Clifford gates
- Measurement of observables in the Pauli group
- Classical control conditioned on the outcome of such measurements

$\Rightarrow$ Such computation may be efficiently simulated on a (probabilistic) classical computer.

Stabilizer formalism

The second non trivial case is when $\dim(\mathcal{T}(\mathcal{S})) = 2^k$ with $k \geq 1$.
$\rightarrow$ This defines a [n,k] stabilizer code $\mathcal{T}(\mathcal{S})$.
Classification of errors : For E $\in \mathcal{P}_n$, there are three possibilities:

1. E $\in \mathcal{S} \iff \forall \left|\psi\right\rangle \in \mathcal{T}(\mathcal{S}) \quad E\left|\psi\right\rangle = \left|\psi\right\rangle \rightarrow$ E does not corrupt the code space at all.
2. E $\notin \mathcal{S}$ and $\exists g \in \mathcal{S}$ such that $\{E, g\} = 0 \rightarrow$ E takes the code space to an orthogonal subspace. Therefore, the error can be detected and corrected.
3. E $\notin \mathcal{S}$ and $\forall g \in \mathcal{S} \quad [E, g] = 0 \rightarrow \forall \left|\psi\right\rangle \in \mathcal{T}(\mathcal{S}) \; E\left|\psi\right\rangle \in \mathcal{T}(\mathcal{S})$ $\rightarrow$ Unitary operations on the code space

Stabilizer formalism

This motivates the definition of the normalizer of $\mathcal{S}$

$$\mathcal{N}(\mathcal{S}) = \{E \in \mathcal{P}_n \mid \forall g \in \mathcal{S} \;\; [E, g] = 0\}$$

According to our previous analysis, errors that are not correctable are element of $\mathcal{N}(\mathcal{S}) - \mathcal{S}$. Moreover, the coset group $\mathcal{N}(\mathcal{S})/\mathcal{S} \simeq \mathcal{P}_k$.

Knill-Laflamme conditions for stabilizer codes : If $\mathcal{T}(\mathcal{S})$ is a stabilizer code and $\{E_r\}$ a set of errors in $\mathcal{P}_n$ such that $E_r^\dagger E_s \notin \mathcal{N}(\mathcal{S}) - \mathcal{S} \Rightarrow \{E_r\}$ is a correctable set of errors for the code $\mathcal{T}(\mathcal{S})$.

Stabilizer formalism

Correcting the errors : If an error $E_j \in \mathcal{P}_n$ occurs, Then
$\{g_1, \ldots, g_{n-k}\} \rightarrow \left\{E_j g_1 E_j^\dagger, \ldots, E_j g_{n-k} E_j^\dagger\right\}$

1. Error-detection is performed by measuring $\{g_1, \ldots, g_{n-k}\}$ to obtain the error syndrome $\{\beta_1, \ldots, \beta_{n-k}\}$
2. Recovery is achieved by applying the right operator :
   - If E_j is the only error having this syndrome $\rightarrow$ apply $E_j^\dagger$
   - If there are $E_j \neq E_{j'}$ giving the same error syndromes $\rightarrow E_j^\dagger E_{j'} \in \mathcal{S}$

Summary : Measure the generators $\{g_1, \ldots, g_{n-k}\}$
$\rightarrow$ obtain the error syndromes $\{\beta_1, \ldots, \beta_{n-k}\}$
$\rightarrow$ identify E_j
$\rightarrow$ apply $E_j^\dagger$ to recover

Stabilizer formalism

Repetition code : Encoding k=1 qubit in n=3 physical qubits with stabilizer $\mathcal{S} = \langle Z_1 Z_2, Z_2 Z_3 \rangle \rightarrow \mathcal{T}(\mathcal{S}) = \text{Span}\left\{ |000\rangle, |111\rangle \right\}$. The error set $\{I, X_1, X_2, X_3\}$ is correctable thanks to Knill-Laflamme conditions since the set of all possible product $\{I, X_1, X_2, X_3, X_1X_2, X_1X_3, X_2X_3\} \notin \mathcal{N}(\mathcal{S}) - \mathcal{S}$.

Stabilizer formalism

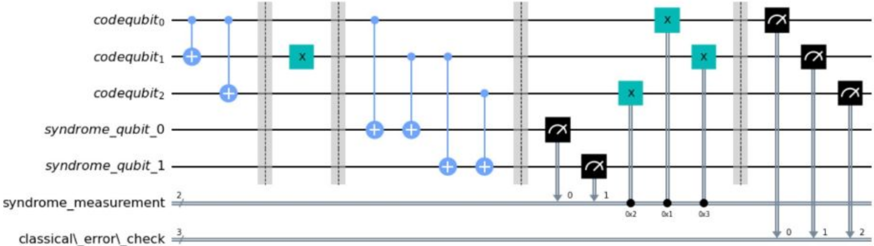

Figure: Correcting 1 bit flip with repetition code

Stabilizer formalism

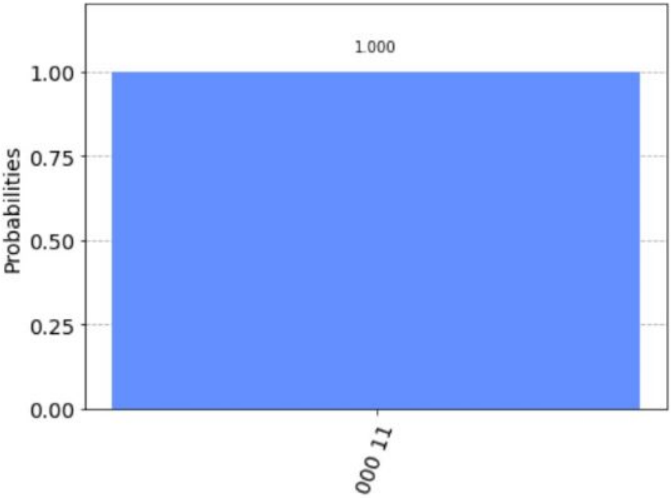

Figure: Correcting 1 bit flip with repetition code

Stabilizer formalism

However, if we add two bit flip to our set of errors $\{I, X_1, X_2, X_3, X_1X_2, X_1X_3, X_2X_3\}$, it is non longer correctable since $X_{log} = X_1X_2X_3 \in \mathcal{N}(\mathcal{S}) - \mathcal{S}$.
In order to correct two bit flip error, we concatenate our repetition code:
$\rightarrow \mathcal{S} = \langle Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9, Z_1Z_4, Z_4Z_7 \rangle$
$\rightarrow \mathcal{T}(\mathcal{S}) = \text{Span}\left\{ |0\rangle^{\otimes 9}, |1\rangle^{\otimes 9} \right\}$
One can easily check that the set of errors $\{I, X_i, X_iX_j, X_iX_jX_k, X_{i_1}X_{j_1}X_{k_2}X_{l_3}, X_{i_1}X_{j_1}X_{k_1}X_{l_2}X_{m_3}\} \notin \mathcal{N}(\mathcal{S}) - \mathcal{S}$.
$\rightarrow$ can be corrected thanks to the concatenation procedure.

Example: $|000\,000\,000\rangle \xrightarrow{X_1X_2X_3X_4X_7} |111\,100\,100\rangle$

$$\xrightarrow{MR/block} |111\,000\,000\rangle$$

$$\xrightarrow{MR-blocks} |000\,000\,000\rangle$$

Stabilizer formalism

The concatenation procedure is efficient if the probability of logical bit flip is reduced.
In other words :

$$p_k < p_{k-1} < \ldots < p_1 < p_0 \equiv p$$

With p_k : the probability of a logical bit flip after k concatenation.
p : the probability of a physical bit flip.

Repetition code : $p_1 = 3p^2(1-p) + p^3$
$p_2 = 3p_1^2(1-p_1) + p_1^3$

Therefore,

$$p_2 < p_1 < p \iff p < \frac{1}{2}$$

Fault tolerant quantum computing &Threshold theorem

Threshold theorem for quantum computation:
A quantum circuit containing $p(n)$ gates may be simulated with probability of error at most ϵ using only $\mathcal{O}(\text{poly}\log\left(\frac{p(n)}{\epsilon}\right)p(n))$ gates provided that the probability of physical error p is below some constant threshold $p < p_{th}$.

Idea: Concatenating our codes multiple times and performing *fault-tolerant* operations on encoded states.

Fault tolerant quantum computing &Threshold theorem

$\rightarrow$ Can we implement a universal set of logical operations on encoded quantum states in *fault-tolerant* manner?

Clifford gates: Any logical Clifford gate on encoded states can be implemented transversely in a stabilizer code.

Proof: if $\mathcal{T}(\mathcal{S})$ is a stabilizer code with stabilizer $\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle$, then the action of a logical Clifford gate U is : $g = \sigma_{j_1} \otimes \ldots \otimes \sigma_{j_n} \rightarrow UgU^\dagger = \sigma_{i_1} \otimes \ldots \otimes \sigma_{i_n}$.
Then if one write $U = \otimes U_\alpha$. One should expect to solve the equation : $U_\alpha \sigma_{j_\alpha} U_\alpha = \sigma_{i_\alpha} \rightarrow U_\alpha \in \{H, S, X, Y, Z\}$

Eastin-Knill Theorem: No quantum error correcting code can transversely implement a universal set of unitary gates.

$\rightarrow$ Logical T gate, and Toffoli gate can not be implemented transversely.

$\rightarrow$ But still can be implemented in a fault-tolerant way if one can prepare fault-tolerantly the state $|\Theta\rangle = \frac{1}{\sqrt{2}}(|0_L\rangle + e^{i\frac{\pi}{4}} |1_L\rangle$