Stabilizer Formalism

Marco Armenta - AlgoLab

Université de Sherbrooke

Groups

A group is a (non-empty) set G together with a function $\star : G \times G \to G$ such that

1. $a \star (b \star c) = (a \star b) \star c \quad \forall\, a, b, c \in G$
2. $\exists e \in G$ such that $e \star a = a \star e = a \quad \forall\, a \in G$
3. $\forall a \in G \;\; \exists a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e \quad \forall\, a \in G$

Examples:

1. $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ with addition.
2. $GL_{\mathbb{C}}(n) = \{n \times n$ invertible matrices$\}$ with matrix product.
3. $\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$ with matrix product.
4. $\mathcal{P}_n = \{P_1 \otimes \cdots \otimes P_n : P_j \in \mathcal{P}_1\}$ with matrix product.

Groups

Let G be a group. A non-empty subset $S \subset G$ is a subgroup if

1. $x \in S \Rightarrow x^{-1} \in S$.
2. $x, y \in S \Rightarrow xy \in S$.

Let G be a group and fix $a \in G$. The subgroup of G generated by a is $< a >= \{a^n : n \in \mathbb{Z}\}$

Let $S \subset G$. A word on S is an element $w \in G$ of the form

$$w = x_1^{e_1} \cdots x_n^{e_n}$$

such that $x_i \in S,\ e_i \in \{+1, -1\},\ n \geq 1$

Theorem: Let $S \subset G$. If S is empty, then $< S >= \{e\}$. If S is not empty, then $< S >= \{\text{words on } S\}$

Groups

A group action $G \curvearrowright X$ of a group G on a non-empty set X is a function $G \times X \to X$ denoted by $(g, x) \mapsto g \cdot x$ such that

1. $e \cdot x = x \ \forall x \in X$
2. $g \cdot (h \cdot x) = (gh) \cdot x \ \forall x \in X$ and $\forall g, h \in G$

Example:

$$\mathcal{P}_n \curvearrowright \mathcal{H}^n$$

Let $G \curvearrowright X$ and fix $x \in X$. The stabilizer of x is defined as

$$G_x = Stab(x) = \{g \in G : g \cdot x = x\}$$

Example:

Consider the Bell pair $|\psi\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$. We have that $X_1 X_2, Z_1 Z_2 \in (\mathcal{P}_2)_{|\psi\rangle}$

Stabilizers

Let S be a subgroup of $\mathcal{P}_n$ with an action $S \curvearrowright \mathcal{H}^n$. We denote the sub vector space stabilized by S by

$$V_S = \{|\psi\rangle \in \mathcal{H}^n : \boxed{P|\psi\rangle = |\psi\rangle} \ \forall P \in S\} \qquad Stab(|\psi\rangle) = \{P \in \mathcal{P}_n : \boxed{P|\psi\rangle = |\psi\rangle}\}$$

Note that $Stab(V_S) = S$ and $V_S \subset \mathcal{H}^n$ is a sub vector space.

Example

Consider the action $\mathcal{P}_3 \curvearrowright \mathcal{H}^3$, and take the subgroup $S =< Z_1Z_2, Z_2Z_3 >= \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$

$$V_{Z_1Z_2} = span\{|000\rangle, |001\rangle, |110\rangle, |111\rangle\}$$

$$V_{Z_2Z_3} = span\{|000\rangle, |011\rangle, |100\rangle, |111\rangle\} \quad \Longrightarrow \quad V_S = span\{|000\rangle, |111\rangle\}$$

$$V_{Z_1Z_3} = span\{|000\rangle, |010\rangle, |101\rangle, |111\rangle\}$$

$$V_I = \mathcal{H}^3$$

Stabilizers

Consider the subgroup $H = \{\pm I, \pm X\} \subset \mathcal{P}_1$. We have that

Non-physical!!!

$$-I|\psi\rangle = |\psi\rangle \quad \Rightarrow \quad |\psi\rangle = 0 \quad \Rightarrow \quad V_H = \{0\}$$

We want subgroups $S \subset \mathcal{P}_n$ such that $V_S \neq \{0\}$

Proposition: $-I \notin S \;\Rightarrow\; \pm iI \notin S$

Any two elements of the Pauli group $M, N \in \mathcal{P}_n$ either commute or ~~anticommute~~.

Assume for the moment that $MN = -NM$ and $V_S \neq \{0\}$ and take $|\psi\rangle \in V_S$ such that $|\psi\rangle \neq 0$

$$|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = -|\psi\rangle$$

Therefore, if we want $V_S \neq \{0\}$ we must have that

1. $-I \notin S$
2. $MN = NM \; \forall M, N \in S$ (S is commutative/Abelian)

Stabilizers

Therefore, if we want $V_S \neq \{0\}$ we must have that

1. $-I \notin S$
2. $MN = NM \; \forall M, N \in S$ (S is commutative/Abelian)

Proposition: Let $S =< g_1, \cdots, g_k >$ be a subgroup of $\mathcal{P}_n$. Then

$$S \text{ is abelian } \Leftrightarrow g_i g_j = g_j g_i \quad \forall i, j$$

Moreover, if $-I \notin S$ then $g^2 = I \quad \forall g \in S$

The whole reason for efficient simulation

Now, we define a function $\boxed{r : \mathcal{P}_n \rightarrow \mathbb{Z}_2^{2n}}$ that assigns to an element of the Pauli group its $ZX-$factors

Forget coefficient

X Z

$$r(X_1X_2X_3) = (1,1,1,0,0,0)$$

$$r(-iY_1Z_3) = (1,0,0,1,0,1)$$

$$r(-X_1Y_2) = (1,1,0,1)$$

$$< Z_1Z_2, Z_2Z_3 >= \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$$

$r(I)$	0 0 0 0 0 0
$r(Z_1Z_2)$	0 0 0 1 1 0
$r(Z_2Z_3)$	0 0 0 0 1 1 $+$
$r(Z_1Z_3)$	0 0 0 1 0 1 $=$

For simulation, use 2 bits to save the coefficient

Stabilizers

Proposition: Let $\mathbb{I}_n$ be the $n \times n$ identity matrix and denote $\Lambda = \begin{pmatrix} 0_n & \mathbb{I}_n \\ \mathbb{I}_n & 0_n \end{pmatrix}$. Let $g, g' \in \mathcal{P}_n$, then

$$gg' = g'g \quad \Leftrightarrow \quad \boxed{r(g)\Lambda r(g')^T} = 0$$

Symplectic form

Moreover, $\boxed{r : \mathcal{P}_n \to \mathbb{Z}_2^{2n}}$ is an epimorphism of groups and $ker(r) = \{\pm I^{\otimes n}, \pm i I^{\otimes n}\}$

We say that the generators $g_1, \cdots, g_k$ of a subgroup $S =< g_1, \cdots, g_n >$ of $\mathcal{P}_n$ are independent

Definition

if the vectors $r(g_1), \cdots, r(g_k)$ are linearly independent.

Proposition: If $-I \notin S =< g_1, \cdots, g_k >$ and the generators are independent, then for any j

the subgroup $< g_1, \cdots, \hat{g}_j, \cdots, g_k >$ is strictly smaller than S.

Stabilizers

Theorem: Let $S =< g_1, \cdots, g_{n-k} >$ be an abelian subgroup of $\mathcal{P}_n$ with independent generators and $-I \notin S$. Then $dim_{\mathbb{C}} V_S = 2^k$

$$X_1 X_2 Z_1 Z_2 = Z_1 Z_2 X_1 X_2$$

Example:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad \mathcal{P}_2 \curvearrowright \mathcal{H}^2 \qquad S = Stab(|\psi\rangle) =< X_1 X_2, Z_1 Z_2 >$$

r

$$(0, 0, 1, 1)$$

$$(1, 1, 0, 0)$$

$$k = 0$$

$$\Rightarrow \quad dim_{\mathbb{C}}(V_S) = 1$$

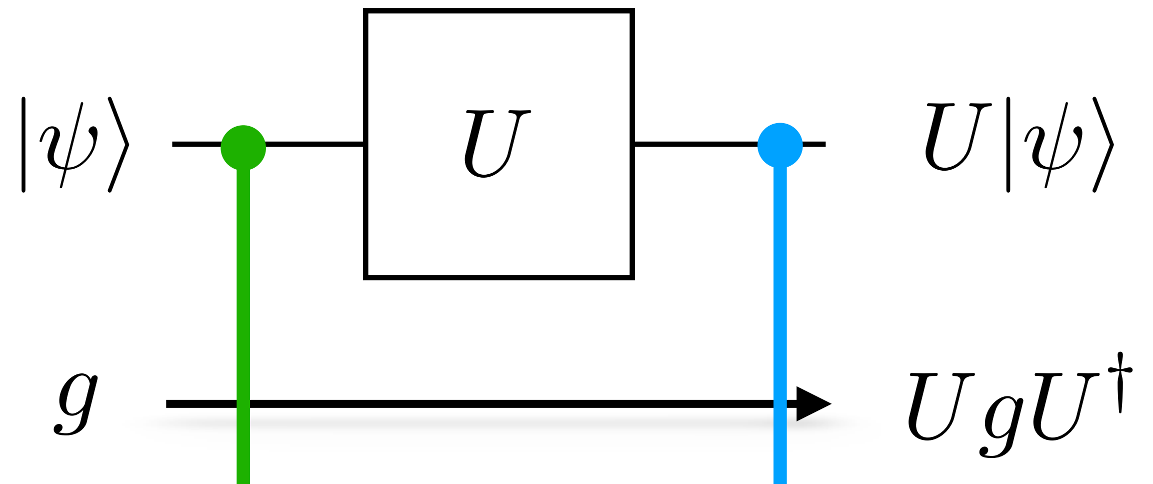
We know the state up to a global phase!

Evolution

Let $S =< g_1, \cdots, g_{n-k} >$ be an abelian subgroup of the Pauli group $\mathcal{P}_n$ with independent generators such that $-I \notin S$ and let $|\psi\rangle \in V_S - 0$. Let U be a unitary on n-qubits. Let $g \in S$. Then

$$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger U|\psi\rangle \qquad U|\psi\rangle = \left(UgU^\dagger\right)U|\psi\rangle$$

This means that the state $U|\psi\rangle$ is stabilized by $UgU^\dagger$



Just like density matrices!

Proposition: The vector space $UV_S = \{U|\psi\rangle : |\psi\rangle \in V_S\}$ is stabilized by the group $USU^\dagger = \{UgU^\dagger : g \in S\}$

In this case, $USU^\dagger =< Ug_jU^\dagger : j = 1, \cdots, n-k >$

$$< g_1, \cdots, g_{n-k} > \longrightarrow < Ug_1U^\dagger, \cdots, Ug_{n-k}U^\dagger >$$

Evolution

Example: $|0\rangle^{\otimes n}$ —$\boxed{H^{\otimes n}}$— $\frac{1}{2^n}\sum_{j=0}^{2^n-1}|j\rangle$

$HZH^\dagger = X$

$$< Z_1, \cdots, Z_n > \longrightarrow < X_1, \cdots, X_n >$$

EXTREMELY IMPORTANT: $dim_{\mathbb{C}}(V_S) = 1$ Same number of generators as qubits

So we know the state up to a global phase from the stabilizers

Yeah, sure…. But what about entanglement?

We do a little bit more algebra!

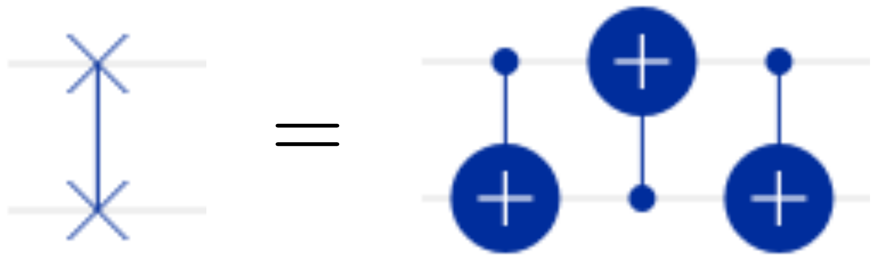
Evolution

Let U be the CNOT gate controlled by qubit 0 and target qubit 1. Then

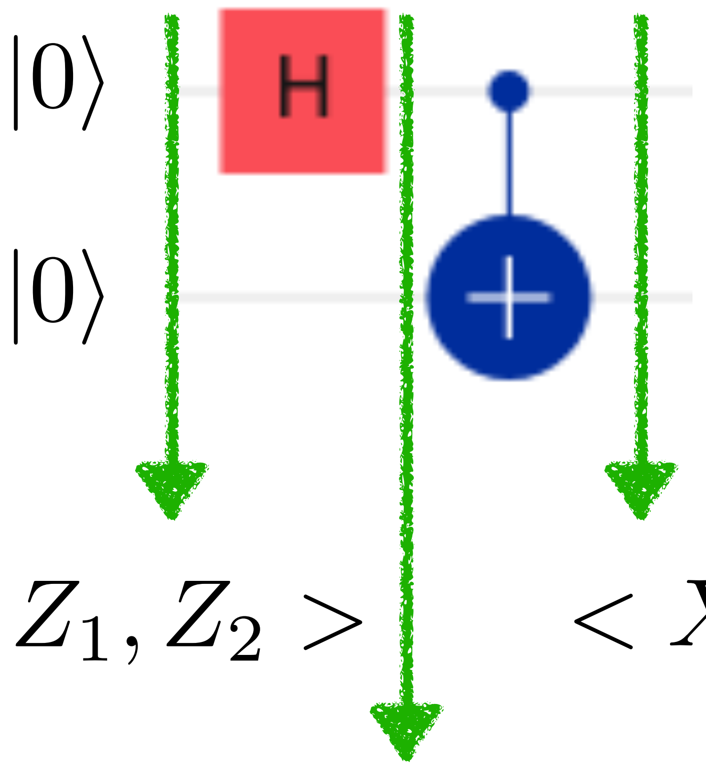
$$UX_1U^\dagger = X_1X_2$$
$$UX_2U^\dagger = X_2$$
$$UZ_1U^\dagger = Z_1$$
$$UZ_2U^\dagger = Z_1Z_2$$

And this is enough because $\mathcal{P}_n =< X_1, \cdots, X_n, Z_1, \cdots, Z_n >$

$$UY_2U^\dagger = iUX_2Z_2U^\dagger = iUX_2U^\dagger UZ_2U^\dagger = iX_2Z_1Z_2 = Z_1Y_2$$



Example:



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

$< Z_1, Z_2 >$

$< X_1, Z_2 >$

$< X_1X_2, Z_1Z_2 >$

Limitations

It is all about group theory

Let G be a group and H a subgroup of G. The normalizer of H on G is

$$N_G(H) = \{U \in G : UHU^\dagger = H\}$$

Clifford group

Examples:

$$N_{U(2^n)}(\mathcal{P}_n) \;=\; \{U \in U(2^n) : U\mathcal{P}_nU^\dagger = \mathcal{P}_n\} \;= < H_i, CX(i,j), S_i : 1 \leq i \neq j \leq n >$$

Let U denote the Toffoli gate controlled by qubits 0 and 1 and target qubit 2. Let $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$

$$UZ_1U^\dagger = Z_1$$

$$UX_3U^\dagger = X_3$$

$$UX_2U^\dagger = X_2 \otimes \frac{I + Z_2 + X_3 - Z_2X_3}{2}$$

$$U \notin N_{U(2^n)}(\mathcal{P}_n)$$

$$TZT^\dagger = Z$$

$$TXT^\dagger = \frac{X+Y}{\sqrt{2}}$$

$$T \notin N_{U(2^n)}(\mathcal{P}_n)$$

Measurements

Assume, without loss of generality, that we measure only in the computational basis.

Let $g \in \mathcal{P}_n$ and assume for the moment that it does not have factors $\boxed{-1, \pm i.}$

Suppose that the system is in state $|\psi\rangle$ with stabilizer group $S =< g_1, \cdots, g_n >$.

We have two possibilities.

$\boxed{dim_{\mathbb{C}}(V_S) = 1}$

1. $[g, g_j] = 0 \;\forall j$

   We get that $g \in S$ because $g_j g|\psi\rangle = gg_j|\psi\rangle = g|\psi\rangle$, which gives that $\underline{g|\psi\rangle \in V_S \text{ is a multiple of } |\psi\rangle}$

   We also know that $\underline{g^2 = I}$ so $\underline{g|\psi\rangle = \pm|\psi\rangle}$. If $\boxed{g \in S,}$ the measurement of g gives $+1$ with probability 1 and the measurement does not change the state. Trick: $g = +\dfrac{I+g}{2} - \dfrac{I-g}{2}$

   If $\boxed{-g \in S}$ then $-g|\psi\rangle = |\psi\rangle$ and the measurement of $-g$ gives $+1$ with probability 1

   Therefore, measuring g does NOT change the state and it leaves the same stabilizers.

Measurements

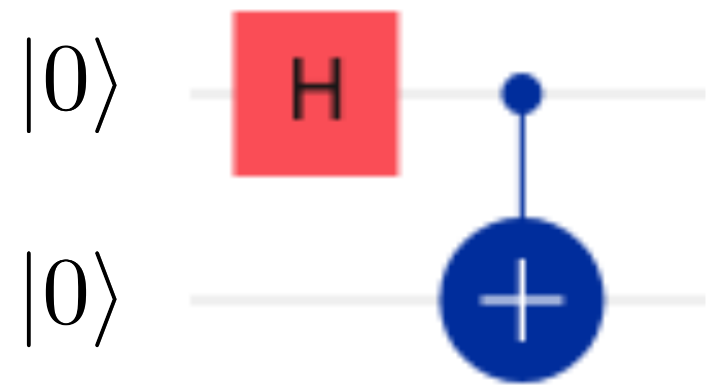
2. $\{g, g_j\} = 0$ for at least one j.

$$
\begin{aligned}
\mathbb{P}_{|\psi\rangle}(\pm 1) &= Tr\left(\frac{I \pm g}{2}|\psi\rangle\langle\psi|\right) \\
&= Tr\left(\frac{I \pm g}{2} g_j |\psi\rangle\langle\psi|\right) && g_j \in S \\
&= Tr\left(g_j \frac{I \mp g}{2}|\psi\rangle\langle\psi|\right) && \{g, g_j\} = 0 \\
&= Tr\left(\frac{I \mp g}{2}|\psi\rangle\langle\psi| g_j\right) && \text{Trace is cyclic} \\
&= Tr\left(\frac{I \mp g}{2}|\psi\rangle\langle\psi|\right) && g_j^\dagger = g_j \in S \\
&= \frac{1}{2}
\end{aligned}
$$

If we measure +1, the state changes to $|\psi^+\rangle \propto P^+|\psi\rangle$
whose stabilizer group is $< g_1, \cdots, g_{j-1}, g, g_{j+1}, \cdots, g_n >$

If we measure -1, the state changes to $|\psi^-\rangle \propto P^-|\psi\rangle$
whose stabilizer group is $< g_1, \cdots, g_{j-1}, -g, g_{j+1} \cdots, g_n >$

Measurements

Example: 

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad < X_1X_2, Z_1Z_2 >$$

Measure Z_1Z_2 :

Gives $+1$ with probability 1 and the state and stabilizers remain the same.

Measure Z_1 :

Gives $\pm$ 1 with probability $1/2$ each. If the measurement gives $+1$, the state changes to $|\psi^+\rangle$

and the stabilizer group changes to $< Z_1, Z_1Z_2 > =< Z_1, Z_2 >$

If the measurement gives -1, the state changes to $|\psi^-\rangle$ and the stabilizer group changes to

$< -Z_1, Z_1Z_2 >=< -Z_1, -Z_2 >$

Gottesman-Knill Theorem

Theorem: Assume a quantum computation is performed that uses only

1.- State preparation in the computational basis.

2.- $H_j, S_j, CX(i,j), P \in \mathcal{P}_n \; \forall 0 \leq i \neq j \leq n-1$

3.- Measurement of any $P \in \mathcal{P}_n$.

4.- Classical control conditioned on the results of these measurements.

Such a quantum computation is efficiently simulable on a classical computer.

Proof: Follow the stabilizers.

Implementations

https://github.com/MarcoArmenta/info_quantique_theorique