Formalisme des stabilisateurs (Stabilizer formalism)

Léo Gagnon

July 7, 2021

Université de Montréal

Motivation et ordre du jour

Objectif :
Développer un nouveau langage pour parler de la correction d'erreur quantique et reformuler ce qu'on sait dans ce langage.

Comment on va faire ca? :
Utilisation astucieuse de la théorie des groupes.

Corolaires :

- Simulation classique efficace de certains calculs quantiques
- Calcul quantique résistant aux erreurs
- Description compacte des états utilisés dans le calcul quantique basé sur la mesure
- ...

Groupe de Pauli et éléments de théorie des groupes

Rappel : Groupe

Un groupe est un ensemble, G, muni d'une opération $\star$ ayant comme domaine $G \times G$. Pour être un groupe, les propriétés suivantes doivent être respectées pour tout $g, h \in G$:

1. $g \star h \in G$ (fermé)
2. $a \star (b \star c) = (a \star b) \star c$ (associatif)
3. $\exists e \in G$ tel que $e \star g = g \star e = g$ (neutre)
4. $\exists g^{-1} \in G$ tel que $g^{-1} \star g = g \star g^{-1} = e$ (inverse)

Groupe de Pauli : Définition

Le groupe de Pauli sur un seul qubit est

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

avec comme opération la multiplication de matrice.

On peux ensuite définir le groupe de pauli sur n qubits

$$G_n = G^{\otimes n}$$

Groupe de Pauli : Propriétés

Le groupe de Pauli a les propriétés suivantes :

1. $G_n \subseteq U_n$
2. Pour tout $M \in G_n$, $M^2 = \pm I$.
3. N'importe quels deux éléments $N, M \in G_n$ commutent ou anti-commutent : $NM = \pm MN$.
4. Pour tout $M \in G_n$, $\lambda(M) = \{+1, -1\}$
5. Pour tout $M \in G_n \setminus \{I^{\otimes n}\}$, $\mathrm{tr}(M) = 0$

Rappel : Action de groupe

Une action d'un groupe G sur un ensemble X est une application

$$G \times X \to X$$
$$(g, x) \mapsto g \circ x$$

telle que

- $\forall x \in X, \quad \mathit{id} \circ x = x$
- $\forall g, h \in G, \forall x \in X, \quad gh \circ x = g \circ (h \circ x)$

Groupe de Pauli : Action sur $\mathbb{C}^{2^n}$

Le groupe de Pauli G_n agit sur $\mathbb{C}^{2^n}$ de la façon suivante :

Pour $M \in G_n$ et $|\psi\rangle \in \mathbb{C}^{2^n}$

$$M \circ |\psi\rangle = M |\psi\rangle$$

On a bien

- $I \circ |\psi\rangle = I |\psi\rangle = |\psi\rangle$
- $MN \circ |\psi\rangle = MN |\psi\rangle = M \circ (N \circ |\psi\rangle)$

Rappel : Stabilisateurs

Soit G un groupe agissant sur un ensemble X.

On dit que $g \in G$ stabilise $x \in X$ ssi

$$g \circ x = x$$

On dit que $S \leq G$ stabilise $V_S \subseteq X$ ssi

$$(\forall x \in V_S)(\forall g \in S)[g \circ x = x]$$

.

Groupe de Pauli : Stabilisateurs

Une opération $M \in G_n$ stabilise $|\psi\rangle \in \mathbb{C}^{2^n}$ ssi

$$M |\psi\rangle = |\psi\rangle$$

Soit $S \leq G_n$ un sous-groupe de G_n, alors $V_S \subseteq \mathbb{C}^{2^n}$ est le sous-espace vectoriel stabilisé par S.

Si $S = \langle M_1, \ldots, M_k \rangle$ est généré par k matrices indépendantes, notons

$$V_i = \{|\psi\rangle \in \mathbb{C}^{2^n} \mid M_i |\psi\rangle = |\psi\rangle\}$$

.

Alors

$$V_S = \bigcap_{i \in [k]} V_i$$

Exemple de stabilisateur

Exemple

Si

$$S = \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\} = \langle Z_1Z_2, Z_2Z_3 \rangle \leq G_3$$

alors

$$V_1 = \mathsf{Vect}\{|001\rangle, |000\rangle, |110\rangle, |111\rangle\}$$
$$V_2 = \mathsf{Vect}\{|100\rangle, |000\rangle, |011\rangle, |111\rangle\}$$
$$V_S = \mathsf{Vect}\{|000\rangle, |111\rangle\}$$

Description d'un sous-espace de $\mathbb{C}^{2^n}$

Propriétés nécéssaires du stabilisateur

Remarque

Le sous-groupe S doit avoir les propriétés suivantes pour que V_S soit non-trivial :

1. S est abélien
2. $-I \notin S$

Propriétés nécéssaires du stabilisateur

Remarque

Le sous-groupe S doit avoir les propriétés suivantes pour que V_S soit non-trivial :

1. S est abélien
2. $-I \notin S$

Preuve

1. Si $\exists M, N \in S$ tels que $MN = -NM$, alors
   $|\psi\rangle = MN\,|\psi\rangle = -NM\,|\psi\rangle = -\,|\psi\rangle$
2. Si $-I \in S$, alors $|\psi\rangle = -I\,|\psi\rangle = -\,|\psi\rangle$

Dimension du sous-espace stabilisé

Théorème

Soit $S = \langle M_1, \ldots, M_{n-k} \rangle \leq G_n$ abélien généré par $n-k$ éléments independents, et tel que $-I \notin S$. Alors $V_S \subseteq \mathbb{C}^{2^n}$ est un sous-espace vectoriel de dimension 2^k

Dimension du sous-espace stabilisé

Preuve

Premièrement, $M_i \neq I^{\otimes n}$ puisque sinon $V_S = \mathbb{C}^{2^n}$.
Définissons $P_1 = \frac{1}{2}(I + M_1)$ le projecteur sur V_1. P_1 a donc seulement des valeurs propres $+1$ et

$$\dim(V_1) = \mathrm{tr}(P_1) = \frac{1}{2}\,\mathrm{tr}(\mathbb{I}) = 2^{n-1}$$

Ensuite, soit $P_{1,2} = \frac{1}{2^2}(I + M_2)(I + M_1)$ le projecteur sur $V_1 \cap V_2$. Puisque $P_{1,2}$ a seulement des valeurs propres $+1$, alors

$$\dim(V_1 \cap V_2) = \mathrm{tr}(P_{1,2}) = \frac{1}{2^2}\,\mathrm{tr}(\mathbb{I}) = 2^{n-2}$$

On peux appliquer ce raisonnement inductivement pour arriver au résultat.

Corol(l)aire

Il faut un sous-groupe stabilisateur de dimension n pour représenter un n-qubit.

Application d'opérations unitaires

Application d'opérations unitaires

Considérons un sous-espace vectoriel V_S stabilisé par $S \leq G_n$ et une opération unitaire U. Alors pour tout $M \in S$ on a

$$U|\psi\rangle = UM|\psi\rangle = UMU^*U|\psi\rangle$$

et donc $U|\psi\rangle$ est stabilisé par UMU^*.

L'espace UV_S est donc stabilisé par le sous-groupe

$$USU^* = \{UMU^* : M \in S\} = \langle UM_1U^*, \ldots, UM_{n-k}U^* \rangle$$

Application d'opérations unitaires

Pour que la description du sous-espace après l'application d'un opération unitaire U soit pratique et compacte on voudrait que $UM_iU^* \in G_n$ pour tout i.

Dans le language de la théorie des groupes, l'ensemble des tels U est le *normalisateur* de G_n :

$$N(G_n) = \{U : UG_nU^* = G_n\}$$

Normalisateur de G_n

Le normalisateur de G_n (souvent appelé groupe de Clifford) est

$$N(G_n) = \langle CNOT, H, S \rangle = \langle CNOT, H, \sqrt{Z} \rangle$$

Exemples

- $HXH^* = Z$
- $CNOT(X_1 \otimes I)CNOT^* = X_1X_2$
- $SXS^* = Y$

Mesure du système quantique

Mesure par un opérateur de Pauli

Supposons qu'on mesure un n-qubit décrit par $S = \langle M_1, \ldots, M_n \rangle$ avec un opérateur de Pauli $g \in G_n$ (mesure projective sur les espaces propres ± 1 de g).

Cas 1 : $g \in C(S)$:

Puisque g commutent avec tout les M_i, alors il partage les mêmes vecteurs propres que les M_i. Ainsi, la mesure n'affecte pas l'état.

Cas 2 : $g \notin C(S)$:

On peux montrer que chacun des résultats a probabilité $\frac{1}{2}$. L'état résultant est

$$\left|\psi^{(\pm)}\right\rangle = \frac{I \pm g}{\sqrt{2}} |\psi\rangle$$

Simulation classique

Remarque : Simulation classique

La description d'un système quantique à n qubits est très compacte si on le représente avec son sous-groupe stabilisateur (provenant de G_n).

Soit un n-qubit $|\psi\rangle \in \mathbb{C}^{2^n}$ représenté avec n générateurs $M_i \in G_n$ qui forment le sous-groupe stabilisateur. La description de chaque M_i nécéssaire $2n+1$ bits : 2 pour chaque matrice de Pauli et 1 pour le signe. Ainsi, on peux représenter un tel système avec $n(2n+1) = O(n^2)$ bits.

Si l'évolution du système se fait seulement avec des portes de Clifford, alors l'évolution également peux être simulé efficacement : on doit seulement actualiser les n générateurs.

Théorème de Gottesman-Knill

Théorème

Tout calcul quantique constitué seulement d'une préparation dans la base de calcul, d'opérations tirées du groupe de Clifford et d'une mesure par un observable de G_n peux être simulé efficacement par un ordinateur classique.

Codes stabilisateurs

Code stabilisateurs

Définition

Un $[n, k]$-code stabilisateur est défini commme étant le sous-espace vectoriel V_S stabilisé par un sous-groupe abélien $S = \langle M_1, \ldots, M_{n-k} \rangle \leq G_n$ d'ordre $n - k$ tel que $-I \notin S$.

Code stabilisateurs : effet des erreurs

On se rappelle qu'une erreur arbitraire E_a peux être décomposé en éléments du groupe de Pauli (I, X, Z et Y). Ainsi, pour tout M_i,

$$E_a M_i E_a^* = \pm M_i$$

En particulier, le stabilisateur M_i devient

1. M_i si E_a commute avec M_i.
2. $-M_i$ si E_a anti-commute avec M_i.

Dans le deuxième cas, une mesure des espaces propres ± 1 de M_i aura comme résultat -1 avec probabilité 100% donc l'erreur est détectable.

Code stabilisateurs : détection des erreurs

Dans un code stabilisateur, la détection des erreurs est effectuée en mesurant les générateurs du stabilisateur $M_1, \ldots, M_{n-k}$ (mesure projective sur les espaces propres ± 1) :

- Si E_a commute avec tout les M_i, l'erreur est indétectable puisque le résultat de toutes les mesures va être $+1$.
- Si E_a anti-commute avec au moins un M_i, alors le on aura $M_i E_a |\psi\rangle = -E_a |\psi\rangle$. Ainsi, $E_a |\psi\rangle$ sera dans l'espace propre -1 de M_i et la mesure de M_i le détectera.

Ainsi, le syndrome d'une erreur E_a sont les signes $s_{a,i}$ tels que

$$M_i E_a |\psi\rangle = s_{a,i} E_a |\psi\rangle$$

Code stabilisateur : détection des erreurs

Une erreur E_a est indétectable si et seulement si

$$E_a \in C(S) \text{ mais } E_a \notin S$$

Code stabilisateurs : conditions pour la correction d'erreur

Théorème

Soit S définissant un code stabilisateur. Supposons que $\{E_j\}$ est un ensemble d'opérateurs dans G_n tels que pour tout j, k on a

$$E_j^* E_k \notin C(S) - S$$

Alors $\{E_j\}$ est un ensemble d'erreurs corrigibles pour le code défini par S.

Autrement dit, pour chaque E_j, E_k, un des deux critères suivants doit être satisfait :

- $E_j^* E_k \in S \implies \langle\psi| E_j^* E_k |\psi\rangle = 1$
- $E_j^* E_k \notin C(S) \implies$
  $\langle\psi| E_j^* E_k |\psi\rangle = \langle\psi| E_j^* E_k M |\psi\rangle = -\langle\psi| E_j^* E_k |\psi\rangle$
  $\implies \langle\psi| E_j^* E_k |\psi\rangle = 0$

Code stabilisateurs : distance

Définition

On dit qu'un code stabilisateur défini par S a distance d ssi tout les éléments de $C(S) - S$ ont un poids $\geq d$

Code stabilisateurs : mots de code

Pour encoder le qubit logique $|\psi\rangle = |x_1, \ldots, x_k\rangle_L$ avec un $[n, k]$-code stabilisateur, on choisi $\bar{Z}_1, \ldots, \bar{Z}_k \in G_n$ de façon à ce que $M_1, \ldots, M_{n-k}, \bar{Z}_1, \ldots, \bar{Z}_k$ forme un ensemble indépendent et commutant. Ensuite, $|\psi\rangle$ sera représenté par le stabilisateur suivant :

$$\langle M_1, \ldots, M_{n-k}, (-1)^{x_1}\bar{Z}_1, \ldots, (-1)^{x_n}\bar{Z}_k \rangle$$

Code stabilisateurs : correction des erreurs

Théorème

Soit $S = \langle M_1, \ldots, M_l \rangle$ un stabilisateur de dimension l tel que $-I \notin S$ et soit $i \in \{1, \ldots, l\}$. Alors il existe $g \in G_n$ tel que $gg_ig^* = -g_i$ et $gg_jg = g_j$ pour tout $i \neq j$.

Corollaire

On peux définir $\bar{X}_1, \ldots, \bar{X}_k \in C(S) - S$ comme les opérateurs qui satifont $\bar{X}_i \bar{Z}_i {\bar{X}_i}^* = -\bar{Z}_i$ et $\bar{X}_i \bar{Z}_i {\bar{X}_i}^* = \bar{Z}_j$ pour tout $i \neq j$

Code stabilisateurs : résumé

Soit $S = \langle M_1, \ldots, M_{n-k} \rangle$ définissant un $[n, k]$-code stabilisateur.

Encodage de l'état $|x_1, \ldots, x_k\rangle$:

1. On a applique les observables $M_1, \ldots, M_{n-k}, \bar{Z}_1, \ldots, \bar{Z}_k$ sur l'état $|0\rangle^{\otimes n}$. L'état résultat est alors décrit par

$$\langle \pm M_1, \ldots, \pm M_{n-k}, \pm \bar{Z}_1, \ldots, \pm \bar{Z}_k \rangle$$

   où les signes sont déterminés par le résultat des mesures.

2. On applique les éléments de G_n appropriés pour obtenir

$$\langle M_1, \ldots, M_{n-k}, (-1)^{x_1} \bar{Z}_1, \ldots, (-1)^{x_n} \bar{Z}_k \rangle$$

Code stabilisateurs : résumé

Soit $S = \langle M_1, \ldots, M_{n-k} \rangle$ définissant un $[n, k]$-code stabilisateur.

Effet d'une erreur E_j

- Si $E_j \in S$, l'erreur ne fait rien.
- Si $E_j \notin C(S) - S$, l'erreur anti-commute avec au moins un générateur de M_i de S et le stabilisateur devient

$$\langle M_1, \ldots, -M_i, \ldots, M_{n-k} \rangle$$

  et l'erreur est détectée en mesurant $-M_i$
- **Si $\mathbf{E_j \in C(S) - S}$, alors $\mathbf{E_j}$ laisse le stabilisateur inchangé mais modifie l'état : l'erreur est indétectable.**

Code stabilisateurs : résumé

Soit $S = \langle M_1, \ldots, M_{n-k} \rangle$ définissant un $[n, k]$-code stabilisateur.

Correction d'une erreur corrigible

1. On mesure tout les M_i et le résultat des mesures nous donne le syndrome de l'erreur.
2. On applique l'opération de récupération associé à l'erreur identifiée.

Code stabilisateurs : résumé

Soit $S = \langle M_1, \ldots, M_{n-k} \rangle$ définissant un $[n, k]$-code stabilisateur.

Décodage de $|x_1, \ldots, x_k\rangle$

- Si on désire récupérer l'état quantique initial, il est possible de rouler un circuit (problème 10.3 du Nielsen & Chuang)
- Si on veux seulement mesurer l'état en base de calcul, on mesure les opérateurs $\bar{Z}_1, \ldots, \bar{Z}_k$ et les résultats ± 1 des mesures nous donne l'état encodé.

Exemple : Code de Shor

M_1	σ_z	σ_z	I	I	I	I	I	I	I
M_2	σ_z	I	σ_z	I	I	I	I	I	I
M_3	I	I	I	σ_z	σ_z	I	I	I	I
M_4	I	I	I	σ_z	I	σ_z	I	I	I
M_5	I	I	I	I	I	I	σ_z	σ_z	I
M_6	I	I	I	I	I	I	σ_z	I	σ_z
M_7	σ_x	σ_x	σ_x	σ_x	σ_x	σ_x	I	I	I
M_8	σ_x	σ_x	σ_x	I	I	I	σ_x	σ_x	σ_x

Figure 1: Générateur du stabilisateur pour le code de Shor

Fin

:^)