DorEmy

Début d'ORdinateur pour EMY-22

Groupe EMY

31 mai 2022

Dans le cadre du développment du protocole EMY-22 (protocole de transmission quantique de clés cryptographiques), ainsi qu'en vue de l'implémentation de l'algorithme de Grover sur un ordinateur classique, ce projet a pour objectif de constituer une base logicielle aisée d'emploi et permettant de simuler, avec un réalisme (c'est-à-dire un abus) et un temps de calcul raisonnable les bases du calcul quantique.

1 Unités de mémoire – Qubits

Un bit est une unité de base de la mémoire qui peut prendre uniquement deux états : 0 et 1. Un qubit, ou bit quantique diffère d'un bit car il son état est une combinaison linéaire des deux états de base (ou *vecteurs propres*) du qubit, $|0\rangle$ et $|1\rangle$. Cette combinaison linéaire doit néanmoins respecter la condition de normalisation, si bien que l'ensemble des états possibles d'un qubit est :

$$E_Q = \{\alpha |0\rangle + \beta |1\rangle \mid \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\}$$

Un cas plus général est celui des qudits, qui sont une généralisation des qubits avec d vecteurs propres. Par exemple avec $d = 3$ on aurait les vecteurs propres $|0\rangle$, $|1\rangle$ et $|2\rangle$. L'ensemble des états d'un qudit est :

$$E_d = \left\{ \sum_{i=0}^{d-1} \alpha_i |i\rangle \,\middle|\, \forall i \in [\![0,\ d-1]\!], \alpha_i \in \mathbb{C}, \sum_{i=0}^{d-1} |\alpha_i|^2 = 1 \right\}$$

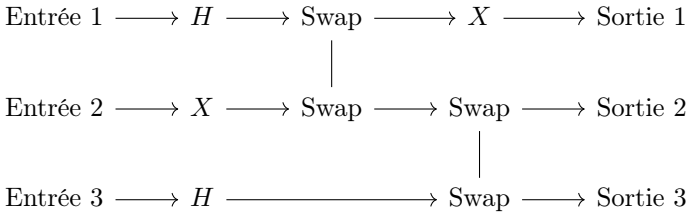
L'état est représenté sous la forme d'une matrice colonne, ce qui facilite l'applications de portes quantiques. Par exemple l'état $|\psi\rangle = a|0\rangle + b|1\rangle$, avec $a, b \in \mathbb{C}$ est assimilé à la matrice $\begin{pmatrix} a \\ b \end{pmatrix}$.

2 Calcul informatique quantique

2.1 Portes et circuits

Le calcul quantique à proprement parlé sera implémenté dans le module `qubit` ainsi que le module `portes`.

De manière analogue aux ordinateurs classiques, les ordinateurs quantiques sont basés sur des circuits électroniques. Ces circuits sont entre autres composés de portes logiques, qui agissent sur un petit nombre d'unités de mémoire (comme des qubits) en modifiant leur état. Un circuit est alors définissable comme : une entrée (avec un état initial de la mémoire connu), et un graphe représentant les différentes portes logiques opérant sur la mémoire, dont fait partie la sortie qui présente l'état de la mémoire qui est le résultat des calculs. Pour des raisons d'efficactité, il a néanmoins été décidé qu'un circuit sera stocké en mémoire sous la forme d'une seule matrice, nommée matrice de circuit `C`.
Exemple : pour le circuit ci-dessous (où H est la porte de Hadamard et X la porte `NOT` ou encore porte de Pauli-X). On aurait en code `C = (H @ X @ H) » (S @ I) » (X @ S)`.



2.2 L'oracle quantique U_f

L'oracle quantique est une porte à part, puisqu'il ne peut pas être représenté par une matrice dans la plupart des cas. Il s'agit néanmoins d'une opération réversible comme toute autre porte. On distingue principalement deux types d'oracles, qui sont utilisés dans deux algorithmes célèbres.

2.2.1 Oracle de phase

Soit $n \in \mathbb{N}^*$, on dispose d'une fonction $f : {\mathbb{F}_2}^n \to \mathbb{F}_2$. On assimile chaque entier $0 \leq i < 2^n - 1$ à sa décomposition en base 2 si bien qu'on a $\tilde{f} : [\![0,\ 2^n - 1]\!] \to \{0, 1\}$ On définit l'oracle de phase U_f tel que pour tout état propre p_i :

$$U_f \left|p_i\right\rangle = (-1)^{\tilde{f}(i)} \left|p_i\right\rangle$$

Pour toute superposition de n qubits $|\psi\rangle$, on peut écrire :

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \langle p_i|q\rangle \left|p_i\right\rangle$$

Cela nous permet, en utilisant la linéarité de U_f, de calculer $U_f \left|\psi\right\rangle$:

$$\begin{aligned} U_f \left|\psi\right\rangle &= U_f \sum_{i=0}^{2^n-1} \langle p_i|q\rangle \left|p_i\right\rangle \\ &= \sum_{i=0}^{2^n-1} \langle p_i|q\rangle U_f \left|p_i\right\rangle \\ &= \sum_{i=0}^{2^n-1} \langle p_i|q\rangle (-1)^{\tilde{f}(i)} \left|p_i\right\rangle \\ &= \sum_{i=0}^{2^n-1} (\langle p_i|q\rangle \left|p_i\right\rangle) \cdot (-1)^{\tilde{f}(i)} \end{aligned}$$

Il suffit donc pour obtenir $U_f \left|\psi\right\rangle$ de multiplier chacune des composantes d'indice i de $\left|\psi\right\rangle$ par $(-1)^{\tilde{f}(i)}$.

2.2.2 Oracle de somme

Cet oracle courant est notamment utilisé dans l'algorithme de Deutch-Jozsa, ou lorsqu'on cherche à résoudre une équation du type :

$$f(x_1, ..., x_n) = (y_1, ..., y_m), \text{avec } n, m \in \mathbb{N}^*.$$

Pour une *fonction d'oracle* notée $f : {\mathbb{F}_2}^n \to {\mathbb{F}_2}^m$, on a en notant $x = x_1, ..., x_n$ les paramètres de f et $y = y_1, ..., y_m$ la valeur recherchée :

$$U_f \left|x, y\right\rangle = \left|x, f(x) \oplus y\right\rangle$$

avec $\oplus$ l'addition usuelle des m-uplets dans le corps $\mathbb{F}_2$ et notant que pour tous $\psi_1, ..., \psi_k$, la notation $\left|\psi_1, ..., \psi_k\right\rangle$ désigne $\left|\psi_1\right\rangle \otimes ... \otimes \left|\psi_k\right\rangle$ (avec $\otimes$ le produit tensoriel, qui est dans notre cas celui des matrices).
Exemple : le calcul serait assez simple si les états $x_1, ..., x_n$ n'étaient pas dans le cas général une superposition d'états. On a donc en pratique des situations comme celle-ci :

On a $n = m = 2$ et la fonction f est donnée par :

$$f : \left| \begin{array}{ccc} {\mathbb{F}_2}^2 & \longrightarrow & {\mathbb{F}_2}^2 \\ (a, b) & \longmapsto & (a \oplus b, b) \end{array} \right.$$

On a $y = (y_1, y_2) = (1, 1)$ donc $\left|y\right\rangle = \left|11\right\rangle$. On fait passer notre état initial $\left|00\right\rangle$, propre, dans deux portes de Hadamard et on obtient $\left|x\right\rangle = \frac{1}{2}\left|00\right\rangle + \frac{1}{2}\left|01\right\rangle + \frac{1}{2}\left|10\right\rangle + \frac{1}{2}\left|11\right\rangle$. Comment alors calculer le résultat de notre oracle ? La clé est d'utiliser le caractère linéaire de U_f (les paramètres x et y ont étés séparés par un virgule pour clarifier) :

$$\begin{aligned}
U_f\left|x,y\right\rangle =& \frac{1}{2}U_f\left|00,11\right\rangle + \frac{1}{2}U_f\left|01,11\right\rangle + \frac{1}{2}U_f\left|10,11\right\rangle + \frac{1}{2}U_f\left|11,11\right\rangle \\
=& \frac{1}{2}\left|00,11+f(0,0)\right\rangle + \frac{1}{2}\left|01,11+f(0,1)\right\rangle + \frac{1}{2}\left|10,11+f(1,0)\right\rangle \\
&+ \frac{1}{2}\left|11,11+f(1,1)\right\rangle \\
=& \frac{1}{2}\left|0011\right\rangle + \frac{1}{2}\left|0100\right\rangle + \frac{1}{2}\left|1001\right\rangle + \frac{1}{2}\left|1110\right\rangle
\end{aligned}$$

Implémentation : En première approche, on fait l'hypothèse que $m = 1$, d'où $f : {\mathbb{F}_2}^n \to \mathbb{F}_2$. Soit $\left|\psi\right\rangle \in \mathbb{C}^{2^{n+1}}$ une superposition des états $\left|x\right\rangle \in \mathbb{C}^{2^n}$ et $\left|y\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle \in \mathbb{C}^2$, d'où $\left|\psi\right\rangle = \left|x,y\right\rangle = \left|x\right\rangle \otimes \left|y\right\rangle$. On note $(\left|p_i\right\rangle)_{1\leq i<2^{n+1}}$ la base canonique de $\mathbb{C}^{2^{n+1}}$ et $(\left|q_i\right\rangle)_{1\leq i<2^n}$ celle de $\mathbb{C}^{2^n}$. On cherche à calculer $U_f\left|\psi\right\rangle$ en ayant uniquement accès aux $\left\langle p_i|\psi\right\rangle$.

Puisqu'il est impossible de récupérer les valeurs de $\left|x\right\rangle$ et $\left|y\right\rangle$ pour des composantes quelconques (si on multiplie $\left|x\right\rangle$ par $e^{i\theta}$ et $\left|y\right\rangle$ par $e^{-i\theta}$, $\left|x\right\rangle\otimes\left|y\right\rangle$ ne change pas), on suppose aussi que les composantes de $\left|x\right\rangle$ et $\left|y\right\rangle$ sont réelles positives, d'où $\beta = \sqrt{1-\alpha^2}$.

Puisque $\left|x\right\rangle$ et $\left|y\right\rangle$ sont non nuls il existe $i_0 \in [\![0,\ 2^{n+1}-1]\!]$ tel que $\left\langle p_{i_0}|\psi\right\rangle \neq 0$. Si i_0 est pair : en notant $i_0 = 2j_0$ on a $\left\langle p_{2j_0}|\psi\right\rangle = \alpha\left\langle q_{j_0}|x\right\rangle \neq 0$ donc $\alpha \neq 0$. On peut en déduire la valeur de α puis celle de β :

$$\alpha = \left(\left(\frac{\left\langle p_{i_0+1}|\psi\right\rangle}{\left\langle p_{i_0}|\psi\right\rangle}\right)^2 + 1\right)^{-1/2}$$

Si i_0 est impair : par un raisonnement similaire, on obtient :

$$\beta = \left(\left(\frac{\left\langle p_{i_0-1}|\psi\right\rangle}{\left\langle p_{i_0}|\psi\right\rangle}\right)^2 + 1\right)^{-1/2}$$

Puisqu'on a la valeur de $\left|y\right\rangle$, on en déduit celle de $\left|x\right\rangle$ par la relation :

$$\forall i \in [\![0,\ 2^n-1]\!], \left\langle q_i|x\right\rangle = \begin{cases} \alpha^{-1}\left\langle p_{2i}|\psi\right\rangle \text{ si } \alpha \neq 0 \\ \beta^{-1}\left\langle p_{2i+1}|\psi\right\rangle \text{ si } \beta \neq 0 \end{cases}$$

On peut alors calculer $U_f\left|\psi\right\rangle$. Puisque par développement de $\left|\psi\right\rangle$:

$$\begin{aligned}
\left|\psi\right\rangle &= \left|x\right\rangle \otimes \left|y\right\rangle \\
&= \left(\sum_{j=0}^{2^n-1}\left\langle q_j|x\right\rangle\left|q_j\right\rangle\right) \otimes \left(\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right) \\
&= \alpha\sum_{j=0}^{2^n-1}\left\langle q_j|x\right\rangle\left|q_j 0\right\rangle + \beta\sum_{j=0}^{2^n-1}\left\langle q_j|x\right\rangle\left|q_j 1\right\rangle
\end{aligned}$$

alors on conclut par linéarité de U_f :

$$\begin{aligned} U_f \left|\psi\right\rangle &= \alpha \sum_{j=0}^{2^n-1} \left\langle q_j|x\right\rangle U_f \left|q_j 0\right\rangle + \beta \sum_{j=0}^{2^n-1} \left\langle q_j|x\right\rangle U_f \left|q_j 1\right\rangle \\ &= \alpha \sum_{j=0}^{2^n-1} \left\langle q_j|x\right\rangle \left|q_j, f(q_j)\right\rangle + \beta \sum_{j=0}^{2^n-1} \left\langle q_j|x\right\rangle \left|q_j, 1+f(q_j)\right\rangle \end{aligned}$$

3 Calcul mathématique

Dans de nombreuses situations on aura besoin de réaliser des calculs de manière plus poussée que ce que permet nativement Python. Pour cela on implémentera un module, nommé `calcul`, dont le rôle sera de réaliser des calculs de manière formelle.

3.1 Ensembles de travail

Dans la construction des mathématiques par laquelle ce module passera, on admettra la construction des entiers relatifs $\mathbb{Z}$ (néanmoins on détaillera $\mathbb{N}$), et on implémentera quelques ensembles de valeurs :

- Les rationnels $\mathbb{Q}$, qu'on assimilera l'ensemble des couples $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ avec p et q premiers entre eux. On prendra garde à toujours simplifier les rationnels lors des calculs de manière à garder un couple d'entiers avec les bons signes et premiers entre eux.
- Les puissances rationnelles de rationnels positifs $\mathbb{P}$. En particulier, $\mathbb{P}$ contient l'ensemble des racines carrées des rationnels, ainsi que $\mathbb{Q}$ lui-même. La multiplication est interne dans $\mathbb{P}$ mais pas l'addition

On aura donc des réels que $\mathbb{P} = \{\sigma x^p \mid \sigma \in \{-1, 1\}, x \in \mathbb{Q}^+, p \in \mathbb{Q}\}$. Les complexes seront construits comme des couples : $x+iy$ sera assimilé à $(x, y) \in \mathbb{P}^2$. Le plus grand ensemble de travail est donc $\mathbb{P}[i] = \{x + iy \mid x, y \in \mathbb{P}\}$.

3.2 Sous-ensemblage

3.2.1 Principe

Une dynamique qu'il sera crucial d'implémenter est le **sous-ensemblage** : toute variable doit avoir à chaque fin de calcul (même partiel) un type (correspodant à un ensemble) le plus fin possible. Par exemple le calcul $\frac{2}{3} \times \frac{3}{2} = \frac{1}{1}$ doit automatiquement être converti en entier (un sous-ensemble des rationnels, ce qu'il est par ailleurs). On note en particulier les inclusions : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{P}$.

Le sous-ensemblage est implémenté dans la fonction `sous`, qui appelle, sauf si aucune simplification n'est possible, la fonction `sous` du sous-type trouvé.

Exemple : pour le rationnel $\frac{2}{1} \in \mathbb{Q}$:

1. La fonction `sous` des rationnels détecte qu'on peut passer aux entiers relatifs. Elle construit donc un entier relatif correspondant : c'est $2 \in \mathbb{Z}$. On apelle ensuite `sous` sur le relatif 2.
2. Dans `sous` de 2, on trouve qu'on peut simplifier au naturel $2 \in \mathbb{N}$
3. On ne peut pas simplifier plus, donc le `sous` de $2 \in \mathbb{N}$ renvoie le même $2 \in \mathbb{N}$.

3.2.2 Simplification des puissances

L'ensemble $\mathbb{P}$ étant le plus grand sous-ensemble de $\mathbb{R}$ implémenté, il est important de mettre au point des techniques de simplification des puissances.

Soit $a = \sigma x^p \in \mathbb{P}$ une puissance. On a $\sigma \in \{-1, 1\}$ le *signe*, $x = \frac{n_x}{d_x} \in \mathbb{Q}^+$ le *signifiant* et $p = \frac{n_p}{d_p} \in \mathbb{Q}^{+*}$ l'*exposant*.

1. Si $p \in \mathbb{Z}$, on calcule $\sigma x^p \in \mathbb{Q}$. Si $p \geq 0$ son numérateur non simplifié est $\sigma {n_x}^p$ et son dénominateur non simplifié est ${d_x}^p$. Si $p < 0$ son numérateur non simplifié est $\sigma {d_x}^p$ et son dénominateur non simplifié est ${n_x}^p$.
2. Sinon, on cherche à savoir si il existe $r = \frac{n_r}{d_r} \in \mathbb{Q}+$ tel que $r^{d_p} = x$. On a alors $x = r^{n_p} \in \mathbb{Q}$.

Algorithme : racine d_p-ième exacte d'un rationnel.
On cherche à déterminer s'il existe un $r \in \mathbb{Q}^+$ tel que $r^{d_p} = x$, et si il existe à déterminer un couple numérateur-dénominateur.

```
Pour d_r allant de 1 à d_x
   Si η = x · {d_r}^{d_p} ∈ ℕ
      Si ∃n_r ∈ ⟦1, ⌊√η⌋⟧ tel que {n_r}^{d_p} = η
         On renvoie r = n_r / d_r
      Fin si
   Fin si
Fin pour
Il n'existe pas de r qui convient
```

3.3 Sur-ensemblage

La dynamique inverse existe aussi : on la nomme **sur-ensemblage**, mis en place dans la fonction `sur`. Elle est néanmoins temporaire puisqu'elle n'est utilisée que pour permettre les calculs entre deux types différents. Exemple pour le calcul $-\frac{1}{2} \times (-2) = 1$:

1. $-2 \notin \mathbb{Q}\backslash\mathbb{Z}$, on le projette sur l'ensemble $\mathbb{Q}$. On obtient $-\frac{2}{1} \in \mathbb{Q}$.
2. $-\frac{1}{2}$ et $-\frac{2}{1}$ sont de même type, on peut les muliplier. On obtient $\frac{1}{1} \in \mathbb{Q}$
3. Fin du calcul : on simplifie en appelant `sous` et on obtient finalement $1 \in \mathbb{N}$.

3.4 Matrices

Le nombre de lignes d'une matrice `m` est `m.p` et son nombre de colonnes est `m.q`, avec $p, q \in \mathbb{N}$. On peut accéder à p et q en même temps en regardant `m.forme`, qui vaut le tuple `(p, q)`. Les élements sont accessibles par un couple $(i, j) \in [\![0,\ p-1]\!] \times [\![0,\ q-1]\!]$, les indices commençant donc à 0. On aura par exemple `m[0, 0]` Pour les matrices lignes et colonnes, il n'est nécessaire que de spécifier l'une des deux coordonnées (l'autre étant forcément 0). On aura dans ce cas `m[2]` par exemple.

Les éléments d'une matrice ne sont jamais des `int`, des `float` et encore moins des `str` : tous les coefficients sont des nombres formellements stockés (voir 3.1), donc des éléments de $\mathbb{P}[i]$.