Calcul et informatique quantique: une introduction formelle

Antoine Groudiev

ENS Ulm

Janvier 2024

Plan

Plan

Introduction

Notation de Dirac

Représentation vectorielle

Visualisation avec la sphère de Bloch

Plan

Circuits quantiques

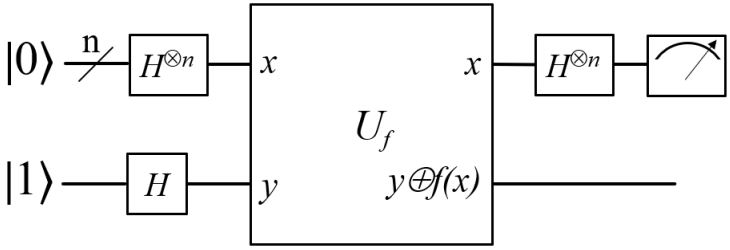

Figure – Un exemple de circuit (Algorithme de Deutsch-Jozsa)

Porte X

Porte Z

Porte de Hadamard

Intrication quantique

Porte *CNOT*

Langage quantique

Retour sur les langages classiques

Soit Σ un alphabet, et $L \subseteq \Sigma^\star$ un langage. L peut être défini alternativement comme un sous-ensemble de $\Sigma^\star$, ou par sa fonction caractéristique χ_L :

$$\chi_L(w) = \begin{cases} 1 & \text{si } w \in L \\ 0 & \text{sinon} \end{cases}$$

Langage quantique

Définition

On peut par analogie définir un *langage quantique* comme une fonction associant des probabilités à des mots :

Définition (Langage quantique)

Un *langage quantique* sur l'alphabet Σ est une fonction f telle que :

$$f : \Sigma^\star \to [0, 1]$$

Remarque

f est un langage classique lorsque $f(\Sigma^\star) \subseteq \{0, 1\}$.

Automate quantique fini

Définition (AQF)

Un *Automate Quantique Fini* $Q = (H, s_{\text{init}}, H_{\text{accept}}, P_{\text{accept}}, \Sigma, \delta)$ constiste en :

- un espace de Hilbert H de dimension n
- un vecteur initial normalisé $s_{\text{init}} \in H$ (i.e. $\|s_{\text{init}}\|^2 = 1$)
- un sous-espace $H_{\text{accept}} \subseteq H$, et un opérateur P_{accept} projettant sur H_{accept}
- un alphabet Σ
- une fonction $\delta : \Sigma \to U_n(\mathbb{C})$, associant à chaque lettre une matrice unitaire U_a (c'est-à-dire $U_a U_a^\dagger = I_n$)

On note $\delta^\star(w = w_1 \cdots w_{|w|}) = \delta(w_{|w|}) \cdots \delta(w_1) = U_{w_{|w|}} \cdots U_{w_1}$. Enfin, le langage reconnu par Q est :

$$f_Q : w \mapsto \|P_{\text{accept}} \delta^\star(w) s_{\text{init}}\|^2$$

Langage quantique régulier et propriétés

Définition (LQR)

Un *Langage Quantique Régulier* est un langage quantique reconnu par un automate quantique fini

Théorème (Clôture des LQR par produit)

Soient f, g des LQRs. Alors, le produit fg est un LQR.

Théorème (Clôture des LQR par combinaison linéaire)

Soient f_i des LQRs, et c_i des constantes telles que $\sum_i c_i \leq 1$. Alors, $\sum_i c_i f_i$ est un LQR.

Langage quantique régulier et propriétés

Théorème (Lemme de pompage quantique)

Si f est un LQR, alors pour tout mot $w \in \Sigma^\star$ et tout $\varepsilon > 0$, il existe $k \in \mathbb{N}^\star$ tel que $\|f(uw^k v) - f(uv)\| < \varepsilon$ pour tout mots u, v. De plus, si l'automate de f est de dimension n, alors il existe une constante c (indépendante de ε) telle que $k < (c\varepsilon)^{-n}$.

Grammaire quantique

Définition (Grammaire Quantique [1])

Une *Grammaire Quantique* $G = (V, T, I, P)$ de *dimensionnalité* n consiste en :

- un alphabet V de variables
- un alphabet T de terminaux
- une variable initiale $I \in V$
- un ensemble fini de productions P de la forme $\alpha \to \beta$, où $(\alpha, \beta) \in V^\star \times (T \cup V)^\star$.

1. https://xkcd.com/1090/

À chaque production de P est associée un ensemble d'amplitudes complexes $(c_k(\alpha \to \beta))_{1 \leq k \leq n}$.
On définit l'amplitude d'*une* suite de productions :

$$c_k(\alpha_1 \to \cdots \to \alpha_m = \beta) := \prod_{i=1}^{m-1} c_k(\alpha_i \to \alpha_{i+1})$$

Et l'amplitude d'une dérivation :

$$c_k(\alpha \Rightarrow \beta) := \sum_{\alpha=\alpha_1 \to \cdots \to \alpha_m = \beta} c_k(\alpha_1 \to \cdots \to \alpha_m)$$

Enfin, G *génère* le langage quantique f définit par :

$$f(w) = \sum_{k=1}^{n} \|c_k(I \Rightarrow w)\|^2$$

Automate à pile quantique

Machine de Turing quantique

Plan

Classe BQP (Bounded-error Quantum Polynomial time)

Un problème Promise-BQP-complet

Positionnement par rapport aux classes de complexité classiques

Thèse de Church-Turing

Plan

Description du problème

Solution classique

Algorithme de Deutsch

Cas général (n quelconque)