Vers les algorithmes de Simon et Shor

Partie 1 : L'algorithme de Simon

Xavier Caruso

Groupe de travail
d'informatique quantique

29 avril 2020

Le problème de Simon

On note $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$

Les données du problème

On se donne une fonction $f : \mathbb{F}_2^n \to X$ telle que :

(1) soit f est injective

(2) soit il existe $a \in \mathbb{F}_2^n$ tel que
$f(x) = f(y)$ ssi $(x = y$ ou $x = y + a)$

La question

Problème de décision : décider si on est dans (1) ou (2)

Problème de calcul : dans (2), déterminer a

Le problème du sous-groupe caché

L'énonce du problème

On se donne un groupe G, un ensemble X et
une fonction $f : G \to X$ avec la promesse suivante :

il existe un sous-groupe H de G tel que
$f(x) = f(y)$ ss'il existe $h \in H$ tel que $x = yh$

i.e. f induit une injection $G/H \hookrightarrow X$

Problème de calcul : déterminer H

Le lien avec le problème de Simon

C'est le cas particulier où

- ☞ $G = \mathbb{F}_2^n$
- ☞ $H = \{0\}$ ou $H = \{0, a\}$

Complexité dans le cas classique

Analyse dans le pire cas

Après N appels à la fonction f,

- ☞ *si deux valeurs renvoyées sont égales*,
  on conclut qu'on est dans le cas (2) et on calcule a
- ☞ *si les valeurs renvoyées sont deux à deux distinctes*,
  on élimine au plus $\frac{N(N-1)}{2}$ valeurs de a

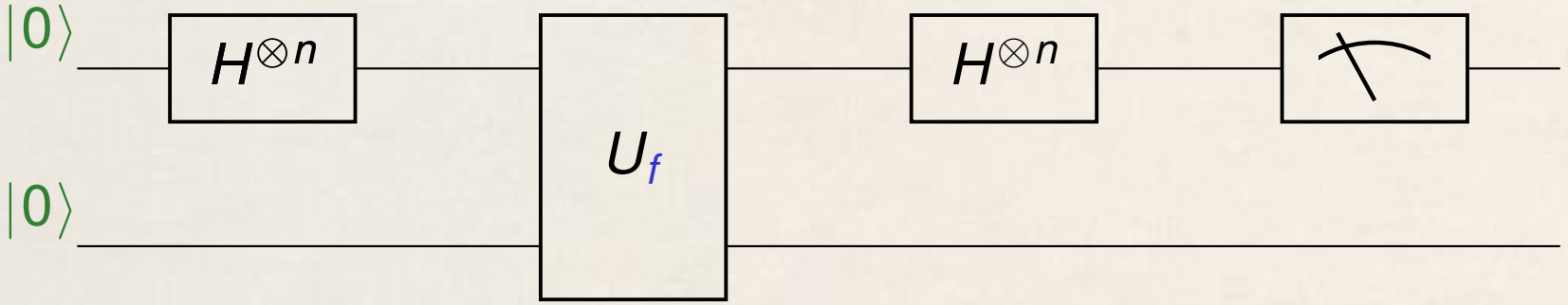
Dans le pire cas, on a donc

$$\frac{N(N-1)}{2} \approx 2^n, \quad \textit{i.e.} \quad N \approx \sqrt{2^{n+1}} \approx 2^{n/2}$$

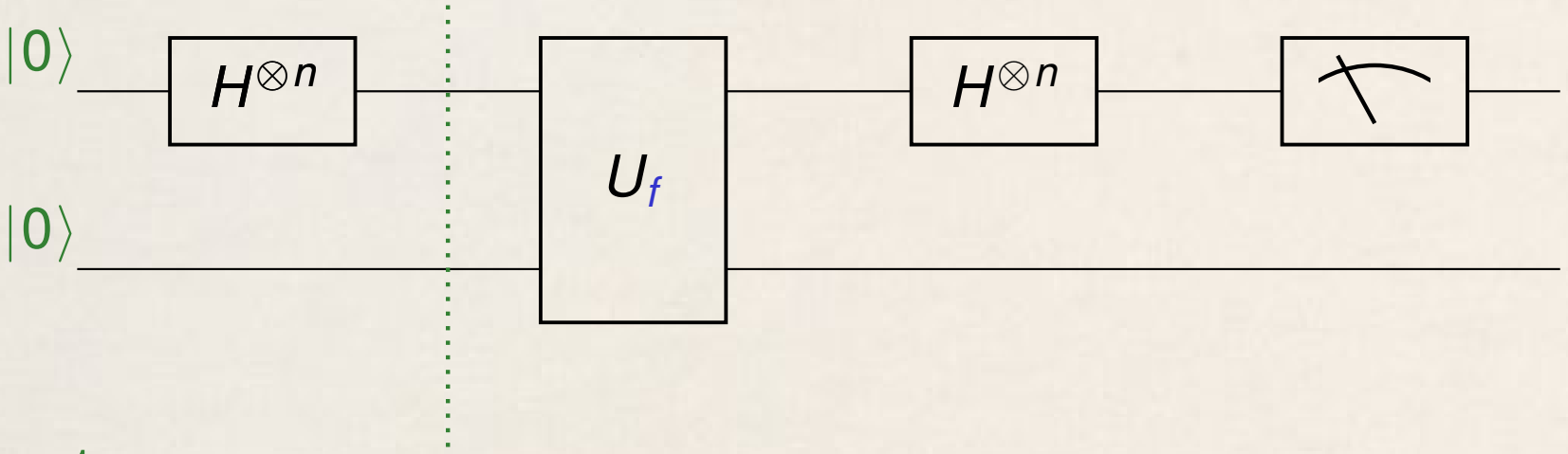
Analyse en moyenne

Paradoxe des anniversaires : $N \gtrsim 2^{n/4}$

Le circuit quantique

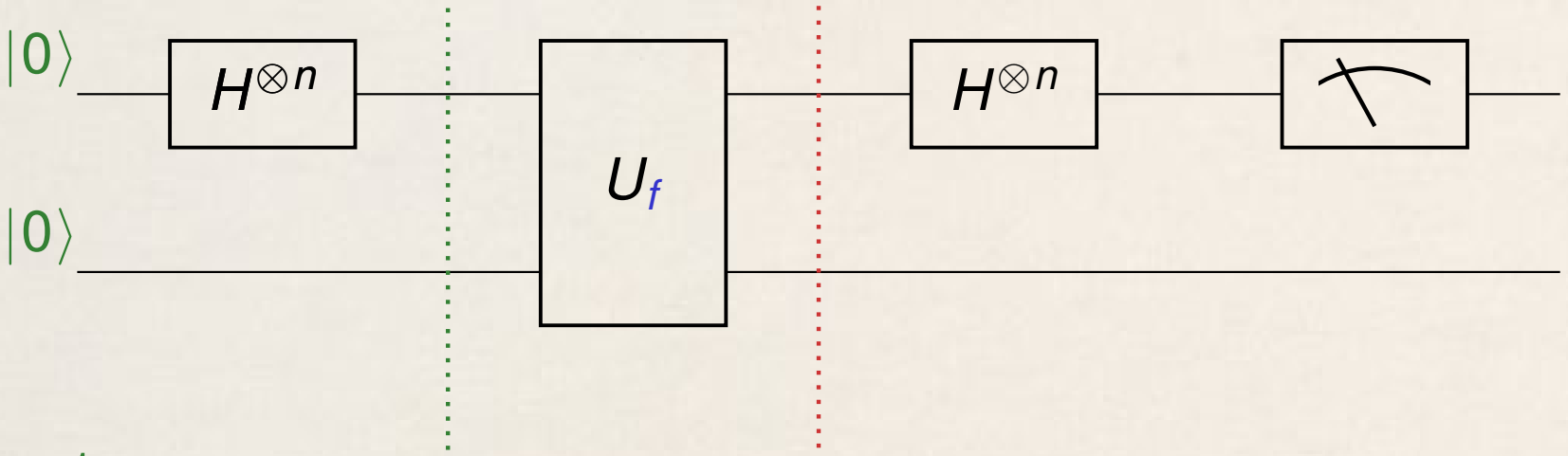


Le circuit quantique



$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes |0\rangle$$

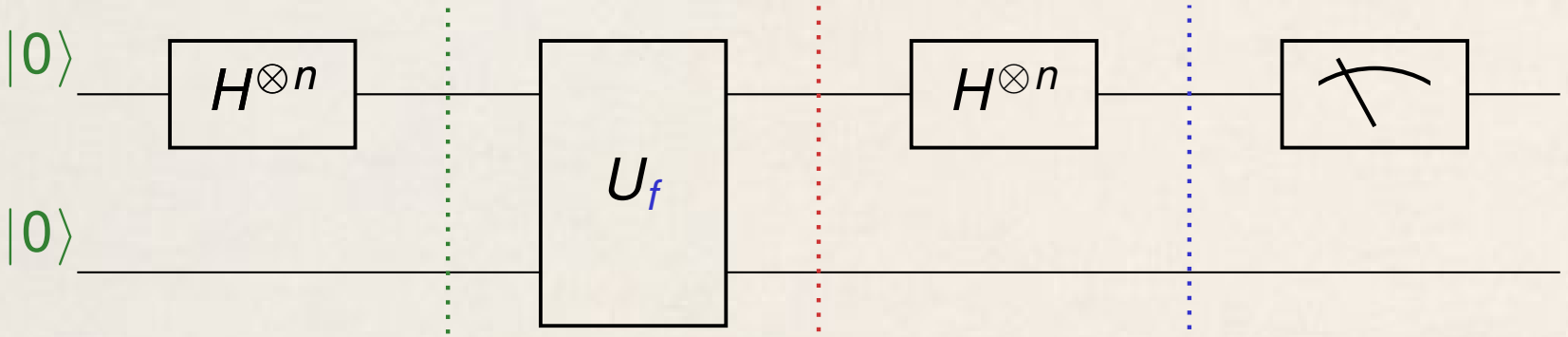
Le circuit quantique



$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes |0\rangle$$

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes |f(x)\rangle$$

Le circuit quantique



$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes |0\rangle$$

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes |f(x)\rangle$$

$$q = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} H^{\otimes n}(|x\rangle) \otimes |f(x)\rangle$$

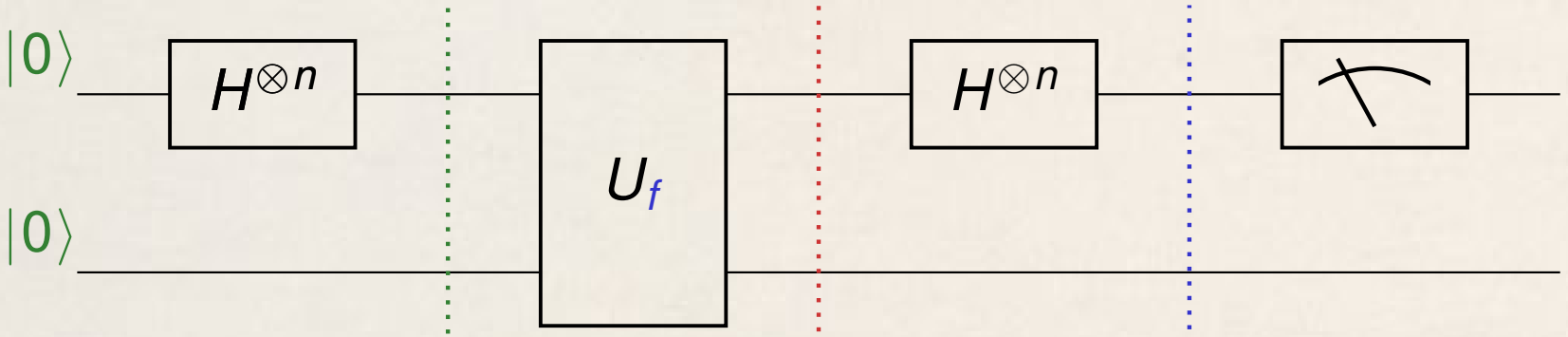
Le calcul de q

Si $x = (x_1, x_2, \ldots, x_n)$, alors

$$
\begin{aligned}
H^{\otimes n}(|x\rangle) &= H(|x_1\rangle) \otimes \cdots \otimes H(|x_n\rangle) \\
&= \left(\frac{|0\rangle + (-1)^{x_1}|1\rangle}{\sqrt{2}}\right) \otimes \cdots \otimes \left(\frac{|0\rangle + (-1)^{x_n}|1\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{2^{n/2}} \cdot \sum_{y \in \mathbb{F}_2^n} (-1)^{x_1 y_1 + \cdots + x_n y_n} |y\rangle \\
&= \frac{1}{2^{n/2}} \cdot \sum_{y \in \mathbb{F}_2^n} (-1)^{\langle x, y \rangle} |y\rangle
\end{aligned}
$$

$$
\begin{aligned}
q &= \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} H^{\otimes n}(|x\rangle) \otimes |f(x)\rangle \\
&= \frac{1}{2^n} \sum_{x, y \in \mathbb{F}_2^n} (-1)^{\langle x, y \rangle} |y\rangle \otimes |f(x)\rangle
\end{aligned}
$$

Le circuit quantique



$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes |0\rangle$$

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes |f(x)\rangle$$

$$q = \frac{1}{2^n} \sum_{x,y \in \mathbb{F}_2^n} (-1)^{\langle x,y \rangle} |y\rangle \otimes |f(x)\rangle$$

La mesure

$$q = \frac{1}{2^n} \sum_{x,y \in \mathbb{F}_2^n} (-1)^{\langle x,y \rangle} |y\rangle \otimes |f(x)\rangle$$

$$= \sum_{y \in \mathbb{F}_2^n} |y\rangle \otimes q_y \qquad\qquad q_y = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x,y \rangle} |f(x)\rangle$$

Le résultat de la mesure est y avec probabilité $\|q_y\|^2$

Cas (1) : f est injective

$\|q_y\|^2 = 2^{-n}$

$\Longrightarrow$ Le résultat de la mesure est équidistribué dans $\mathbb{F}_2^n$

La mesure

$$q = \frac{1}{2^n} \sum_{x,y \in \mathbb{F}_2^n} (-1)^{\langle x,y \rangle} |y\rangle \otimes |f(x)\rangle$$

$$= \sum_{y \in \mathbb{F}_2^n} |y\rangle \otimes q_y \qquad\qquad q_y = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x,y \rangle} |f(x)\rangle$$

Le résultat de la mesure est y avec probabilité $\|q_y\|^2$

Cas (2) : $f(x) = f(y)$ ssi $(x = y$ ou $x = y + a)$

$$q_y = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n / \langle a \rangle} \left((-1)^{\langle x,y \rangle} + (-1)^{\langle x+a,y \rangle} \right) |f(x)\rangle$$

☞ si $\langle a, y \rangle = 1$, alors $q_y = 0$

☞ si $\langle a, y \rangle = 0$, alors $q_y = \frac{1}{2^{n-1}} \sum_{x \in \mathbb{F}_2^n / \langle a \rangle} (-1)^{\langle x,y \rangle} |f(x)\rangle$

$\Longrightarrow$ Le résultat de la mesure est équidistribué dans $\langle a \rangle^{\perp}$

L'algorithme de Simon

1. En exécutant N fois le « circuit de Simon », on obtient des vecteurs $y_1, \ldots, y_N$
2. On calcule $V = \langle y_1, \ldots, y_N \rangle^{\perp}$
3. **Si** $V = 0$, on est dans le cas (1)

   Sinon, on décrète qu'on est dans le cas (2) et on renvoie un élément non nul de V

Preuve de correction

Soit H le sous-groupe caché

Les y_i sont aléatoirement distribués dans $H^{\perp}$

L'algorithme est correct si les y_i engendrent $H^{\perp}$

Proba de succès : $\prod_{i=1}^{\dim H^{\perp}} \left(1 - \frac{1}{2^{N+1-i}}\right) = 1 - O\left(\frac{1}{2^{N-n}}\right)$

Un petit calcul de probabilité

Proposition

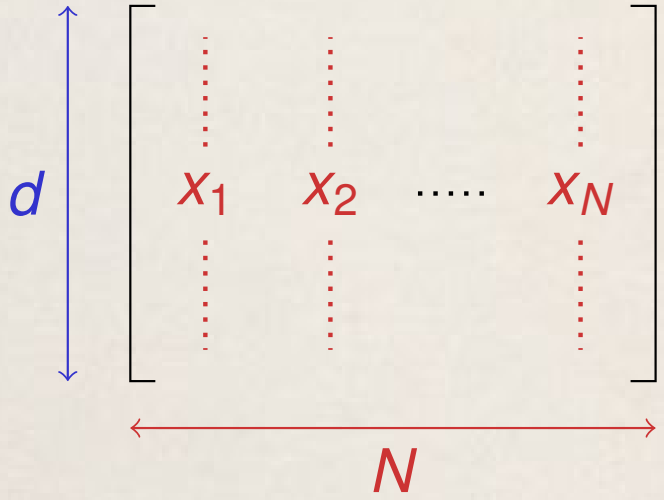
Soit E un espace vectoriel de dimension d sur $\mathbb{F}_p$

Soient $x_1, \ldots, x_N$ des vecteurs aléatoires de E

La probabilité que les x_i engendrent E est

$$\prod_{i=1}^{d} \left(1 - \frac{1}{p^{N+1-i}}\right)$$

Démonstration



Nombre de cas :
p^{Nd}

Nombre de cas favorables :
$(p^N - 1)(p^N - p) \cdots (p^N - p^{d-1})$