Algoritmo de Periodicidade de Simon

Adenilton J. da Silva
www.cin.ufpe.br/~ajsilva

Seção 1

Introdução

Introdução

O problema de Simon pode ser resolvido com ganho exponencial em um computador quântico em relação a uma solução em um computador clássico.

Introdução

- Dada uma função $f : \{0,1\}^n \rightarrow \{0,1\}^n$, onde $f(x) = f(y)$ se e somente se $x \oplus c = y$.

Introdução

- Dada uma função $f : \{0,1\}^n \to \{0,1\}^n$, onde $f(x) = f(y)$ se e somente se $x \oplus c = y$.
- O algoritmo de Simon tem como objetivo determinar o valor de c.

Introdução

Se $c = 100$.
$f(000) =$

Introdução

Se $c = 100$.
$f(000) = f(100)$
$f(001) =$

Introdução

Se $c = 100$.
$f(000) = f(100)$
$f(001) = f(101)$
$f(010) =$

Introdução

Se $c = 100$.
$f(000) = f(100)$
$f(001) = f(101)$
$f(010) = f(110)$
$f(011) =$

Introdução

Se $c = 100$.
$f(000) = f(100)$
$f(001) = f(101)$
$f(010) = f(110)$
$f(011) = f(111)$
$f(100) =$

Introdução

Se $c = 100$.
$f(000) = f(100)$
$f(001) = f(101)$
$f(010) = f(110)$
$f(011) = f(111)$
$f(100) = f(000)$
$f(101) = f(001)$
$f(110) = f(010)$
$f(111) = f(011)$

Introdução

Por exemplo, para

Se $c = 100$.

$$f(000) = f(100)$$
$$f(001) = f(101)$$
$$f(010) = f(110)$$
$$f(011) = f(111)$$
$$f(100) = f(000)$$
$$f(101) = f(001)$$
$$f(110) = f(010)$$
$$f(111) = f(011)$$

$$f(x) : \{0,1\}^n \rightarrow \{0,1\}^n$$
$$b_0 b_1 b_2 \mapsto 0 b_1 b_2$$

$$f(000) = f(100) = 000$$
$$f(001) = f(101) = 001$$
$$f(010) = f(110) = 010$$
$$f(011) = f(111) = 011$$

Introdução

Se $c = 100$.

$$
\begin{aligned}
f(000) &= f(100)\\
f(001) &= f(101)\\
f(010) &= f(110)\\
f(011) &= f(111)\\
f(100) &= f(000)\\
f(101) &= f(001)\\
f(110) &= f(010)\\
f(111) &= f(011)
\end{aligned}
$$

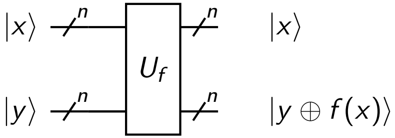
Por exemplo, para

$$
\begin{aligned}
f(x) : \{0,1\}^n &\to \{0,1\}^n\\
b_0 b_1 b_2 &\mapsto 0 b_1 b_2
\end{aligned}
$$

$$
\begin{aligned}
f(000) = f(100) &= 000\\
f(001) = f(101) &= 001\\
f(010) = f(110) &= 010\\
f(011) = f(111) &= 011
\end{aligned}
$$

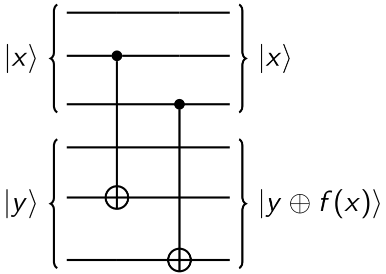
A entrada do algoritmo de Simon será:

- Em um computador clássico a função f.
- Em um computador quântico o operador U_f.



Introdução

$$f(x) : \{0,1\}^n \rightarrow \{0,1\}^n$$
$$b_0 b_1 b_2 \mapsto 0 b_1 b_2$$



Seção 2

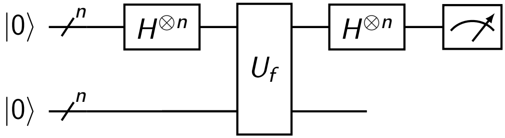
Algoritmo de Simon

Algoritmo de Simon

- O algoritmo de Simon pode ser resolvido com $O(n)$ chamadas da função em um dispositivo quântico.
- O algoritmo é híbrido, por possuir uma parte clássica e uma parte quântica.

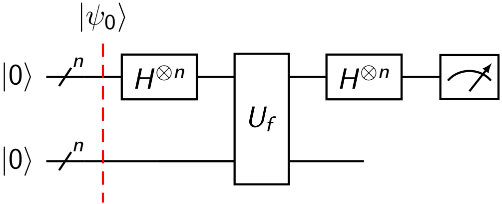
Algoritmo de Simon

Parte quântica



Algoritmo de Simon

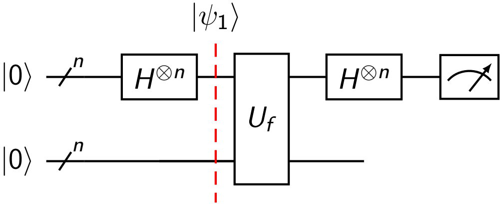
Parte quântica



$$|\psi_0\rangle = |0\rangle^{\otimes n} |0\rangle^{\otimes n}$$

Algoritmo de Simon

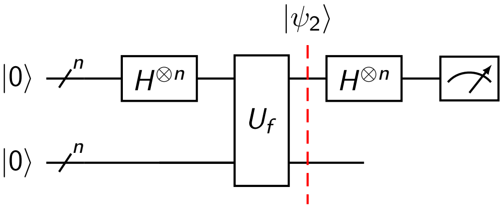
Parte quântica



$$|\psi_1\rangle = (H^{\otimes n} \otimes I^{\otimes n}) |0\rangle |0\rangle$$
$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$$

Algoritmo de Simon

Parte quântica

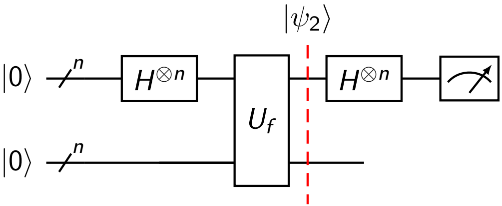


$$|\psi_1\rangle = (H^{\otimes n} \otimes I^{\otimes n}) |0\rangle |0\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$$

Algoritmo de Simon

Parte quântica



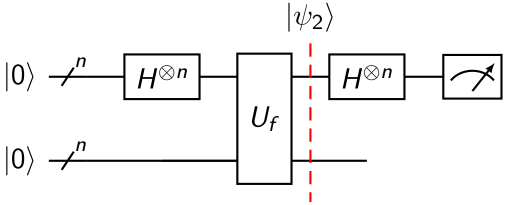
$$|\psi_1\rangle = (H^{\otimes n} \otimes I^{\otimes n}) |0\rangle |0\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

Algoritmo de Simon

Parte quântica

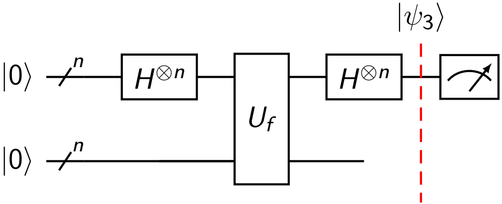


$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \, |f(x)\rangle$$

Adenilton Silva www.cin.ufpe.br/~ajsilva

Algoritmo de Simon

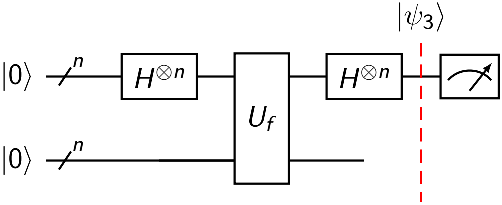
Parte quântica



$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

Algoritmo de Simon

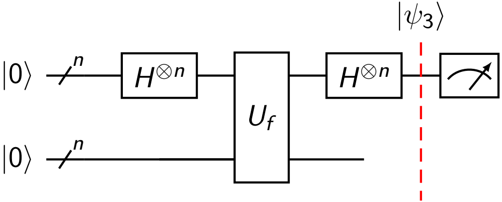
Parte quântica



$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} H(|x\rangle)\,|f(x)\rangle$$

Algoritmo de Simon

Parte quântica

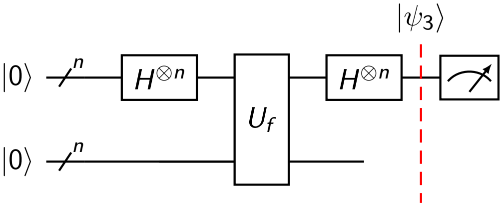


$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} H(|x\rangle)\,|f(x)\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z}\,|z\rangle\,|f(x)\rangle$$

Algoritmo de Simon

Parte quântica



$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} H(|x\rangle)\,|f(x)\rangle$$

$$= \boxed{\frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}\,|z\rangle\,|f(x)\rangle}$$

Algoritmo de Simon

Parte quântica

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle |f(x)\rangle$$

Algoritmo de Simon

Parte quântica

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle |f(x)\rangle$$

- Pela suposição do problema existe um c onde $f(x) = f(x \oplus c)$, então

$$|z\rangle |f(x)\rangle = |z\rangle |f(x \oplus c)\rangle$$

Algoritmo de Simon

Parte quântica

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle |f(x)\rangle$$

- Pela suposição do problema existe um c onde $f(x) = f(x \oplus c)$, então

$$|z\rangle |f(x)\rangle = |z\rangle |f(x \oplus c)\rangle$$

- Amplitude de $|z\rangle |f(x)\rangle$.

$$\frac{(-1)^{x \cdot z}}{2^n} + \frac{(-1)^{(x \oplus c) \cdot z}}{2^n}$$

Algoritmo de Simon

Parte quântica

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}\sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle|f(x)\rangle$$

- Pela suposição do problema existe um c onde $f(x) = f(x\oplus c)$, então

$$|z\rangle|f(x)\rangle = |z\rangle|f(x\oplus c)\rangle$$

- Amplitude de $|z\rangle|f(x)\rangle$.

$$\frac{(-1)^{x\cdot z}}{2^n}+\frac{(-1)^{(x\oplus c)\cdot z}}{2^n}$$

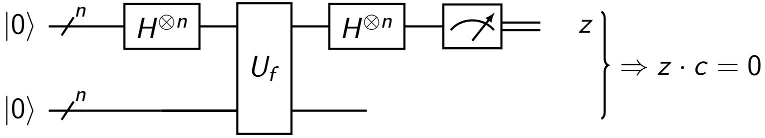
$$= \frac{(-1)^{x\cdot z}}{2^n}+\frac{(-1)^{x\cdot z\oplus c\cdot z}}{2^n}$$

$$= \frac{(-1)^{x\cdot z}}{2^n}+\frac{(-1)^{x\cdot z}(-1)^{c\cdot z}}{2^n}$$

$$= \begin{cases} 0 & \text{se } c\cdot z = 1 \\ \pm\frac{2}{2^n} & \text{se } c\cdot z = 0 \end{cases}$$

Algoritmo de Simon

Parte quântica



Algoritmo de Simon

- Obtenha $z_0, \cdots, z_{n-1}$ strings binários diferentes executando a parte quântica do algoritmo de Simon.
- Resolva o sistema com incognitas $c = c_0, \ldots, c_{n-1}$.

$$\left\{\begin{array}{ccccccc} z_0[0] \cdot c_0 & \oplus & \cdots & \oplus & z_0[n-1] \cdot c_{n-1} & = 0 \\ \vdots & & \vdots & & \vdots & \vdots \\ z_{n-1}[0] \cdot c_0 & \oplus & \cdots & \oplus & z_{n-1}[n-1] \cdot c_{n-1} & = 0 \end{array}\right.$$