Informatique quantique IFT6155

Complexité de la communication

Combien de bits dans un qubit?

Théorème:
L'intrication ne peut être utilisée pour transmettre un message classique ou pour le comprimer.

Théorème [Holevo 73]:
Pas plus de n bits d'information ne peuvent être transmis par un message de n qubits si les participants ne partagent pas d'intrication.

Théorème [Cleve, van Dam, Nielsen, Tapp]:
Même avec un canal quantique bidirectionnel entre Alice et Bob, $\lceil n/2 \rceil$ qubits doivent être transmis par Alice pour transmettre n bits d'information classique à Bob.

Resources

1. Communication classique
2. Communication quantique
3. Intrication
4. Tolérance à l'erreur
5. Bits aléatoires en commun
6. Promesse

Complexité de la communication

Toutes les communications classiques sont des *broadcasts*.
Toutes les communications quantiques sont deux à deux.
La complexité est toujours définie pour les pires données.
Le domaine de la fonction peut satisfaire une promesse.
Tous les participants doivent apprendre f (ou une chaîne y).
Un bit est un cas particulier d'un qubit.

- $C(f)$: Nombre minimal de bits communiqués pour calculer f avec certitude.
- $R(f)$: Nombre minimal de bits communiqués pour calculer f avec probabilité $1/2$.
- $Q(f)$: Nombre minimal de qubits communiqués pour calculer f avec certitude.
- $C^*(f)$: Nombre minimal de bits communiqués pour calculer f si les participants partagent de l'intrication.
- $Q^*(f)$: Nombre minimal de qubits communiqués pour calculer f si les participants partagent de l'intrication.
- $RQ(f)$: Nombre minimal de qubits communiqués pour calculer f avec probabilité $1/2$.

Complexité de la communication

Nous pouvons tout de suite faire les observations suivantes.

Clairement nous avons que pour tout f

$$R(f) \leq C(f) \qquad C^*(f) \leq C(f) \qquad Q(f) \leq C(f)$$

$$Q^*(f) \leq Q(f) \qquad RQ(f) \leq Q(f) \qquad RQ(f) \leq R(f)$$

puisqu'un protocole dans la classe de droite des inégalités est aussi un protocole dans la classe de gauche.

Puisque la communication d'un qubit peut être remplacée par l'utilisation d'un ebit plus deux bits de communication classique, on obtient que

$$C^*(f) \leq 2Q(f)$$

À cause du codage dense, qui permet la transmission de 2 bits en utilisant un ebit et un qubit de communication, on obtient

$$2Q^*(f, f) \leq C(f, f)$$

Égalité déterministe

Soit f une fonction à deux entrées de n bits définie par

$$x = y \Rightarrow f(x, y) = 1 \qquad x \neq y \Rightarrow f(x, y) = 0$$

.

Clairement

$$C(f) \leq n + 1$$

puisqu'Alice peut transmettre x à Bob, qui calcule la fonction et transmet la réponse à Alice.

En fait on peut montrer que

$$C(f) = n + 1$$

puisqu'il est impossible de faire mieux.

Qu'en est-il si Alice et Bob partagent des chaines de bits aléatoires préalablement?

Égalité probabiliste

Supposons qu'Alice et Bob partagent une chaine aléatoire uniformément distribuée z de n bits.

Si $x = y$ alors forcément $z \cdot x = z \cdot y$.

Par contre si $x \neq y$ on a que $(z \cdot x) \oplus (z \cdot y) = (z \cdot (x \oplus y)) = z \cdot v$ avec $v \neq 0$. Nous avons déjà démontré qu'exactement la moitié des z sont tels que $z \cdot v = 1$ et avec une chance sur deux $(z \cdot x) \oplus (z \cdot y) = 1$ auquel cas on sait que $x \neq y$.

Clairement $R(f) = 2$.

Alice calcule $z \cdot x$ et le transmet à Bob puis Bob calcule $z \cdot y$ et le transmet à Alice; si les deux valeurs sont égales il répond que $f(x, y) = 1$, sinon $f(x, y) = 0$.

Peu importe l'entrée leur probabilité de succès est au moins 1/2.

Nous avons donc un exemple où

$$\boxed{C(f) = n + 1 \qquad R(f) = 2}$$

Naissance d'un domaine de recherche

Le premier résultat obtenu en complexité de la communication quantique a été obtenu par R. Cleve et H. Buhrman en 1997. Ce fut la naissance d'un domaine de recherche. Voici un exemple obtenu à la même époque par Cleve, Buhrman et van Dam.

Protocole à trois participants.

Alice reçoit $x = x_1x_0 \in \{00, 01, 10, 11\} = \{0, 1, 2, 3\}$
Bob reçoit $y = y_1y_0 \in \{00, 01, 10, 11\} = \{0, 1, 2, 3\}$
Charlie reçoit $z = z_1z_0 \in \{00, 01, 10, 11\} = \{0, 1, 2, 3\}$
avec la promesse que $x + y + z = 0 \ mod \ 2$.

Ils veulent apprendre

$$f(x, y, z) \ = \ \frac{x + y + z \ mod \ 4}{2} \ = \ (x_0 \vee y_0 \vee z_0) \oplus (x_1 \oplus y_1 \oplus z_1)$$

qui ne peut prendre que les valeurs 0 et 1 à cause de la promesse.

$$\boxed{C(f) = 4 \qquad C^*(f) = 3}$$

$C(f) = 4$

Pour montrer que $C(f) \leq 4$ considérons le protocole suivant. Bob transmet y_0 et y_1, Charlie transmet $z_0 \oplus z_1$ ce qui permet à Alice de déduire z_0 et z_1 et donc de calculer $f(x, y, z)$, qu'elle transmet.

Il est plus ardu de démontrer que $C(f) \geq 4$. Supposons que $C(f) = 3$ et qu'Alice est la dernière à parler. Alice peut donc apprendre le résultat avec la communication de deux bits par Bob et Charlie. Ils doivent donc transmettre chacun un bit. On peut, par une recherche exhaustive, montrer que c'est impossible.

$C^*(f) = 3$

Clairement $C^*(f) \geq 3$, chaque participant doit transmettre au moins un bit d'information puisque f dépend de toutes les données.

Les participants partagent

$$|\psi\rangle = \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$

Si $x_0 = 1$, Alice applique H, puis Alice mesure a et transmet $a \oplus x_1$.
Si $y_0 = 1$, Bob applique H, puis Bob mesure b et transmet $b \oplus y_1$.
Si $z_0 = 1$, Charlie applique H, puis Charlie mesure c et transmet $c \oplus z_1$.
On remarque que $a \oplus b \oplus c = x_0 \vee y_0 \vee z_0$ puisque

$$\begin{aligned}
I \otimes I \otimes I|\psi\rangle &= \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle) \\
I \otimes H \otimes H|\psi\rangle &= \frac{1}{2}(|001\rangle + |010\rangle - |100\rangle + |111\rangle) \\
H \otimes I \otimes H|\psi\rangle &= \frac{1}{2}(|001\rangle - |010\rangle + |100\rangle + |111\rangle) \\
H \otimes H \otimes I|\psi\rangle &= \frac{1}{2}(-|001\rangle + |010\rangle + |100\rangle + |111\rangle)
\end{aligned}$$

$$\begin{aligned}
(a \oplus x_1) \oplus (b \oplus y_1) \oplus (c \oplus z_1) &= (a \oplus b \oplus c) \oplus (x_1 \oplus y_1 \oplus z_1) \\
&= (x_0 \vee y_0 \vee z_0) \oplus (x_1 \oplus y_1 \oplus z_1) \\
&= f(x, y, z)
\end{aligned}$$

Première séparation non constante

La première séparation non constante a été obtenue aussi en 1997 par Buhrman, van Dam, Hoyer et Tapp.

Le problème met en scène k participants. C'est un problème avec une promesse qui peut aussi être vue comme une relation.

Chaque joueur i reçoit la donnée $x^{(i)} \in \{0 \ldots 2^n - 1\}$ avec la promesse que

$$\sum_{i=1}^{k} x^{(i)} \equiv 0 \text{ mod } 2^{n-1}$$

et ils veulent calculer

$$f(x^{(1)}, \cdots, x^{(k)}) \;=\; \left(\frac{1}{2^{n-1}}\right) \sum_{i=1}^{k} x^{(i)} \text{ mod } 2^{n}$$

$$\boxed{C(f) \simeq k \log(k) \qquad C^*(f) = k}$$

Version schématique

$$
\begin{array}{cccccc}
 & x_1^{(1)} & x_2^{(1)} & \dots & x_n^{(1)} \\
+ & x_1^{(2)} & x_2^{(2)} & \dots & x_n^{(2)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
+ & x_1^{(k)} & x_2^{(k)} & \dots & x_n^{(k)} \\
\hline
? \ \dots \ ? & f & 0 & \dots & 0
\end{array}
$$

Pour $k \geq \log n$, en utilisant des techniques combinatoires et algébriques, nous avons démontré que

$$\boxed{C(f) \ \simeq \ k \log(k)}$$

États de Shrodinger

La solution quantique au problème met à profit des propriétés de l'état de Schrödinger.

$$M_k^+ = \frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle)$$

$$M_k^- = \frac{1}{\sqrt{2}}(|00\ldots0\rangle - |11\ldots1\rangle)$$

$$\begin{aligned}
HM_1^+ &= H\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |0\rangle \\
HM_1^- &= H\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |1\rangle \\
H^{\otimes 2}M_2^+ &= H^{\otimes 2}\frac{1}{\sqrt{2}}(|00\rangle) + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle) + |11\rangle \\
H^{\otimes 2}M_2^- &= H^{\otimes 2}\frac{1}{\sqrt{2}}(|00\rangle) - |11\rangle = \frac{1}{\sqrt{2}}(|01\rangle) + |10\rangle) \\
H^{\otimes 3}M_3^+ &= H^{\otimes 3}\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = (1/2)(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\
H^{\otimes 3}M_3^- &= H^{\otimes 3}\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) = (1/2)(|001\rangle + |010\rangle + |100\rangle + |111\rangle)
\end{aligned}$$

États de Schrödinger

$$M_k^+ = \frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle) \qquad H^{\otimes k}|x\rangle = \frac{1}{\sqrt{2^k}}\left(\sum_{y=0}^{2^k-1}(-1)^{x\cdot y}|y\rangle\right)$$

$$x\cdot y = x_1y_1 + x_2y_2\cdots + x_ny_n \ mod\ 2, \quad P(x) = x_1 + x_2 + \cdots x_n \ mod\ 2, \quad x\cdot 11\ldots1 = P(x)$$

$$\begin{aligned}
H^{\otimes k}M_k^+ &= H^{\otimes k}\frac{1}{\sqrt{2}}(|00\ldots0\rangle + |1\ldots1\rangle) \\
&= \frac{1}{\sqrt{2}}\left(H^{\otimes k}|00\ldots0\rangle + H^{\otimes k}|1\ldots1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^k}}\sum_{y=0}^{2^k-1}(-1)^{0\cdot y}|y\rangle + \frac{1}{\sqrt{2^k}}\sum_{y=0}^{2^k-1}(-1)^{1\ldots1\cdot y}|y\rangle\right) \\
&= \frac{1}{\sqrt{2^{k+1}}}\left(\sum_{y=0}^{2^k-1}|y\rangle + \sum_{y=0}^{2^k-1}(-1)^{P(y)}|y\rangle\right) \\
&= \frac{1}{\sqrt{2^{k+1}}}\left(\sum_{y=0}^{2^k-1}(1+(-1)^{P(y)})|y\rangle\right) = \frac{1}{\sqrt{2^{k-1}}}\left(\sum_{y=0,2^k-1,P(y)=0}|y\rangle\right)
\end{aligned}$$

États de Shrödinger

$$M_k^- = \frac{1}{\sqrt{2}}(|00\ldots0\rangle - |11\ldots1\rangle) \qquad H^{\otimes k}|x\rangle = \frac{1}{\sqrt{2^k}}\left(\sum_{y=0}^{2^k-1}(-1)^{x\cdot y}|y\rangle\right)$$

$$x\cdot y = x_1y_1 + x_2y_2\cdots + x_ny_n \ mod\ 2, \quad P(x) = x_1 + x_2 + \cdots x_n \ mod\ 2, \quad x\cdot 11\ldots1 = P(x)$$

$$\begin{aligned}
H^{\otimes k}M_k^- &= H^{\otimes k}\frac{1}{\sqrt{2}}(|00\ldots0\rangle - |1\ldots1\rangle) \\
&= \frac{1}{\sqrt{2}}\left(H^{\otimes k}|00\ldots0\rangle - H^{\otimes k}|1\ldots1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^k}}\sum_{y=0}^{2^k-1}(-1)^{0\cdot y}|y\rangle - \frac{1}{\sqrt{2^k}}\sum_{y=0}^{2^k-1}(-1)^{1\ldots1\cdot y}|y\rangle\right) \\
&= \frac{1}{\sqrt{2^{k+1}}}\left(\sum_{y=0}^{2^k-1}|y\rangle - \sum_{y=0}^{2^k-1}(-1)^{P(y)}|y\rangle\right) \\
&= \frac{1}{\sqrt{2^{k+1}}}\left(\sum_{y=0}^{2^k-1}(1-(-1)^{P(y)})|y\rangle\right) = \frac{1}{\sqrt{2^{k-1}}}\left(\sum_{y=0,2^k-1,P(y)=1}|y\rangle\right)
\end{aligned}$$

État de Schrödinger

$$S_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

$$(I_{2^{n-1}} \otimes S_\theta \otimes I_{2^{k-n}}) M_k^+ \;=\; \frac{1}{\sqrt{2}} \left(|00\ldots0\rangle + e^{i\theta} |11\ldots1\rangle \right)$$

$$(S_{\theta_1} \otimes \cdots \otimes S_{\theta_k}) M_k^+ = (S_{(\theta_1 + \cdots + \theta_k)} \otimes I_{2^{k-1}}) M_k = \frac{1}{\sqrt{2}} \left(|00\ldots0\rangle + e^{i\theta} |11\ldots1\rangle \right)$$

$$(S_\pi \otimes I_{2^{k-1}}) M_k^+ = M_k^-$$

Si $\sum \theta_i = q\pi$ pour q pair, alors

$$(H^{\otimes k})(S_{\theta_1} \otimes \cdots \otimes S_{\theta_k}) M_k = \frac{1}{\sqrt{2^{n-1}}} \sum_{P(i)=0} |i\rangle$$

et si $\sum \theta_i = q\pi$ pour q impair, alors

$$(H^{\otimes k})(S_{\theta_1} \otimes \cdots \otimes S_{\theta_k}) M_k = \frac{1}{\sqrt{2^{n-1}}} \sum_{P(i)=1} |i\rangle$$

Protocole avec intrication

Les participants partagent un état de Schrödinger.

- Chaque participant i
  - $\theta_i = \frac{2\pi x^{(i)}}{2^n}$
  - applique S_{θ_i} sur son qubit
  - applique H sur son qubit
  - mesure le qubit et obtient r_i
  - transmet r_i
- Les participants calculent

$$f(x^{(1)}, \ldots, x^{(k)}) = \sum r_i \pmod 2.$$

Analyse

On peut facilement vérifier que si

$$\left(\frac{1}{2^{n-1}}\right)\sum_{i=1}^{k} x^{(i)} = 0 \text{ (mod } 2^{\text{n}})$$

alors

$$\sum \theta_i = q\pi \text{ avec } q \text{ pair}$$

et si

$$\left(\frac{1}{2^{n-1}}\right)\sum_{i=1}^{k} x^{(i)} = 1 \text{ (mod } 2^{\text{n}})$$

alors

$$\sum \theta_i = q\pi \quad \text{avec } q \text{ impair}$$

et donc le protocole est correct.

Séparation exponentielle

Buhrman, Cleve et Wigderson ont introduit la première fonction f à deux participants pour laquelle

$$C(f) \in \Omega(n) \qquad Q(f) \in O(\log(n))$$

Il sagit d'une version en complexité de la communication du problème de Deutsch-Josza.

Deutsch-Josza distribué

Alice reçoit x (n bits)
Bob reçoit y (n bits)
tels que $D(x, y) = 0$ ou $D(x, y) = n/2$.

On définit f par $f(x, y) = 0$ si $x = y$ et $f(x, y) = 1$ si $x \neq y$.

Sans perte de généralité nous considérons que n est une puissance de deux.

Il est particulièrement difficile, mais possible, de montrer que

$$\boxed{C(f) \in \Theta(n)}$$

Avec communication quantique

Alice construit

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle$$

puis Alice applique U_A où

$$U_A|i\rangle = (-1)^{x_i}|i\rangle.$$

Alice transmet le registre à Bob.
Bob applique U_B où

$$U_B|i\rangle = (-1)^{y_i}|i\rangle.$$

Bob applique H sur chaque qubit et mesure pour obtenir $|j\rangle$. S'il obtient $j = 0$, alors $f(x, y) = 0$ et s'il obtient $j \neq 0$ alors $f(x, y) = 1$. Bob transmet le résultat à Alice.

Soit $z = x \oplus y$ alors $f(x, y) = 0$ ssi $z = 0$, constant, et $f(x, y) = 1$ ssi z est balancé.
On note aussi que $U = U_B U_A$ tel que $U|i\rangle = (-1)^{z_i}|i\rangle$.

Par la preuve de l'algorithme de Deutsch-Josza on obtient que Bob va mesurer 0 ssi $z = 0$.

$$\boxed{Q(f) \leq \log(n) + 1 \qquad C^*(f) \leq \log(n) + 1}$$

Une réduction étrange

Produit interne (IP)

$IP(x, y) = x_1y_1 + x_2y_2 + \cdots + x_ny_n$ (mod 2)

$C(IP) = n + 1$

Une question naturelle:
L'intrication ou la communication quantique peuvent-elles nous aider à calculer IP?

Protocole propre

Un protocole qui calcule $f(x, y)$ est *clean* si, lorsqu'exécuté sur l'état initial,

$$\underbrace{|z\rangle|x_1, \ldots, x_n\rangle|0 \ldots 0\rangle|\varphi_{AB}\rangle}_{\text{qubits d'Alice}}\underbrace{|y_1, \ldots, y_n\rangle|0 \ldots 0\rangle}_{\text{qubits de Bob}}$$

le protocole se termine dans l'état

$$\underbrace{|z \oplus f(x, y)\rangle|x_1, \ldots, x_n\rangle|0 \ldots 0\rangle|\varphi_{AB}\rangle}_{\text{qubits d'Alice}}\underbrace{|y_1, \ldots, y_n\rangle|0 \ldots 0\rangle}_{\text{qubits de Bob}}$$

Protocole propre

Lemme 1:
Soit P un protocole qui calcule f exactement. Soit $m_{ab}(P)$ la quantité de communication d'Alice vers Bob et $m_{ba}(P)$ la quantité de communication de Bob vers Alice. Il existe toujours un protocole *propre* P' tel que $m_{ab}(P') = m_{ba}(P') = m_{ab}(P) + m_{ba}(P)$.

Preuve
On peut rendre le protocole complètement unitaire.

À la fin du protocole, comme la réponse est déterministe elle doit être en produit avec le reste de l'état global.

On peut copier la réponse (elle est classique) et défaire (refaire à l'envers) le protocole.

Le protocole obtenu est propre.

QED

Protocole propre

Un protocole P qui calcule $f(x, y)$.

L'état initial est

$$\underbrace{|z\rangle|0\rangle|x_1, \ldots, x_n\rangle|0 \ldots 0\rangle}_{\text{qubits d'Alice}}\underbrace{|\varphi_{AB}\rangle|y_1, \ldots, y_n\rangle|0 \ldots 0\rangle}_{\text{qubits de Bob}}$$

après l'exécution du protocole on est dans l'état

$$\underbrace{|z\rangle|f(x, y)\rangle|\psi}_{\text{A}}\underbrace{_{AB}\rangle}_{\text{B}}$$

on copie la réponse:

$$\underbrace{|z \oplus f(x, y)\rangle|f(x, y)\rangle|\psi}_{\text{A}}\underbrace{_{AB}\rangle}_{\text{B}}$$

puis on refait le protocole à l'envers:

$$\underbrace{|z \oplus f(x, y)\rangle|x_1, \ldots, x_n\rangle|0 \ldots 0\rangle}_{\text{qubits d'Alice}}\underbrace{|\varphi_{AB}\rangle|y_1, \ldots, y_n\rangle|0 \ldots 0\rangle}_{\text{qubits de Bob}}$$

Réduction

Lemme 2:
Un protocole *propre* P qui calcule $IP(x, y)$ peut être utilisé pour transmettre n bits de Bob vers Alice, même si le protocole est donné comme une boîte noire.

Preuve

$$H^{\otimes n}|x_1, \ldots, x_n\rangle = \sum_{y_1,\ldots,y_n \in \{0,1\}} (-1)^{IP(x,y)} |y_1, \ldots, y_n\rangle$$

Alice exécute le protocole avec $|z\rangle = H|1\rangle$ et $|x\rangle = H^{\otimes n}|0\rangle$ et Bob avec $|y\rangle$.

Alice et Bob exécutent le protocole propre.

Alice mesure son registre de données et obtient $|y\rangle$.

Réduction

Preuve (Suite)
Regardons la partie du système appartenant à Alice

$$H^{\otimes n+1}|1\rangle|0,\ldots,0\rangle$$

$$\sum_{z,x_1,\ldots,x_n\in\{0,1\}} (-1)^z|z\rangle|x_1,\ldots,x_n\rangle$$

Alice et Bob exécutent le protocole propre pour IP

$$\sum_{z,x_1,\ldots,x_n\in\{0,1\}} (-1)^z|z+x_1y_1+\cdots+x_ny_n\rangle|x_1,\ldots,x_n\rangle$$

on remplace $c = z+x_1y_1+\cdots+x_ny_n$

$$\sum_{c,x_1,\ldots,x_n\in\{0,1\}} (-1)^{c+x_1y_1\oplus\cdots\oplus x_ny_n}|c\rangle|x_1,\ldots,x_n\rangle$$

Alice applique

$$|1\rangle|y_1,\ldots,y_n\rangle$$

CQFD

IP avec communication quantique et intrication

Théorème:

$$Q^*(IP) = \lceil n/2 \rceil$$

Preuve:
Soit P un protocole optimal qui calcule exactement $IP(x, y)$, i.e.
$Q^*(IP) = m_{ab}(P) + m_{ba}(P)$.

Par le **lemme 1**, il existe un protocole propre P' tel que

$$m_{ab}(P') = m_{ba}(P') = m_{ab}(P) + m_{ba}(P)$$

Par le **lemme 2**, le protocole P' peut être utilisé pour transmettre n bits de Bob vers Alice.

Par le **Théorème [CvDNT98]:** on doit avoir que
$Q^*(P) = m_{ab}(P) + m_{ba}(P) = m_{ba}(P') \geq \lceil n/2 \rceil$.

QED

Séparation pour une fonction totale

Supposons qu'Alice et Bob ont un horaire avec n possibilités de rendez-vous. Comment peuvent-ils déterminer un moment où ils sont tous les deux libres avec le moins de communication possible?

$$f(x,y) = 0 \text{ si } x_1y_1 + x_2y_2 + \cdots + x_ny_n = 0$$

$$f(x,y) = 1 \text{ si } x_1y_1 + x_2y_2 + \cdots + x_ny_n \geq 0$$

On peut démontrer que, classiquement, même un algorithme probabiliste nécessite une quantité linéaire de communication.

$$R(f) \in \Theta(n)$$

Nous allons montrer que

$$RQ(f) \in O(\sqrt{n}\log(n))$$

Intuitivement, pour calculer $f(x,y)$ Alice et Bob veulent trouver i tel que $x_iy_i = 1$.

Ceci ressemble beaucoup à Grover!

f et Grover

Soit z tel que $z_i = x_i y_i$. Clairement, Alice et Bob cherchent i tel que $z_i = 1$.

Pour réaliser Grover, ils doivent avoir un registre de $\log(n)$ qubits.

Il doivent pouvoir faire S_0, H, mais surtout G_z.

$$G_z|i\rangle = (-1)^{z_i}|i\rangle$$

Alice peut initialiser un registre à $H^{\otimes \log(n)}|0\rangle$, elle peut réaliser S_0 et H, mais comment réaliser G_z?

G_z

Soit un registre de $\log(n)+1$ qubits dans l'état

$$\sum \alpha_i |i\rangle.$$

Alice et Bob veulent effectuer la transformation

$$U \sum \alpha_i |i\rangle = \sum \alpha_i (-1)^{z_i} |i\rangle$$

. Pour ce faire, Alice transmet le registre à Bob ($\log(n)$ qubits).

Bob ajoute un bit ancillaire $|0\rangle$ et obtient

$$\sum \alpha_i |i\rangle |0\rangle$$

, puis il applique la transformation suivante:

$$U_B |i\rangle |b\rangle = |i\rangle |y_i \oplus b\rangle$$

. Le registre se trouve dans l'état

$$\sum \alpha_i |i\rangle |y_i\rangle.$$

Bob transmet le registre à Alice ($\log(n)+1$ qubits).

G_z

Alice effectue la transformation

$$U_A|i\rangle|b\rangle = (-1)^{x_i b}|i\rangle|b\rangle$$

; le registre se retrouve donc dans l'état

$$\sum \alpha_i (-1)^{x_i y_i}|i\rangle|y_i\rangle = \sum \alpha_i (-1)^{z_i}|i\rangle|y_i\rangle.$$

Alice transmet le registre à Bob ($\log(n)+1$ qubits).
Bob effectue une deuxième fois U_B et obtient

$$\sum \alpha_i (-1)^{z_i}|i\rangle|y_i \oplus y_i\rangle = \sum \alpha_i (-1)^{z_i}|i\rangle|0\rangle.$$

Bob se débarasse de l'ancille ($|0\rangle$) et renvoie le registre à Alice.

Le registre se trouve donc dans l'état

$$\sum \alpha_i (-1)^{z_i}|i\rangle|0\rangle.$$

, ce qui est bel et bien ce que l'on désire.

Le tout a nécessité $4\log(n)+2$ qubits de communication.

Pour calculer f, Alice va effectuer l'algorithme de Grover, qui nécessite $O(\sqrt{n})$ itérations. Chaque itération nécessite $4\log(n)+2$ qubit de communication donc

$$RQ(f) \in O(\sqrt{n}\log(n))$$

Références

Gilles Brassard, Richard Cleve and Alain Tapp, The cost of exactly simulating quantum entanglement with classical communication, Physical Review Letter, vol. 83(9), August 1999, pp.1874-1878. (quant-ph/9901035)

Wim van Dam, Peter Høyer and Alain Tapp, Multiparty Quantum Communication Complexity, Physical Review A, vol. 60(4), Oct. 1999, pp.2737-2741. (quant-ph/9710054)

Richard Cleve, Wim van Dam, Michael Nielsen and Alain Tapp, Quantum Entanglement and the Communication Complexity of the Inner Product Function, Quantum computing and quantum communication: First NASA International Conference (QCQC'98). Springer-Verlag, LNCS, vol.1509, Feb. 1998, pp.61-74. (quant-ph/9708019).