Devoir 3 IFT 6155 H2009

Question 1

Donnez un circuit qui effectue la transformation S_0 de l'itération de Grover. Vous pouvez utiliser les portes à 1, 2 et 3 qubits que nous avons vues dans le cours. Les bits ancillaires (bits de calcul) doivent être initialisés à $|0\rangle$ au début et doivent retrouver la valeur $|0\rangle$ à la fin de la transformation.

Question 2

Dans l'algorithme de Grover, qu'arrive-t-il quand $t = N/4$, c'est-à-dire qu'exactement $1/4$ des éléments du domaine sont des solutions?

Question 3

Supposons que nous arrivions à construire un ordinateur quantique, mais que sa vitesse d'horloge soit particulièrement lente. Si pour une fonction $f : \{0,1\}^n \to \{0,1\}$ donnée, un ordinateur classique effectue le calcul de f un million de fois plus vite qu'une évaluation de f sur l'ordinateur quantique, à partir de quelle taille d'input (n) l'algorithme de Grover est-il plus rapide que la recherche probabiliste classique? Vous pouvez faire une approximation du temps de calcul d'une itération de Grover par le temps de calcul quantique de f, et vous pouvez supposer qu'il n'y a qu'une solution.

Question 4

Supposons que vous ayez une fonction $f : \{0,1\}^n \to \{0,1\}^{n/2}$ (évidemment n est pair). Donnez un algorithme qui trouve (x_1, x_2) tel que $f(x_1) = f(x_2)$. Faites l'analyse de votre algorithme pour la pire fonction f possible.