Évaluation du potentiel des machines quantiques pour l'optimisation combinatoire

Julien Rodriguez
Encadrant : Éric Bourreau

Soutenance de stage
Master 2 Informatique Théorique

2 Juillet 2020

Introduction
- Contexte
- "Hello World" quantique

Algorithmique de recherche
- Algorithme de Grover
- 3-SAT

Optimisation Combinatoire
- Boite à outils
- VC (Vertex-Cover)
- TSP (Travelling Salesman problem)

Conclusion

Introduction
- Contexte
- "Hello World" quantique

Algorithmique de recherche
- Algorithme de Grover
- 3-SAT

Optimisation Combinatoire
- Boite à outils
- VC (Vertex-Cover)
- TSP (Travelling Salesman problem)

Conclusion

Contexte

- 1970-80 : Naissance de l'idée de créer des calculateurs quantiques [Richard Feynman, Paul Benioff, David Deutsch, Charles H. Bennett]
- 1994 : Factorisation en temps polynomiale [Peter Shor [3]]
- 1996 : Recherche dans une base non structurée en $O(\sqrt{2^n})$ [Lov Grover [2]]
- 1998 : Première machine à deux qubits [IBM]
- Aujourd'hui : Des machines allant de 5 à 53 qubits et des simulateurs de 32 qubits.

Contexte

- 1970-80 : Naissance de l'idée de créer des calculateurs quantiques [Richard Feynman, Paul Benioff, David Deutsch, Charles H. Bennett]
- 1994 : Factorisation en temps polynomiale [Peter Shor [3]]
- 1996 : Recherche dans une base non structurée en $O(\sqrt{2^n})$ [Lov Grover [2]]
- 1998 : Première machine à deux qubits [IBM]
- Aujourd'hui : Des machines allant de 5 à 53 qubits et des simulateurs de 32 qubits.

Contexte

- 1970-80 : Naissance de l'idée de créer des calculateurs quantiques [Richard Feynman, Paul Benioff, David Deutsch, Charles H. Bennett]
- 1994 : Factorisation en temps polynomiale [Peter Shor [3]]
- 1996 : Recherche dans une base non structurée en $O(\sqrt{2^n})$ [Lov Grover [2]]
- 1998 : Première machine à deux qubits [IBM]
- Aujourd'hui : Des machines allant de 5 à 53 qubits et des simulateurs de 32 qubits.

Contexte

- 1970-80 : Naissance de l'idée de créer des calculateurs quantiques [Richard Feynman, Paul Benioff, David Deutsch, Charles H. Bennett]
- 1994 : Factorisation en temps polynomiale [Peter Shor [3]]
- 1996 : Recherche dans une base non structurée en $O(\sqrt{2^n})$ [Lov Grover [2]]
- 1998 : Première machine à deux qubits [IBM]
- Aujourd'hui : Des machines allant de 5 à 53 qubits et des simulateurs de 32 qubits.

Contexte

- 1970-80 : Naissance de l'idée de créer des calculateurs quantiques [Richard Feynman, Paul Benioff, David Deutsch, Charles H. Bennett]
- 1994 : Factorisation en temps polynomiale [Peter Shor [3]]
- 1996 : Recherche dans une base non structurée en $O(\sqrt{2^n})$ [Lov Grover [2]]
- 1998 : Première machine à deux qubits [IBM]
- Aujourd'hui : Des machines allant de 5 à 53 qubits et des simulateurs de 32 qubits.

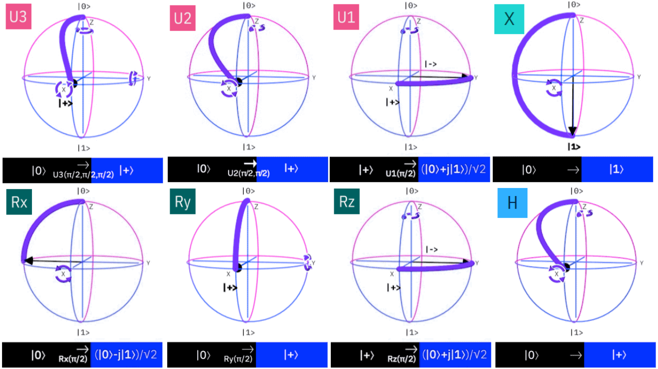
Introduction
Contexte
"Hello World" quantique

Algorithmique de recherche
Algorithme de Grover
3-SAT

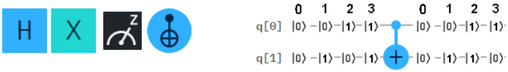
Optimisation Combinatoire
Boite à outils
VC (Vertex-Cover)
TSP (Travelling Salesman problem)

Conclusion

Opérations sur les qubits

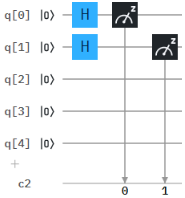


Portes quantiques

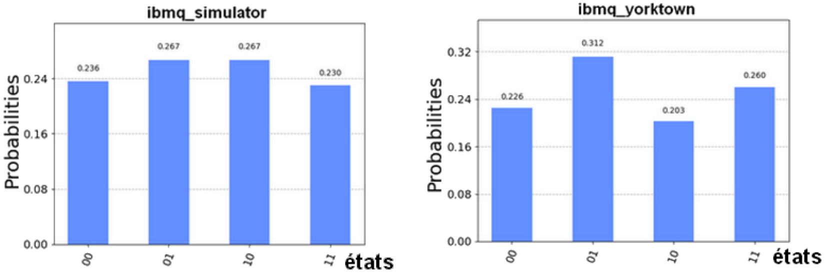


Les portes H, X, mesure et CX de droite à gauche

"Hello World" 1 : superposition

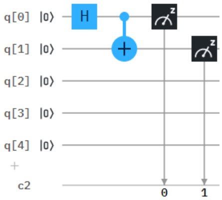


Circuit : superposition

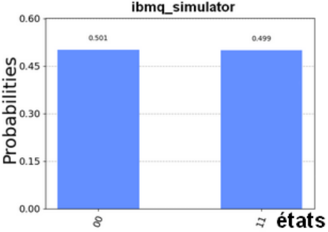


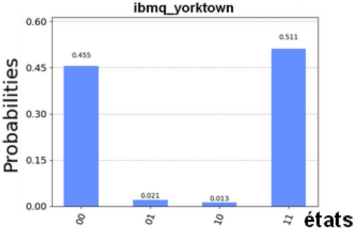
Résultats obtenus pour le circuit ci-dessus

"Hello World" 2 : intrication



Circuit : intrication





Résultats obtenus pour le circuit ci-dessus

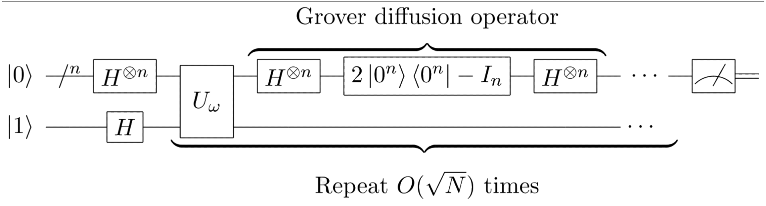
Introduction
- Contexte
- "Hello World" quantique

Algorithmique de recherche
- Algorithme de Grover
- 3-SAT

Optimisation Combinatoire
- Boite à outils
- VC (Vertex-Cover)
- TSP (Travelling Salesman problem)

Conclusion

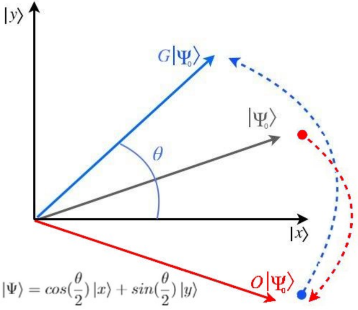
Recherche dans une base non structurée

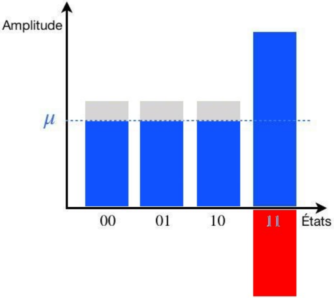


Algorithme de Grover

Recherche dans une base non structurée

- Initialisation : superposition des états : H^n
- Mettre en évidence la solution : XH $= \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- Révéler la solution





Révélation de la solution $|11\rangle$

Introduction
Contexte
"Hello World" quantique

Algorithmique de recherche
Algorithme de Grover
3-SAT

Optimisation Combinatoire
Boite à outils
VC (Vertex-Cover)
TSP (Travelling Salesman problem)

Conclusion

Rappels

- Une formule est sous forme normale conjonctive (CNF)
- Opérations nécessaires : $\neg$, $\wedge$ et $\vee$:

$$(x_0 \vee x_1) \equiv \neg(\neg x_0 \wedge \neg x_1)$$

- Exemple :
  $f = (x_0 \vee x_1 \vee \neg x_2) \wedge (\neg x_0 \vee \neg x_1 \vee \neg x_2) \wedge (\neg x_0 \vee x_1 \vee x_2)$
- Réécriture de la formule :
  $f = \neg(\neg x_0 \wedge \neg x_1 \wedge x_2) \wedge \neg(x_0 \wedge x_1 \wedge x_2) \wedge \neg(x_0 \wedge \neg x_1 \wedge \neg x_2)$

Rappels

- Une formule est sous forme normale conjonctive (CNF)
- Opérations nécessaires : $\neg$, $\wedge$ et $\vee$:

$$(x_0 \vee x_1) \equiv \neg(\neg x_0 \wedge \neg x_1)$$

- Exemple :
  $f = (x_0 \vee x_1 \vee \neg x_2) \wedge (\neg x_0 \vee \neg x_1 \vee \neg x_2) \wedge (\neg x_0 \vee x_1 \vee x_2)$
- Réécriture de la formule :
  $f = \neg(\neg x_0 \wedge \neg x_1 \wedge x_2) \wedge \neg(x_0 \wedge x_1 \wedge x_2) \wedge \neg(x_0 \wedge \neg x_1 \wedge \neg x_2)$

Rappels

- Une formule est sous forme normale conjonctive (CNF)
- Opérations nécessaires : $\neg$, $\wedge$ et $\vee$:

$$(x_0 \vee x_1) \equiv \neg(\neg x_0 \wedge \neg x_1)$$

- Exemple :
  $f = (x_0 \vee x_1 \vee \neg x_2) \wedge (\neg x_0 \vee \neg x_1 \vee \neg x_2) \wedge (\neg x_0 \vee x_1 \vee x_2)$
- Réécriture de la formule :
  $f = \neg(\neg x_0 \wedge \neg x_1 \wedge x_2) \wedge \neg(x_0 \wedge x_1 \wedge x_2) \wedge \neg(x_0 \wedge \neg x_1 \wedge \neg x_2)$

Rappels

- Une formule est sous forme normale conjonctive (CNF)
- Opérations nécessaires : $\neg$, $\wedge$ et $\vee$:

$$(x_0 \vee x_1) \equiv \neg(\neg x_0 \wedge \neg x_1)$$

- Exemple :
  $f = (x_0 \vee x_1 \vee \neg x_2) \wedge (\neg x_0 \vee \neg x_1 \vee \neg x_2) \wedge (\neg x_0 \vee x_1 \vee x_2)$
- Réécriture de la formule :
  $f = \neg(\neg x_0 \wedge \neg x_1 \wedge x_2) \wedge \neg(x_0 \wedge x_1 \wedge x_2) \wedge \neg(x_0 \wedge \neg x_1 \wedge \neg x_2)$

Circuit 3-SAT

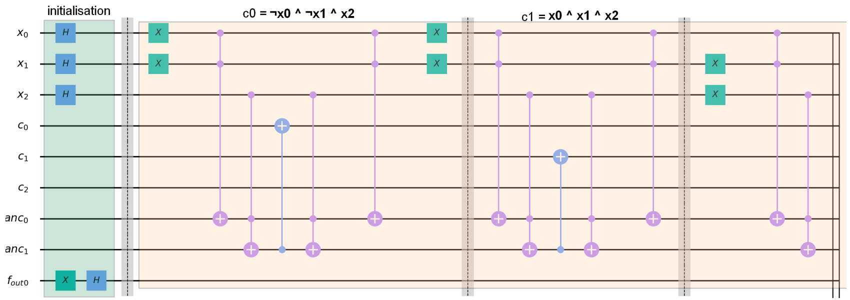


FIGURE – Première partie du circuit 3-SAT

Circuit 3-SAT

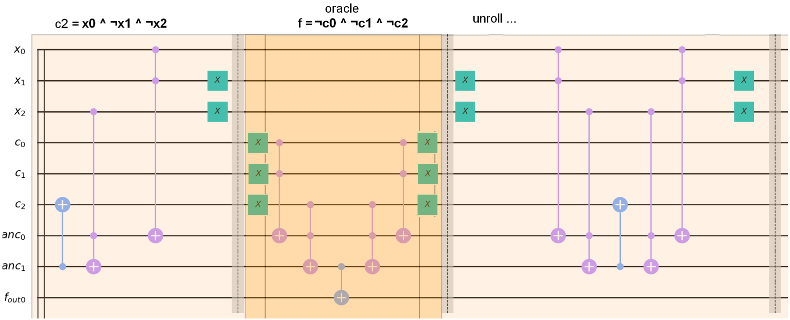


Figure – Deuxième partie du circuit 3-SAT

Circuit 3-SAT

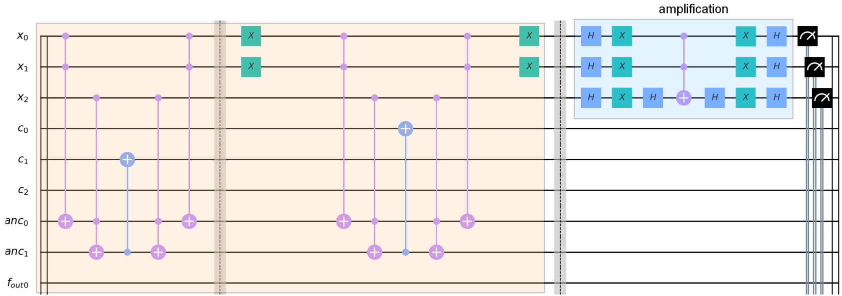
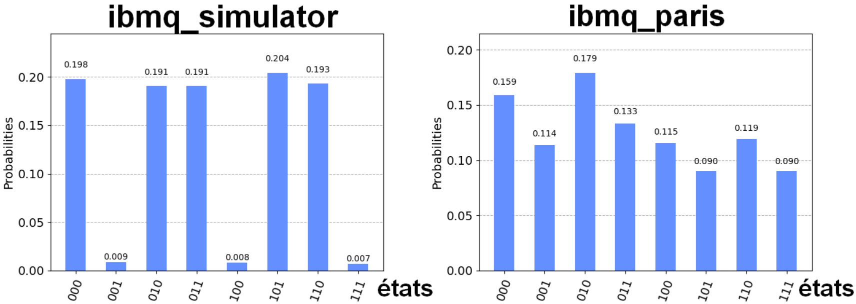


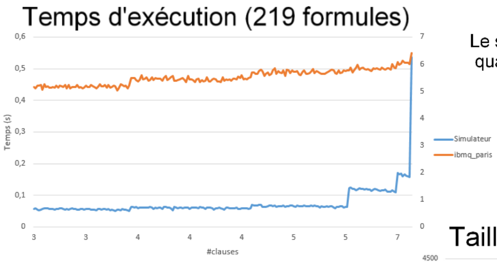
FIGURE – Troisième partie du circuit 3-SAT

Exécution et résultat du circuit



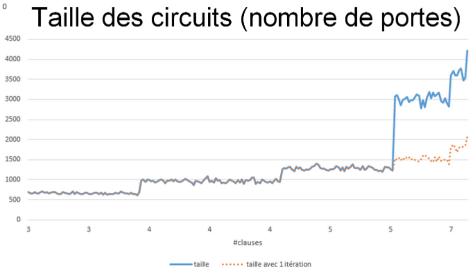
Résultats pour l'exécution du circuit 3-SAT présenté

Exécutions de formules 3-SAT



Le simulateur doit calculer tous les phénomènes quantiques.

La taille des circuits varie en fonction du nombre de clauses et du nombre d'itérations de l'algorithme de Grover.



Introduction
- Contexte
- "Hello World" quantique

Algorithmique de recherche
- Algorithme de Grover
- 3-SAT

Optimisation Combinatoire
- Boite à outils
- VC (Vertex-Cover)
- TSP (Travelling Salesman problem)

Conclusion

Circuits nécessaires

- Représenter les entiers
- Représentation de la structure : *clé* $\rightarrow$ *valeur*
- addition et soustraction
- $=, \neq, <, >$
- Min, Max, Somme, avec la recherche de Grover

Circuits nécessaires

- Représenter les entiers
- Représentation de la structure : *clé* $\rightarrow$ *valeur*
- addition et soustraction
- $=, \neq, <, >$
- Min, Max, Somme, avec la recherche de Grover

Circuits nécessaires

- Représenter les entiers
- Représentation de la structure : *clé* $\rightarrow$ *valeur*
- addition et soustraction
- $=, \neq, <, >$
- Min, Max, Somme, avec la recherche de Grover

Circuits nécessaires

- Représenter les entiers
- Représentation de la structure : *clé* $\rightarrow$ *valeur*
- addition et soustraction
- $=, \neq, <, >$
- Min, Max, Somme, avec la recherche de Grover

Circuits nécessaires

- Représenter les entiers
- Représentation de la structure : *clé* $\rightarrow$ *valeur*
- addition et soustraction
- $=, \neq, <, >$
- Min, Max, Somme, avec la recherche de Grover

Introduction
- Contexte
- "Hello World" quantique

Algorithmique de recherche
- Algorithme de Grover
- 3-SAT

Optimisation Combinatoire
- Boite à outils
- VC (Vertex-Cover)
- TSP (Travelling Salesman problem)

Conclusion

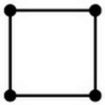
Couverture par sommets

Algorithme 4 : Oracle : couverture de cardinalité minimale

Input : circuit, $|nodes\rangle$, pour les sommets, $|aux\rangle$ pour les qubits auxiliaires, $|sum\rangle$ et $|carry\rangle$ pour la somme, $|k\rangle$ pour k, $|ancillas\rangle$, pour le registre d'ancillas, $G = (V, E)$ un graphe

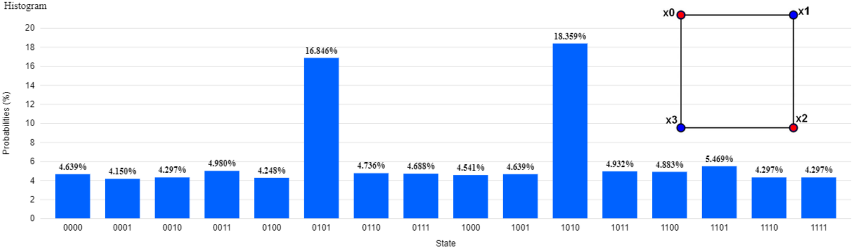
Out : circuit : Circuit quantique

clauses $\leftarrow$ []
pour chaque $v_i v_j \in E$ **faire**
  clauses.add($v_i \vee v_j$) //Satisfaire la clause $v_i \vee v_j$, revient à couvrir $v_i v_j$
fin
Oracle_SAT(circuit, clauses, $|aux\rangle$, $|ancillas\rangle$)
somme($|nodes\rangle$, $|sum\rangle$, $|carry\rangle$) // $\sum_{i=0}^{|V|} v_i$
inferieur_k($|sum\rangle$, $|k\rangle$, $|f_{out}\rangle$)
`Unroll circuit`
retourner circuit



C_4

Exemple : C_4



Exécution sur simulateur sur le graphe : C_4

Autres problèmes traités

- Couverture par sommet de poids minimal
- Coupe maximum dans un graphe
- Coloration de graphe

Autres problèmes traités

- Couverture par sommet de poids minimal
- Coupe maximum dans un graphe
- Coloration de graphe

Autres problèmes traités

- Couverture par sommet de poids minimal
- Coupe maximum dans un graphe
- Coloration de graphe

Introduction
Contexte
"Hello World" quantique

Algorithmique de recherche
Algorithme de Grover
3-SAT

Optimisation Combinatoire
Boite à outils
VC (Vertex-Cover)
TSP (Travelling Salesman problem)

Conclusion

Voyageur de commerce

- Algorithme pour résoudre le TSP en $O(n^2 2^n)$ [Bellman-Held-Karp [1]]
- Algorithme quantique pour résoudre le TSP en $O(n\sqrt{2^n})$
- Lorsque les machines seront fiables nous pourrons résoudre le TSP avec une accélération quadratique

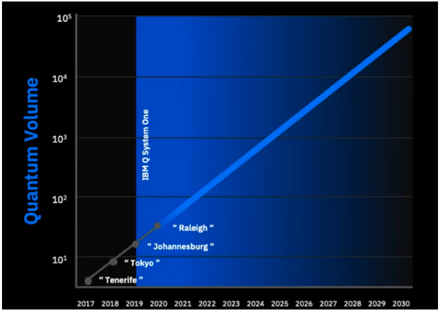
Introduction
- Contexte
- "Hello World" quantique

Algorithmique de recherche
- Algorithme de Grover
- 3-SAT

Optimisation Combinatoire
- Boite à outils
- VC (Vertex-Cover)
- TSP (Travelling Salesman problem)

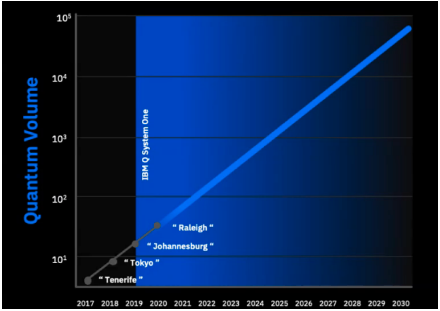
Conclusion

- Le schéma proposé par Grover fourni une accélération quadratique
- La superposition permet d'obtenir toutes les solutions avec une exécution
- La progression technique va rendre les machines plus performantes



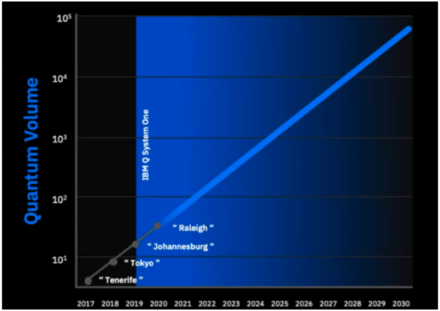
Prévision de l'évolution des machines par IBM

- Le schéma proposé par Grover fourni une accélération quadratique
- La superposition permet d'obtenir toutes les solutions avec une exécution
- La progression technique va rendre les machines plus performantes



Prévision de l'évolution des machines par IBM

- Le schéma proposé par Grover fourni une accélération quadratique
- La superposition permet d'obtenir toutes les solutions avec une exécution
- La progression technique va rendre les machines plus performantes

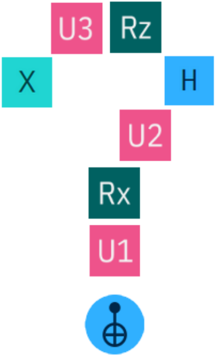


Prévision de l'évolution des machines par IBM

Conclusion

Merci pour votre attention !

Questions ?



Point d'interrogation avec des portes quantiques

Bibliographie

[1] Richard Bellman. Dynamic programming treatment of the travelling salesman problem. *J. ACM*, 9(1) :61–63, January 1962.

[2] Lov K. Grover. Quantum Computers Can Search Rapidly by Using Almost Any Transformation. 80(19) :4329–4332, May 1998.

[3] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5) :1484–1509, Oct 1997.