量子計算與資訊導論

期末專題

College of Electrical Engineering and Computer Science

National Taiwan University

Final project

Hamiltonian Cycle Problem based on Grover's Algorithm and its Application

課堂指導教授：管希聖 教授

學號：B08901136

系級：電機工程學系大學部二年級

姓名：劉承瀚

中華民國 110 年 6 月

June 2020

壹、 摘要

Hamiltonian Cycle Problem (HCP)屬於 NP-Complete 問題，本文由 Grover algorithm, Quantum Counting, Polynomial reduction to 3SAT(Boolean satisfiability problem), QUBO (quadratic unconstrained binary optimization)四種角度切入。在 Grover algorithm 部分提出 Rotation oracle 與 Counter oracle 兩種概念，並在 Qiskit 中實作來比較優劣；Quantum Counting 目的是為了找解的個數，可以視為 Grover algorithm 的前驅步驟，目的是找到 Grover operator 的特徵值；HCP 問題也可以轉換成 SAT、QUBO 等問題，來從不同角度切入並解決。

關鍵字：Grover Algorithm、Hamiltonian Cycle、Oracle、Quantum Counting

貳、 簡介

Hamiltonian Cycle Problem (HCP)是經典的 NP-Complete 問題，此問題想要在有向或無向圖中找到一條迴圈，沿著這迴圈行走就能正好走訪每個頂點一次再回到原始的出發點。而 NP-Complete 是一系列滿足以下兩種性質的問題：

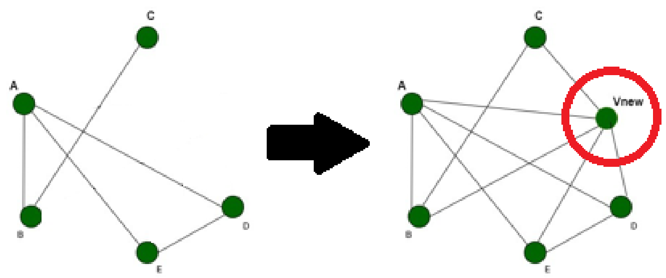
(1) 屬於 NP 的範疇，也就是能在多項式內驗證一組輸入是否是合法的解。

(2) $\exists Y \in NPC, Y \leq_P X$ (若 X 滿足此條件，則$X \in NP - hard$)，也就是已知有方法將另一個 NP-Complete 的問題在多項式時間內約化為此問題。

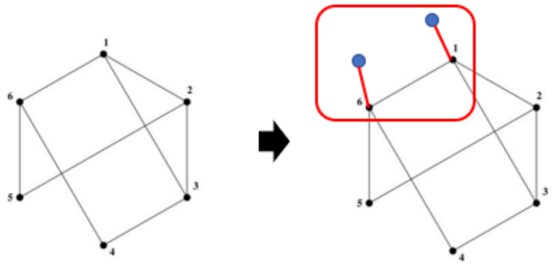
關於這兩種性質，我們可以以另一個 NPC 問題—Hamiltonian Path Problem(HPP)來說明。HPP 是想找到一條路徑，沿著此路徑能恰好走訪每個頂點一次，而此問題可以跟 HCP 互相約化，方法如下：

(1) $HPP \leq_P HCP$：加入一個額外的點 V_{new}，並讓其他點都與 V_{new} 相連，如此一來任何 HPP 問題可以視為由 V_{new} 出發的 HCP 問題。

(2) $HCP \leq_P HPP$：在原圖中找到兩個相鄰點 v 與 v'，分別增加點 s, t 且與 v, v' 相連，則任一條 HCP 可以視為從 s 到 t 的 HPP 問題。



圖一、$HPP \leq_P HCP$範例圖



圖二、$HCP \leq_P HPP$範例圖

因此在 NP-Complete 問題間可以互相在多項式時間內被約化，因此若是 HCP 在量子電腦中有在多項式時間內完成的演算法，則這系列的問題都能解決，因此我們期望運用量子運算的平行性來解決。

關於此問題，前人統整出了幾種可以努力的方向[1]，包含Grover algorithm, Quantum Counting, Polynomial reduction to 3SAT(Boolean satisfiability problem), Quantum walk, Adiabatic quantum computing, QUBO (quadratic unconstrained binary optimization)等方法，而我們目前的研究著重於Grover algorithm與Quantum Counting的實作，另外也會提及Polynomial reduction to 3SAT與QUBO的概念。

參、 研究內容

一、傳統演算法—以 Dynamic Programming 為例

在傳統演算法中，若是以窮舉法分別找出每一種頂點的排列是否為一條合法路徑的話，那麼時間複雜度將會是$O(V!)$；而用動態規劃(Dynamic Programming)[2]的方法，則能夠在空間複雜度為$O(V \times 2^V)$、時間複雜度為$O(V^2 \times 2^V)$下找到所有合法的 HP，其做法可以寫成以下形式：

$$HPP(S,\, j) \;= \bigcup_{k \in S} \left[HPP(S - \{j\}\,,\, k) \;\bigwedge \mathrm{adj}(k, j) \right]$$

其中，$HPP(S,j)$代表一條合法的哈密頓子路徑並以頂點V_j做為結尾，因此若是有另一條哈密頓子路徑$HPP(S-\{j\},k)$存在，且存在E_{kj}這一條邊，則$HPP(S,j)$也必然存在，因此在表格相應位置紀錄成 1；此外，也有論文[3]運用排容原理(inclusion-exclusion principle)與蒙地卡羅法(Monte Carlo algorithm)，讓時間複雜度降為$O(1.657^V)$。

二、Grover algorithm[4][10]

Grover algorithm 的精神在於能透過適當的 Oracle 將答案的相位進行反轉，之後再透過 Diffuser 將負相位沿著$|\psi\rangle$軸鏡向反轉，就能讓答案的相位振幅上

升，因此量測到解答的機率也隨之提升。而關於 Oracle 的部分會跟題目有關，而根據 HCP 我們找到了兩種 oracle，分別為 rotation oracle 與 counter oracle，而他們的運作原理同樣是在一條 HC 中，每個頂點都只會有兩條邊與之相連，以此找到可能的邊的組合並用 Grover 方法來放大振幅。

(一) Rotation oracle[7]

1. 設計架構

(1) 輸入為 vertex, edge, flag，其中 vertex 數目=V，edge 數目=E，flag 數目=1。初始化上將所有 edge qubits 都加上 Hardamard gate(H gate)，讓 edge qubits 處於疊加態而能夠平行化運算；flag qubit 會加上 X gate 與 H gate 使其變為$|-\rangle$。

(2) 我們以圖三為例來探討如何設計 Rotation Oracle。圖三是四個頂點五條邊的圖，而 oracle 的設計有分為 encoder, mcx-gate, relaxer 三個部分(圖四、圖五)。encoder 是利用 edge qubit 來調控 vertex qubit 的旋轉，比如 e0 的兩端點分別為 v0 與 v1，因此 e0 分別對 v0 與 v1 進行$RY(\pi/2)$的旋轉，而其他邊也是依此類推，如此形成 encoder 的部分，因此對於某頂點而言，若是有兩條邊被選取，則 vertex qubit 會從$|0\rangle$ 轉成$|1\rangle$，符合哈密頓路徑所需的條件。mcx_gate 的作用在於找出所有可能的解，並且將其相位反轉，因此在一條哈密頓路徑中，所有的 vertex qubit 都會轉成$|1\rangle$，mcx_gate 便會作用在 flag qubit，之後便會有 phase kickback 的效果。

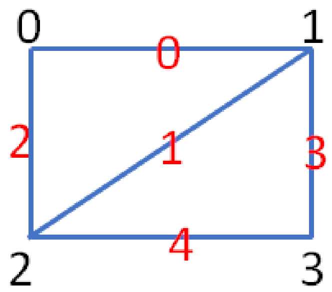
Phase kickback：

$$\begin{aligned}\mathrm{U\omega}|\mathrm{x}\rangle|-\rangle &= \mathrm{U\omega}|\mathrm{x}\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= |\mathrm{x}\rangle \otimes \frac{1}{\sqrt{2}}(|0 \oplus \mathrm{f(x)}\rangle - |1 \oplus \mathrm{f(x)}\rangle)\end{aligned}$$

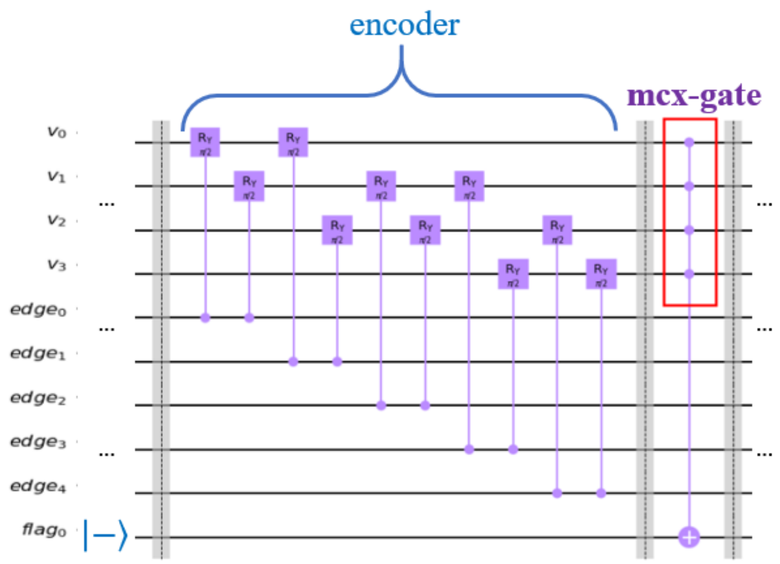
當 f(x)=1 時：

$$\begin{aligned}&= |\mathrm{x}\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \\ &= |\mathrm{x}\rangle \otimes \frac{-1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= -|\mathrm{x}\rangle|-\rangle\end{aligned}$$

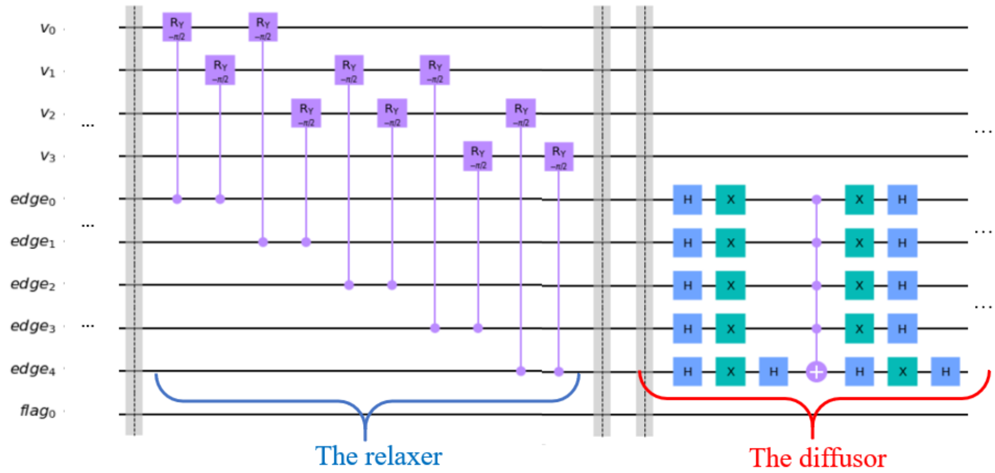
可以看出經由 phase kickback 後，vertex qubits 相位被反轉。而 relaxer 形式與 encoder 大致相同，差別在於邊對頂點旋轉$RY(-\pi/2)$，期望能夠將 vertex qubits 都轉回初始狀態$|0\rangle$，因此 Grover operator 才能反覆使用以得到最大振幅，然而 relaxer 的設計目前仍有缺陷，在之後會有更詳盡的討論；而 relaxer 尚有另一個功能，就是能夠將 vertex qubits 的負相位資訊傳遞給 edge qubits，之後 edge qubits 再代入 Diffuser 中來進行相位放大。



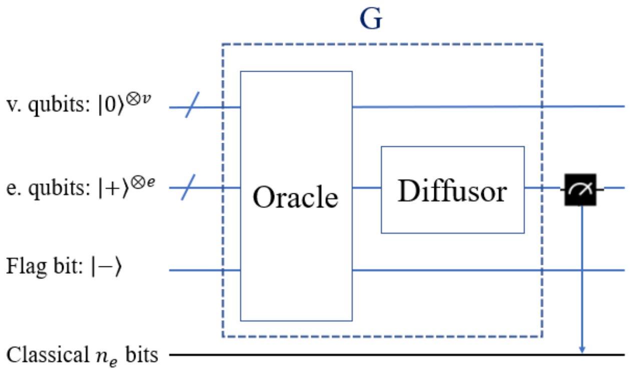
圖三、含有四個頂點五條邊的圖



圖四、Grover Algorithm 的 Rotation Oracle (front)



圖五、Grover Algorithm 的 Rotation Oracle (back)



圖六、Grover Algorithm 整體架構

(3) Diffuser 的設計形式為$H^{\otimes n}X^{\otimes n}(MCZ)X^{\otimes n}H^{\otimes n}$，它也可以寫成

$$D = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = (2|\psi\rangle\langle\psi| - I)$$

因此若是把 edge qubits 寫成

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle = cos\frac{\theta}{2}|\alpha\rangle + sin\frac{\theta}{2}|\beta\rangle$$

理論上經過 k 次放大後，solution space$|\beta\rangle$的相位會從$\sin(\theta/2)$增加為 $\sin(\theta \times ((k+1)/2))$。理論中，當解的個數$M \ll N$，則需要的遞迴次數

$$R = CI\left[\frac{\frac{\pi}{2} - \frac{\theta}{2}}{\theta}\right] \le CI\left[\frac{\pi}{4} \times \frac{2}{\theta}\right] - (1)$$

當$M \le N/2$，$\frac{\theta}{2} \ge \sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}}$，因此迭代次數的上界為$R \le \frac{\pi}{4}\sqrt{\frac{N}{M}} \propto O(\sqrt{N})$

(4) 由此 oracle 求出的解可能只是多個子迴圈，而非一條完整的哈密頓迴圈，因此在得到可能結果後還需要利用 BFS(Breadth-First Search，廣度優先搜尋)來確認是否所有的點都相連。

2. 複雜度分析

空間複雜度：需用到$V + E + 1$個 qubits。

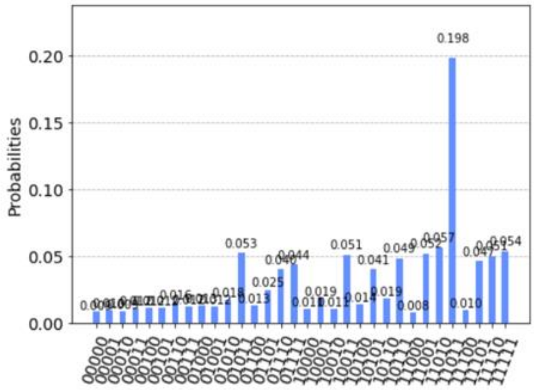
時間複雜度：

- 初始化 edge & flag：E+2 個 gate
- Oracle：在 encoder 與 relaxer 共需要 4E 個 gate，mcx gate 可以視為多個 Toffoli gate 組成，複雜度計算上應該視為 O(V)
- Diffuser：使用 4E+O(E)個 gate，而 O(E)也是因為有 mcz gate 的緣故
  →整個 Grover operator 需用到$8E + O(V + E) \in O(V + E)$個 gate
- 最佳迭代次數：根據上述推導，$R \propto \sqrt{N/M} \simeq \sqrt{2^E}$

→整體複雜度為$O((V+E)\times 2^{E/2})$，相比於傳統 DP 需要$O(V\times 2^{V})$，因此在$E\propto V$時 Grover 演算法有平方加速的效果，但在$E\propto V^2$時，傳統演算法反而有較好的表現。

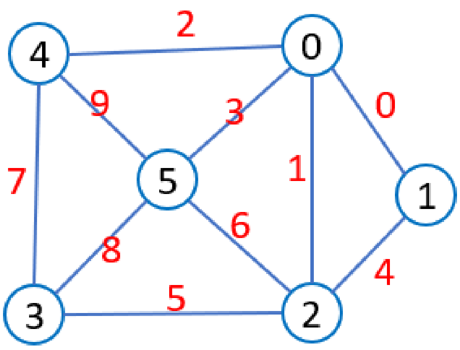
3. 範例

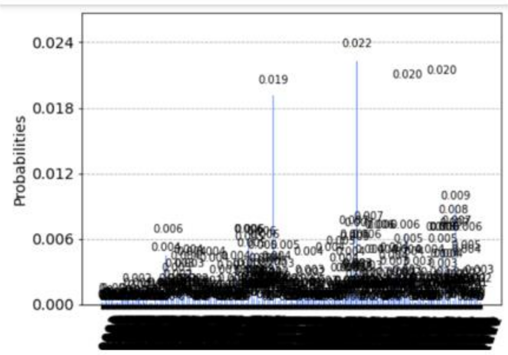
在圖三的例子中，當選取第 0, 2, 3, 4 條邊時是一條 HC，而在實驗結果中能看到(11011)的機率最高，正是我們想要的結果。



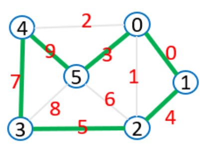
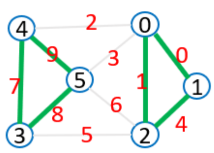
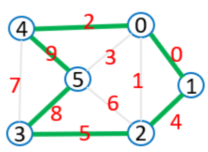
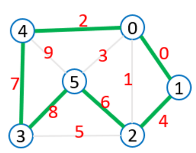
圖七、Rotation oracle 範例一結果

在圖八的例子中，我們預期有三條 HC，而量測結果如圖九所示有出現四個峰值，當結果為 1010111001、1100110101、0111010101 都是 HC，但是第二個結果 1110010011 並非 HC，而是由兩個子迴圈組成，因為此 oracle 無法排除此類可能性，因此需要用 BFS 來去除這項結果。





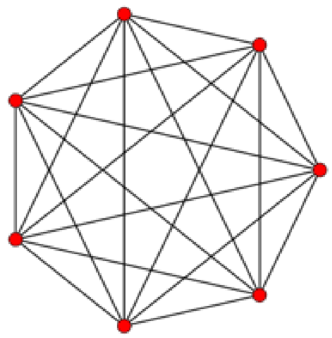
圖八、Rotation oracle 範例二　　圖九、Rotation oracle 範例二測量結果

			
1010111001	1110010011	1100110101	0111010101

表一、Rotation oracle 範例二的四種結果

4. 缺陷

(1) 此 Oracle 的選擇方式是選取 vertex qubits 都是$|1\rangle$的狀況，但是我們可以預期作用(4k+2)的$RY(\pi/2)$旋轉後都能讓 vertex qubits=$|1\rangle$，像在圖十中每個頂點都有六條邊與之相連，因此全選下也會被 oracle 視為一條 HC。



圖十、Rotation oracle 缺陷_範例圖一

(2) 對 vertex qubits 進行(2k+1)的$RY(\pi/2)$旋轉後，vertex qubits=$|+\rangle$或$|-\rangle$，因此在 mcx gate 中仍然有 1/2 的機率被視為是$|1\rangle$而被選取，因此被錯誤的放大。在圖七的結果中，可以發現除了最大振幅外，另外還有部分可能性也被放大，其機率約為最大振幅的 1/4，這些結果正是因為只有其中兩點是$|+\rangle$或$|-\rangle$，其餘點皆為$|1\rangle$，因此有$(1/2)^2$機率被錯誤放大。此問題也能在範例二中發現，根據理論計算，滿足 oracle 的解 M=4，所有可能性 N=1024，代入(1)式後得到最佳迭代次數為 12，但是實際上最佳迭代次數約為 3，原因是有太多不滿足 oracle 的解被錯誤地放大，因此若是以下列式子來計算每條路徑通過 oracle 的機率：

$$\prod_{i=1}^{V} p_{i,count} - (2)$$

$$p_{i,count} = 1 \; if \; v_{i,count} = 4k+2$$

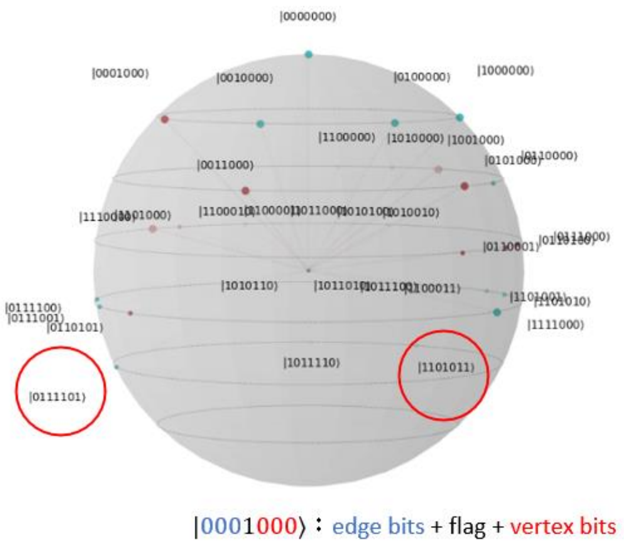
$$p_{i,count} = 0.5 \; if \; v_{i,count} = 2k+1$$

$$p_{i,count} = 0 \; if \; v_{i,count} = 4k$$

其中$v_{i,count}$代表在選定的路徑上v_i連接的邊數。算完每條路徑通過 oracle 的機率後，就能夠把所有路徑的機率相加來得到等效解的個數，經過計算總和為 48.5，以 M=48.5 代入(1)式可算出最佳迭代次數為 3，與實驗結果吻合，代表此現象確實存在。

(3) 在 relax 階段我們控制邊對頂點進行$RY(-\pi/2)$的旋轉，期望能把 vertex qubits 都歸零，然而經實測後發現 relax 階段仍有缺陷，仍有些許 vertex qubits 尚未恢復成$|0\rangle$，因此下一次迭代時就會有非理想效應出現，使得此 oracle 最多只能迭代數次。以圖十一為例，圖形為三頂點三條邊的三角形，所有頂點全選時是一條 HC，而圖十一代表通過 oracle 之後所有位元可能的狀態，觀察後三位元(vertex qubits)時，我們預期應該要全部恢復成$|0\rangle$，然而實測後發現仍有不為

$|0\rangle$的可能性，因此推論是 mcx gate 與 RY gate 同時作用所造成。

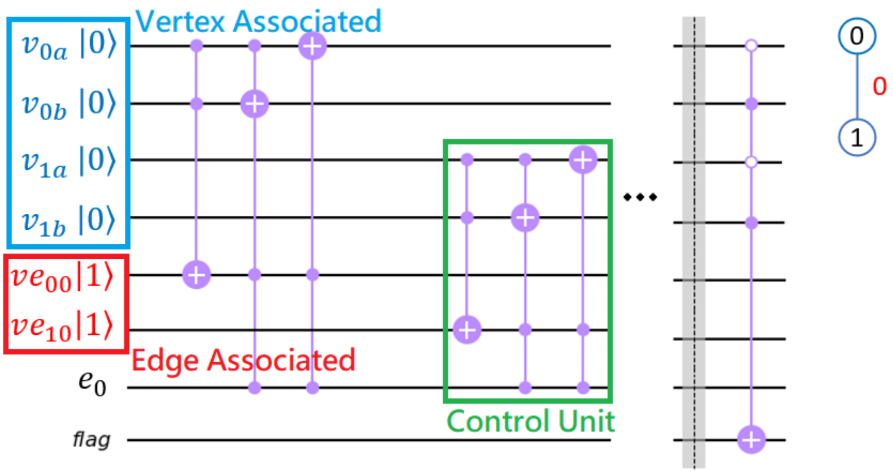


圖十一、Rotation oracle 缺陷_範例圖二

(二) Counter oracle

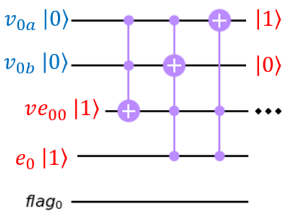
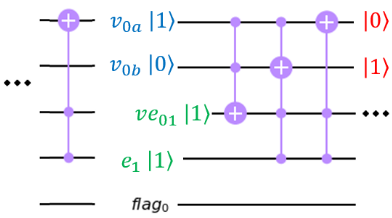
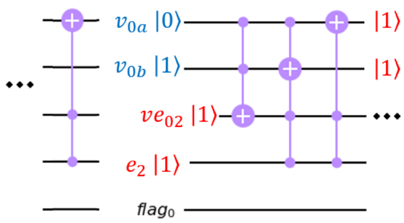
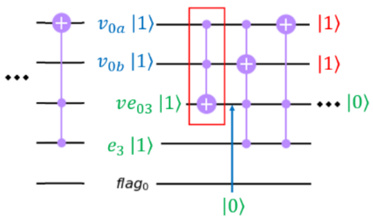
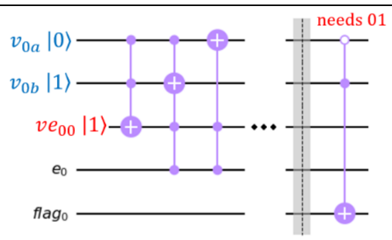
1. 設計架構

(1) 輸入分為 vertex, edge, flag，其中 vertex 數目=2V，edge 數目=3E，flag 數目=1。對於每個頂點都有兩個位元，可以代表二位元計數器；對於每條邊，除了原來的 edge qubits，還額外增加了兩個輔助位元ve_{mn}，代表此位元是第 n 個邊控制第 m 個頂點的輔助位元。初始化的部分是將所有輔助位元ve都設成$|1\rangle$，將所有 edge qubits 設為$|+\rangle$，將 flag 設為$|-\rangle$。



圖十二、Counter oracle 設計架構

(2) Counter oracle 設計上也是利用一條 HC 上每個頂點有兩條邊被選取的特性。運作原理以圖八作為範例，並分別選取 e0, e1, e2, e3 來與 v0 作用，詳細推導如表二所述：

<table>
<tr><th>目前電路狀態</th><th>說明</th></tr>
<tr><td></td><td>選取 e0 時 v0 第一次被調控，因此在第三個 mcx gate 作用下$|v_{0a}v_{0b}\rangle$從$|00\rangle$變成$|10\rangle$。</td></tr>
<tr><td></td><td>選取 e1 時 v0 第二次被調控，在第二、三個 mcx gate 作用下從$|10\rangle$變成$|01\rangle$，此時符合 HC 的性質，因此是我們想量測到的結果。</td></tr>
<tr><td></td><td>選取 e2 時 v0 第三次被調控，因此在第三個 mcx gate 作用下從$|01\rangle$變成$|11\rangle$。</td></tr>
<tr><td></td><td>當 v0 的調控次數大於三次，則第一個 mcx gate 發揮作用，輔助位元會變成$|0\rangle$，進而關閉後兩個 mcx gate，因此$|v_{0a}v_{0b}\rangle$會穩定處於$|11\rangle$狀態，不會發生如 Rotation oracle 中每旋轉四次一循環的情況。</td></tr>
<tr><td></td><td>在 phase kickback 階段，我們希望選取 vertex qubit 被二次調控的情況，也就是$|v_{ia}v_{ib}\rangle = |01\rangle, v_i \in V$，此選取能用 mcx gate 與 x gate 來完成。</td></tr>
</table>

表二、Counter oracle 運作原理

(3) phase kickback 階段如表二所描述。而 relaxer 就是 encoder 的反電路，因此能以 control unit 左右反轉連接來實現，而使 vertex qubits 都能恢復成$|0\rangle$，並將負相位資訊由 vertex qubits 傳至 edge qubits。Diffuser 的架構與 rotation oracle 相同，都是作用在 edge qubits 上來達到相位放大。同樣地，此 oracle 也無法保證所有頂點互相連接，因此得到結果後仍需以 BFS 進行驗證。

2. 複雜度分析

空間複雜度：需用到$2V+3E+1$個 qubits，約為 rotation oracle 的三倍。

時間複雜度：

- 初始化輔助位元 ve & edge & flag：3E+2 個 gate
- Oracle：一個 control unit 需要 3 gate，在 encoder 與 relaxer 中都各有 2E 個 control unit，相乘後約有 12E 個 gate；mcx gate 可以視為多個 Toffoli gate 組成，複雜度計算上應該視為 O(V)
- Diffuser：使用 4E+O(E)個 gate，而 O(E)也是因為有 mcz gate 的緣故
  →整個 Grover operator 需用到$16E + O(V+E) \in O(V+E)$個 gate，數量級與 Rotation oracle 相同，但實際數量約為兩倍。
- 最佳迭代次數：根據上述推導，$R \propto \sqrt{N/M} \simeq \sqrt{2^E}$
  →整體複雜度為 $O((V+E)*2^{E/2})$，相比於傳統 DP 需要 $O(V*2^V)$，$E \propto V$時 Grover 演算法有平方加速的效果，但在$E \propto V^2$時，反而是 DP 較快。

3. 範例

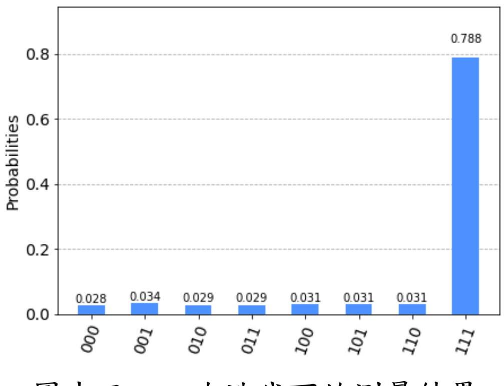
由於 Qiskit 的模擬器上目前提供的 qubit 數目有限，因此以三頂點三條邊的三角形作為例子，測試此 oracle 的可行性。圖十三與圖十四是迭代一次與兩次的結果，可以看出 edge qubits=$|111\rangle$能被有效放大，且根據理論計算：

$$\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}} = \sqrt{\frac{1}{2^3}}, \theta \approx 41.41°$$

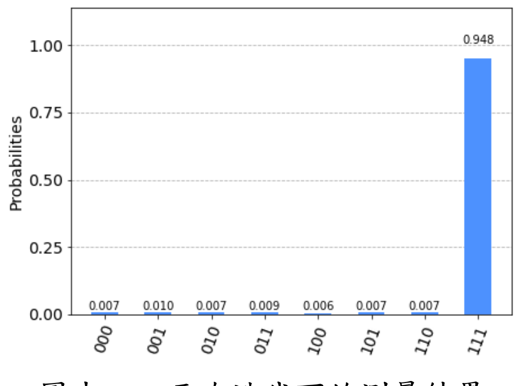
因此放大後的機率分別為

$$\left|\sin\left(\frac{3}{2}\theta\right)^2\right| = 0.781, \left|\sin\left(\frac{5}{2}\theta\right)^2\right| = 0.9453$$

在理論與實驗中的放大機率吻合，而最佳迭代次數由(1)式可算出是兩次，也與測量結果相當吻合。另外，可以觀察到其他的可能性並沒有被錯誤放大(如$|110\rangle$與$|000\rangle$振幅相同，但如果同樣情況在 rotation oracle 中會因為缺陷二而導致$|110\rangle$振幅較高)，代表 counter oracle 能克服 rotation oracle 中的缺陷二；而關於 rotation oracle 的缺陷三，則會因為 counter oracle 在設計上都採用 mcx gate 而能夠有效 relax。



圖十三、一次迭代下的測量結果



圖十四、兩次迭代下的測量結果

三、Quantum Counting[4][11]

在 Grover algorithm 中，由(1)式可知最佳迭代次數與解的個數 M 有關，因此希望能用 Quantum Counting 來找到 M。此方法的想法就是用 Quantum Phase Estimation(QPE)來獲得 Grover operator(G)的特徵值$e^{i\theta}$中的θ，進而回推 M。

(一)設計架構

G 可以寫成一旋轉矩陣，即

$$G=\begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix}, \sin\left(\frac{\theta}{2}\right)=\sqrt{\frac{M}{N}}, \cos\left(\frac{\theta}{2}\right)=\sqrt{\frac{N-M}{N}}$$

因此 G 的特徵值與特徵向量為

$$e^{i\theta}, |\mathrm{a}\rangle=\frac{1}{\sqrt{2}}(i|\alpha\rangle+|\beta\rangle), |\alpha\rangle=\frac{1}{\sqrt{N-M}}\sum_{x}|\mathrm{x}\rangle$$

$$e^{i(2\pi-\theta)}, |\mathrm{b}\rangle=\frac{1}{\sqrt{2}}(-i|\alpha\rangle+|\beta\rangle), |\beta\rangle=\frac{1}{\sqrt{M}}\sum_{x'}|\mathrm{x}'\rangle$$

因此測量θ的電路如圖十五所示，輸入位元有 t, v, e, flag，而 v, e, flag 的位元數由 G operator 決定，而 t 的選擇可由以下式子決定：

$$t=m+\log(2+1/2\epsilon)$$

假設我們希望 QPE 的量測結果成功機率為$(1-\epsilon)=0.9375, \epsilon=1/16$，我們選擇$t=m+1$，則量測出的相位$|\Delta\theta|\leq(1/2^{t-1})$。在一開始，我們令$t=|+\rangle, v=|0\rangle,\ e=|+\rangle, flag=|-\rangle$，之後$t_j$當作$(C_G)$^$(2$^$j)$的 control bit，可得到

$$C\_G^{2^j}\left[\frac{1}{\sqrt{2}}(\,|0\rangle+\,|1\rangle)\right]|\mathrm{u}\rangle=\frac{1}{\sqrt{2}}[\,|0\rangle+e^{2\pi i\phi*2^j}\,|1\rangle]\,|\mathrm{u}\rangle$$

其中$|\mathrm{u}\rangle$就是 v + e + flag，因此在進入$QFT^{\dagger}$(inverse fourier transform)前

$$t^{\otimes t}=\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi ij\phi}\,|\mathrm{j}\rangle$$

之後$t^{\otimes t}$在$QFT^{\dagger}$後量測出結果為$value$，則$value=2^t\phi$是代表$eigenvalue=e^{2\pi i\phi}$的量測結果，因此

$$\theta=value\times 2\pi/2^t$$

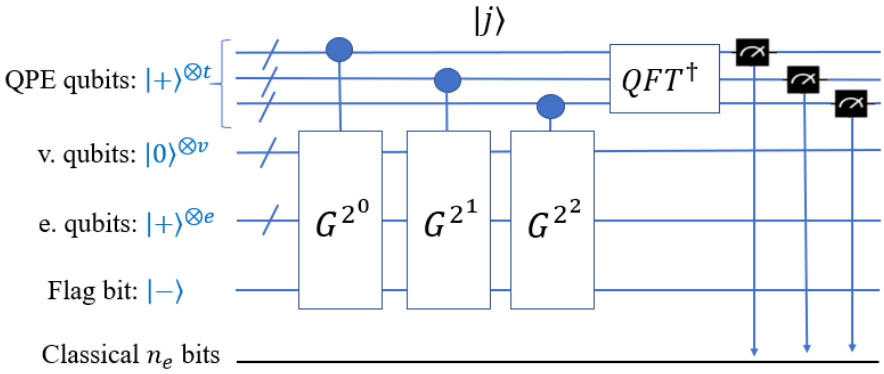
另外，由於在 G operator 中的 diffuser 會有負相位的產生，因此在 QPE 量測到的結果是非正解的數目，因此解的個數

$$M=N-N\times sin^2(\frac{\theta}{2})$$

而錯誤率

$$|\Delta M|<\left[\sqrt{2(N-M)M}+\frac{N}{2^t}\right]\times\frac{1}{2^{(t-1)}}$$

因此若是想要$|\Delta M| < 1$，也就是想了解 HC 的確切個數，則$t \geq E + 2$。



圖十五、Quantum Counting 電路架構

(二)複雜度分析 (以 Rotation oracle 為例)

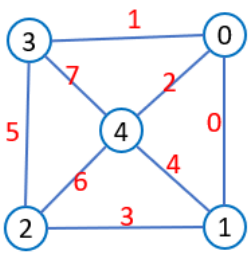
空間複雜度：需用到$t + V + E + 2 \approx 2E + V + 2$個 qubits

時間複雜度：

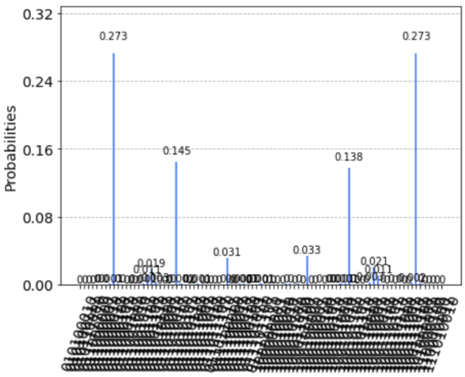
- 初始化需要 2E+2 個 gate
- 一個 G operator 需要 8E+O(V+E)個 gate，總共需要$2^0 + 2^1 + \cdots + 2^t = 2^{t+1} - 1$個 G operator，因此在$t \approx E$的前提下，$C_G^{|j\rangle}$共花費$O((V + E) \cdot 2^E)$個 gate。
- $QFT^\dagger$需要$O(t^2) \approx O(E^2)$個 gate
- 整體花費$O((V + E) \cdot 2^E)$個 gate，與傳統 DP 的花費時間$O(V^2 \cdot 2^V)$相比，若是$E \propto V$，則 Q_Counting 與 DP 花費時間相當；若是$E \propto V^2$，則時間複雜度為$O\left((V^2) \cdot 2^{V^2}\right)$，比傳統演算法慢了許多。

(三)範例

第一個例子是用 Rotation oracle，圖形如圖十六，已知有四條 HC，分別是(01367, 12345, 01456, 02357)四種邊的組合，而在 t=E+1=9 的設定下，計算出$(100111100)_2 = 316$機率最高(1397/5120 shots)，量測出$(\pi - \theta) = 3.8779$(弧度)，而理論上$\theta = 14.36°$，顯然與測量值$\theta = -42.188°$相去甚遠，因此測量上$M = 33.16, |\Delta M| \leq 1.36$也與實際結果有落差，這也反應出 Rotation oracle 有部分機率將錯誤解放大，而用(2)式算出等效解的個數 M’=26.25 也較接近測量結果；另外測量結果也反應出此 oracle 較無法多次迭代的特性。

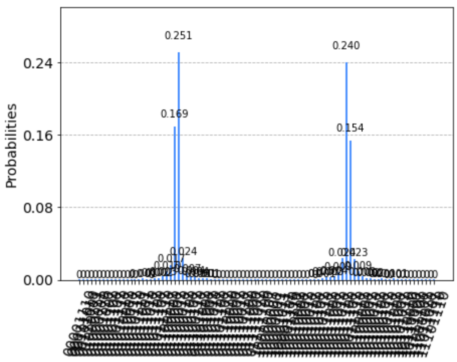


圖十六、Quantum counting 範例一



圖十七、Quantum counting 範例一量測結果

第二個例子是用 Counter oracle，同樣因為可用位元的限制，因此以三頂點三條邊的三角形為例，此圖形已知有一條 HC，而在 t=E+5=8 的設定下，可以算出特徵值的角度$\langle\alpha|\psi\rangle = 2.42983$(弧度)$= 139.22°$，此角度是$|\psi\rangle$與非正解向量$|\alpha\rangle$之間的夾角，而$|\psi\rangle$與正解向量$|\beta\rangle$間的角度$\theta = 40.78°$，與理論值$41.41°$相當吻合，而計算出$M = 0.97, |\Delta M| \leq 0.08$，可看出 Quantum Counting 能夠精準的量測出 G operator 的相位，也代表 Counter oracle 的 relaxation 有把 vertex qubit 恢復成$|0\rangle$，因此能多次迭代來得到最大振幅。而在表三也列出機率前四高的結果，能夠發現測量結果有兩組特徵值，每組都代表θ & $(2\pi - \theta)$，而此兩組特徵值正是實際值的上下逼近值，因此可以預期若是 t 的數目上升，則會有更好的逼近結果。



圖十八、Quantum counting 範例二量測結果

t bit	shots	$\langle\alpha\|\psi\rangle$(弧度)	$\langle\alpha\|\psi\rangle$(°)	$\langle\beta\|\psi\rangle$(°)	M
01100011	1027	2.42983	139.22	40.781	0.97
10011101	984	3.85336	220.78	-40.781	0.97
01100010	691	2.40528	137.81	42.188	1.04
10011110	630	3.87790	222.19	-42.188	1.04

表三、Quantum counting 範例二結果統整

四、HCP to SAT

前面提及 HCP 是 NP-Complete 的問題，而 SAT 也屬於 NP-Complete 的問題，SAT 問題是對於 n 個變數(variable)與 m 個布林函數(clause)，嘗試找到一組解來滿足所有的布林函數，以 CNF(Conjunctive Normal Form)為例，我們可以找到[x1=T, x2=F, x3=T]來滿足$[(\neg x1 \vee \neg x2) \wedge (x1 \vee \neg x3)]$此函數。因為 SAT 問題發展已久，因此有許多 SAT solver 運用各種演算法來解決此問題；在 Qiskit.aqua 中的 LogicalExpressionOracle 也有將 SAT 問題轉化為 Grover 的 oracle 的功能，因此我們也嘗試用轉化的方式解決 HCP。

(一)設計架構

有論文[5]嘗試以 SAT 的角度解決 HCP，轉換方式也是利用一條 HC 中每個點都只會有兩邊與之連接的特性，來將 HCP 問題轉化為 2inK-SAT。但此處我們採用另一種轉化方式[6]，我們將 G(V, E) (|V|=n, |E|=m)轉換成有 n^2 個 variable 的 SAT，其中x_{ij}代表在走訪第 i 個點時是原圖中的點 j，之後會根據下圖的五條規則來增加 clause：

(1) 每個頂點V_j都必須出現在 HC 中

$$(x_{1j} \vee x_{2j} \vee \ldots \vee x_{nj})\ for\ j \leq n$$

(2) 每個頂點V_j都只在 HC 中出現一次

$$(\neg x_{ij} \vee \neg x_{kj})\ for\ i \neq k$$

(3) 在 HC 中走訪第 i 步時會對應到一個頂點

$$(x_{i1} \vee x_{i2} \vee \ldots \vee x_{in})\ for\ i \leq n$$

(4) 不能同時有兩個頂點V_j, V_k同時對應到第 i 步

$$(\neg x_{ij} \vee \neg x_{ik})\ for\ j \neq k$$

(5) 非相鄰的兩點無法依序走訪

$$(\neg x_{ki} \vee \neg x_{k+1j})\ for\ (i,j) \notin G, k \in [1, n-1]$$

而在轉換後就能輸入 LogicalExpressionOracle[12]來轉換成 oracle 放大所求相位。輸入為 variable +clause +flag，oracle 中同樣有 encoder、mcx gate、relaxer 三個架構，電路架構是由 variable 控制 clause，之後由 mcx gate 收集是否所有 clause 都被滿足，如果是的話則會經過 flag 產生 kickback 的效果，之後 relaxer 再把負相位資訊由 clause 傳回 variable，variable 再進入 diffuser 來放大振幅。

(二)複雜度分析

空間複雜度：由[6]證明 variable 個數為$O(n^2)$、clause 個數為$O(n^3)$，因此需要$O(n^3)$個 qubits。

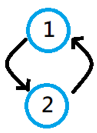
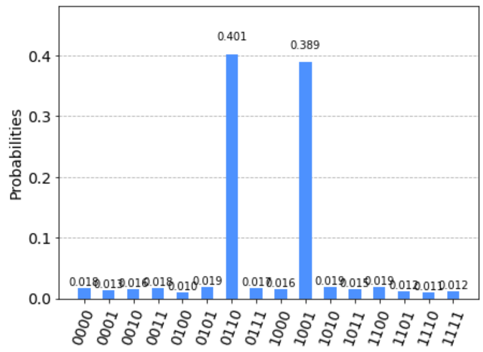
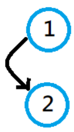
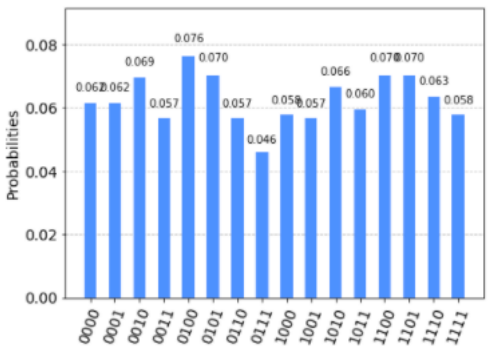
時間複雜度：

- HCP 轉換成 SAT 的部分是用傳統演算法完成，時間為$O(n^3)$。
- G operator 所需的 gate 數目為 O(variable+clause)= $O(n^3)$
- 最佳迭代次數$\propto O(\sqrt{N}) = O\left(\sqrt{2^{n^2}}\right) = O(2^{\frac{n^2}{2}})$，因此整體複雜度為

$O(n^3 \times 2^{\frac{n^2}{2}})$，相比於傳統 DP 演算法慢了許多，而失去了 Grover algorithm 平方加速的優勢。

(三)範例

因為此方法所消耗的位元數過多，因此只以兩個頂點為例。當 E={(1,2),(2,1)}在一次迭代下就能得到不錯的放大效果，其中"0110"代表$x_{11} = 0, x_{12} = 1, x_{21} = 1, x_{22} = 0$，代表有一條曼哈頓迴圈是以"2→1→2"的方式來行進，而"1001"代表"1→2→1"的行進方式。當 E={(1,2) }時因為只有單向邊，因此用 Grover algorithm 無法有效放大。

圖形	SAT 形式	測量結果
	$(x_{11} \vee x_{21})$ $\wedge (x_{12} \vee x_{22})$ $\wedge (\neg x_{11} \vee \neg x_{21})$ $\wedge (\neg x_{12} \vee \neg x_{22})$ $\wedge (x_{11} \vee x_{12})$ $\wedge (x_{21} \vee x_{22})$ $\wedge (\neg x_{11} \vee \neg x_{12})$ $\wedge (\neg x_{21} \vee \neg x_{22})$	
	$(x_{11} \vee x_{21})$ $\wedge (x_{12} \vee x_{22})$ $\wedge (\neg x_{11} \vee \neg x_{21})$ $\wedge (\neg x_{12} \vee \neg x_{22})$ $\wedge (x_{11} \vee x_{12})$ $\wedge (x_{21} \vee x_{22})$ $\wedge (\neg x_{11} \vee \neg x_{12})$ $\wedge (\neg x_{21} \vee \neg x_{22})$ $\wedge (\neg x_{12} \vee \neg x_{21})$ $\wedge (\neg x_{22} \vee \neg x_{11})$	

表四、$HCP \leq_P SAT$範例

五、QUBO

(一)設計架構

QUBO(quadratic unconstrained binary optimization)是屬於NP-Hard的範疇($\exists Y \in NPC, Y \leq_P X$)，其目的是幫$f(x) = x^{\intercal} Qx$找到最小的解，也就是

$$x^* = min_x \sum_{i \le j} x_i Q_{(i,j)} x_j,\ where\ x_i \in \{0,1\}$$

其中x是維度為n的二元向量，Q 是大小為$n \times n$的上三角矩陣。

而對於 HCP 而言，論文[1]中提供一種方法來將 HCP 轉為 QUBO。轉法與 SAT 部分有些許類似，都將 G(V, E) (|V|=n, |E|=m)轉換成x_{ij}形式，其中

$$x_{ij} = \begin{cases} 1, if\ vertex\ i\ is\ at\ position\ j\ of\ the\ sequence \\ 0, otherwise \end{cases}$$

因此x的維度是n^2。而函式$F(x) = H(x) + P_1(x) + P_2(x)$

$$H(x) = \sum_{(i_1,i_2) \in V \times V - E(G)} (x_{i_1,0} x_{i_2,n-1} - \sum_{j=0}^{n-2} x_{i_1,j} x_{i_2,j+1})$$

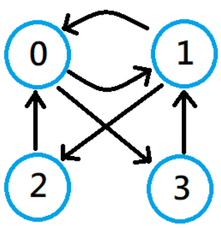
$$P_1(x) = \sum_{i=0}^{n-1} (1 - \sum_{j=0}^{n-1} x_{i,j})^2$$

$$P_2(x) = \sum_{j=0}^{n-1} (1 - \sum_{i=0}^{n-1} x_{i,j})^2$$

其中$H(x)$負責判斷選擇路徑的前後兩點之間是否有邊相連，而$P_1(x)$ & $P_2(x)$則負責確定此路徑正好走訪所有頂點，因此構成 HCP。若是x不符合 HCP 的特性，則$F(x) > 0$，因此若能確定$\exists x'\ s.t.\ F(x') \le 0$，則$x'$就是一條 HC。

(二)範例[7]

將 HCP 轉化為 QUBO 之後，若以量子演算法計算之，則可以用 VQE (Variational Quantum Eigensolver)與 QAOA(Quantum Approximate Optimization Algorithm)來解決最佳化問題，然而因為目前能運用的位元數與計算資源有限，因此暫時以 NumPyMinimumEigensolver 代替 QAOA 進行實驗。在用上述方法求出$F(x)$後，利用 QuadraticProgram 將 Ising Hamiltonian 轉換成 Quadratic Program，之後再用 MinimumEigenOptimizer 得到最佳解，並用 NumPyMinimumEigensolver 來確認值的大小，若是值大於零，則此圖形不存在 HC。以圖十九為例，求出$F(x) \le 0$，因此是一條 HC，$x_{ij} = 1$處分別對應$x_{01}, x_{13}, x_{20}, x_{32}$，代表”2→0→3→1→2”的行徑方式，而這正是一條 HC。



圖十九、QUBO 範例

```
optimal function value: -8.0
optimal value: [0. 1. 0. 0. 0. 0. 0. 1. 1. 0. 0. 0. 0. 0. 1. 0.]
status: SUCCESS
solution : [2, 0, 3, 1]
```

圖二十、QUBO 範例_計算結果

肆、 結論

HCP 問題屬於 NP-Complete，而我們以四種角度切入來嘗試解決此問題。

第一種方法為 Grover algorithm，有 Rotation oracle 與 Counter oracle 兩種形式，Rotation oracle 的優點為直觀、空間與時間複雜度較低，因此在目前可用位元數目有限的情況下能計算較大的圖，但是缺點就是錯誤解會低機率的被放大，因此限制了正解的振幅大小，且 rotation oracle 的 relaxer 仍有缺陷，因此在多次迭代後會失去放大振幅的效果。Counter oracle 有效解決上述問題，並且放大振幅與理論之間有良好的對應關係，缺點是空間與時間複雜度高，因此目前只能測試$|V| \leq 4$的結果。

第二種方法為 Quantum Counting，目的是為了求出解的個數，也算是 Grover algorithm 的前驅步驟，而求法是用 QPE 找到 G operator 的特徵值$e^{i\theta}$，在使用 Rotation oracle 時，因為 oracle 本身缺陷而會過度估計解的個數；反之在使用 Counter oracle 時，能夠發現最佳與次佳的測量結果正好是解的上下界，因此可推斷 t 的增加能有效逼近解的個數。

第三種方法是將 HCP 轉化為 SAT，好處是求出來的解不需要再用 BFS 來確認是否相連，而且相比於前兩種方法需假設邊是無向的，此方法能解出有向圖的 HCP，缺點也是空間與時間複雜度高。

第四種方法是將 HCP 轉化為 QUBO，好處與第三種方法相同，缺點是目前 VQE 與 QAOA 方法的運算效能不足，因此只能以傳統電腦來進行驗證，但我認為第三種與第四種方法是較為廣泛的，因此若是將來在解決 SAT 與 QUBO 問題上有重大突破，這兩種方法的時間複雜度也會大幅降低，因此前瞻性高。

伍、 參考文獻

[1] Mahasinghe, A., Hua, R., Dinneen, M. J., & Goyal, R. (2019, January). Solving the Hamiltonian cycle problem using a quantum computer. In *Proceedings of the Australasian Computer Science Week Multiconference* (pp. 1-9).

[2] Bellman, Richard. "Dynamic programming treatment of the travelling salesman problem." *Journal of the ACM (JACM)* 9.1 (1962): 61-63.

[3] Bjorklund, Andreas. "Determinant sums for undirected hamiltonicity." *SIAM Journal on Computing* 43.1 (2014): 280-299.

[4] Michael A. Nielsen and Isaac L. Chuang. 2011. Quantum Computation and Quantum Information: 10th Anniversary Edition (10th ed.). Cambridge University Press, New York, NY, USA.
[5] Mandra, Salvatore, Gian Giacomo Guerreschi, and Alán Aspuru-Guzik. "Faster than classical quantum algorithm for dense formulas of exact satisfiability and occupation problems." *New Journal of Physics* 18.7 (2016): 073003.
[6] 呂育道.(2011). Hamiltonian Path. Retrieved from https://www.csie.ntu.edu.tw/~lyuu/complexity/2011/20111018.pdf (June 8, 2021)
[7] ho0-kim. (2021) Hamiltonian_Cycle_Problem_with_QC. Retrieved from https://github.com/ho0-kim/Hamiltonian_Cycle_Problem_with_QC (June 7, 2021)
[8] 國立臺灣師範大學教職員工生個人網頁空間. Dynamic Programming. Retrieved from http://web.ntnu.edu.tw/~algo/DynamicProgramming.html (June 18, 2021)
[9] 國立臺灣師範大學教職員工生個人網頁空間. Hamilton Circuit. Retrieved from http://web.ntnu.edu.tw/~algo/Circuit.html (June 18, 2021)
[10] Qiskit textbook. (2021) Grover's Algorithm. Retrieved from https://qiskit.org/textbook/ch-algorithms/grover.html (May 27, 2021)
[11] Qiskit textbook. (2021) Quantum Counting. Retrieved from https://qiskit.org/textbook/ch-algorithms/quantum-counting.html (June 18, 2021)
[12] Qiskit textbook. (2021) Solving Satisfiability Problems using Grover's Algorithm. Retrieved from https://qiskit.org/textbook/ch-applications/satisfiability-grover.html (June 18, 2021)

陸、 附錄

[1] 報告用投影片
https://drive.google.com/file/d/1CFNPTrV954xDv7dIbNxbJRkPtpBySZ6Z/view

[2] 程式碼

- Grover algorithm & Quantum counting
  https://drive.google.com/file/d/1Xk4DShzHy633VxhmQu6zKIYPDzr-ackj/view?usp=sharing
- HCP to SAT
  https://drive.google.com/file/d/1O9hDsGVSZrZTPXaoXjP4NjPVyjFyf4Aw/view?usp=sharing
- QUBO
  https://drive.google.com/file/d/1HU2EoFiZII6yzIRZywcspSPayPPBMOz_/view?usp=sharing