

第三次习题课

2022 年 1 月 7 日

1 第一章计算普适性与复杂度

1: 按照图灵机中两态转移矩阵的定义 (PPT 7,8 页), 说明 4+5 的算法过程。

解 : 根据 PPT 内容或者讲义内容, 稍作数字改变即可。注意 4 和 5 的二进制编码方式分别为 1111 和 11111, 中间有个比特 0。

2: 给出第 67-68 页中的 Pauli 算符与标准 Pauli 算符之间的关系。

解 : $(\sigma_x)_{mn}$ 表示第 m 、 n 两行与 m 、 n 两列交叉所形成的 2×2 子矩阵为 σ_x , 而其它矩阵元都为 0。当然也可以视为子空间和 $\mathbf{0}$ 空间的直和, $(\sigma_x)_{mn} = V \oplus W = \sigma_x \oplus \mathbf{0}$ 。但是 $I \otimes I \otimes \sigma_x \neq (\sigma_x)_{mn}$ 。

3: 按参数个数估计用 Deutsch 门逼近任意 n 比特么正变换时所需的门数目。

解法 1 : 只有 Deutsch 门很难生成任意 n 比特么正变换, 这里我们认为题目中忽略了单比特门的个数。若线路的拓扑是由单比特门和 Deutsch 门构成, 我们可以根据《量子计算 note》72 页的思路来做这道题。

我们用占位符来标记单比特算符, 如果两个邻近的占位符之间没有 Deutsch 门, 则两个占位符就可以归并为 1 个; 如果两个占位符之间有 Deutsch 门, 我们来计算有效的占位符个数。

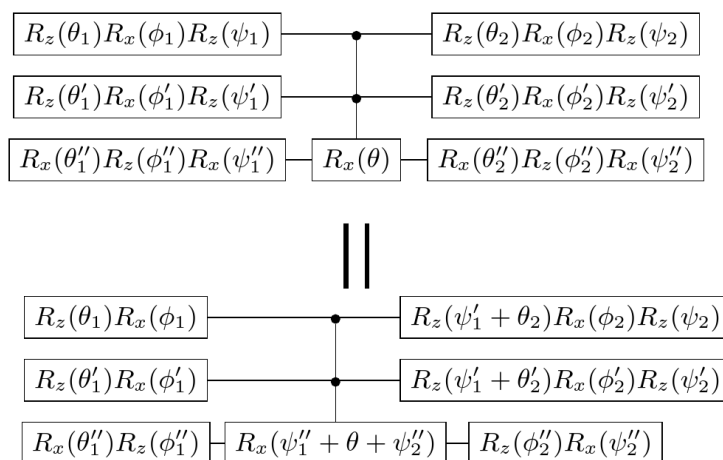


图 1: 利用 Deutsch 门和单比特门之间的对易关系可减少线路的有效参数个数。

假如线路中有 k 个 Deutsch 门，单门参数有 $3 \otimes (n + 3k) - 4k = 3n + 5k$ ，再加上 k 个 Deutsch 门的参数个数，总共为 $3n + 6k$ 。而 $SU(2^n)$ 变换的自由参数个数为 $4^n - 1$ ，为了能够模拟 $SU(2^n)$ 变换，自由参数的个数不应少于这个数目。这就要求： $3n + 6k \geq 4^n + 1$ ，所以 $k \geq \frac{1}{6}(4^n - 3n - 1)$

解法 2：讲义 74 页，定理 16。此处从略。

2 第二章量子算法

4: 给出 15 的因式分解 Shor 算法线路图。

解：

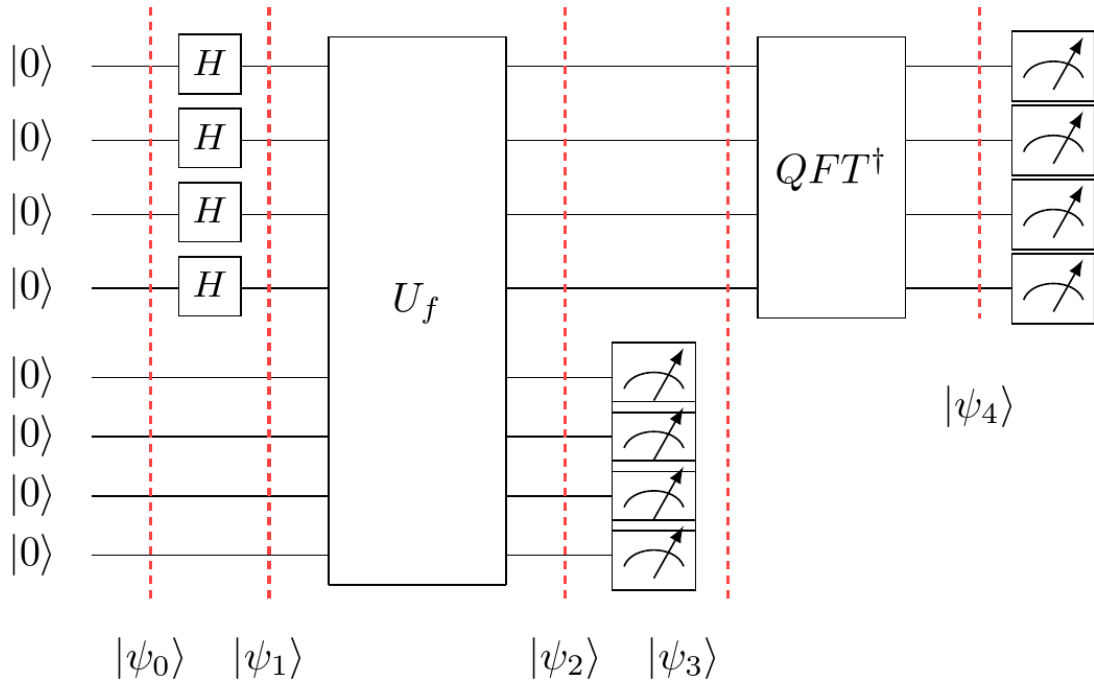


图 2: 数字 15 的 Shor 算法线路图

$$|\psi_0\rangle = |0\rangle^{\otimes 4} |0\rangle^{\otimes 4}$$

$$|\psi_1\rangle = \frac{1}{4} \sum_{i=0}^{15} |i\rangle |0\rangle^{\otimes 4}$$

$$|\psi_2\rangle = \frac{1}{4} \sum_{i=0}^{15} |i\rangle |0 \oplus a^i \bmod 15\rangle$$

测量第二个寄存器的四个比特（个人认为对第二个寄存器的比特数没有特殊的要求，只要可以进行相应的 oracle 即可）。如果取 $a = 7$ ，测得的结果为 4，那么

$$|\psi_3\rangle = \frac{1}{2}(|2\rangle + |6\rangle + |10\rangle + |14\rangle)$$

对其进行量子傅里叶逆变换，得到

$$QFT^\dagger |x\rangle = \frac{1}{4} \sum_{y=0}^{15} e^{-2\pi i xy/16} |y\rangle$$

后面的对照书上内容看一下吧。QFT 逆变换相当于实现线路转置共轭，门的顺序与 QFT 相反，控制旋转门取相应负值。图不画了。

5: 给出计算两个未知两比特量子态 $|\psi\rangle$ 和 $|\phi\rangle$ 保真度的算法线路图。

解 : 将两个态在计算基展开:

$$|\psi\rangle = \sum_{ij} a_{ij} |i\rangle \otimes |j\rangle \quad |\phi\rangle = \sum_{mn} b_{mn} |m\rangle \otimes |n\rangle$$

$$\begin{aligned} |0\rangle|\psi\rangle|\phi\rangle &= |0\rangle \sum_{ijmn} a_{ij} b_{mn} |i\rangle |j\rangle |m\rangle |n\rangle \\ &\xrightarrow{H} \frac{1}{\sqrt{2}} |0\rangle \sum_{ijmn} a_{ij} b_{mn} |i\rangle |j\rangle |m\rangle |n\rangle + \frac{1}{\sqrt{2}} |1\rangle \sum_{ijmn} a_{ij} b_{mn} |i\rangle |j\rangle |m\rangle |n\rangle \\ &\xrightarrow{C\text{-}swap} \frac{1}{\sqrt{2}} |0\rangle \sum_{ijmn} a_{ij} b_{mn} |i\rangle |j\rangle |m\rangle |n\rangle + \frac{1}{\sqrt{2}} |1\rangle \sum_{ijmn} a_{ij} b_{mn} |m\rangle |n\rangle |i\rangle |j\rangle \\ &\xrightarrow{H} \frac{1}{2} |0\rangle \sum_{ijmn} a_{ij} b_{mn} |i\rangle |j\rangle |m\rangle |n\rangle + \frac{1}{2} |1\rangle \sum_{ijmn} a_{ij} b_{mn} |i\rangle |j\rangle |m\rangle |n\rangle \\ &\quad + \frac{1}{2} |0\rangle \sum_{ijmn} a_{ij} b_{mn} |m\rangle |n\rangle |i\rangle |j\rangle - \frac{1}{2} |1\rangle \sum_{ijmn} a_{ij} b_{mn} |m\rangle |n\rangle |i\rangle |j\rangle \\ &= |0\rangle \frac{1}{2} (|\psi\rangle |\phi\rangle + |\phi\rangle |\psi\rangle) + |1\rangle \frac{1}{2} (|\psi\rangle |\phi\rangle - |\phi\rangle |\psi\rangle) = |\Psi\rangle \end{aligned}$$

测量辅助比特，得到 0 的概率为:

$$P_0 = \langle \Psi | 0 \rangle \langle 0 | \Psi \rangle = \frac{1 + |\langle \psi | \phi \rangle|^2}{2} \quad (1)$$

最后:

$$\mathcal{F}(|\psi\rangle, |\phi\rangle) = |\langle \psi | \phi \rangle|^2 = 2p_0 - 1$$

6: 查阅文献，说明 Grover 算法的最优性。

解 : 讲义 page 101-106，有兴趣的同学自己推一下。

3 第三章量子计算的不同模式

7: 证明两种图态定义的等价性。

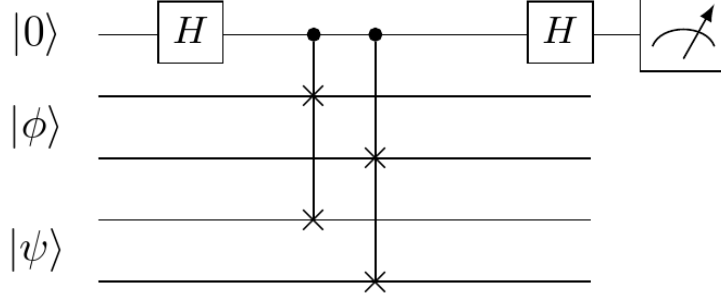


图 3: 计算两个未知两比特量子态 $|\psi\rangle$ 和 $|\phi\rangle$ 保真度的线路图。

解: 我们只需要证明图态 $|G\rangle = S_c|+\rangle^n = \prod_{(a,b) \in E} CZ_{ab}|+\rangle^n$ 是任意稳定子 $K_p = \sigma_p^x \prod_{q \in N_p} \sigma_q^z$ 的本征值为 1 的本征态: 由于所有的 CZ 全部对易, 并且有 $CZ_{ab} = CZ_{ba}$ 和 $CZ^2 = I$, 我们有:

$$\begin{aligned}
 K_p S_c |+\rangle^n &= S_c \prod_{(m,n) \in E} CZ_{mn} K_p \prod_{(a,b) \in E} CZ_{ab} |+\rangle^n \\
 &= S_c \prod_{m \neq p, n \neq p, (m,n) \in E} CZ_{mn} \prod_{k \in N_p} CZ_{pk} \sigma_p^x \prod_{k \in N_p} CZ_{pk} \prod_{m' \neq p, n' \neq p, (m',n') \in E} CZ_{m'n'} \prod_{k'' \in N_p} \sigma_{k''}^z |+\rangle^n \\
 &= S_c \prod_{m \neq p, n \neq p, (m,n) \in E} CZ_{mn} \sigma_p^x \prod_{k' \in N_p} \sigma_{k'}^z \prod_{m' \neq p, n' \neq p, (m',n') \in E} CZ_{m'n'} \prod_{k'' \in N_p} \sigma_{k''}^z |+\rangle^n \\
 &= S_c \sigma_p^x |+\rangle^n = S_c |+\rangle^n = |G\rangle
 \end{aligned}$$

8: 证明图态的 LC(local complementary) 变换。

解: 要验证一个给定量子态是否是一个给定的图对应的图态, 最简单的办法就是验证它是否是此图对应稳定子群 S 的本征值为 1 的共同本征态。设图 G 中点 p 对应的稳定子为 K_p , 且简记 $U_a^\tau(G)$ 为 U_a 。由于

$$U_a(G) = U_a K_p U_a^\dagger U_a |G\rangle = U_a K_p U_a^\dagger |\tau_a(G)\rangle$$

我们只需要验证算符 $U_a K_p U_a^\dagger$ 对应于图 $|\tau_a(G)\rangle$ 的稳定子即可。

$$U_a^\tau(G) \equiv U_a = e^{-i\frac{\pi}{4}X_a} \prod_{b \in N_a} e^{i\frac{\pi}{4}Z_b}$$

• 当 $p = a$

$$\begin{aligned}
 U_a K_p U_a^\dagger &= e^{-i\frac{\pi}{4}X_a} \prod_{b \in N_a} e^{i\frac{\pi}{4}Z_b} (X_a \prod_{b \in N_a} Z_b) e^{i\frac{\pi}{4}X_a} \prod_{b \in N_a} e^{-i\frac{\pi}{4}Z_b} \\
 &= \sqrt{-iX_a X_a} \sqrt{iX_a} \prod_{b \in N_a} \sqrt{iZ_b Z_b} \sqrt{-iZ_b} \\
 &= X_a \prod_{b \in N_a} Z_b = K_p
 \end{aligned}$$

- 当 $p \notin N_a$

$$U_a K_p U_a^\dagger = \left(\sqrt{-iX_a} \prod_{b \in N_a, b \notin N_p} \sqrt{iZ_b} \prod_{b \in N_a, b \in N_p} \sqrt{iZ_b} \right) \\ \times \left(X_p \prod_{q \in N_p, q \in N_a} Z_q \prod_{q \in N_p, q \notin N_a} Z_q \right) \left(\sqrt{iX_a} \prod_{b \in N_a, b \notin N_p} \sqrt{-iZ_b} \prod_{b \in N_a, b \in N_p} \sqrt{-iZ_b} \right) = K_p$$

- 当 $p \in N_a$:

$$U_a K_p U_a^\dagger = \left(\sqrt{-iX_a} \prod_{b \in N_a, b \notin N_p} \sqrt{iZ_b} \prod_{b \in N_a, b \in N_p} \sqrt{iZ_b} \right) \\ \times \left(X_p \prod_{q \in N_p, q \in N_a} Z_q \prod_{q \in N_p, q \notin N_a} Z_q \right) \left(\sqrt{iX_a} \prod_{b \in N_a, b \notin N_p} \sqrt{-iZ_b} \prod_{b \in N_a, b \in N_p} \sqrt{-iZ_b} \right) \\ = \sqrt{-iX_a} Z_a \sqrt{iX_a} \sqrt{iZ_p} X_p \sqrt{-iZ_p} \prod_{q \in N_p} Z_q \\ = Y_a Y_p \prod_{q \in N_p} Z_q \\ = \left(X_a \prod_{b \in N_a} Z_b \right) \times \left(X_p \prod_{q \in N_p, q \notin N_a} Z_q \prod_{q \in N_a, q \notin N_p} Z_q \right) = K_a K'_p$$

可以发现，此时实现了局域补操作。（稳定子群封闭 $K_a K_a K'_p = K'_p$ ）

9: 推导 PPT page12 图态的 Px 方向测量结果。

解: 选取 $b_0 \in N_a$ ，记 $U_{b_0}^\tau(G) \equiv U_{b_0}$ 有：

$$U_{b_0}^\dagger P_a^{y,\pm} U_{b_0} = \sqrt{-iZ_a} P_a^{y,\pm} \sqrt{iZ_a} = \sqrt{-iZ_a} \sqrt{iZ_a} P_a^{x,\mp} = P_a^{x,\mp}$$

上式用到了对易关系 $P^{y,\pm} \sqrt{iZ} = \sqrt{iZ} P^{x,\mp}$ 。因此我们有：

$$P_a^{x,\pm} = U_{b_0}^\dagger P_a^{y,\mp} U_{b_0}$$

于是：

$$P_a^{x,\pm} |G\rangle = U_{b_0}^\dagger P_a^{y,\mp} U_{b_0} |G\rangle = U_{b_0}^\dagger P_a^{y,\mp} |\tau_a(G)\rangle$$

测量结果为 1：记：

$$k_1 = \{k \in N_a - N_{b_0} - b_0\} \quad k_2 = N_a \cap N_{b_0} \quad k_3 = \{k \in N_{b_0} - N_a - a\}$$

$$\begin{aligned}
P_a^{x,+}|G\rangle &= U_{b_0}^\dagger P_a^{y,-}|\tau_{b_0}(G)\rangle \\
&= \left(\sqrt{iX_{b_0}} \prod_{k \in N_{b_0}} \sqrt{-iZ_k} \right) \left(\frac{1}{\sqrt{2}}|y, -\rangle_a \otimes \prod_{k' \in N_a} \sqrt{iZ_{k'}}|\tau_a\tau_{b_0}(G) - a\rangle \right) \\
&= \left(\sqrt{iX_{b_0}} \sqrt{-iZ_a} \prod_{k \in k_2 \cup k_3} \sqrt{-iZ_k} \right) \left(\frac{1}{\sqrt{2}}|y, -\rangle_a \otimes \sqrt{iZ_{b_0}} \prod_{k' \in k_1 \cup k_2} \sqrt{iZ_{k'}}|\tau_a\tau_{b_0}(G) - a\rangle \right) \\
&= \sqrt{-iZ_a} \frac{1}{\sqrt{2}}|y, -\rangle_a \sqrt{iX_{b_0}} \sqrt{iZ_{b_0}} \prod_{k' \in k_3} \sqrt{-iZ_{k'}} \prod_{k \in k_1} \sqrt{iZ_k}|\tau_a\tau_{b_0}(G) - a\rangle
\end{aligned}$$

上式比特 a 和 b_0 与连乘号后的 Z 项均对易, 单独提取放在式子前。 $\prod_{k \in k_2 \cup k_3} \sqrt{-iZ_k}$ 与 $\prod_{k' \in k_1 \cup k_2} \sqrt{iZ_{k'}}$ 含有 k_2 集合的可以消去。 $\sqrt{-iZ_a} \frac{1}{\sqrt{2}}|y, -\rangle_a$ 相当于对 y 本征态做旋转, 得到 $\frac{1}{\sqrt{2}}|x, +\rangle_a$, $\sqrt{iX_{b_0}} \sqrt{iZ_{b_0}} = \sqrt{-iY_{b_0}} \sqrt{iX_{b_0}}$, 忽略全局相位。后面的连乘我们想凑出局域补的形式,

$$\begin{aligned}
&\prod_{k' \in k_3} \sqrt{-iZ_{k'}} \prod_{k \in k_1} \sqrt{iZ_k} \\
&\propto \prod_{k \in k_3} \sqrt{-iZ_{k'}} \prod_{k \in k_3} \sqrt{-iZ_k} \prod_{k \in k_3} \sqrt{iZ_k} \prod_{k \in k_1} \sqrt{iZ_k} \\
&\propto \prod_{k \in k_3} Z_k \prod_{k \in k_1 \cup k_3} \sqrt{iZ_k} \\
P_a^{x,+}|G\rangle &\propto \frac{1}{\sqrt{2}}|x, +\rangle_a \sqrt{-iY_{b_0}} \sqrt{iX_{b_0}} \prod_{k \in k_1} Z_k \prod_{k \in k_1 \cup k_3} \sqrt{iZ_k}|\tau_a\tau_{b_0}(G) - a\rangle \\
&= \frac{1}{\sqrt{2}}|x, +\rangle_a \sqrt{-iY_{b_0}} \prod_{k \in k_1} Z_k \sqrt{iX_{b_0}} \prod_{k \in k_1 \cup k_3} \sqrt{iZ_k}|\tau_a\tau_{b_0}(G) - a\rangle \\
&= \frac{1}{\sqrt{2}}|x, +\rangle_a \sqrt{-iY_{b_0}} \prod_{k \in k_1} Z_k |\tau_{b_0}(\tau_a\tau_{b_0}(G) - a)\rangle \\
&= \frac{1}{\sqrt{2}}|x, +\rangle_a U_a^{x,+}|\tau_{b_0}(\tau_a\tau_{b_0}(G) - a)\rangle
\end{aligned}$$

注意 PPT 中给出的 $U_a^{x,\pm}$ 定义颠倒了!!! 测量结果为-1 时, 方法同上。 U_a^\dagger 也为 LC 算符。需要注意, 每次做完局域补操作之后, 虽然操作点的相连接点没有变化, 但是其连接点的连接点发生了变化。

10: 推导 PPT page18 对易过程。

解: 首先我们有如下的关系式:

- $HZH = X$
- $HZ = XH, ZH = HX$
- $e^{iaP} = \cos aI + i \sin aP$
- $He^{iaZ}H = e^{iaX}$

- $e^{iaZ}X = Xe^{-iaZ}$

证明如下：

$$\begin{aligned}
& He^{ia_4Z/2}Z^{s_4}He^{ia_3Z/2}Z^{s_3}He^{ia_2Z/2}Z^{s_2}HZ^{s_1} \\
& = He^{ia_4Z/2}HX^{s_4}e^{ia_3Z/2}Z^{s_3}He^{ia_2Z/2}HX^{s_2}Z^{s_1} \\
& = e^{ia_4X/2}X^{s_4}e^{ia_3Z/2}Z^{s_3}e^{ia_2X/2}X^{s_2}Z^{s_1} \\
& = X^{s_4}Z^{s_3}e^{i(-1)^{s_3}a_4X/2}e^{ia_3Z/2}e^{ia_2X/2}X^{s_2}Z^{s_1} \\
& = X^{s_4}Z^{s_3}X^{s_2}Z^{s_1}e^{i(-1)^{s_3+s_1}a_4X/2}e^{i(-1)^{s_2}a_3Z/2}e^{i(-1)^{s_1}a_2X/2} \\
& \propto Z^{s_1+s_3}X^{s_2+s_4}e^{i(-1)^{s_3+s_1}a_4X/2}e^{i(-1)^{s_2}a_3Z/2}e^{i(-1)^{s_1}a_2X/2}(\text{phase} = (-1)^{s_1+s_4})
\end{aligned}$$

11： 推导 CNOT 门构造中的关系式。

解： 注意：作用在不同位置的比特是互相对易的。对于 CNOT 我们有：

$$CNOT_{ct} = |0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes X_t$$

所以：

$$\begin{aligned}
CNOT(X_c)CNOT &= (|0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes X_t)X_c(|0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes X_t) \\
&= (|0\rangle\langle 1|_c \otimes I_t + |1\rangle\langle 0|_c \otimes X_t)(|0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes X_t) \\
&= (|0\rangle\langle 1|_c + |1\rangle\langle 0|_c) \otimes x_T = x_C \otimes X_t
\end{aligned}$$

随后按照定理，我们需要计算 $\sigma_{i \in S_i}^x U \sigma_{i \in S_o}^x U^\dagger |\Phi\rangle_{S_i \cup S_o}$ 和 $\sigma_{i \in S_i}^z U \sigma_{i \in S_o}^z U^\dagger |\Phi\rangle_{S_i \cup S_o}$ ，其中 $|\Phi\rangle$ 为图态 $|G\rangle$ 在 S_M 上测量之后的态。这里我们选择第一个进行计算：在这个构型中我们对 2,3,4,5,6,8,12 位置进行 Y 测量，对 10,11,13,14 位置进行 X 测量。1,9 和 7,15 分别为输入输出。那么我们有：

$$|\phi\rangle_{1,7,9,15} = Y_2 Y_3 Y_4 Y_5 Y_6 Y_8 X_{10} X_{11} Y_{12} X_{13} X_{14} |G\rangle$$

在 $|\phi\rangle_{1,7,9,15}$ 中，其他位置的比特按照之前的测量理论已经坍塌为对应测量算符的本征态 $|k, \pm\rangle, k = x/y$ ，其中 \pm 的选取和测量结果 s 有关。稳定子乘法运算比较简单，这里不做证明。

我们选取其中之一进行说明，其他的计算方法相同。

$$\begin{aligned}
X_1 CNOT(X_7) CNOT |\phi\rangle_{1,7,9,15} &= X_1 X_7 X_{15} |\phi\rangle_{1,7,9,15} (\text{代入上面表达式}) \\
&= X_1 Y_2 Y_3 Y_4 Y_5 Y_6 X_7 Y_8 X_{10} X_{11} Y_{12} X_{13} X_{14} X_{15} |G\rangle
\end{aligned}$$

通过稳定子连乘我们有：

$$K_1 K_3 K_4 K_5 K_7 K_8 K_{13} K_{15} = -X_1 Y_3 Y_4 Y_5 X_7 Y_8 X_{13} X_{15}$$

代入上面表达式：

$$X_1 Y_2 Y_3 Y_4 Y_5 Y_6 X_7 Y_8 X_{10} X_{11} Y_{12} X_{13} X_{14} X_{15} |G\rangle = -Y_2 Y_6 X_{10} X_{11} Y_{12} X_{14} K_1 K_3 K_4 K_5 K_7 K_8 K_{13} K_{15} |G\rangle$$

由稳定子性质我们可以简化为 $-Y_2Y_6X_{10}X_{11}Y_{12}X_{14}|G\rangle$. 这些算子仅仅是一开始得到 $|\phi\rangle_{1,7,9,15}$ 中的测量算子的一部分。并且泡利矩阵的平方为单位阵，我们补全测量算子：

$$\begin{aligned} -Y_2Y_6X_{10}X_{11}Y_{12}X_{14}|G\rangle &= (Y_3Y_4Y_5Y_8X_{13}Y_3Y_4Y_5Y_8X_{13}) - Y_2Y_6X_{10}X_{11}Y_{12}X_{14}|G\rangle \\ &= -Y_3Y_4Y_5Y_8X_{13}|\phi\rangle_{1,7,9,15} \end{aligned}$$

对于 $\sigma_k, k = x/y$ 的测量，按照之前的约定，结果为 $|k+\rangle, s = 0$ ；结果为 $|k-\rangle, s = 1$ 。我们有：

$$\sigma_k = |k+\rangle\langle k+| - |k-\rangle\langle k-| \quad \sigma_k|k\pm\rangle = \pm|k\pm\rangle = (-1)^s|k\pm\rangle$$

因此上面表达式结果为：

$$-(-1)^{s_3+s_4+s_5+s_8+s_{13}}|\phi\rangle_{1,7,9,15} = (-1)^{1+s_3+s_4+s_5+s_8+s_{13}}|\phi\rangle_{1,7,9,15}$$