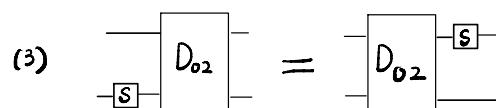
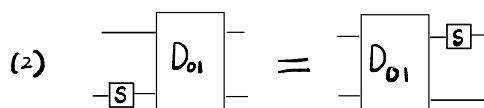
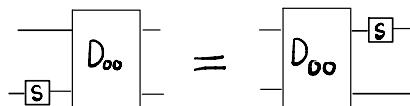


Def 3: $\text{X} := \text{H} \text{---} \bullet \text{---} \text{H} \text{---} \bullet \text{---} \text{H} \text{---} \bullet$

C_7 : (1) $\text{S} = \text{S}$ (2) $\text{S} = \text{S}$ $C_3 : S^3 = I$

R_{18} : (1) $\text{S} \text{---} \text{X} = \text{X} \text{---} \text{S}$ (2) $\text{S} \text{---} \text{X} = \text{X} \text{---} \text{S}$

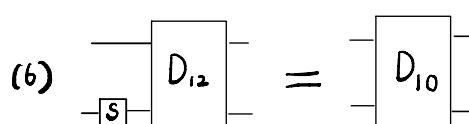
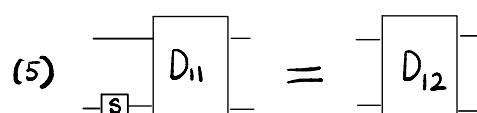
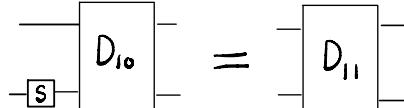
Lem 8 By Def 3, C_3 , C_7 & R_{18} , q. (1)



Proof: q. (1)/(2)/(3). LHS = $\text{S} \text{---} \text{X} \text{---} \text{CZ}^{2b} \stackrel{R_{18}}{=} \text{X} \text{---} \text{S} \text{---} \text{CZ}^{2b}$

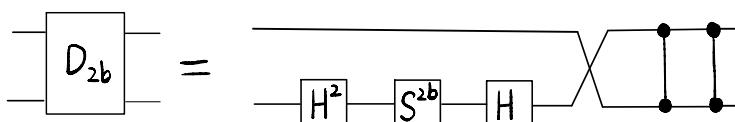
$\stackrel{C_7}{=} \text{S} \text{---} \text{X} \text{---} \text{CZ}^{2b} \stackrel{\text{def}}{=} D_{ob} = \text{q. (1)/(2)/(3). RHS. } \square$

Lem 9 By C_3 , q. (4)



Proof: q. (4)/(5)/(6). LHS = $D_{1b} := S^b S^b H$ $\stackrel{C_3}{=}$

$\text{S}^{b+1} \text{---} \text{H} \text{---} \text{X} \text{---} \text{S}^{b+1} \text{---} \text{H} \stackrel{\text{def}}{=} D_{1,b+1} = \text{q. (4)/(5)/(6). RHS. } \square$



Def 3:

$$R_{13}: (1) \quad \begin{array}{c} \bullet \\ \text{---} \end{array} \otimes \begin{array}{c} \bar{z} \\ \text{---} \end{array} = \begin{array}{c} \bar{z} \\ \text{---} \end{array} \otimes \begin{array}{c} \bullet \\ \text{---} \end{array} \quad (2) \quad \begin{array}{c} \bullet \\ \text{---} \end{array} \otimes \begin{array}{c} \bar{z} \\ \text{---} \end{array} = \begin{array}{c} \bar{z} \\ \text{---} \end{array} \otimes \begin{array}{c} \bullet \\ \text{---} \end{array}$$

$$R_{14}: (1) \quad \begin{array}{c} \bullet \\ \text{---} \end{array} \otimes \begin{array}{c} X \\ \text{---} \end{array} = \begin{array}{c} X \\ \text{---} \end{array} \otimes \begin{array}{c} \bullet \\ \text{---} \end{array} \quad (2) \quad \begin{array}{c} \bullet \\ \text{---} \end{array} \otimes \begin{array}{c} X \\ \text{---} \end{array} = \begin{array}{c} X \\ \text{---} \end{array} \otimes \begin{array}{c} \bullet \\ \text{---} \end{array}$$

$$(3) \quad \begin{array}{c} X \\ \text{---} \end{array} \otimes \begin{array}{c} \bullet \\ \text{---} \end{array} = \begin{array}{c} \bullet \\ \text{---} \end{array} \otimes \begin{array}{c} X \\ \text{---} \end{array} \quad (4) \quad \begin{array}{c} X \\ \text{---} \end{array} \otimes \begin{array}{c} \bullet \\ \text{---} \end{array} = \begin{array}{c} \bullet \\ \text{---} \end{array} \otimes \begin{array}{c} X \\ \text{---} \end{array}$$

$$R_{18}: (1) \quad \begin{array}{c} S \\ \text{---} \end{array} \otimes \begin{array}{c} \times \\ \text{---} \end{array} = \begin{array}{c} \times \\ \text{---} \end{array} \otimes \begin{array}{c} S \\ \text{---} \end{array} \quad (2) \quad \begin{array}{c} S \\ \text{---} \end{array} \otimes \begin{array}{c} \times \\ \text{---} \end{array} = \begin{array}{c} \times \\ \text{---} \end{array} \otimes \begin{array}{c} S \\ \text{---} \end{array}$$

$$R_{19}: (1) \quad \begin{array}{c} H \\ \text{---} \end{array} \otimes \begin{array}{c} \times \\ \text{---} \end{array} = \begin{array}{c} \times \\ \text{---} \end{array} \otimes \begin{array}{c} H \\ \text{---} \end{array} \quad (2) \quad \begin{array}{c} H \\ \text{---} \end{array} \otimes \begin{array}{c} \times \\ \text{---} \end{array} = \begin{array}{c} \times \\ \text{---} \end{array} \otimes \begin{array}{c} H \\ \text{---} \end{array} \quad R_{12}: \bar{z}^3 = I$$

Lem 10 By Def 3, C₂, C₃, C₅,

R₄, R₁₀, R₁₂, R₁₃, R₁₄, R₁₈ & R₁₉,

$$q.(7) \quad \begin{array}{c} D_{20} \\ \text{---} \end{array} = \begin{array}{c} D_{22} \\ \text{---} \end{array} \otimes \begin{array}{c} X \\ \text{---} \end{array}$$

$$(8) \quad \begin{array}{c} D_{21} \\ \text{---} \end{array} = \begin{array}{c} D_{20} \\ \text{---} \end{array} \otimes \begin{array}{c} X \\ \text{---} \end{array}$$

$$(9) \quad \begin{array}{c} D_{22} \\ \text{---} \end{array} = \begin{array}{c} D_{21} \\ \text{---} \end{array} \otimes \begin{array}{c} X \\ \text{---} \end{array}$$

$$\text{Proof: } q.(7)/(8)/(9). LHS = \begin{array}{c} D_{2b} \\ \text{---} \end{array} := \begin{array}{c} \boxed{S \otimes H^2 \otimes S^{2b} \otimes H} \otimes \begin{array}{c} \times \\ \text{---} \end{array} \end{array}$$

$$\begin{array}{c} \bar{z} \\ \text{---} \end{array} \otimes \begin{array}{c} S \otimes H^2 \otimes S^{2b} \otimes H \\ \text{---} \end{array} \quad (1)$$

$$q.(7)/(8)/(9). RHS = \begin{array}{c} \boxed{H^2 \otimes S^{2b+1} \otimes H} \otimes \begin{array}{c} X \\ \text{---} \end{array} \end{array} \quad S^{2(b+2)} = S^{2b+4} = S^{2b+1}$$

$$\begin{array}{c} \bar{z} \\ \text{---} \end{array} \otimes \begin{array}{c} H^2 \otimes S^{2b+1} \otimes H \\ \text{---} \end{array} \quad (2)$$

$$\begin{array}{c} \bar{z} \\ \text{---} \end{array} \otimes \begin{array}{c} H^2 \otimes S^{2b+1} \otimes H \otimes X \\ \text{---} \end{array} \quad \begin{array}{c} \bar{z} \\ \text{---} \end{array} \otimes \begin{array}{c} H^2 \otimes S^{2b+1} \otimes H \otimes X \\ \text{---} \end{array} \quad (2)$$

$$R_4 : \boxed{H} - \boxed{Z} - \boxed{H^+} = \boxed{X}$$

$$C_5 : SH^2SH^2 = H^2SH^2S$$

$$SS' = S'S$$

$$R_{10} : \boxed{Z} = \boxed{S'} - \boxed{S'} - \boxed{S}$$

$$\text{Def: } S' := H^2SH^2 \quad S'^2 := H^2S^2H^2 \quad C_2 : H^4 = I \quad C_3 : S^3 = I$$

To show (1) = (2), it is sufficient to show

$$\boxed{S} - \boxed{H^2} - \boxed{S^{2b}} - \boxed{H} = \boxed{H^2} - \boxed{S^{2b+1}} - \boxed{H} - \boxed{X} \quad (3)$$

Composition
in diagrammatic
order →

$$(3) \text{ RHS} = H^2 S^{2b+1} H \boxed{X} \stackrel{R_4}{=} H S^{2b+1} H H \boxed{Z} H^+ \stackrel{R_{10}}{=} H S^{2b+1} H^2 \boxed{S'S'} S H^+ \stackrel{\text{def}}{=} \\ H^2 S^{2b+1} \boxed{H^2} \boxed{H^2} S^2 H^2 S H^+ \stackrel{C_2}{=} H^2 \boxed{S^{2b+1}} \boxed{S^2} H^2 S H^+ \stackrel{C_3}{=} H^2 S^{2b} \boxed{H^2} S H^+ \stackrel{\text{def}}{=} \\ H^2 \boxed{S^{2b}} \boxed{S'} H \stackrel{C_5}{=} H^2 S' S^{2b} H \stackrel{\text{def}}{=} \boxed{H^2 H^2} S H^2 S^{2b} H \stackrel{C_2}{=} S H^2 S^{2b} H = (3) \text{ LHS}$$



Lem 10

$$\boxed{S} - \boxed{H^2} - \boxed{S^{2b}} - \boxed{H} = \boxed{H^2} - \boxed{S^{2b+1}} - \boxed{H} - \boxed{X}$$