

Def 3: :=

$R_{16}$ : =

Lem A By Def 3 &  $R_{16}$ ,  $R_{18}:(1)$  = implies  $R_{18}:(2)$  =

Proof:  $R_{18}:(2)$ . LHS :=  $\stackrel{R_{16}}{=}$   $\stackrel{R_{18}:(1)}{=}$

$\stackrel{R_{16}}{=}$  =  $R_{18}:(2)$ . RHS □

Lem B By Def 3 &  $R_{16}$ ,  $R_{19}:(1)$  = implies  $R_{19}:(2)$  =

Proof:  $R_{19}:(2)$ . LHS :=  $\stackrel{R_{16}}{=}$   $\stackrel{R_{19}:(1)}{=}$

$\stackrel{R_{16}}{=}$  =  $R_{19}:(2)$ . RHS □

Prop 1 Let  $\ell_1 := \langle H, S, -w \rangle$ .  $\forall u \in \ell_1$  = (1) and = (2)

Proof:  $\forall u \in \ell_1$ ,  $\exists t \in \mathbb{Z}_6$  and  $m \in \mathbb{N}$  st.  $u = (-w)^t H^{a_0} S^{b_0} H^{a_1} S^{b_1} \dots H^{a_m} S^{b_m}$ , composition in diagrammatic order,  $a_i, b_i \in \mathbb{Z}_2$ ,  $0 \leq i \leq m$ . We proceed by induction on  $m$ .

Base Case: ①  $m=0$ ,  $a_0=b_0=0$ .  $u = (-w)^t$  is a scalar. (1) & (2) hold trivially.

②  $m=0$ ,  $a_0=1$  and  $b_0=0$ .  $u = (-w)^t H$ . By Lem A, (1) & (2) hold.

③  $m=0$ ,  $a_0=0$  and  $b_0=1$ .  $u = (-w)^t S$ . By Lem B, (1) & (2) hold.

Induction Hypothesis: (1) & (2) hold for  $m \geq 0$ . That is, when  $u = (-w)^t H^{a_0} S^{b_0} H^{a_1} S^{b_1} \dots H^{a_m} S^{b_m}$

= (3) and = (4)

Induction Step: When  $u' = u H^{a_{m+1}} S^{b_{m+1}}$ , WTS = (5) & = (6).

(5). LHS :=  $\stackrel{\text{Lem A}}{=}$   $\stackrel{\text{Lem B}}{=}$   $\stackrel{\text{IH}}{=}$   $\stackrel{\text{def}}{=}$

=: (5). RHS (6). LHS :=  $\stackrel{\text{Reasoning analogously as before}}{=}$  =: (6). RHS

This completes the proof. □

Def 1 :  $\boxed{s'} := \boxed{H} \rightarrow \boxed{H} \rightarrow \boxed{S} \rightarrow \boxed{H} \rightarrow \boxed{H}$

R5 :  $\boxed{x} = \boxed{H} \rightarrow \boxed{S} \rightarrow \boxed{H} \rightarrow \boxed{H} \rightarrow \boxed{S} \rightarrow \boxed{S} \rightarrow \boxed{H}$

R10 :  $\boxed{z} = \boxed{H} \rightarrow \boxed{H} \rightarrow \boxed{S} \rightarrow \boxed{S} \rightarrow \boxed{H} \rightarrow \boxed{H} \rightarrow \boxed{S} = \boxed{s'} \rightarrow \boxed{S'} \rightarrow \boxed{S}$

Prop 1 Let  $\ell_1 := \langle H, S, -w \rangle$ .  $\forall u \in \ell_1$

$$\begin{array}{c} \boxed{u} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{u} \end{array} \text{ (1) and } \begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{u} \end{array} = \begin{array}{c} \boxed{u} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \end{array} \text{ (2)}$$

Cor 1 R<sub>20</sub>: (1)  $\begin{array}{c} \boxed{x} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{x} \end{array}$

(2)  $\begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{x} \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{x} \end{array}$

R<sub>21</sub>: (1)  $\begin{array}{c} \boxed{z} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{z} \end{array}$

(2)  $\begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{z} \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{z} \end{array}$

R<sub>22</sub>: (1)  $\begin{array}{c} \boxed{s'} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{s'} \end{array}$

(2)  $\begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{s'} \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \boxed{s'} \end{array}$

Proof: By Def 1, R<sub>5</sub>, R<sub>10</sub> & Prop 1.

$$\text{Def 3: } \text{Diagram} := \text{Diagram} \quad R_{16}: \text{Diagram} = \text{Diagram} \quad R_{17}: \text{Diagram} = \text{Diagram}$$

$$R_{18}: (1) \text{Diagram} = \text{Diagram} \quad (2) \text{Diagram} = \text{Diagram}$$

$$R_{19}: (1) \text{Diagram} = \text{Diagram} \quad (2) \text{Diagram} = \text{Diagram}$$

$$R_{21}: (1) \text{Diagram} = \text{Diagram} \quad (2) \text{Diagram} = \text{Diagram}$$

Lem C By Def3,  $R_{16}$ ,  $R_{17}$  &  $R_{18}$ ,

$$C_7: (1) \text{Diagram} = \text{Diagram} \quad \text{implies} \quad (2) \text{Diagram} = \text{Diagram}$$

$$\text{Proof: } C_7.(2). \text{RHS} := \text{Diagram} \stackrel{R_{16}}{=} \text{Diagram} \stackrel{R_{17}}{=} \text{Diagram} \stackrel{R_{18}}{=} \text{Diagram} \stackrel{C_7.(1)}{=}$$

$$\text{Diagram} \stackrel{R_{17}}{=} \text{Diagram} \stackrel{R_{16}}{=} \text{Diagram} \stackrel{R_{16}}{=} \text{Diagram} =: C_7.(2). \text{LHS} \quad \square$$

Lem D By Def3,  $R_{16}$ ,  $R_{17}$  &  $R_{19}$ ,

$$C_8: (1) \text{Diagram} = \text{Diagram} \quad \text{implies} \quad (2) \text{Diagram} = \text{Diagram}$$

$$\text{Proof: } C_8.(2). \text{RHS} := \text{Diagram} \stackrel{R_{16}}{=} \text{Diagram} \stackrel{R_{17}}{=} \text{Diagram} \stackrel{R_{19}}{=} \text{Diagram}$$

$$\text{Diagram} \stackrel{R_{17}}{=} \text{Diagram} \stackrel{R_{16}}{=} \text{Diagram} \stackrel{R_{16}}{=} \text{Diagram} =: C_8.(2). \text{LHS} \quad \square$$

Lem E By Def3,  $R_{16}$ ,  $R_{17}$  &  $R_{21}$ ,

$$R_{13}: (1) \text{Diagram} = \text{Diagram} \quad \text{implies} \quad (2) \text{Diagram} = \text{Diagram}$$

$$\text{Proof: } R_{13}.(2). \text{RHS} := \text{Diagram} \stackrel{R_{16}}{=} \text{Diagram} \stackrel{R_{17}}{=} \text{Diagram} \stackrel{R_{21}}{=} \text{Diagram}$$

$$\text{Diagram} \stackrel{R_{17}}{=} \text{Diagram} \stackrel{R_{16}}{=} \text{Diagram} =: R_{13}.(2). \text{LHS} \quad \square$$

Def 1 :  $s' := H H S H H$

Def 3 :  $\times := H \cdot H \cdot H \cdot H \cdot H$        $R_{16} : \times \times \times = \quad$        $R_{17} : \bullet \bullet \times \times = \times \times \bullet \bullet$

$R_{13} : (1) \times \bullet Z = Z \bullet \times$       (2)  $\bullet Z = Z \bullet$

$R_{20} : (1) X \times = \times X \times$       (2)  $X \times = \times X$

$R_{21} : (1) Z \times = \times \times Z$       (2)  $Z \times = \times Z \times$

$$R_{12} : Z^3 = I$$

Lem F By Def3,  $R_{16}$ ,  $R_{17}$ ,  $R_{20}$  &  $R_{21}$ ,

$R_{14} : (1) \bullet X = \bullet Z Z \bullet \text{ implies } (2) \bullet \bullet X = \bullet Z Z \bullet X$

Proof:  $R_{14}.(2).RHS := \bullet Z Z \bullet X \stackrel{R_{16}}{=} \bullet Z Z \bullet \times \times \times \stackrel{\frac{R_{17}, R_{20}}{R_{21}}}{=} \times \times \times \bullet Z Z \bullet X$

$\underline{R_{14}.(1)} \times \bullet X \stackrel{R_{17}}{\underline{R_{20}}} \times \times \times \bullet X \stackrel{R_{16}}{=} \bullet \bullet X =: R_{14}.(2).LHS$   $\square$

Lem G By  $R_{12}$  &  $R_{13}$ ,

$R_{14} : (1) \bullet X = \bullet Z Z \bullet \text{ implies } (3) \bullet X = \bullet \bullet Z$

Proof:  $R_{14}.(3).LHS := \bullet X \bullet \bullet \stackrel{R_{12}}{=} \bullet Z Z^2 \bullet \stackrel{R_{14}.(1)}{=} \bullet Z \bullet X \stackrel{R_{13}}{=} \bullet X \bullet Z$   
 $=: R_{14}.(3).RHS.$   $\square$

Lem H By Def3,  $R_{16}$ ,  $R_{17}$ ,  $R_{20}$  &  $R_{21}$ ,

$R_{14} : (3) \bullet X \bullet = \bullet \bullet X \bullet \text{ implies } (4) \bullet X \bullet = \bullet \bullet Z$

Proof:  $R_{14}.(4).RHS := \bullet Z \bullet X \stackrel{R_{16}}{=} \bullet Z \bullet \times \times \times \stackrel{\frac{R_{17}, R_{20}}{R_{21}}}{=} \times \times \times \bullet Z \bullet X$

$\underline{R_{14}.(3)} \times \bullet X \bullet \stackrel{R_{17}}{\underline{R_{20}}} \times \times \times \bullet X \stackrel{R_{16}}{=} \bullet \bullet X =: R_{14}.(4).LHS$   $\square$

$$\text{Def 1 : } \boxed{s'} := \boxed{H} \quad \boxed{H} \quad \boxed{S} \quad \boxed{H} \quad \boxed{H} \quad C_6 : \quad \begin{array}{c} \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \end{array} = \quad \quad \quad$$

$$R_{13} : (1) \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \boxed{Z} = \quad \boxed{Z} \quad (2) \quad \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{Z} = \quad \quad \quad$$

$$C_7 : (1) \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \boxed{S} = \quad \boxed{S} \quad (2) \quad \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{S} = \quad \quad \quad$$

$$C_8 : (1) \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \boxed{H^2} = \quad \boxed{H^2} \quad (2) \quad \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^2} = \quad \quad \quad$$

$$\text{Def 3 : } \begin{array}{c} \diagup & \diagdown \\ \diagdown & \diagup \end{array} := \quad \boxed{H} \quad \boxed{H} \quad \boxed{H} \quad \boxed{H} \quad \quad R_{16} : \quad \begin{array}{c} \diagup & \diagdown & \diagup & \diagdown \\ \diagdown & \diagup & \diagdown & \diagup \end{array} = \quad \quad \quad R_{17} : \quad \begin{array}{c} \bullet \\ \bullet \end{array} \quad \begin{array}{c} \diagup & \diagdown \\ \diagdown & \diagup \end{array} = \quad \quad \quad \begin{array}{c} \diagup & \diagdown \\ \diagdown & \diagup \end{array} \quad \begin{array}{c} \bullet \\ \bullet \end{array}$$

$$R_{19} : (1) \quad \begin{array}{c} \diagup & \diagdown \\ \diagdown & \diagup \end{array} \boxed{H} = \quad \begin{array}{c} \diagup & \diagdown \\ \diagdown & \diagup \end{array} \quad (2) \quad \begin{array}{c} \diagup & \diagdown \\ \diagdown & \diagup \end{array} \boxed{H} = \quad \begin{array}{c} \diagup & \diagdown \\ \diagdown & \diagup \end{array} \quad C_2 : \quad H^4 = I$$

Lem K By Def3,  $R_{16}$ ,  $R_{17}$ ,  $R_{19}$ ,  $C_6$ ,  $C_2$  &  $C_8$ ,

$$C_8^1 : (1) \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \boxed{H^2} = \quad \boxed{H^2} \quad (2) \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \boxed{H^2} = \quad \quad \quad$$

$$C_8^2 : \quad \boxed{H^2} \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} = \quad \begin{array}{c} \bullet \\ \bullet \end{array} \quad C_8^4 : \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} \quad \boxed{H^2} = \quad \begin{array}{c} \bullet \\ \bullet \end{array}$$

$$C_8^3 : \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} = \quad \boxed{H^2} \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} = \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} = \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array}$$

$$\text{Proof: } C_8^1.(1).LHS := \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} \quad \underline{\underline{C_8}} \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} \quad \underline{\underline{C_8}} \quad \begin{array}{c} \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \end{array} \quad \boxed{H^2} \quad \underline{\underline{C_6}} \quad \begin{array}{c} \bullet \\ \bullet \end{array}$$

$$=: C_8^1.(1).RHS. \quad C_8^1.(2).LHS := \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} \quad \underline{\underline{R_{16}}} \quad \begin{array}{c} \diagup & \diagdown & \diagup & \diagdown \\ \diagdown & \diagup & \diagdown & \diagup \end{array} \quad \boxed{H^2} \quad \underline{\underline{R_{19}}} \quad \begin{array}{c} \bullet \\ \bullet \end{array} \quad \underline{\underline{R_{17}}}$$

$$\begin{array}{c} \diagup & \diagdown & \diagup & \diagdown \\ \diagdown & \diagup & \diagdown & \diagup \end{array} \quad \boxed{H^2} \quad \underline{\underline{C_8^1.(1)}} \quad \begin{array}{c} \diagup & \diagdown & \diagup & \diagdown \\ \diagdown & \diagup & \diagdown & \diagup \end{array} \quad \boxed{H^2} \quad \underline{\underline{R_{19}}} \quad \begin{array}{c} \diagup & \diagdown & \diagup & \diagdown \\ \diagdown & \diagup & \diagdown & \diagup \end{array} \quad \boxed{H^2} \quad \underline{\underline{R_{16}}} \quad \begin{array}{c} \bullet \\ \bullet \end{array}$$

$$=: C_8^1.(2).RHS.$$

$$C_8^2.LHS := \quad \boxed{H^2} \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} \quad \underline{\underline{C_8^1}} \quad \begin{array}{c} \bullet & \bullet \\ \bullet & \bullet \end{array} \quad \boxed{H^2} \quad \underline{\underline{C_2}} \quad \begin{array}{c} \bullet \\ \bullet \end{array} =: C_8^2.RHS$$

Def 1 :  $s' := H \otimes H \otimes S \otimes H \otimes H$

$$C_6 : \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \quad \quad \quad$$

$$R_{13} : (1) \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} \quad (2) \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}$$

$$C_7 : (1) \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} \quad (2) \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}$$

$$C_8 : (1) \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} \quad (2) \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}$$

Def 3 :  $\begin{array}{c} \diagup \\ \diagdown \end{array} := \begin{array}{c} H \\ H \\ H \\ H \end{array}$

$$R_{16} : \begin{array}{c} \diagup \\ \diagdown \\ \diagup \\ \diagdown \end{array} = \quad \quad \quad$$

$$R_{17} : \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \diagup \\ \diagdown \\ \diagup \\ \diagdown \end{array}$$

$$R_{19} : (1) \quad \begin{array}{c} H \\ \diagup \\ \diagdown \end{array} = \begin{array}{c} \diagup \\ \diagdown \\ H \end{array} \quad (2) \quad \begin{array}{c} H \\ \diagup \\ \diagdown \end{array} = \begin{array}{c} \diagup \\ H \\ \diagdown \end{array}$$

$$C_2 : H^4 = I$$

Lem K By Def3,  $R_{16}$ ,  $R_{17}$ ,  $R_{19}$ ,  $C_6$ ,  $C_2$  &  $C_8$ ,

$$C_8^1 : (1) \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} \quad (2) \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}$$

$$C_8^2 : \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} \quad C_8^4 : \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}$$

$$C_8^3 : \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}$$

$$\text{Proof cont: } C_8^4. \text{LHS} := \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} \quad \stackrel{R_{16}}{=} \quad \boxed{\begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}} \quad \begin{array}{c} \diagup \\ \diagdown \\ \diagup \\ \diagdown \end{array} \quad \stackrel{R_{19}}{=} \quad \boxed{\begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}} \quad \begin{array}{c} \diagup \\ \diagdown \\ \diagup \\ \diagdown \end{array} \quad \stackrel{R_{17}}{=}$$

$$\begin{array}{c} \diagup \\ \diagdown \\ \diagup \\ \diagdown \end{array} \quad \stackrel{C_8^2}{=} \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} \quad \stackrel{R_{17}}{=} \quad \begin{array}{c} \diagup \\ \diagdown \\ \diagup \\ \diagdown \end{array} \quad \stackrel{R_{16}}{=} \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} =: C_8^4. \text{RHS.}$$

$$C_8^3. \text{MID} := \boxed{\begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}} \quad \stackrel{C_8^1}{=} \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} =: C_8^3. \text{RHS.}$$

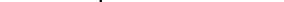
$$C_8^3. \text{MID} := \boxed{\begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}} \quad \stackrel{C_2}{=} \quad \boxed{\begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}} \quad \stackrel{C_8^2}{=} \quad \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} =: C_8^3. \text{LHS.}$$

$$\text{Def 3: } \begin{array}{c} \text{Diagram of two crossed lines} \end{array} := \begin{array}{c} \text{Diagram of two crossed lines} \\ \text{with a horizontal line above it containing three boxes labeled H} \end{array} \quad R_{16}: \begin{array}{c} \text{Diagram of four crossed lines} \end{array} = \begin{array}{c} \text{Diagram of four crossed lines} \\ \text{with a horizontal line above it containing three boxes labeled H} \end{array} \quad R_{17}: \begin{array}{c} \text{Diagram of four crossed lines} \end{array} = \begin{array}{c} \text{Diagram of four crossed lines} \\ \text{with a horizontal line above it containing three boxes labeled H} \end{array}$$

$$R_{22} : (1) \quad \begin{array}{c} S' \\ \square \end{array} \quad \begin{array}{c} \diagup \\ \diagdown \end{array} = \begin{array}{c} \diagdown \\ \diagup \end{array} \quad \begin{array}{c} S' \\ \square \end{array}$$

$$C_7:(1) \quad \text{Diagram: Two horizontal lines. The top line has a dot at the left end and a square box labeled 'S' at the right end. The bottom line has a dot at the left end and a vertical line segment connecting it to the 'S' box. An equals sign follows. Diagram: Two horizontal lines. The top line has a square box labeled 'S' at the left end and a dot at the right end. The bottom line has a dot at the left end and a vertical line segment connecting it to the 'S' box.} = (2) \quad \text{Diagram: Two horizontal lines. The top line has a dot at the left end and a vertical line segment connecting it to a square box labeled 'S' at the right end. The bottom line has a dot at the left end and a vertical line segment connecting it to the 'S' box. An equals sign follows. Diagram: Two horizontal lines. The top line has a dot at the left end and a vertical line segment connecting it to a square box labeled 'S' at the right end. The bottom line has a dot at the left end and a vertical line segment connecting it to the 'S' box.}$$

$$R_{15}: (1) \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \quad S' \quad = \quad \begin{array}{c} S' \\ \boxed{\phantom{S'}} \end{array} \quad (2) \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \quad S' \quad = \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \quad S' \quad \boxed{\phantom{S'}}$$

Lem I By  $C_7$  &  $C_8$ ,  $R_{15} : (1)$  

$$\text{Proof: R}_{15}.(1). \text{ LHS} := \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \boxed{S'} \quad \stackrel{\text{def}}{=} \quad \begin{array}{c} \bullet \\ \text{---} \\ \bullet \\ \text{---} \\ \bullet \end{array} \boxed{H^2} - S - \boxed{H^2} \quad \stackrel{C_8}{=} \quad \begin{array}{c} \bullet \\ \text{---} \\ \bullet \\ \text{---} \\ \bullet \end{array} \boxed{H^2} - \begin{array}{c} \bullet \\ \text{---} \\ \bullet \\ \text{---} \\ \bullet \end{array} \boxed{S} - \boxed{H^2} \quad \stackrel{C_7}{=}$$

$$\boxed{H^2 \quad S} \quad \boxed{\bullet \quad \bullet \quad H^2} \quad \stackrel{C_8'}{=} \quad \boxed{H^2 \quad S \quad H^2} \quad \stackrel{\text{def}}{=} \quad \boxed{S'} \quad =: R_{15}.(1).RHS$$

Lem J By Def3,  $R_{16}, R_{17}, R_{22}$ ,

$$R_{15}: (1) \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \boxed{S'} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{S'} \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \quad \text{implies} \quad (2) \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \boxed{S'} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{S'} \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array}$$

$$\text{Proof: } R_{15}.(2). \text{ RHS} := \begin{array}{c} \text{Diagram of } R_{15} \text{ with } S \text{ highlighted} \\ \equiv \end{array} \quad \begin{array}{c} \text{Diagram of } R_{15} \text{ with } S' \text{ highlighted} \\ \boxed{\text{Diagram of } R_{15} \text{ with } S' \text{ highlighted}} \\ \equiv \end{array} \quad \begin{array}{c} \text{Diagram of } R_{15} \text{ with } S' \text{ highlighted} \\ \boxed{\text{Diagram of } R_{15} \text{ with } S' \text{ highlighted}} \\ \equiv \end{array} \quad \begin{array}{c} \text{Diagram of } R_{15} \text{ with } S' \text{ highlighted} \\ \boxed{\text{Diagram of } R_{15} \text{ with } S' \text{ highlighted}} \\ \equiv \end{array} \quad \begin{array}{c} \text{Diagram of } R_{15} \text{ with } S' \text{ highlighted} \\ \boxed{\text{Diagram of } R_{15} \text{ with } S' \text{ highlighted}} \\ \equiv \end{array}$$

$$\text{Diagram 1} \quad \boxed{\text{Diagram 2}} \quad \stackrel{R_{17}}{=} \quad \text{Diagram 3} \quad \stackrel{R_{16}}{=} \quad \text{Diagram 4} =: R_{15}.(2).LHS$$

$$\text{Lem L By } C_7 \& R_{15}, R_{24}: \quad \begin{array}{c} \oplus \\ \bullet \\ S \end{array} = \begin{array}{c} \oplus \\ \bullet \\ S \end{array} \quad \& \quad R_{24}^1: \quad \begin{array}{c} \oplus \\ \bullet \\ S' \end{array} = \begin{array}{c} \oplus \\ \bullet \\ S' \end{array}$$

$$\text{Proof: } \begin{array}{c} I \\ \textcircled{+} \\ S \end{array} \quad := \quad \begin{array}{c} I \\ H^+ \\ H \\ H \\ H \\ H \\ S \end{array}$$

The diagram illustrates the decomposition of a single-qubit gate into a sequence of Hadamard gates. On the left, a circuit symbol for a single-qubit gate is shown with two horizontal lines labeled  $I$  and  $S'$ . This is followed by an equals sign ( $=$ ). To the right of the equals sign, the circuit is expanded into a sequence of four Hadamard gates ( $H$ ) connected in series. The first Hadamard gate is preceded by the label  $I$  above it and  $S'$  below it. The last Hadamard gate is followed by the label  $I$  above it and  $S'$  below it. A red arrow points to the right at the bottom of the expanded circuit.

$$R4 : H \bar{z}^2 H^+ = X \quad \text{---} \quad \boxed{\bar{z}^2} \boxed{H} = \boxed{H} \boxed{X}$$

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

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

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

Lem M

$$R_{26} : (1) \quad \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \boxed{X} \oplus = \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{X} \quad (2) \quad \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \boxed{\bar{z}} \oplus = \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{\bar{z}}$$

$$(3) \quad \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{X} = \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{X} \quad (4) \quad \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{\bar{z}} = \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{\bar{z}}$$

$$(5) \quad \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{X^2} = \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{X^2} \quad (6) \quad \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{\bar{z}^2} = \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \oplus \boxed{\bar{z}^2}$$

Proof: By R<sub>4</sub>, R<sub>13</sub> & R<sub>4</sub>,

$$\begin{array}{c} X \\ \text{---} \\ \bullet \end{array} \oplus := \begin{array}{c} X \\ \text{---} \\ \bullet \end{array} \boxed{H} \boxed{\bar{z}} \boxed{z} \boxed{X^2} \boxed{\bar{z}^2} \boxed{X} \quad \xrightarrow{\hspace{10cm}}$$

$$\begin{array}{c} z \\ \text{---} \\ \bullet \end{array} \oplus := \begin{array}{c} z \\ \text{---} \\ \bullet \end{array} \boxed{H} \boxed{X^2} \boxed{X} \boxed{\bar{z}^2} \boxed{H} \boxed{H} \quad \xrightarrow{\hspace{10cm}}$$

$$\begin{array}{c} I \\ \text{---} \\ \bullet \end{array} \oplus := \begin{array}{c} I \\ \text{---} \\ \bullet \end{array} \boxed{H} \boxed{\bar{z}} \boxed{X^2} \boxed{\bar{z}^2} \quad \xrightarrow{\hspace{10cm}}$$

$$\begin{array}{c} z \\ \text{---} \\ \bullet \end{array} \oplus := \begin{array}{c} z \\ \text{---} \\ \bullet \end{array} \boxed{H} \boxed{I} \quad \xrightarrow{\hspace{10cm}}$$

$$\begin{array}{c} \bullet \\ \text{---} \\ X \end{array} \oplus := \begin{array}{c} \bullet \\ \text{---} \\ X \end{array} \boxed{H} \boxed{\bar{z}^2} \quad \xleftarrow{\hspace{10cm}}$$

$$\begin{array}{c} z \\ \text{---} \\ \bullet \end{array} \oplus := \begin{array}{c} z \\ \text{---} \\ \bullet \end{array} \boxed{H} \boxed{X^2} \boxed{X} \quad \xleftarrow{\hspace{10cm}}$$

□