

$$R_{10}: \bar{z} = S' S' S$$

$$R_{11}: \bar{z}^2 = S' S S$$

$$R_{15}: (1) \quad \begin{array}{c} \bullet \\ \square \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \square \\ \bullet \end{array}$$

$$C_1: w^3 = I \quad C_2: H^4 = I \quad C_3: S^3 = I$$

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

Lem N  $R_B: (1) \quad \begin{array}{c} \bullet \\ \square \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bar{z} \\ \bullet \end{array}$

Proof:  $R_B. (1). LHS := \begin{array}{c} \bullet \\ \square \\ \bullet \end{array} \stackrel{R_{10}}{=} \boxed{\begin{array}{c} \bullet \\ S' S' S \\ \bullet \end{array}} \stackrel{C_7}{=} \boxed{\begin{array}{c} \bullet \\ S' S' S \\ \bullet \end{array}} \stackrel{R_{15}}{=} \begin{array}{c} \bullet \\ \bar{z} \\ \bullet \end{array}$

$\stackrel{R_{10}}{=} \begin{array}{c} \bullet \\ \bar{z} \\ \bullet \end{array} =: R_B. (1). RHS \quad \square$

Lem O:  $R_{23}: \begin{array}{c} \square \\ S \\ \oplus \\ \bullet \end{array} = \begin{array}{c} \oplus \\ \bullet \\ S \\ \bar{z} \\ \bar{z} \\ S \end{array} \cdot w^2 \quad \text{implies}$

$R_{23}^1: \begin{array}{c} \square \\ S \\ \oplus \\ \bullet \end{array} = \begin{array}{c} \oplus \\ \bullet \\ S \\ \bar{z} \\ \bar{z} \\ S' \end{array} \cdot w^2, \quad R_{23}^2: \begin{array}{c} \oplus \\ \bullet \\ S \\ \bar{z} \\ \bar{z} \\ S \end{array} = \begin{array}{c} \square \\ S \\ S \\ \oplus \\ \bullet \\ S \\ S \end{array} \cdot w^2$

$R_{23}^3: \begin{array}{c} \square \\ S \\ \oplus \\ \bullet \\ S' \\ S' \end{array} \cdot w = \begin{array}{c} \oplus \\ \bullet \end{array}$

Proof:  $R_{23}^1. LHS := \begin{array}{c} \square \\ S \\ \oplus \\ \bullet \end{array} \stackrel{R_{23}}{=} \begin{array}{c} \oplus \\ \bullet \\ S \\ \bar{z} \\ \bar{z} \\ S \end{array} \cdot w^2 \stackrel{R_{11}}{=}$

$\begin{array}{c} \oplus \\ \bullet \\ S \\ S' \\ \bar{z} \\ \bar{z} \\ S \end{array} \cdot w^2 \stackrel{C_3}{=} \begin{array}{c} \oplus \\ \bullet \\ S \\ S' \\ \bar{z} \\ \bar{z} \\ S \end{array} \cdot w^2 =: R_{23}^1. RHS$

$R_{23}^2. LHS := \begin{array}{c} \oplus \\ \bullet \\ S \\ S' \\ \bar{z} \\ \bar{z} \\ S \end{array} \stackrel{C_3}{=} \begin{array}{c} \square^2 \\ S^2 \\ \oplus \\ \bullet \\ S \\ S' \end{array} \stackrel{R_{23}^1}{=} \begin{array}{c} \square^2 \\ S^2 \\ \oplus \\ \bullet \\ S \\ S' \end{array} \cdot w^2 =: R_{23}^2. RHS$

$R_{23}^3. LHS := \begin{array}{c} \square \\ S \\ \oplus \\ \bullet \\ S' \\ S' \end{array} \cdot w \stackrel{R_{23}^1}{=} \begin{array}{c} \oplus \\ \bullet \\ S \\ S' \\ S \\ S' \end{array} \cdot w^2 \cdot w \quad \frac{C_1, C_2}{C_3}$

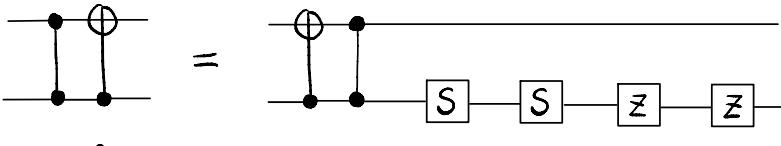
$\begin{array}{c} \oplus \\ \bullet \\ S \\ S' \\ S' \end{array} =: R_{23}^3. RHS \quad \square \quad 9$

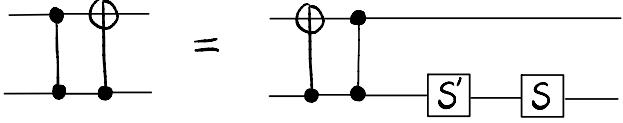
$$R_{11} : \bar{z}^2 = \bar{s}' s s$$

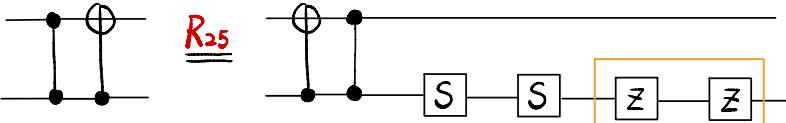
$$C_5 : SH^2 SH^2 = H^2 S H^2 S \quad SS' = s's \quad C_3 : S^3 = I$$

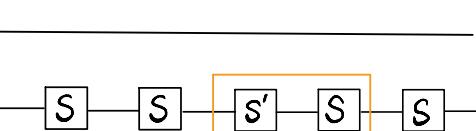
$$R_{11}^I : \bar{z}^2 s = \bar{s}'$$

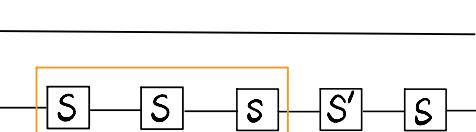

---

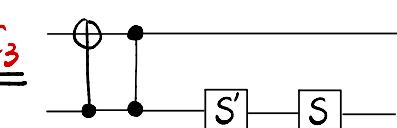
Lem P     $R_{25}$ :  • w iff

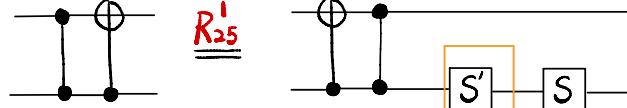
$R_{25}^I$ :  • w

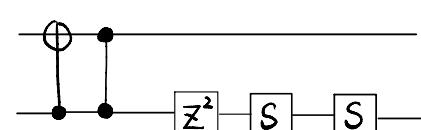
Proof:  $R_{25}^I$ . LHS :=  • w

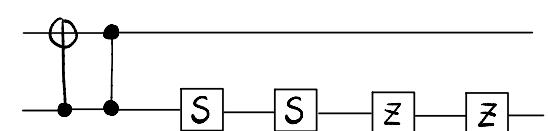
$\underline{R_{11}}$   • w

$\underline{C_5}$   • w

$\underline{C_3}$   • w =:  $R_{25}^I$  RHS.

$R_{25}$ . LHS :=  • w

$\underline{R_{11}^I}$   • w

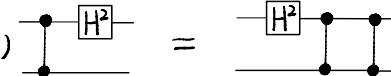
$\underline{C_5}$   • w =:  $R_{25}$ . RHS.

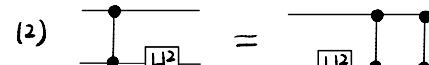
□

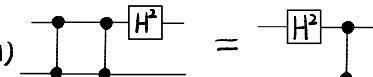
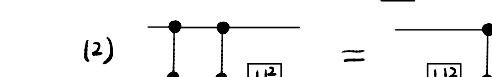
**Def 1:**  $\boxed{S'} := \boxed{H} \boxed{H} \boxed{S} \boxed{H} \boxed{H}$      $\boxed{S'} \boxed{S'} = \boxed{H} \boxed{H} \boxed{S} \boxed{S} \boxed{H} \boxed{H}$

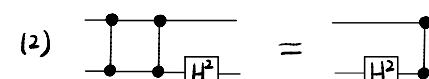
**R10:**  $\boxed{Z} = \boxed{S'} \boxed{S'} \boxed{S}$

**C2:**  $H^4 = I$     **C3:**  $S^3 = I$     **C5:**  $SH^2SH^2 = H^2SH^2S$      $SS' = S'S$

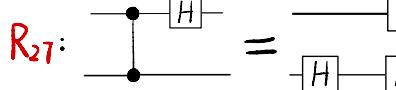
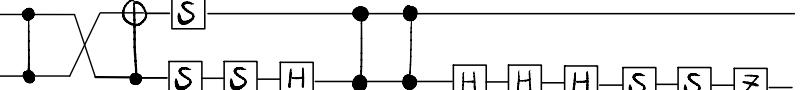
**C8:** (1)  = 

(2)  = 

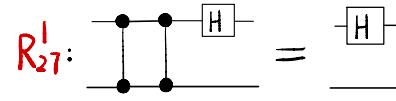
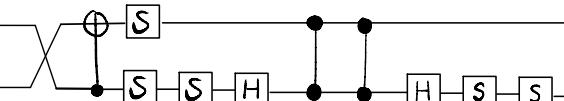
**C8':** (1)  = 

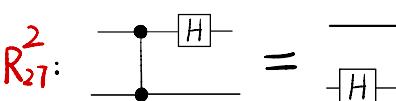
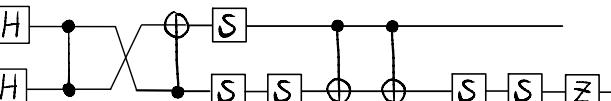
(2)  = 

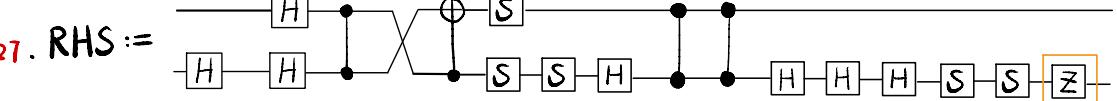
**Lem Q**

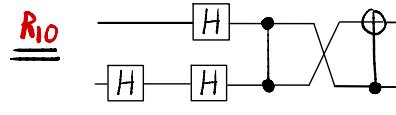
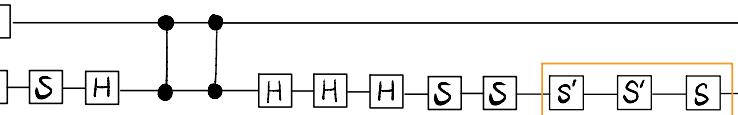
**R27:**  =  • w

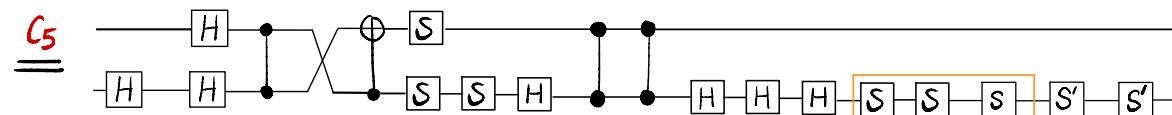
implies

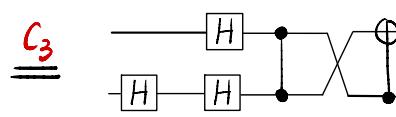
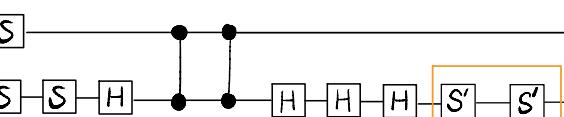
**R27<sup>1</sup>:**  =  • w &

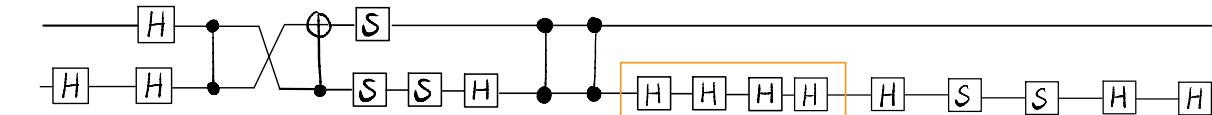
**R27<sup>2</sup>:**  =  • w

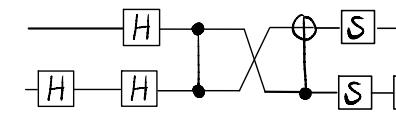
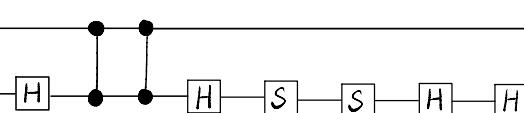
**Proof:** **R27.** RHS :=  • w

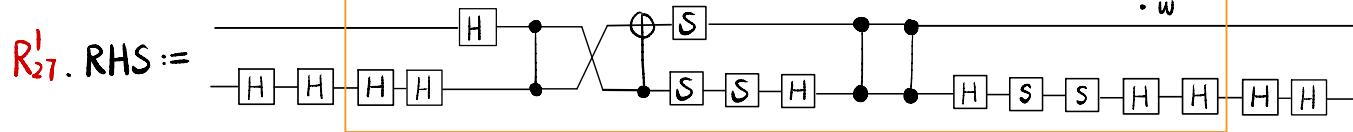
**R10**  =  • w

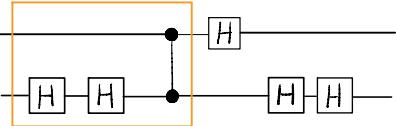
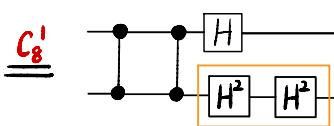
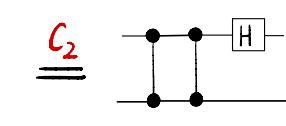
**C5**  • w

**C3**  =  • w

**Def1**  • w

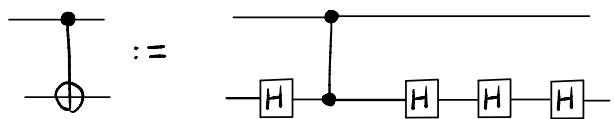
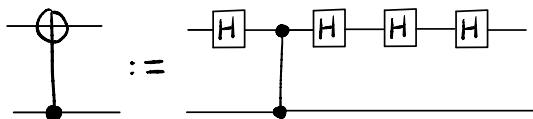
**C2**  =  • w

**R27<sup>1</sup>.** RHS :=  • w

**R27**  **C8'**  **C2**  =: **R27<sup>1</sup>.** LHS

**C2:  $H^4 = I$**

**Def 2:**



**Lem Q**  $R_{27}^1:$

implies  $R_{27}^1:$

$R_{27}^2:$

**Proof Cont.**  $R_{27}^2. LHS :=$

$\underline{R_{27}^2}:$

$\underline{C_2}:$

$\underline{\underline{Def 2}}:$

$$\text{Def 2: } \textcircled{1} := \text{H H H H}$$

$$C_2 : H^4 = I$$

$$C_3 : S^3 = I$$

$$R_{10} : \textcircled{z} = \text{S' S' S'}$$

$$C_5 : SH^2SH^2 = H^2SH^2S \quad SS' = S'S$$

$$\text{Lem R} \quad R_{28}: \text{H H H H} = \text{S S H H H H S H} \cdot w$$

$$\text{implies } R_{28}^1: \text{H H H H} = \text{S S H H H H S H} \cdot w \quad \&$$

$$R_{28}^2: \text{H H H H} = \text{S S O O S H} \cdot w$$

$$\text{Proof: } R_{28}^1. \text{ LHS} := \text{H H H H} = \text{S S H H H H S H} \cdot w$$

$$R_{10}: \text{S S H H H H S H} \cdot w$$

$$C_5: \text{S S H H H H S H} \cdot w$$

$$C_3: \text{S S H H H H S H} \cdot w =: R_{28}^1. \text{ RHS.}$$

$$R_{28}^2. \text{ LHS} := \text{H H H H} \underset{R_{28}^1}{=} \text{S S H H H H S H} \cdot w$$

$$C_2: \text{S S H H H H H H S H} \cdot w$$

$$\text{Def 2} \quad \text{S S O O S H} \cdot w =: R_{28}^2. \text{ RHS.}$$

□

$$\text{Def 2: } \begin{array}{c} \textcircled{+} \\ \parallel \end{array} := \begin{array}{c} \text{H} \quad \text{H} \quad \text{H} \quad \text{H} \\ \parallel \quad \parallel \quad \parallel \quad \parallel \end{array}$$

$$\begin{array}{c} \bullet \\ \parallel \end{array} := \begin{array}{c} \bullet \\ \text{H} \quad \text{H} \quad \text{H} \quad \text{H} \end{array}$$

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

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

Lem T By Def 2,  $R_{17}$  &  $R_{19}$ ,

$$R_{31}: (1) \begin{array}{c} \bullet \\ \bullet \\ \diagup \quad \diagdown \\ \diagdown \quad \diagup \\ \oplus \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \oplus \\ \diagup \quad \diagdown \\ \diagdown \quad \diagup \\ \bullet \end{array} \quad (2) \begin{array}{c} \bullet \\ \bullet \\ \diagup \quad \diagdown \\ \diagdown \quad \diagup \\ \oplus \\ \bullet \end{array} = \begin{array}{c} \oplus \\ \bullet \\ \bullet \\ \diagup \quad \diagdown \\ \diagdown \quad \diagup \\ \bullet \end{array}$$

$$\text{Proof: } R_{31}.(1). \text{ LHS} := \begin{array}{c} \bullet \\ \bullet \\ \diagup \quad \diagdown \\ \diagdown \quad \diagup \\ \oplus \\ \bullet \end{array} \stackrel{\text{Def 2}}{=} \begin{array}{c} \text{H} \quad \text{H} \quad \text{H} \quad \text{H} \\ \parallel \quad \parallel \quad \parallel \quad \parallel \end{array}$$

$$\begin{array}{c} \text{R}_{17} \\ \text{R}_{19} \end{array} \begin{array}{c} \text{H} \quad \text{H} \quad \text{H} \quad \text{H} \\ \parallel \quad \parallel \quad \parallel \quad \parallel \end{array} \stackrel{\text{Def 2}}{=} \begin{array}{c} \bullet \\ \bullet \\ \oplus \\ \bullet \end{array} =: R_{31}.(1). \text{ RHS}$$

$$R_{31}.(2). \text{ LHS} := \begin{array}{c} \bullet \\ \bullet \\ \oplus \\ \bullet \end{array} \stackrel{\text{Def 2}}{=} \begin{array}{c} \text{H} \quad \text{H} \quad \text{H} \quad \text{H} \\ \parallel \quad \parallel \quad \parallel \quad \parallel \end{array}$$

$$\begin{array}{c} \text{R}_{17} \\ \text{R}_{19} \end{array} \begin{array}{c} \text{H} \quad \text{H} \quad \text{H} \quad \text{H} \\ \parallel \quad \parallel \quad \parallel \quad \parallel \end{array} \stackrel{\text{Def 2}}{=} \begin{array}{c} \oplus \\ \bullet \\ \bullet \\ \diagup \quad \diagdown \\ \diagdown \quad \diagup \\ \bullet \end{array} =: R_{31}.(2). \text{ RHS}$$

□

$C_2 : H^4 = I$

$$R_{17} : \text{Diagram} = \text{Diagram}$$

Def 2:

$$\text{Diagram} := \text{Diagram}$$

$$\text{Diagram} := \text{Diagram}$$

$R_{31} : (1)$

$$\text{Diagram} = \text{Diagram} \quad (2) \quad \text{Diagram} = \text{Diagram}$$

Lem U  $R_{30}$ :

$$\text{Diagram} = \text{Diagram}$$

implies  $R_{30}^1$ :

$$\text{Diagram} =$$

$$\text{Diagram} = \text{Diagram}$$

$R_{30}^2$ :

$$\text{Diagram} = \text{Diagram}$$

&

Proof:  $R_{30}^1$ . LHS :=

$$\text{Diagram} \stackrel{\text{Def 2}}{=} \text{Diagram}$$

$R_{30}$

$$\text{Diagram} = \text{Diagram}$$

$R_{17}$

Def 2

$$\text{Diagram} = \text{Diagram}$$

$C_2$

$$\text{Diagram} =: R_{30}^1 . \text{RHS}$$

$R_{30}$ :

$$\text{Diagram} = \text{Diagram}$$

$R_{17} \parallel R_{31}$

$R_{30}$ :

$$\text{Diagram} = \text{Diagram}$$

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

$$(2) \quad \text{Diagram} = \text{Diagram}$$

$$C_2 : H^4 = I$$

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

$$(2) \quad \text{Diagram} = \text{Diagram}$$

$$C_8^2 : \quad \text{Diagram} = \text{Diagram}$$

$$C_8^3 : \quad \text{Diagram} = \text{Diagram} = \text{Diagram}$$

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

$$R_{17} : \quad \text{Diagram} = \text{Diagram}$$

$$R_{31} : (1) \quad \text{Diagram} = \text{Diagram} \quad (2) \quad \text{Diagram} = \text{Diagram}$$

$$R_{16} : \quad \text{Diagram} = \text{Diagram}$$

Proof Cont.

$$R_{30} : \quad \text{Diagram} = \text{Diagram} \quad \text{Diagram} \quad \text{Diagram} \quad S \quad H \quad H \quad S \quad \oplus \quad S \quad Z$$

$R_{17}, R_{19} \parallel R_{31}$

$$R_{30} : \quad \text{Diagram} = \text{Diagram} \quad \text{Diagram} \quad \text{Diagram} \quad S \quad H \quad H \quad S \quad \oplus \quad S \quad Z$$

$R_{16} \parallel$  Appending both sides by a SWAP to the left

$$R_{30} : \quad \text{Diagram} = \text{Diagram} \quad \text{Diagram} \quad \text{Diagram} \quad S \quad H \quad H \quad S \quad \oplus \quad S \quad Z$$

$C_2 \parallel$  Appending both sides by an  $H^2$  to the left

$$R_{30} : \quad \text{Diagram} = \text{Diagram} \quad \text{Diagram} \quad \text{Diagram} \quad S \quad H \quad H \quad S \quad \oplus \quad S \quad Z$$

$C_8 \parallel$

$$R_{30}^2 : \quad \text{Diagram} = \text{Diagram} \quad \text{Diagram} \quad \text{Diagram} \quad S \quad H \quad H \quad S \quad \oplus \quad S \quad Z$$

□