

$C_8^4:$ = =

$C_7:$ =

$C_1:$ $w^3 = 1$

$\text{Def 2}:$:=

\oplus :=

$C_8^8:$ =

$R_{23}^4:$ = $\cdot w^2$

$R_{15}^3:$ (1) =

(2) =

$R_{24}^3:$ =

$R_{25}^3:$ = $\cdot w$

$\text{Def 1}:$:=

Lem U Def 1-3, C1-8, R15, R23, R24 & R25 imply

$R_{29}:$ = $\cdot w^2$

$\text{Proof: } R_{29} \cdot \text{RHS} :=$ $\cdot w^2 \xrightarrow{\frac{C_8^4}{C_7}}$ $\cdot w^2$

$=$ $\cdot w^2$

$\underline{\text{Def 2}}$ $\cdot w^2$

$\underline{\text{C}_8^8}$ $\cdot w^2$

$\underline{\text{R}_{23}^4}$ $\cdot w^2 \cdot w^2$

$\underline{\text{R}_{23}^4}$ $\cdot w \cdot w^2$

$\underline{\text{C}_1}$

$\underline{\text{R}_{15}, \text{R}_{23}^4}$

Def 1 : $S' := H H S H H$ C1: $w^3 = I$ C2: $H^4 = I$ C3: $S^3 = I$

$$C_8^3: \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^2} = \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^2} \begin{array}{c} \bullet \\ \bullet \end{array} \quad C_5: SS' = S'S$$

$$C_8^8: \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^2} \oplus = \begin{array}{c} \bullet \\ \bullet \end{array} \oplus \oplus \boxed{H^2} = \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^2}$$

$$C_7: \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{S} = \begin{array}{c} \bullet \\ \bullet \end{array} S$$

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

$$R_{25}^3: \begin{array}{c} \bullet \\ \bullet \end{array} \oplus = \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{S'} S \cdot w$$

$$R_{15}: (1) \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{S'} = \begin{array}{c} \bullet \\ \bullet \end{array} S' \quad (2) \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{S'} = \begin{array}{c} \bullet \\ \bullet \end{array} S' \quad C_6: \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \underline{\hspace{2cm}}$$

$$\text{Lem U} \quad R_{29}: \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H} \begin{array}{c} \times \\ \times \end{array} \begin{array}{c} \bullet \\ \bullet \end{array} \oplus = \begin{array}{c} \bullet \\ \bullet \end{array} H \begin{array}{c} \bullet \\ \bullet \end{array} S \begin{array}{c} \bullet \\ \bullet \end{array} S \cdot w^2$$

Proof cont.

$$\begin{array}{c} \bullet \\ \bullet \end{array} H \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{S'^2} S^2$$

$$\begin{array}{c} \bullet \\ \bullet \end{array} H \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{S' S} \begin{array}{c} \bullet \\ \bullet \end{array} S'^2 S^2 \cdot w$$

$$\begin{array}{c} \bullet \\ \bullet \end{array} H \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{S' S S'^2 S^2} \cdot w$$

$$\begin{array}{c} \bullet \\ \bullet \end{array} H \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^2} \begin{array}{c} \bullet \\ \bullet \end{array} H^2 S \begin{array}{c} \bullet \\ \bullet \end{array} H^2 S \cdot w$$

$$\begin{array}{c} \bullet \\ \bullet \end{array} H \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^2} \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^2 S H^2 S} \cdot w$$

$$\begin{array}{c} \bullet \\ \bullet \end{array} H \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^2} \begin{array}{c} \bullet \\ \bullet \end{array} S' S \cdot w$$

$$\begin{array}{c} \bullet \\ \bullet \end{array} H^2 \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^3} \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^3} \begin{array}{c} \bullet \\ \bullet \end{array} \circledast S' S \cdot w$$

$$\begin{array}{c} \bullet \\ \bullet \end{array} H^2 \begin{array}{c} \bullet \\ \bullet \end{array} \boxed{H^3} \begin{array}{c} \bullet \\ \bullet \end{array} \circledast \begin{array}{c} \bullet \\ \bullet \end{array} S' S \cdot w$$

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

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

$$C_6^2: \begin{array}{c} \oplus \\ \parallel \\ \bullet \\ \parallel \end{array} = \begin{array}{c} \parallel \\ \parallel \end{array}$$

$$\text{Def 7: } \begin{array}{c} \times \\ \parallel \end{array} = \begin{array}{c} \oplus \\ \parallel \\ \bullet \\ \oplus \\ \parallel \end{array}$$

$$R_{25}^1: \begin{array}{c} \bullet \\ \oplus \\ \parallel \end{array} = \begin{array}{c} \oplus \\ \parallel \\ \text{S} \quad \text{S} \end{array} \cdot w$$

$$\text{Lem U} \quad R_{29}: \begin{array}{c} \bullet \\ \text{H} \quad \times \\ \parallel \end{array} = \begin{array}{c} \text{H} \quad \text{S} \quad \text{S} \\ \parallel \quad \text{S} \quad \text{H} \end{array} \cdot w^2$$

Proof cont.

$$\begin{array}{c} \bullet \\ \text{H} \quad \text{H} \quad \text{H}^3 \\ \parallel \quad \text{H}^* \end{array} \cdot w$$

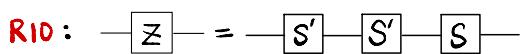
$$\underline{\text{Def 2}}: \begin{array}{c} \bullet \\ \text{H} \quad \oplus \\ \parallel \quad \text{H}^* \end{array} \cdot w$$

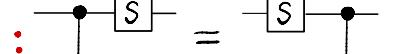
$$\underline{\text{C}_6^2}: \begin{array}{c} \bullet \\ \text{H} \quad \oplus \\ \parallel \quad \text{H}^* \end{array} \cdot w$$

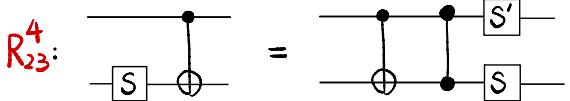
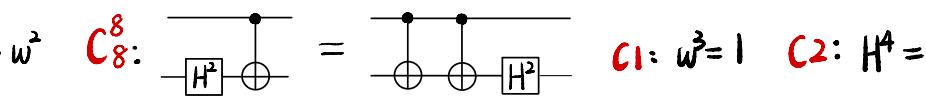
$$\underline{\text{Def 7}}: \begin{array}{c} \bullet \\ \text{H} \quad \times \\ \parallel \end{array} \cdot w$$

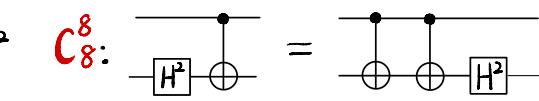
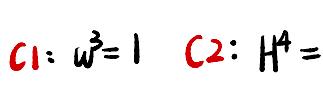
$$\underline{R_{25}^1}: \begin{array}{c} \bullet \\ \text{H} \quad \times \\ \parallel \end{array} =: R_{29} \cdot \text{LHS.}$$

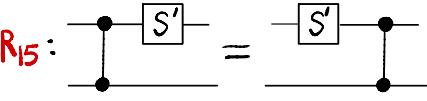
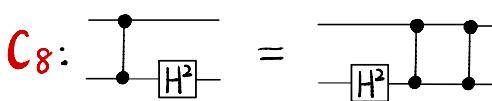
□

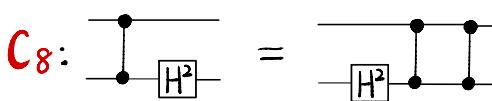
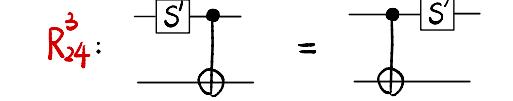
$R_{10}:$  $=$ 

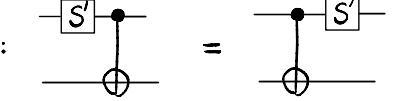
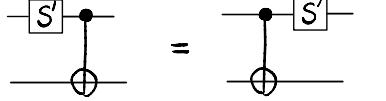
 $C_5:$ $SS' = S'S$ $C_3:$ $S^3 = I$ $C_7:$ 

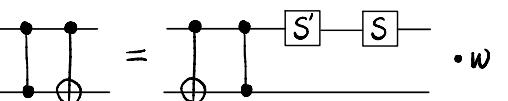
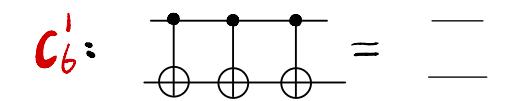
 $R_{23}^4:$  $=$ 

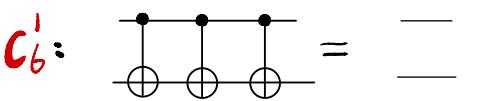
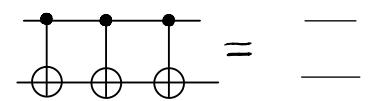
 $\cdot w^2$ $C_8^8:$  $=$ 

 $R_{15}:$  $=$ 

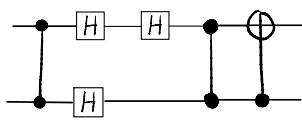
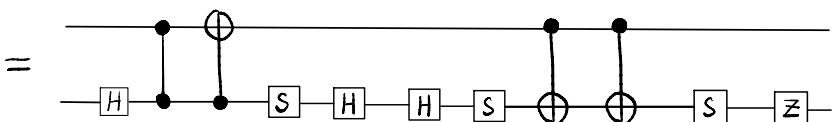
 $C_8:$  $=$ 

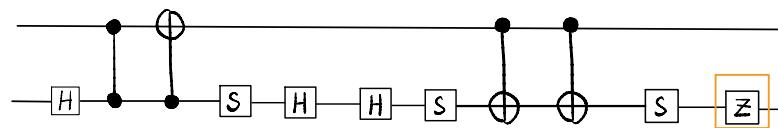
 $R_{24}^3:$  $=$ 

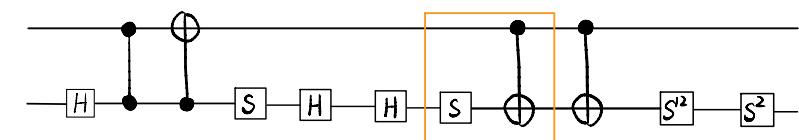
 $Def\ 1:$ $\boxed{S'} := H^2 S H^2$ $R_{25}^3:$  $=$ 

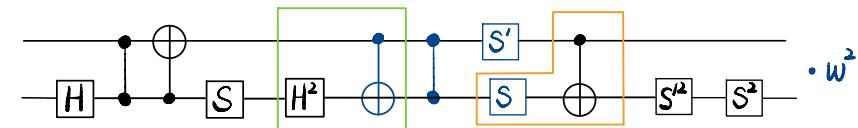
 $\cdot w$ $C_6^1:$  $=$ 

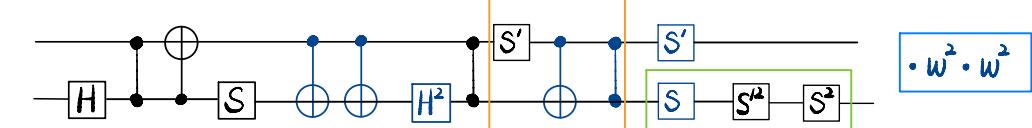
Lem V Def 1-3, C1-8, R15, R23, R24, R25 & R36 imply

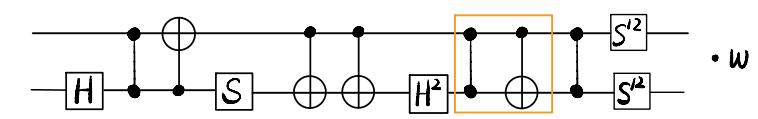
$R_{30}:$  $=$ 

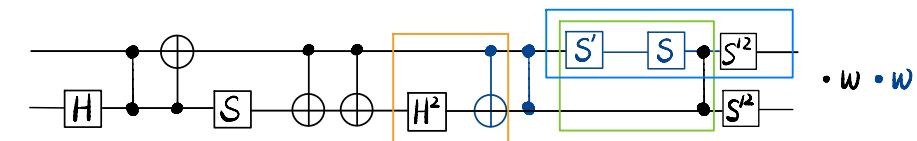
Proof: $R_{30} \cdot RHS :=$  $SZ = S(S'^2 S) \stackrel{C_5}{=} S'^2 S^2$

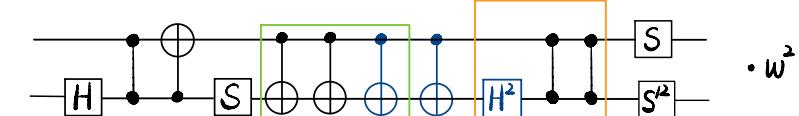
$\stackrel{R_{10}}{=} \stackrel{C_5}{=}$ 

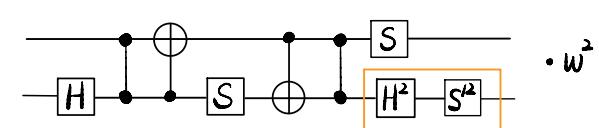
$\stackrel{R_{23}^4}{=} \stackrel{C_8}{=}$  $\cdot w^2$

$\stackrel{R_{23}^4}{=} \stackrel{C_8}{=}$  $\cdot w^2 \cdot w^2$

$\stackrel{C_1, C_3, C_5}{=} \stackrel{R_{15}, R_{24}^3}{=}$  $\cdot w$

$\stackrel{R_{25}^3}{=}$  $\cdot w \cdot w$

$\stackrel{C_5, C_7, C_8}{=} \stackrel{Def\ 1, C_2, C_3, R_{15}}{=}$  $\cdot w^2$

$\stackrel{C_8}{=} \stackrel{C_6^1}{=}$  $\cdot w^2$

Def 1: $S' := H^2 S H^2$ C1: $w^3 = I$ C2: $H^4 = I$ C3: $S^3 = I$ C5: $SS' = S'S$

$$R_{23}^4: \begin{array}{c} \text{Circuit diagram} \\ \text{S} \end{array} = \begin{array}{c} \text{Circuit diagram} \\ S' \end{array} \cdot w^2 \quad R_{15}: \begin{array}{c} \text{Circuit diagram} \\ S' \end{array} = \begin{array}{c} \text{Circuit diagram} \\ S' \end{array}$$

$$C_7: \begin{array}{c} \text{Circuit diagram} \\ S \end{array} = \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \quad R_{32}^4: \begin{array}{c} \text{Circuit diagram} \\ H^3 \end{array} = \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \quad R_{32}^3: \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} = \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array}$$

Lem V

$$R_{30}: \begin{array}{c} \text{Circuit diagram} \\ H \end{array} = \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ \oplus \end{array} = \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ \oplus \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ Z \end{array}$$

Proof cont.

$$\begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S^2 \end{array} \cdot w^2 \stackrel{\text{Def 1}}{=} H^2 H^2 S^2 H^2 = S^2 H^2 \stackrel{\text{C2}}{=} S^2 H^2$$

$$C_2 \stackrel{\text{Def 1}}{=} \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S^2 \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot w^2$$

$$R_{23}^4 \stackrel{\text{WTS}}{=} \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S' \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S^2 \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot w^2 \cdot w^2$$

$$\begin{array}{c} C_1, C_2, C_3 \\ G_7, R_{15} \end{array} \stackrel{\text{WTS}}{=} \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S' \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot w$$

$$\text{Then } R_{30}: \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} = \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S' \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot w$$

$$R_{30}: \begin{array}{c} \text{Circuit diagram} \\ H^3 \end{array} \stackrel{\text{WTS}}{=} \begin{array}{c} \text{Circuit diagram} \\ H^3 \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S' \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot w$$

$$R_{30}: \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} = \begin{array}{c} \text{Circuit diagram} \\ H^3 \end{array} \stackrel{\text{WTS}}{=} \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S' \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ S \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot w$$

$$R_{30}: \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ \oplus \end{array} = \begin{array}{c} \text{Circuit diagram} \\ \oplus \end{array} \cdot \begin{array}{c} \text{Circuit diagram} \\ H^2 \end{array} \cdot w$$

$$C_8^8: \quad \begin{array}{c} \text{H}^2 \\ \text{S} \\ \oplus \end{array} = \begin{array}{c} \text{H}^2 \\ \text{S} \\ \oplus \end{array}$$

$$C_8^1: \quad \begin{array}{c} \text{H}^2 \\ \oplus \\ \text{S} \end{array} = \begin{array}{c} \text{H}^2 \\ \text{S} \\ \oplus \end{array}$$

$$C_5: ss' = s's$$

$$C_8^6: \quad \begin{array}{c} \text{H}^2 \\ \oplus \\ \text{S} \end{array} = \begin{array}{c} \text{H}^2 \\ \text{S} \\ \oplus \end{array}$$

$$R_{25}^1: \quad \begin{array}{c} \oplus \\ \text{S} \\ \text{S}' \end{array} = \begin{array}{c} \oplus \\ \text{S}' \\ \text{S} \end{array} \cdot w$$

$$C_7: \quad \begin{array}{c} \text{S} \\ \text{S} \end{array} = \begin{array}{c} \text{S} \\ \text{S} \end{array}$$

$$R_{24}: \quad \begin{array}{c} \oplus \\ \text{S} \end{array} = \begin{array}{c} \oplus \\ \text{S} \end{array}$$

$$R_{15}: \quad \begin{array}{c} \text{S} \\ \text{S}' \end{array} = \begin{array}{c} \text{S}' \\ \text{S}' \end{array}$$

$$R_{24}^1: \quad \begin{array}{c} \oplus \\ \text{S} \end{array} = \begin{array}{c} \oplus \\ \text{S}' \end{array}$$

$$\text{Def 1: } \boxed{\text{S}'} := H^2 S H^2$$

Lem V

$$R_{30}: \quad \begin{array}{c} \text{H} \\ \text{H} \\ \text{H} \\ \oplus \end{array} = \begin{array}{c} \text{H} \\ \text{S} \\ \text{H} \\ \text{H} \\ \text{S} \\ \oplus \\ \text{S} \\ \text{z} \end{array}$$

Proof cont.

$$R_{30}: \quad \begin{array}{c} \text{H}^2 \\ \oplus \end{array} \stackrel{\text{WTS}}{=} \begin{array}{c} \oplus \\ \text{S}' \\ \text{S} \\ \text{H}^2 \end{array} \cdot w$$

$$R_{30}.LHS := \begin{array}{c} \text{H}^2 \\ \oplus \end{array} \stackrel{C_8^8}{=} \begin{array}{c} \text{H}^2 \\ \oplus \end{array} \stackrel{C_8^1}{=} \begin{array}{c} \text{H}^2 \\ \oplus \end{array}$$

$$\stackrel{C_8^6}{=} \begin{array}{c} \oplus \\ \text{H}^2 \end{array} \stackrel{R_{25}^1}{=} \begin{array}{c} \oplus \\ \text{S}' \\ \text{S} \\ \text{H}^2 \end{array} \cdot w$$

$$\stackrel{R_{25}^1}{=} \begin{array}{c} \oplus \\ \text{S}' \\ \text{S} \\ \text{S}' \\ \text{S} \end{array} \cdot w \cdot w$$

$$\begin{array}{c} C_5, C_7, R_{15} \\ \hline R_{24}, R_{24}^1 \end{array} \quad \begin{array}{c} \oplus \\ \text{H}^2 \\ \text{S}^2 \\ \text{S}'^2 \end{array} \cdot w^2$$

$$\stackrel{R_{25}^1}{=} \begin{array}{c} \oplus \\ \text{S}' \\ \text{S} \\ \text{S}^2 \\ \text{S}'^2 \end{array} \cdot w^2 \cdot w$$

$$\begin{array}{c} C_1, C_2 \\ \hline C_3 \end{array} \quad \begin{array}{c} \oplus \\ \text{H}^2 \end{array} \stackrel{R_{25}^1}{=} \begin{array}{c} \oplus \\ \text{S}' \\ \text{S} \end{array} \cdot w$$

$$\begin{array}{c} G \\ \hline R_{15} \end{array} \quad \begin{array}{c} \oplus \\ \text{H}^2 \\ \text{S} \\ \text{S}' \end{array} \cdot w \stackrel{\text{Def 1}}{=} \begin{array}{c} \oplus \\ \text{S} \\ \text{H}^2 \\ \text{S} \\ \text{H}^2 \end{array} \cdot w$$

Hence $R_{30}: \quad \begin{array}{c} \oplus \\ \text{S} \\ \text{H}^2 \\ \text{S} \\ \text{H}^2 \end{array} \cdot w \stackrel{\text{WTS}}{=} \begin{array}{c} \oplus \\ \text{S}' \\ \text{S} \\ \text{H}^2 \end{array} \cdot w$

$R_{25}^1:$ = $\cdot w$ $C_3: S^3 = I$ $C_5: SS' = S'S$ $Def 1: \boxed{S'} := H^2 SH^2$
 $R_{23}^4:$ = $\cdot w^2$ $C_1: w^3 = I$ $C_2: H^4 = I$ $C_6:$ =
 $C_7:$ =
 $R_{25}^3:$ = $\cdot w$

Lem V

$R_{30}:$ =

Proof cont. $R_{30}:$ $\cdot w$ $\stackrel{WTS}{=}$ $\cdot w$
 $Def 1, C_1 \parallel C_2, C_5$

$R_{30}:$ $\stackrel{WTS}{=}$

$R_{30.RHS} :=$

$\underline{R_{25}^1}:$ $\cdot w$

$\underline{R_{23}^4}:$ $\cdot w \cdot w^2$

$\underline{C_6, C_7}$

$\underline{R_{15}}:$

$SSS'SH^2S \stackrel{C_5}{=} S^2 \boxed{S^{12}} H^2 S \stackrel{Def 1}{=}$

$S^2 H^2 S^2 \boxed{H^2 H^2} S \stackrel{C_2}{=} S^2 H^2 \boxed{S^2} S$

$C_3 = S^2 H^2$

$\underline{\text{Def 1}}$ $\cdot w$

$$\begin{array}{lll}
C_8^8: & \text{Diagram} = \text{Diagram} & C_8^1: \text{Diagram} = \text{Diagram} \\
R_{23}^4: & \text{Diagram} = \text{Diagram} \cdot w^2 & C_6: \text{Diagram} = \text{Diagram} \\
C_7: & \text{Diagram} = \text{Diagram} & R_{15}: \text{Diagram} = \text{Diagram} = \text{Diagram} \\
R_{24}^3: & \text{Diagram} = \text{Diagram} & R_{25}^3: \text{Diagram} = \text{Diagram} \cdot w
\end{array}$$

Lem V

$$\begin{array}{lll}
R_{30}: & \text{Diagram} = \text{Diagram} &
\end{array}$$

Proof cont.

$$\begin{array}{lll}
R_{30}: & \text{Diagram} & \text{WTS} \quad \text{Diagram} \\
R_{30} \cdot \text{RHS} = & \text{Diagram} \cdot w & \\
\underline{C_8^8}: & \text{Diagram} \cdot w & \\
\underline{C_8^1}: & \text{Diagram} \cdot w & \\
\underline{R_{23}^4}: & \text{Diagram} \cdot w \cdot w^2 & \\
\underline{R_{23}^4}: & \text{Diagram} \cdot w^2 & \\
\underline{C_7, R_{24}^3}: & \text{Diagram} \cdot w^2 & \\
\underline{C_6}: & \text{Diagram} \cdot w^2 & \\
\underline{R_{25}^3}: & \text{Diagram} \cdot w^2 \cdot w & \\
\underline{\underline{C_1, C_2, C_3}}: & \text{Diagram} & \\
\text{Def1, } \underline{C_5}: & \text{Diagram} &
\end{array}$$