

$$[A_{01}] := \dots \quad [A_{02}] := [H] [H] \dots$$


---

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


---

$$\text{Lem 33 By } C_8, \quad 3.(1) \quad \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{A_{01}} \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{A_{01}} \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array}$$

$$(2) \quad \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{A_{02}} \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \boxed{A_{02}} \end{array}$$

Proof: 3.(1). LHS :=  $\begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{A_{01}} \\ | \\ \bullet \end{array}$  def  $\begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{A_{01}} \\ | \\ \bullet \end{array}$  def  $\begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \boxed{A_{01}} \end{array} =: 3.(1). \text{RHS.}$

$$3.(2). \text{LHS} := \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{A_{02}} \\ | \\ \bullet \end{array} \stackrel{\text{def}}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{H} \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \stackrel{C_8}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{H} \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array}$$

$$\stackrel{\text{def}}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{A_{02}} \\ | \\ \bullet \end{array} =: 3.(2). \text{RHS}$$

□

$$A_{1b} = S^b H \quad b \in \mathbb{Z}_3$$

$$A_{02} := H H$$

$$B_{1b} = S^b H \quad \text{with CNOT gate}$$

$$\text{Def 3: } \text{X} := \text{H H H} \quad \text{R17: } \text{X} = \text{X}$$

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

$$R_{27}: \text{H H H} = \text{H H H} \quad \text{S} \quad \text{S} \quad \text{H} \quad \text{S} \quad \text{S} \quad \text{H} \quad \text{S} \quad \text{S} \quad \text{Z} \quad \cdot w$$

Lem 34 By Def 3, G<sub>7</sub>, R<sub>17</sub> & R<sub>27</sub>,

$$3. (3) \quad A_{10} = A_{02} B_{10} S \quad \text{S} \quad \text{S} \quad \text{H} \quad \text{H} \quad \text{H} \quad \text{S} \quad \text{S} \quad \text{Z} \quad \cdot w$$

$$(4) \quad A_{11} = A_{02} B_{11} S \quad \text{S} \quad \text{S} \quad \text{H} \quad \text{H} \quad \text{H} \quad \text{S} \quad \text{S} \quad \text{Z} \quad \cdot w$$

$$(5) \quad A_{12} = A_{02} B_{12} S \quad \text{S} \quad \text{S} \quad \text{H} \quad \text{H} \quad \text{H} \quad \text{S} \quad \text{S} \quad \text{Z} \quad \cdot w$$

$$\text{Proof: } 3.(3)-(5). \text{LHS} := A_{1b} \stackrel{\text{def}}{=} S^b H \stackrel{G_7}{=} S^b H$$

$$\stackrel{R_{27}}{=} \text{S}^b H \quad \text{H H} \quad \text{S} \quad \text{S} \quad \text{H} \quad \text{S} \quad \text{S} \quad \text{Z} \quad \cdot w$$

$$\stackrel{\text{def}}{=} \text{S}^b H \quad A_{02} \quad \text{S} \quad \text{S} \quad \text{H} \quad \text{S} \quad \text{S} \quad \text{Z} \quad \cdot w$$

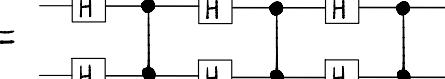
$$\stackrel{\text{def}}{=} B_{1b} \quad A_{02} \quad \text{S} \quad \text{S} \quad \text{H} \quad \text{S} \quad \text{S} \quad \text{Z} \quad \cdot w$$

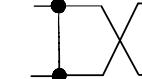
$=: 3.(3)-(5). \text{RHS}$

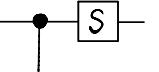
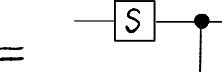
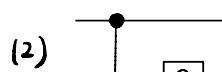
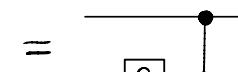
$$A_{2b} := \boxed{H^2} \quad \boxed{S^{2b}} \quad \boxed{H} \quad b \in \mathbb{Z}_3$$

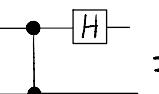
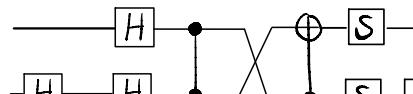
$$A_{01} := \boxed{\dots}$$

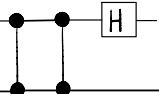
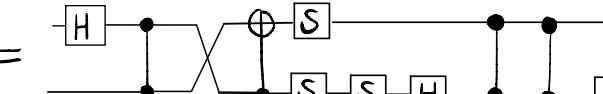
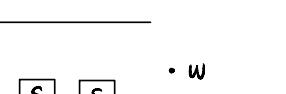
$$B_{2b} = \boxed{H^2} \quad \boxed{S^{2b}} \quad \boxed{H} \quad \text{with } \dots$$

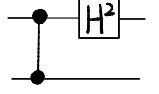
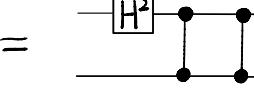
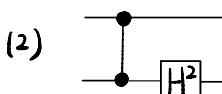
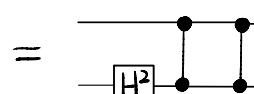
Def 3:  := 

R<sub>17</sub>:  = 

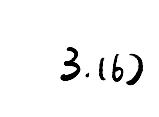
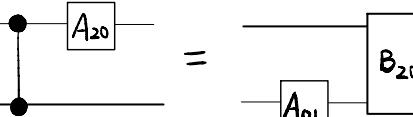
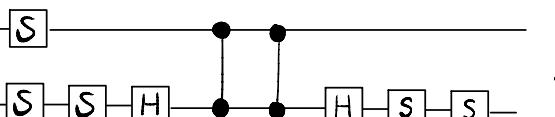
C<sub>7</sub>: (1)  =  (2)  = 

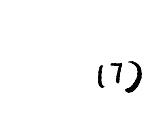
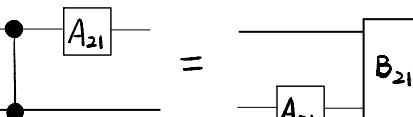
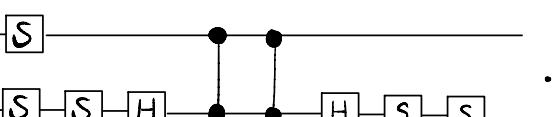
R<sub>27</sub>:  =  + w 

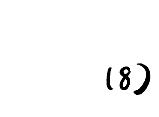
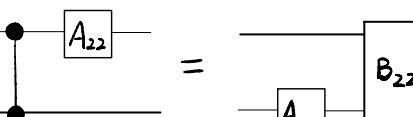
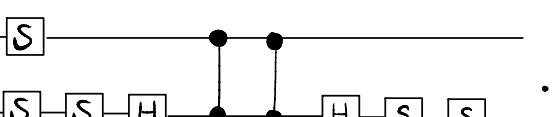
R<sub>27</sub><sup>1</sup>:  =  + w 

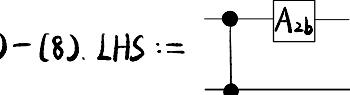
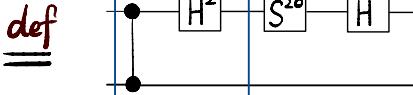
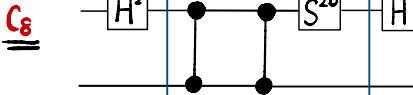
C<sub>8</sub>: (1)  =  (2)  = 

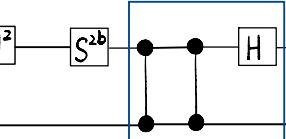
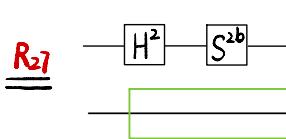
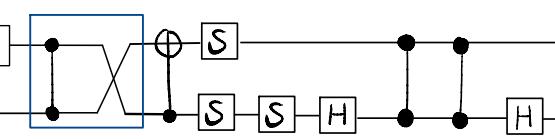
Lem 35 By Def 3, C<sub>7</sub>, C<sub>8</sub>, R<sub>17</sub> & R<sub>27</sub>,

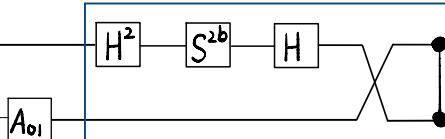
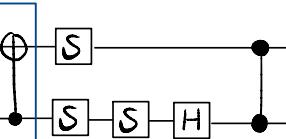
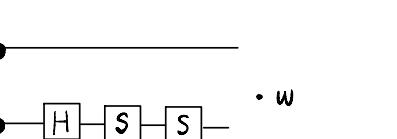
3.(6)  =  + w 

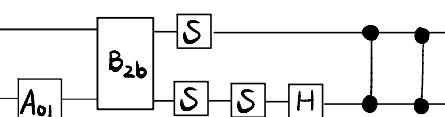
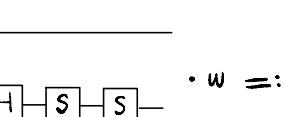
(7)  =  + w 

(8)  =  + w 

Proof: 3.(6)-(8). LHS :=  def  C8 

C7  R27  + w 

R17  def  + w 

def   + w =: 3.(6)-(8).RHS

□

3