

$$A_{02} = \text{---} [H] \text{---} [H] \text{---} \quad B_{00} = \text{---} X \text{---}$$


---

$$\text{Def 3: } \text{---} X \text{---} := \text{---} [H] \text{---} [H] \text{---} [H] \text{---} \quad R_{17}: \text{---} \bullet \text{---} X \text{---} = \text{---} X \text{---} \bullet \text{---}$$

$$C_8: (1) \text{---} \bullet [H^2] \text{---} = \text{---} [H^2] \text{---} \bullet \text{---} \quad (2) \text{---} \bullet [H^2] \text{---} = \text{---} [H^2] \text{---} \bullet \text{---}$$


---

Lem 41 By Def 3,  $C_8$  &  $R_{17}$ ,

$$4.(1) \text{---} \bullet [A_{02}] \text{---} [B_{00}] \text{---} = \text{---} [A_{02}] \text{---} [B_{00}] \text{---} \bullet \text{---}$$

$$\text{Proof: } 4.(1). \text{LHS} := \text{---} \bullet [A_{02}] \text{---} [B_{00}] \text{---} \stackrel{\text{def}}{=} \text{---} \bullet [H] \text{---} [H] \text{---} X \text{---} \stackrel{C_8}{=} \text{---} [H] \text{---} [H] \text{---} X \text{---} \bullet \text{---}$$

$$\stackrel{R_{17}}{=} \text{---} [H] \text{---} [H] \text{---} \bullet \text{---} X \text{---} \stackrel{\text{def}}{=} \text{---} [A_{02}] \text{---} [B_{00}] \text{---} \bullet \text{---} =: 4.(1). \text{RHS}$$

□



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

R17:  $\boxed{\text{X}} = \boxed{\text{X}}$

C8: (1)  $\boxed{H^2} = \boxed{H^2}$

(2)  $\boxed{H^2} = \boxed{H^2}$

R15: (1)  $\boxed{S'} = \boxed{S'}$

(2)  $\boxed{S'} = \boxed{S'}$

C7: (1)  $\boxed{S} = \boxed{S}$

(2)  $\boxed{S} = \boxed{S}$

R25:  $\boxed{\oplus} = \boxed{\oplus} \quad \boxed{S'} \quad \boxed{S}$

• w Def:  $\boxed{S'} \quad \boxed{S'} = \boxed{H} \quad \boxed{H} \quad \boxed{S} \quad \boxed{S} \quad \boxed{H} \quad \boxed{H}$   
 $S'^2 = (H^2 S H^2)(H^2 S H^2) = H^2 S^2 H^2$

C5:  $S H^2 S H^2 = H^2 S H^2 S \quad S S' = S' S$

Lem 42 By Def 3, C5, C7, C8, R15, R17 & R25,

4. (2)  $A_{02} \quad \boxed{B_{01}} = A_{02} \quad \boxed{B_{01}} \quad \boxed{H} \quad \boxed{H} \quad \boxed{S} \quad \boxed{S} \quad \boxed{H} \quad \boxed{H} \quad \boxed{S} \quad \boxed{S}$  • w<sup>2</sup>

Proof: 4. (2). LHS :=  $A_{02} \quad \boxed{B_{01}}$  def  $\boxed{H} \quad \boxed{H}$   $\times \quad \oplus$

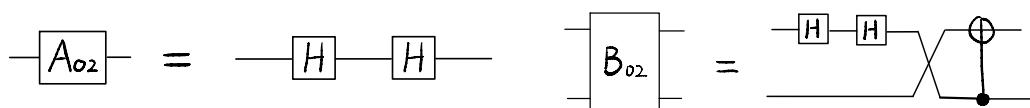
C8  $\boxed{H} \quad \boxed{H} \quad \boxed{\text{X}} \quad \oplus$  R17  $\boxed{H} \quad \boxed{H} \quad \boxed{\text{X}} \quad \oplus$

R25 def  $\boxed{\text{X}} \quad \oplus \quad \boxed{S'} \quad \boxed{S}$  • w

R25  $\boxed{\text{X}} \quad \oplus \quad \boxed{S'} \quad \boxed{S}$  • w • w

R15, C7 def  $\boxed{B_{01}} \quad \boxed{H} \quad \boxed{H} \quad \boxed{S} \quad \boxed{S} \quad \boxed{H} \quad \boxed{H} \quad \boxed{S} \quad \boxed{S}$  • w<sup>2</sup> C5 def

$A_{02} \quad \boxed{B_{01}} \quad \boxed{H} \quad \boxed{H} \quad \boxed{S} \quad \boxed{S} \quad \boxed{H} \quad \boxed{H} \quad \boxed{S} \quad \boxed{S}$  • w<sup>2</sup> =: 4. (2). RHS □



Def 3:  $\bigtimes := \boxed{H \quad H \quad H}$       R<sub>17</sub>:  $\bigtimes = \bigtimes$

C<sub>8</sub><sup>3</sup>:  $\boxed{H^2 \quad H^2} = \boxed{H^2 \quad H^2} = \boxed{H^2}$

R<sub>B</sub>: (1)  $\boxed{Z} = \boxed{Z}$       (2)  $\boxed{Z} = \boxed{Z}$

C<sub>7</sub>: (1)  $\boxed{S} = \boxed{S}$       (2)  $\boxed{S} = \boxed{S}$

R<sub>25</sub>:  $\bigoplus = \bigoplus \cdot w$

Lem 43 By Def 3, C<sub>7</sub>, C<sub>8</sub>, R<sub>B</sub>, R<sub>17</sub> & R<sub>25</sub>,

4.(3)  $A_{02} \boxed{B_{02}} = A_{02} \boxed{B_{02}} \cdot w$

Proof: 4.(3).LHS :=  $A_{02} \boxed{B_{02}} \stackrel{\text{def}}{=} \boxed{H \quad H} \bigtimes \bigoplus \stackrel{C_8}{=} \boxed{H^2} \bigtimes \bigoplus \cdot w$

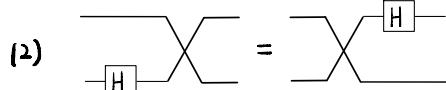
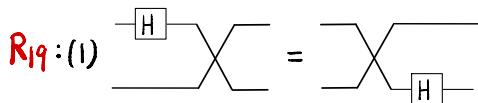
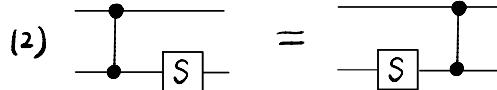
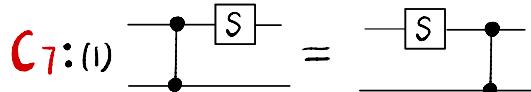
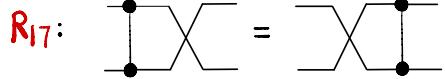
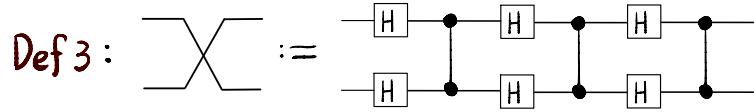
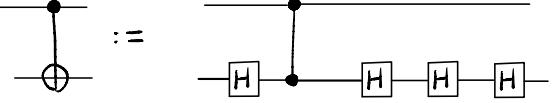
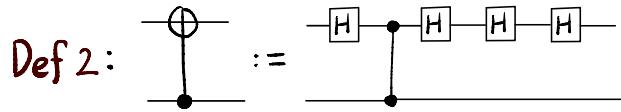
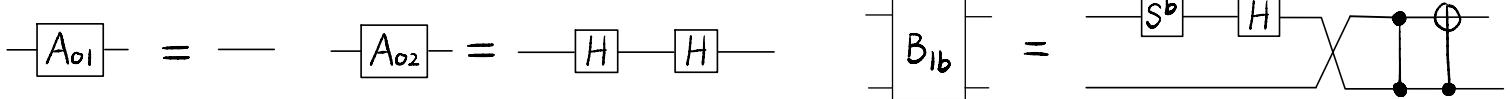
R<sub>17</sub>  $\boxed{H \quad H} \bigtimes \bigoplus$

R<sub>25</sub>  $\boxed{H \quad H} \bigtimes \bigoplus \cdot w$

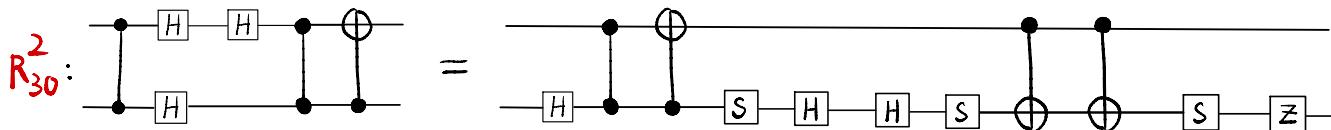
R<sub>13</sub>  $\boxed{H \quad H} \bigtimes \bigoplus \cdot w$   
C<sub>7</sub>  $\boxed{H \quad H} \bigtimes \bigoplus \cdot w$

def  $A_{02} \boxed{B_{02}} \cdot w =: 4.(3).RHS$

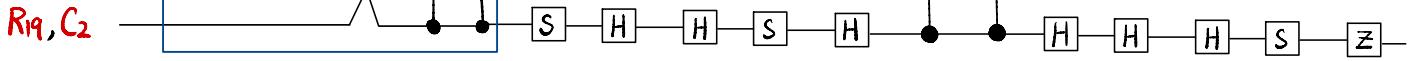
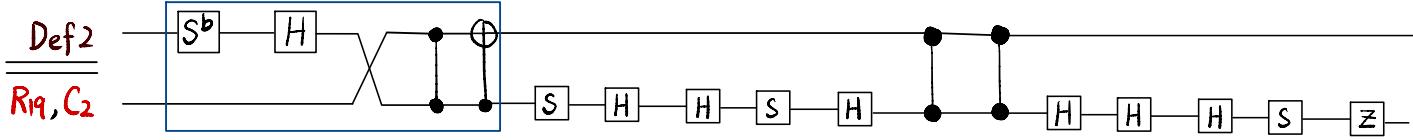
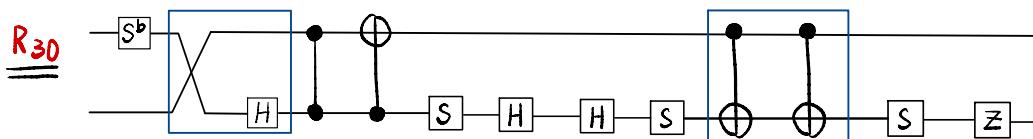
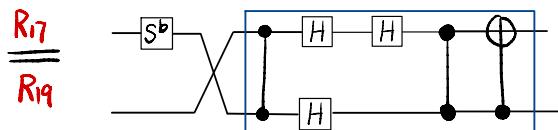
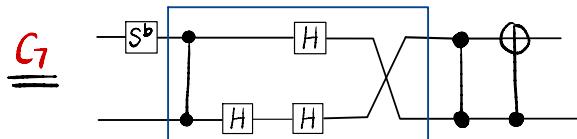
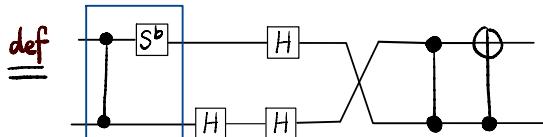
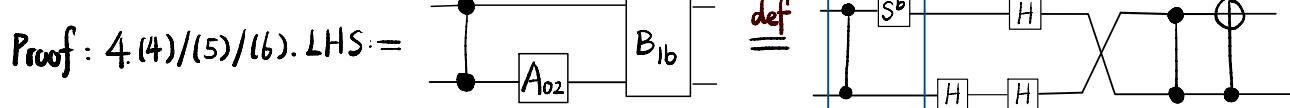
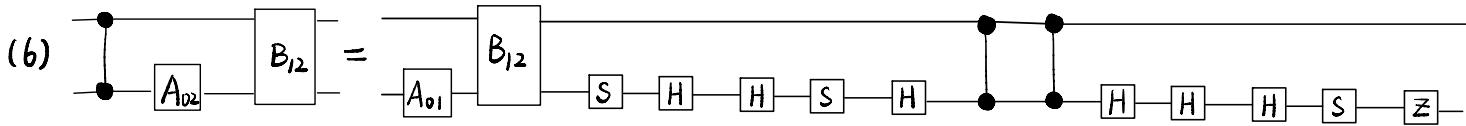
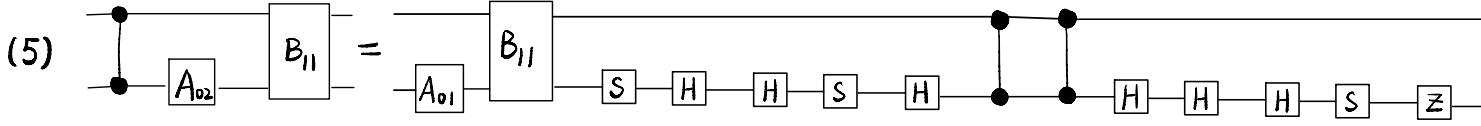
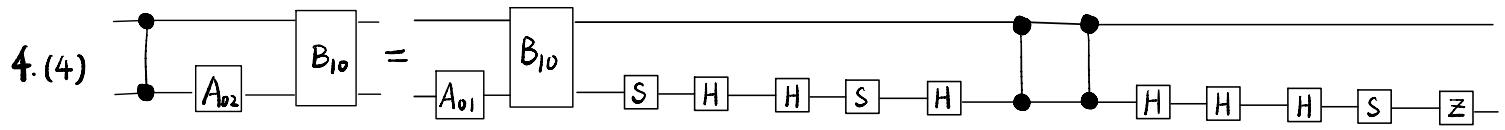
□



C<sub>2</sub>:  $H^4 = I$



Lem 44 By Def 2, Def 3, C<sub>7</sub>, R<sub>17</sub>, R<sub>19</sub> & R<sub>30</sub>,



B<sub>1b</sub>

$= 4(4)/(5)/(6). \text{ RHS}$

4

$$A_{02} = \boxed{H} \quad A_{2b} = \boxed{H^2} \quad S^{2b} \quad H$$

$$B_{2b} = \boxed{H^2} \quad S^{2b} \quad H \quad \oplus \quad \otimes$$

Def 2:  $\oplus := \boxed{H} \quad \otimes := \boxed{H} \quad H \quad H \quad H$

Def 3:  $\times := \boxed{H} \quad H \quad H \quad H \quad H$

C<sub>7</sub>: (1)  $\boxed{S} = \boxed{S}$  (2)  $\boxed{S} = \boxed{S}$

C<sub>8</sub><sup>3</sup>:  $\boxed{H^2} = \boxed{H^2} \quad = \quad \boxed{H^2}$

R<sub>29</sub>:  $\begin{array}{c} \oplus \\ \times \end{array} = \begin{array}{c} H \quad S \quad S \\ S \quad H \quad H \end{array} \cdot w^2$

Lem 45 By Def 2, Def 3, C<sub>7</sub>, C<sub>8</sub> & R<sub>29</sub>,

4. (7)  $A_{02} \quad B_{20} = \begin{array}{c} A_{20} \quad S \quad S \\ H \quad H \quad S \quad H \quad H \quad S \end{array} \cdot w^2$

(8)  $A_{02} \quad B_{21} = \begin{array}{c} A_{21} \quad S \quad S \\ H \quad H \quad S \quad H \quad H \quad S \end{array} \cdot w^2$

(9)  $A_{02} \quad B_{22} = \begin{array}{c} A_{22} \quad S \quad S \\ H \quad H \quad S \quad H \quad H \quad S \end{array} \cdot w^2$

Proof: 4.(7)/(8)/(9). LHS :=  $A_{02} \quad B_{2b} \stackrel{\text{def}}{=} \boxed{H^2} \quad S^{2b} \quad H \quad \oplus \quad \otimes$

$\stackrel{C_8}{=} \boxed{H^2} \quad \boxed{S^{2b}} \quad H \quad \times \quad \oplus \quad \stackrel{C_7}{=} \boxed{H^2} \quad \boxed{S^{2b}} \quad \boxed{H} \quad \times \quad \oplus$

$\stackrel{R_{29}}{=} \boxed{H^2} \quad \boxed{S^{2b}} \quad H \quad S \quad S \quad \cdot w^2$

$\stackrel{\text{def}}{=} \boxed{A_{2b}} \quad S \quad S \quad \cdot w^2 =: 4.(7)/(8)/(9). \text{ RHS}$