

Lem 18 Def 1-5, Def 7,  $C_3$ ,  $C_7$ ,  $C_8$ ,  $C_{15}$ ,  $R_5$ ,  $R_{10}$ ,  $R_{11}$ ,  $R_{16}$ ,  $R_{17}$ ,  $R_{19}$ ,  $R_{31}$  &  $R_{51}$  imply

7.2.(7)-(9)

Proof: 7.2.(7)-(9). LHS :=

$\underline{\underline{C_8}} \quad \underline{\underline{R_{19}}}$

$\underline{\underline{C_7, R_{17}, R_{31}}} \quad \underline{\underline{C_{15}^4, C_5^{14}}}$

$\underline{\underline{C_{15}^1}}$

$$\begin{array}{c}
 B_{2d} = \text{H}^2 S^{2d} H \quad B_{02} = \text{H}^2 \\
 R_{19}: \quad \text{H} \quad \text{X} = \text{X} \quad \text{H} \quad R_{31}: \quad \text{X} \oplus \text{H} = \text{H} \oplus \text{X} \\
 C_{15}^{14}: \quad \text{H}^2 \quad \text{X} \quad \text{H}^2 = \text{H}^2 \quad \text{X} \quad \text{H}^2 \\
 R_5: \quad X = H S H H S S H \quad C_3: S^3 = I \\
 R_{10}: \quad Z = S' S' S \quad R_{11}: \quad Z^2 = S' S S
 \end{array}$$

Lem 18

$$7.2.(7)-(9) \quad B_{01} B_{2d} = B_{02} \text{H}^2 H H H S H \cdot S H S Z Z X \cdot (-\omega)$$

Proof cont:

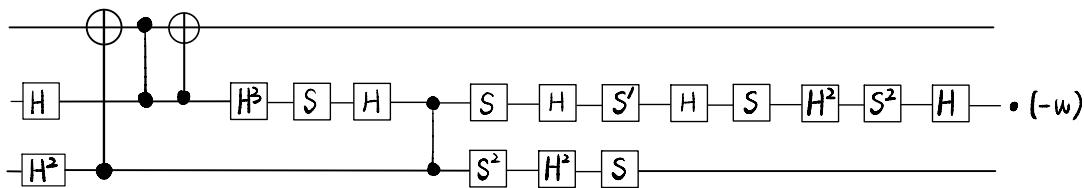
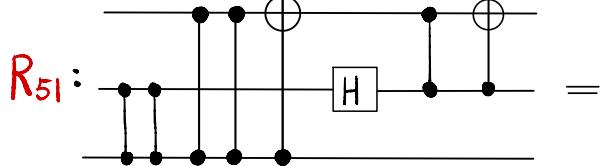
$$7.2.(7)-(9).RHS := B_{02} \text{H}^2 H H H S H \cdot S H S Z Z X \cdot (-\omega)$$

$$\underline{\text{def}} \quad \text{H}^2 S^{2d} H \quad \text{H}^2 \quad \text{X} \oplus \text{H} \quad \text{H}^2 H H H S H \cdot S H S Z Z X \cdot (-\omega)$$

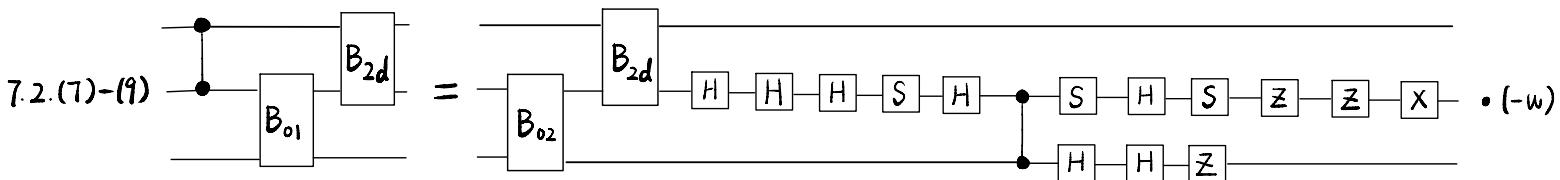
$$\begin{array}{c}
 R_{31} \\
 C_{15}^{14}
 \end{array} \quad \text{H}^2 S^{2d} H \quad \text{H}^2 \quad \text{X} \oplus \text{H} \quad \text{H}^2 H H H S H \cdot S H S Z^2 X \cdot (-\omega)$$

$$\underline{R_{19}} \quad \text{H}^2 S^{2d} \quad \text{H} \quad \text{H}^2 \quad \text{H}^2 H H H S H \cdot S H S Z^2 X \cdot (-\omega)$$

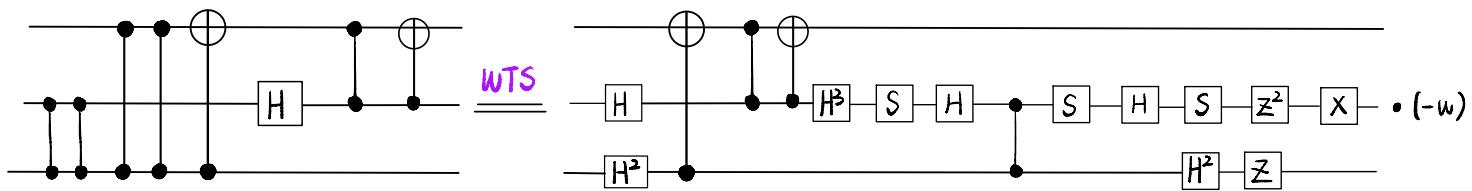
$$\text{Hence,} \quad \text{WTS} \quad \text{H}^2 \quad \text{H} \quad \text{H}^2 \quad \text{H}^2 H H H S H \cdot S H S Z^2 X \cdot (-\omega)$$



Lem 18



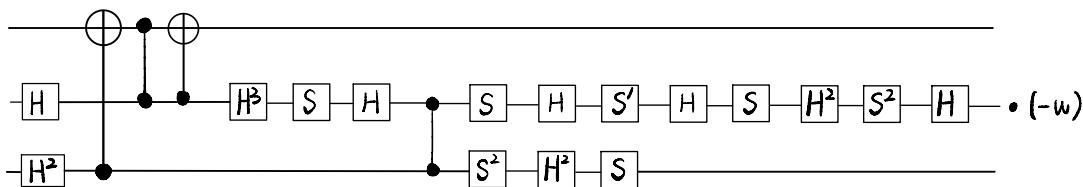
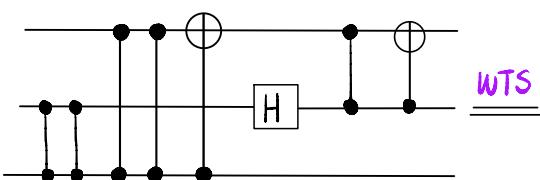
Proof cont :



$C_2, C_3, \text{Def 1} \parallel R_5, R_{10}, R_{11}$

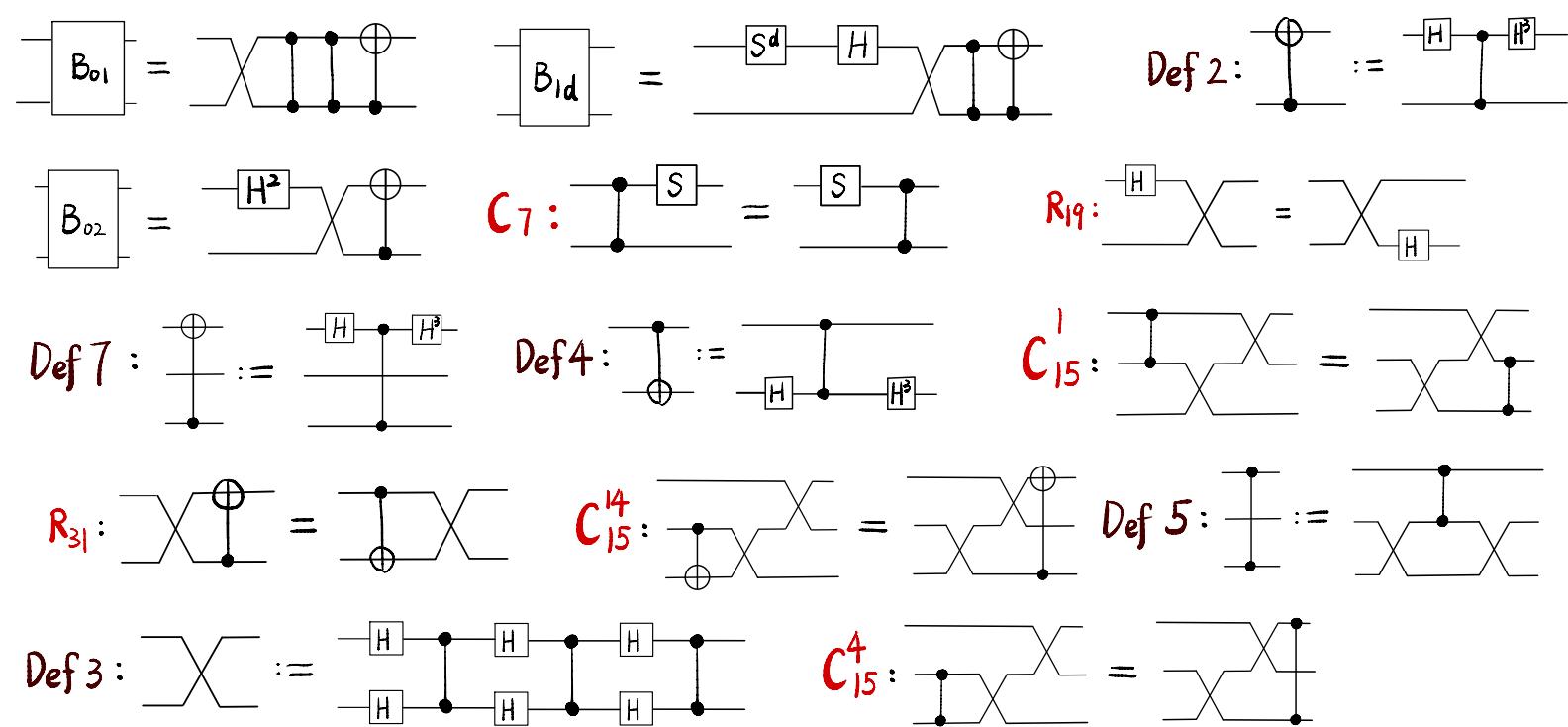
$$SHS\cancel{Z}X \xrightarrow{\frac{R_{11}}{R_5}} SHSS'S^2 \underline{HS}\underline{H^2}\underline{S^2}H \stackrel{C_3}{=} SHS'HSH^2S^2H$$

$$H^2\cancel{Z} \stackrel{R_{10}}{=} H^2S'S'S \stackrel{\text{Def 1}}{=} H^2H^2S^2H^2S \stackrel{C_2}{=} S^2H^2S$$



By  $R_{51}$ , this completes the proof.





Lem 19 Def 1-5, Def 7,  $C_3, C_7, C_8, C_{15}, R_5, R_{10}, R_{11}, R_{16}, R_{17}, R_{19}, R_{31}$  &  $R_{52}$  imply

7.3.(4)-(6)  $=$   $\bullet (-w)$

Proof: 7.3.(4)-(6). LHS :=  $\underline{\text{def}}$

$\underline{R_{31}, C_7}$   $\underline{C_{15}^{14}}$

$\underline{R_{19}}$

$\underline{C_{15}^1}$

$$\begin{aligned}
 B_{01} &= \text{Circuit Diagram} & B_{1d} &= \text{Circuit Diagram} & R_{19}: & \text{Circuit Diagram} \\
 R_{31}: & \text{Circuit Diagram} = \text{Circuit Diagram} & R_{17}: & \text{Circuit Diagram} = \text{Circuit Diagram} & C_{15}^{14}: & \text{Circuit Diagram} = \text{Circuit Diagram} \\
 C_{15}^4: & \text{Circuit Diagram} = \text{Circuit Diagram} \\
 R_5: & \boxed{X} = \boxed{H} \boxed{S} \boxed{H} \boxed{H} \boxed{S} \boxed{S} \boxed{H} \quad HSH^2S^2H \\
 R_{10}: & \boxed{Z} = \boxed{S'} \boxed{S'} \boxed{S} & R_{11}: & \boxed{Z^2} = \boxed{S'} \boxed{S} \boxed{S} & C_3: & S^3 = I
 \end{aligned}$$

Lem 19

$$7.3.(4)-(6) \quad \text{Circuit Diagram} = \text{Circuit Diagram} \cdot (-w)$$

Proof cont:

$$7.3.(4)-(6). \text{RHS} := \text{Circuit Diagram} \cdot (-w)$$

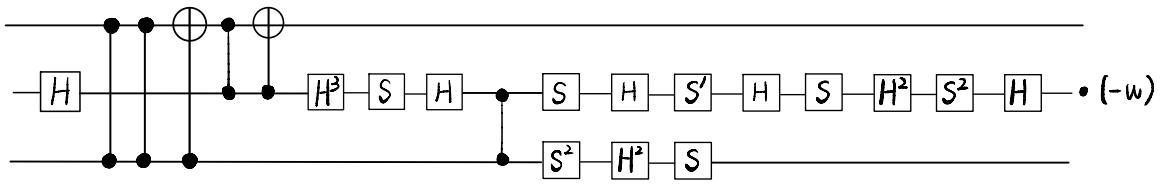
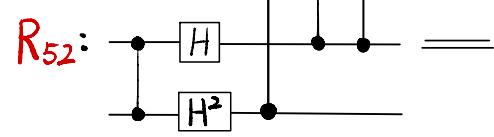
$$\text{def} \quad \text{Circuit Diagram} \cdot (-w)$$

$$\frac{R_{17}, R_{31}}{C_{15}^4, C_{15}^{14}} \quad \text{Circuit Diagram} \cdot (-w)$$

$$\frac{R_{19}}{\text{WTS}} \quad \text{Circuit Diagram} \cdot (-w)$$

Hence

$$\text{Circuit Diagram} \cdot (-w)$$



Lem 19

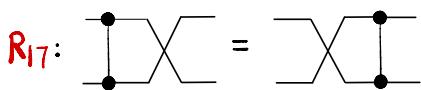
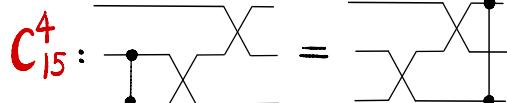
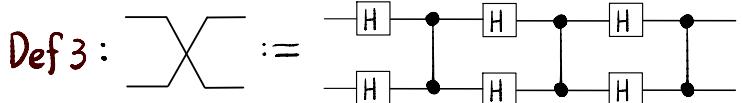
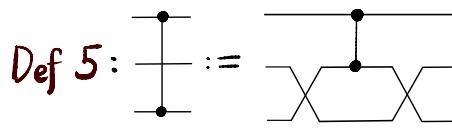
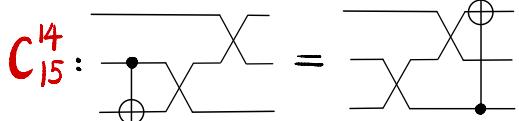
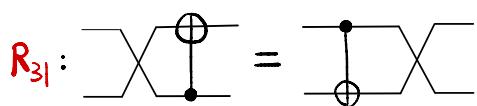
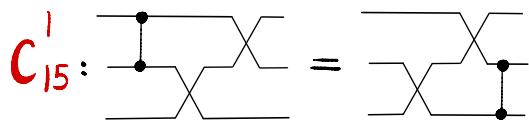
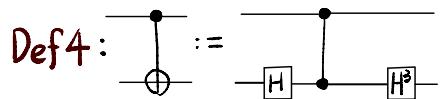
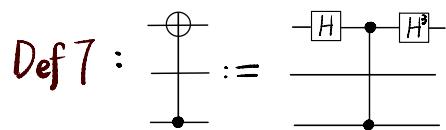
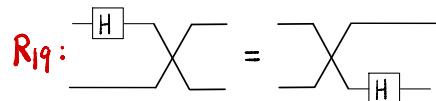
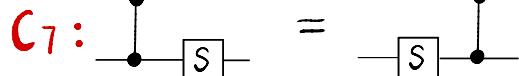
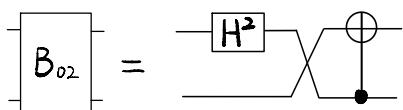
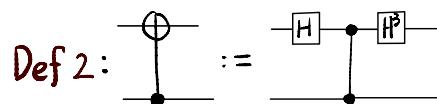
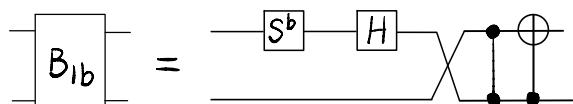
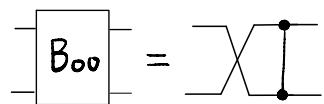
$$7.3.(4)-(6) \quad \text{Circuit: } B_{02} \xrightarrow{\text{WTS}} B_{01} \xrightarrow{\text{H, H, H, S, H}} S \xrightarrow{\text{H, H, Z}} Z \xrightarrow{\text{H, H, Z}} X \cdot (-w)$$

Proof cont :

$$\begin{aligned} C_2, C_3, \text{Def 1} \parallel R_5, R_{10}, R_{11} \quad & SHS\bar{Z}^2X \xrightarrow[R_5]{R_{11}} SHSS'S^2 HSH^2S^2H \xrightarrow{C_3} SHS'HSH^2S^2H \\ & H^2\bar{Z} \xrightarrow{R_{10}} H^2S'S'S \xrightarrow{\text{Def 1}} H^2H^2S^2H^2S \xrightarrow{C_2} S^2H^2S \end{aligned}$$

By  $R_{52}$ , this completes the proof.

□



Lem 20 Def 2-5, Def 7, C<sub>2</sub>, C<sub>3</sub>, C<sub>7</sub>, C<sub>8</sub>, C<sub>15</sub>, R<sub>16</sub>, R<sub>17</sub>, R<sub>19</sub>, R<sub>31</sub> & R<sub>53</sub> imply

7.4-6.(1) • w<sup>2</sup>

Proof: 7.4-6.(1). LHS :=

def

G<sub>7</sub>

R<sub>17</sub>, R<sub>31</sub>  
C<sub>15</sub><sup>4</sup>, C<sub>15</sub><sup>14</sup>

R<sub>19</sub>  
C<sub>15</sub><sup>1</sup>