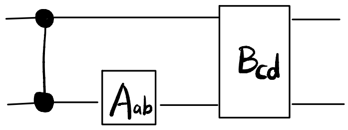
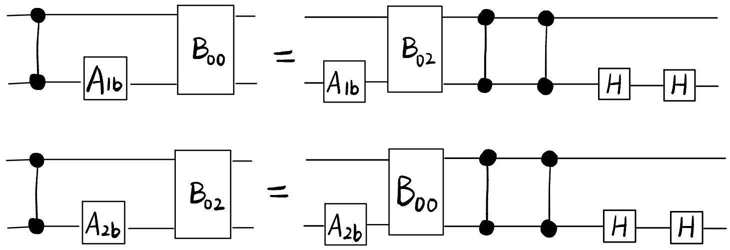
For 4.(3) – 4.(8) : $a \neq 0,\ b \in \mathbb{Z}_3$

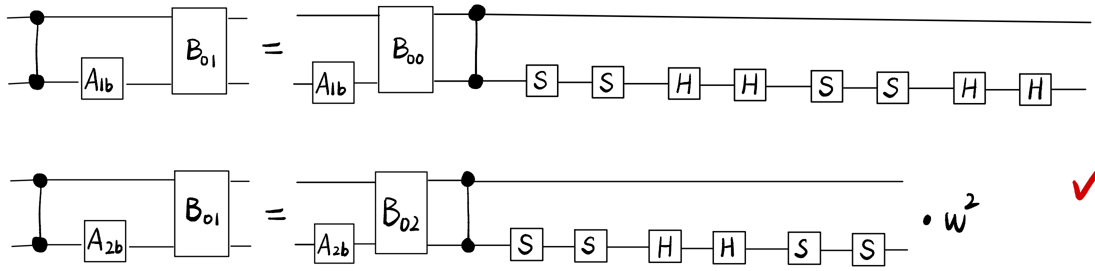


Type	Count
(a), (b) ✓ $b \in \mathbb{Z}_3$	$3 \times 2 = 6$
(c) $\cdot\ w^2$	3
(d) $\cdot\ w^2$ ✓ $b \in \mathbb{Z}_3$	3
(e) $\cdot\ w$ ✓ $b \in \mathbb{Z}_3$	3
(f) $\cdot\ w$	3
(g) $\cdot(-w^2)$ ✓ $b, d \in \mathbb{Z}_3$	$3 \times 3 = 9$
(h) $\cdot(-w^2)$	$3 \times 3 = 9$
(i) $\cdot\ w$ ✓ $b, d \in \mathbb{Z}_3$	$3 \times 3 = 9$
(j) $\cdot\ w$	$3 \times 3 = 9$

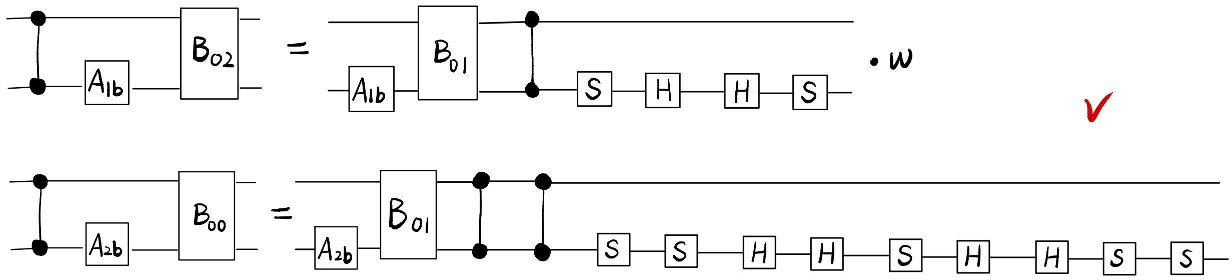
(a), (b)



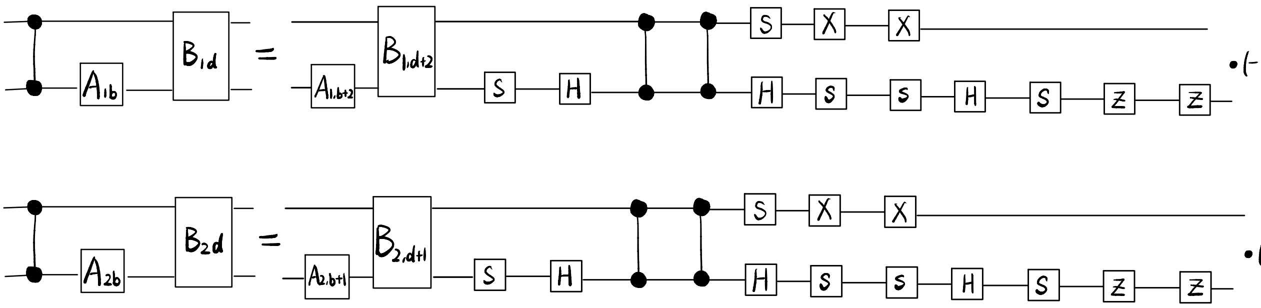
(c), (d)



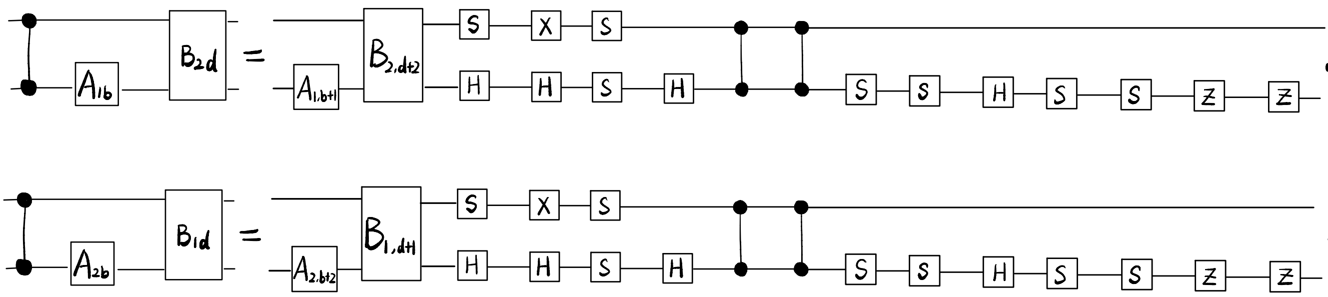
(e), (f)



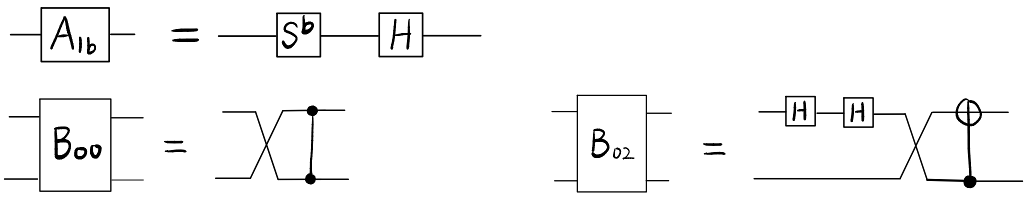
(g), (h)

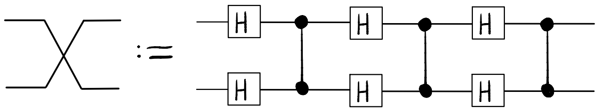


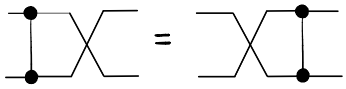
(i), (j)

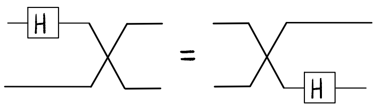


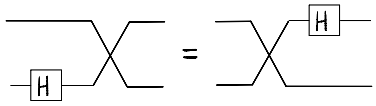
Total 54

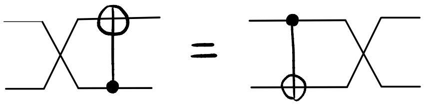


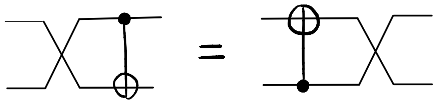
Def 3 : 

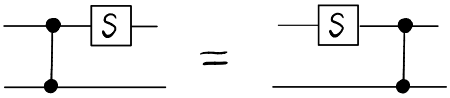
R_{17}: 

R_{19} : (1) 

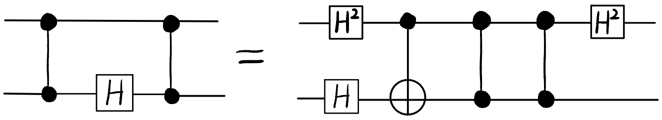
(2) 

R_{31} : (1) 

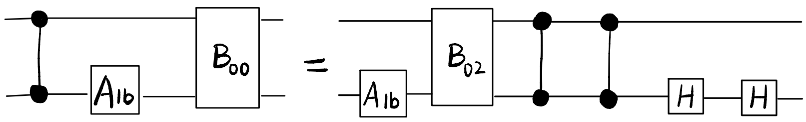
(2) 

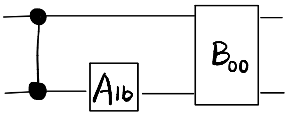
C_7 : (1) 

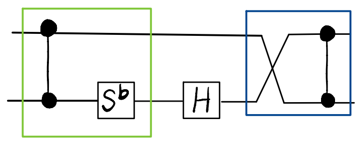
(2) 

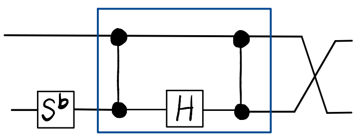
R_{32}^{7} : 

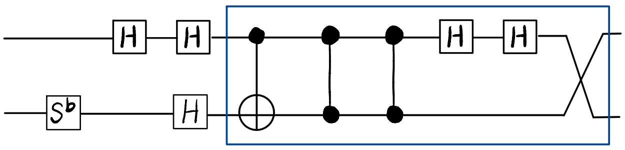
Lem 46 By Def 3 , C_7 , R_{17} , R_{19} , R_{31} & R_{32} ,

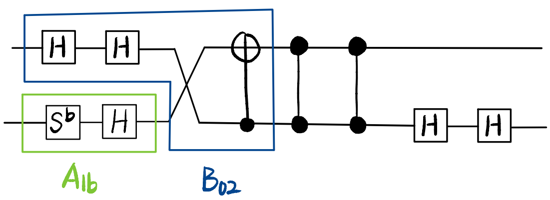
4. (a) 

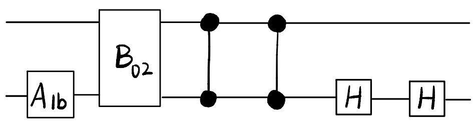
Proof: 4.(a).LHS := 

$\overset{def}{=\!=}$ 

$\underset{R_{17}}{\overset{C_7}{=\!=}}$ 

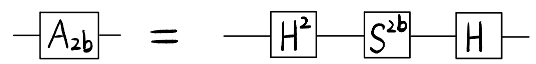
$\overset{R_{32}^{7}}{=\!=}$ 

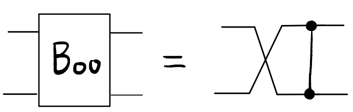
$\underset{R_{31}}{\overset{R_{17}, R_{19}}{=\!=}}$ 

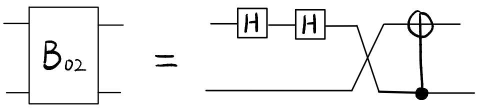
$\overset{def}{=\!=}$ 

=: 4.(a).RHS

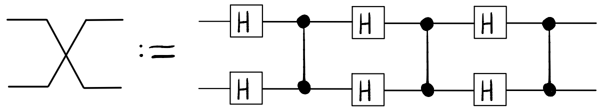
∎



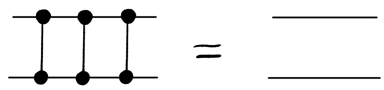




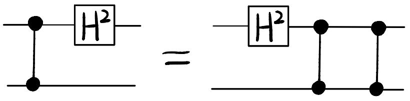
Def 3 :



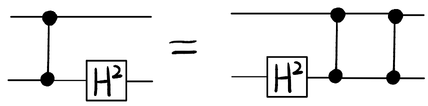
C_6 :



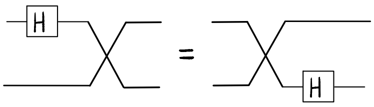
C_8 : (1)



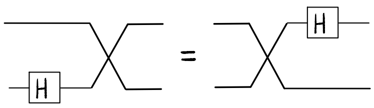
(2)



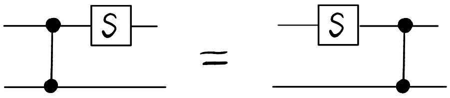
R_{19} : (1)



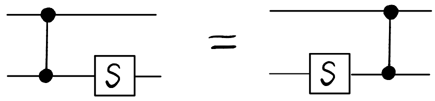
(2)



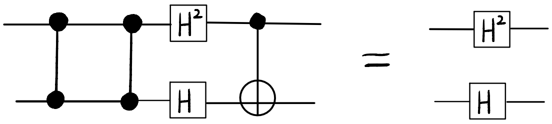
C_7 : (1)



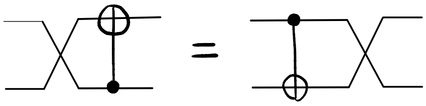
(2)



R_{32} :

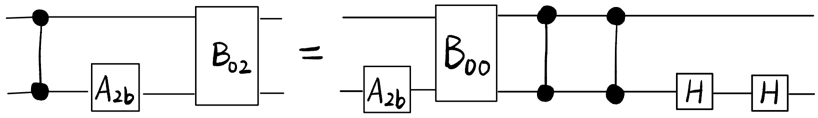


R_{31} : (1)

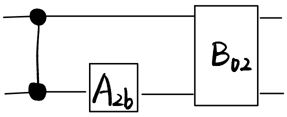


Lem 47 By Def 3, C_6, C_7, C_8, R_{19}, R_{31} & R_{32},

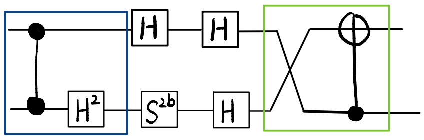
4.(b)



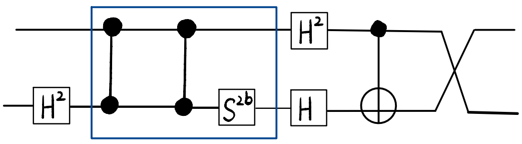
Proof: 4.(b).LHS :=



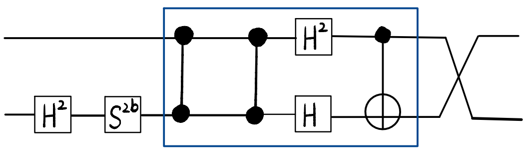
def



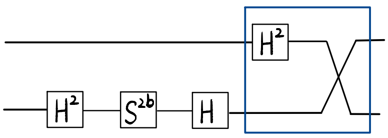
C_8 = R_{31}



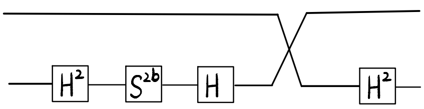
C_7



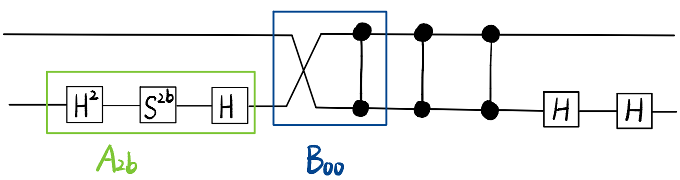
R_{32}



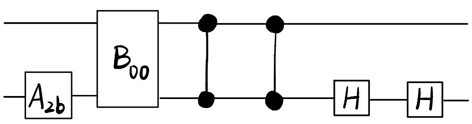
R_{19}



C_6

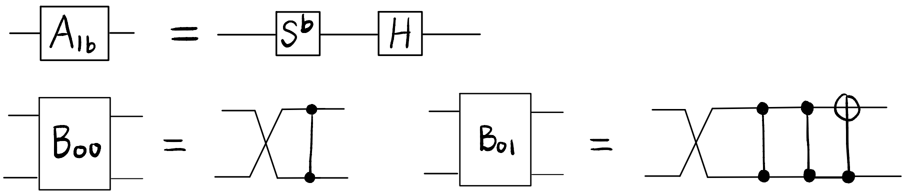


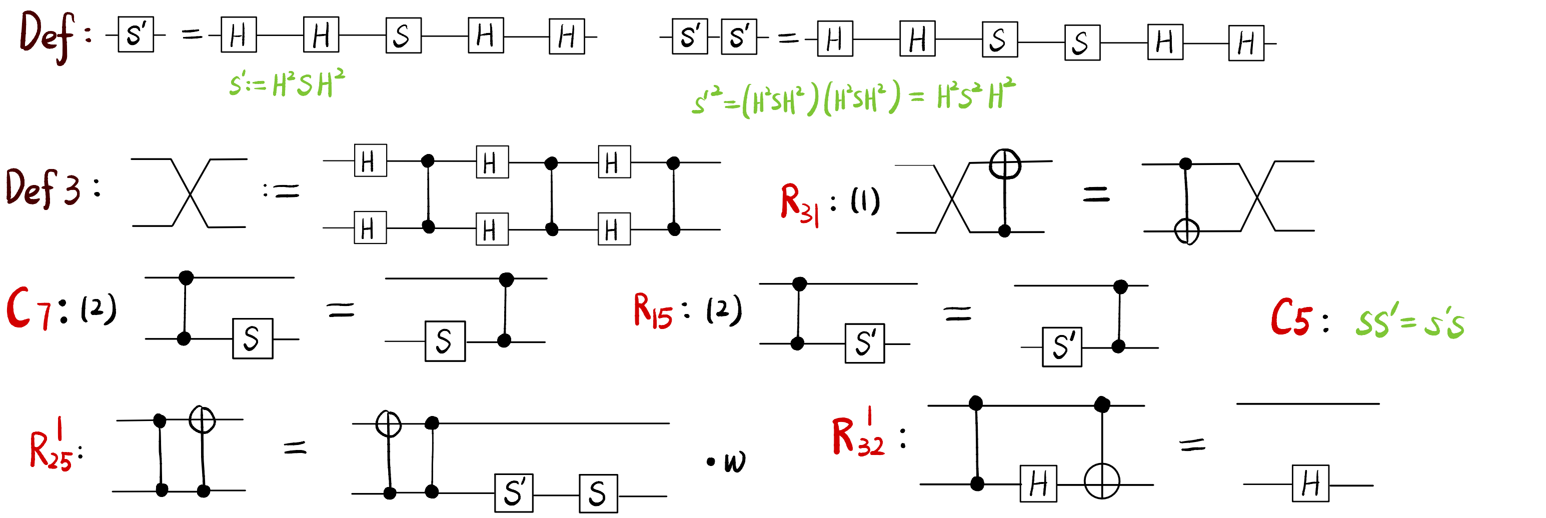
def



=: 4.(b).RHS

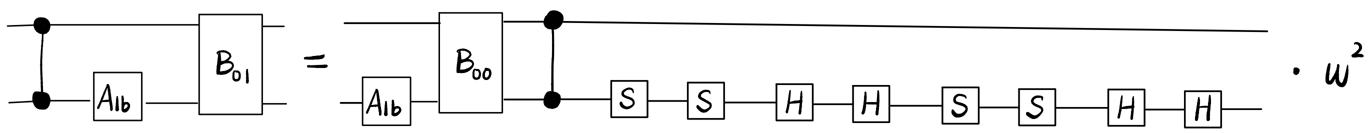
∎



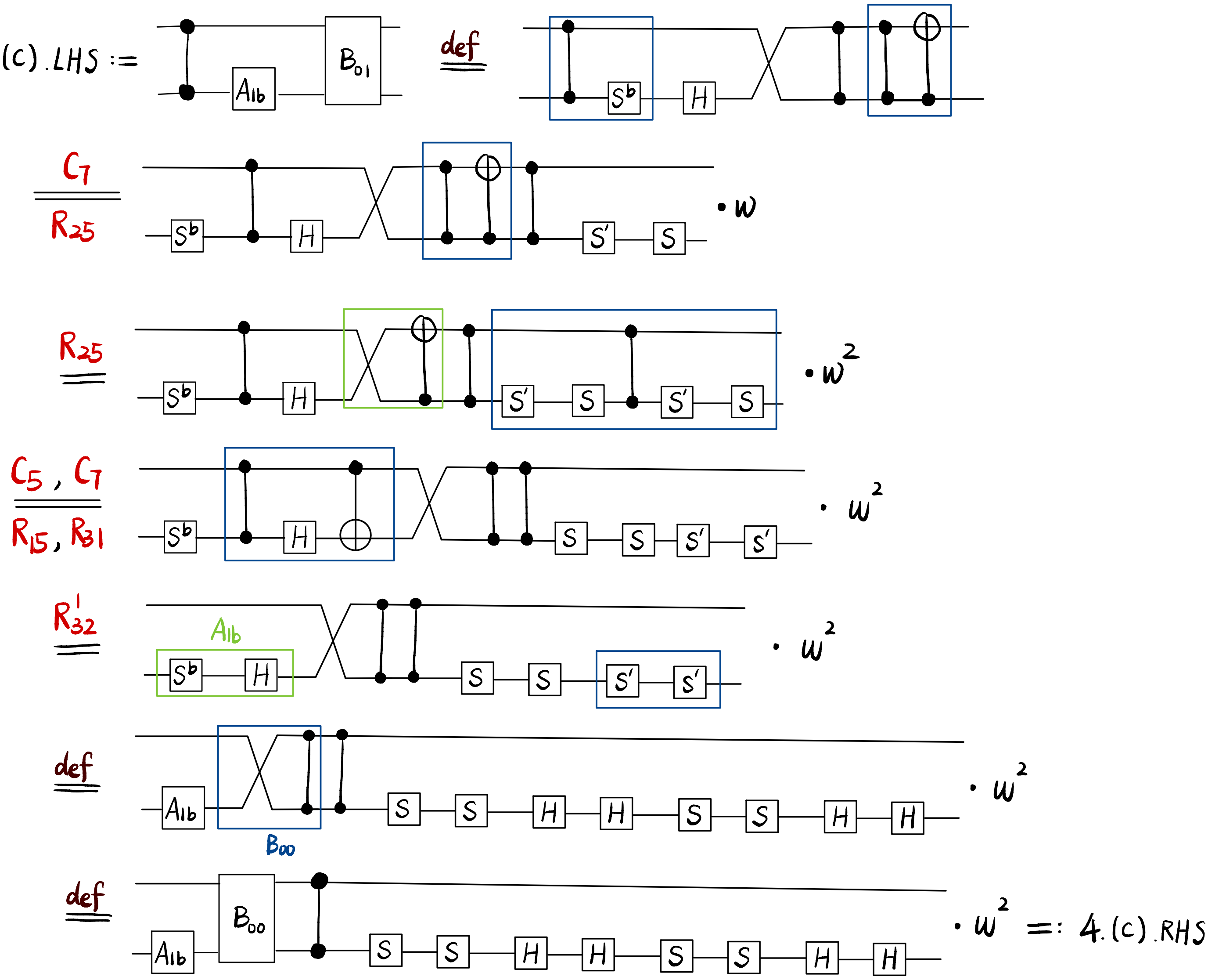


Lem 48 By Def 3, C_5, C_7, R_{15}, R_{25}, R_{31} & R_{32},

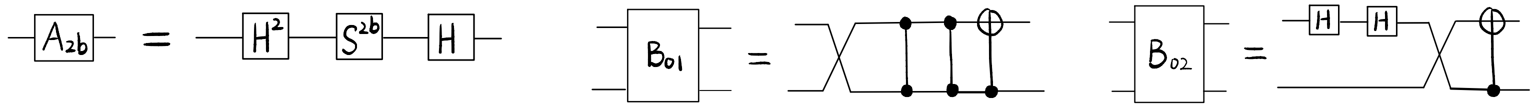
4. (c)

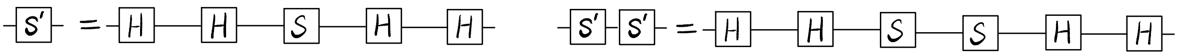


Proof: 4.(c).LHS :=

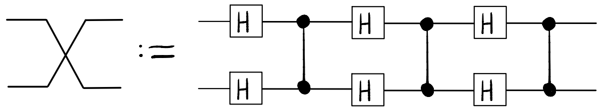


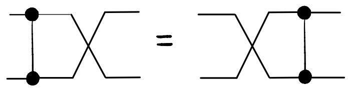
☐

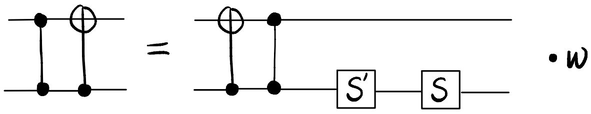


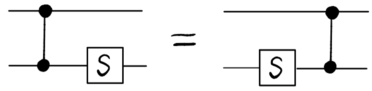
Def : 

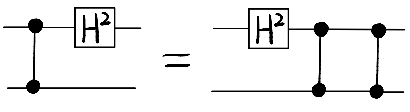
$s' := H^2 S H^2$ $s'^2 = (H^2SH^2)(H^2SH^2) = H^2S^2H^2$

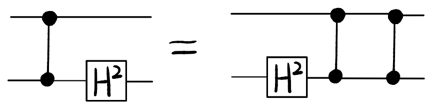
Def 3 : 

R_{17} : 

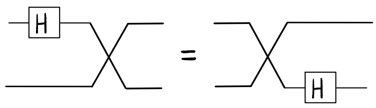
R^1_{25} : 

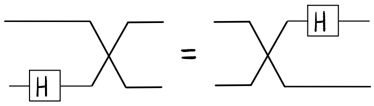
C_7 : (2) 

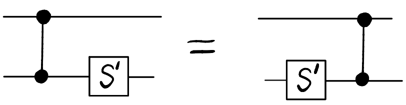
C_8 : (1) 

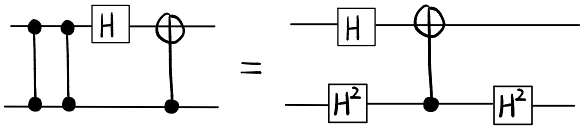
(2) 

$C5$: $ss' = s's$

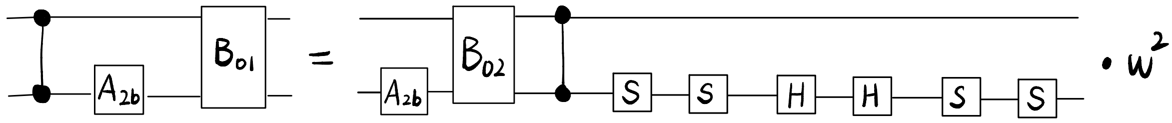
R_{19} : (1) 

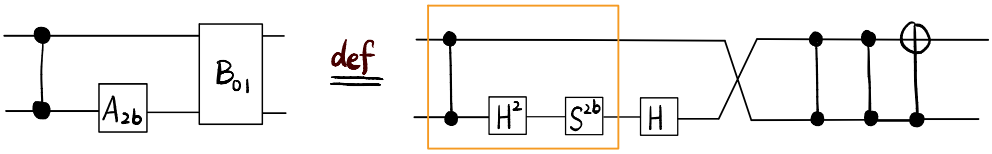
(2) 

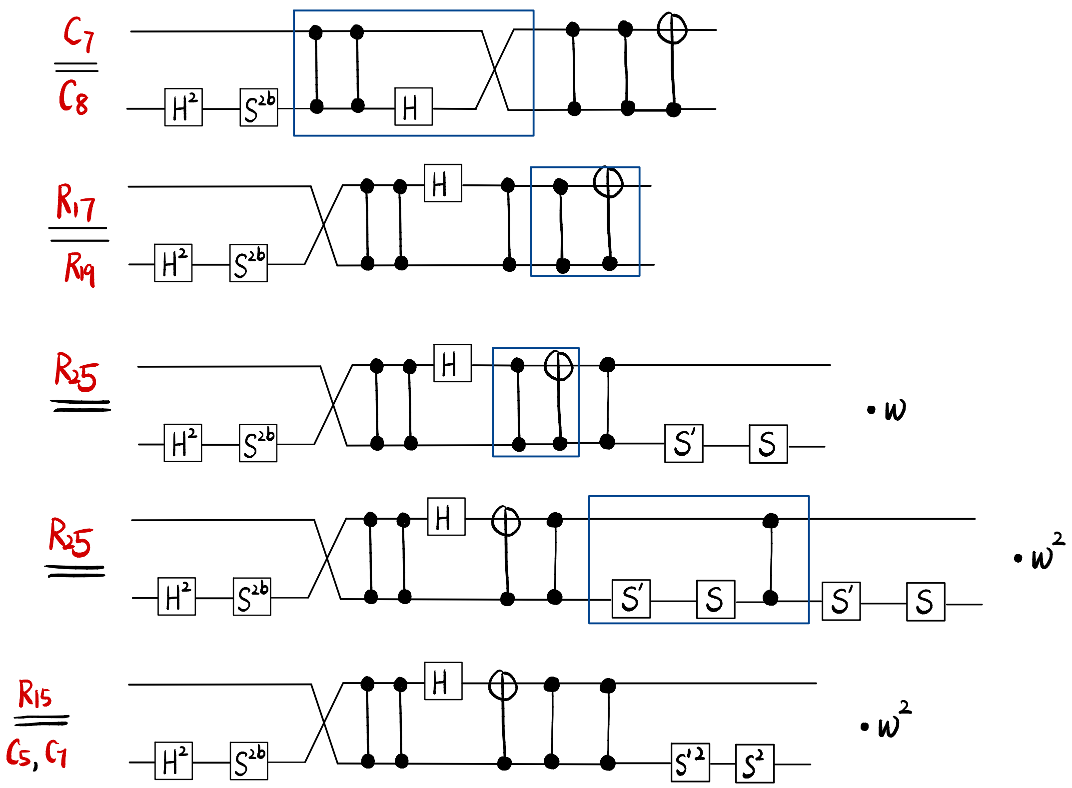
R_{15} : (2) 

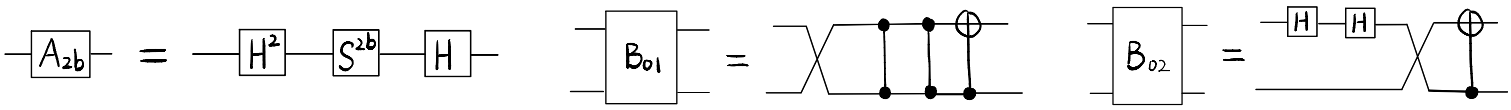
R^6_{32} : 

Lem 49 By Def 3, C_2, C_5, C_7, C_8, R_{15}, R_{17}, R_{19}, R_{25} & R_{32},

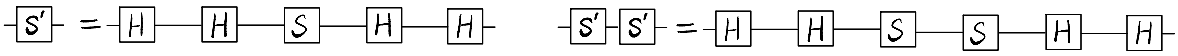
4.(d) 

Proof: 4.(d).LHS := 





Def :

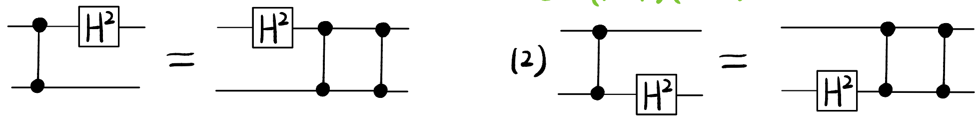


$S' := H^2 S H^2$

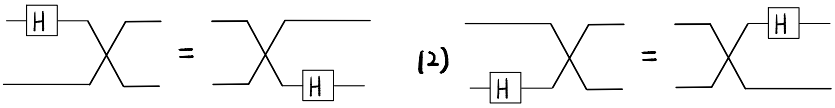
$S'^2 = (H^2 S H^2)(H^2 S H^2) = H^2 S^2 H^2$

C2 : $H^4 = I$

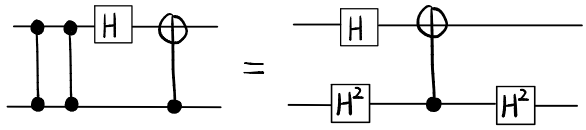
C_8 : (1)



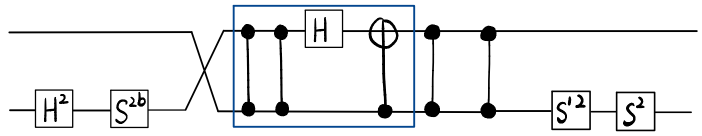
R_{19} : (1)



R_{32}^6 :

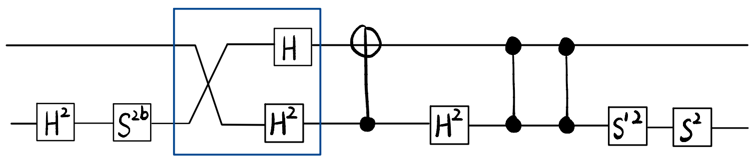


Proof cont.



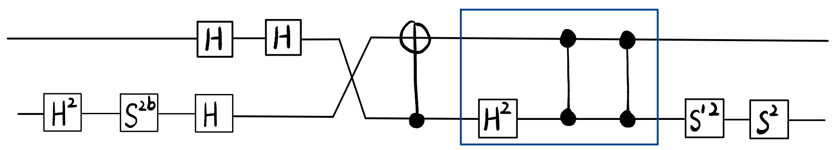
$\cdot w^2$

R_{32}^6



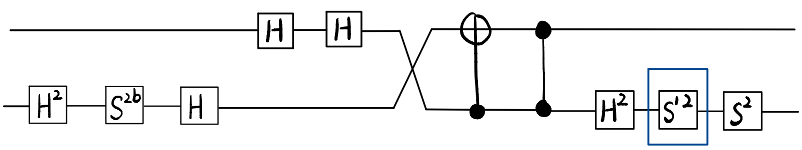
$\cdot w^2$

R_{19}



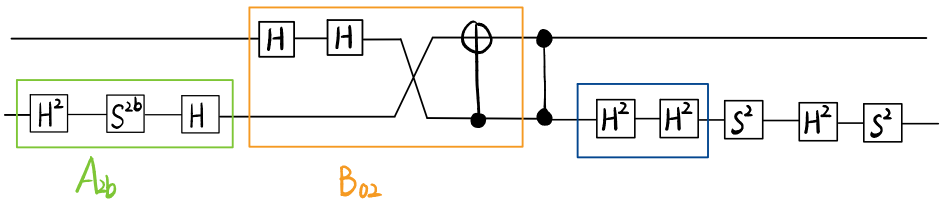
$\cdot w^2$

C_8



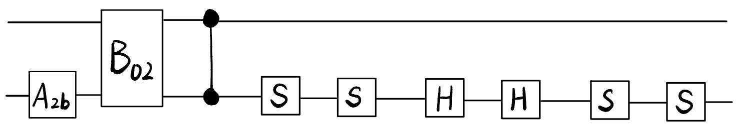
$\cdot w^2$

def



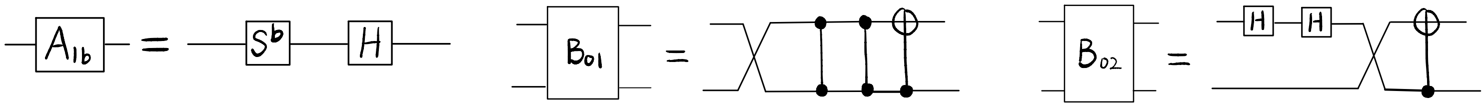
$\cdot w^2$

def
C_2

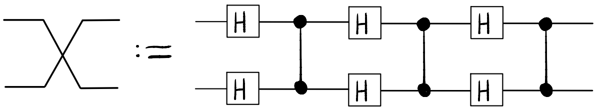


$\cdot w^2 =: 4.(d).\ RHS$

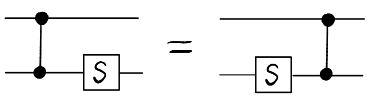
∎



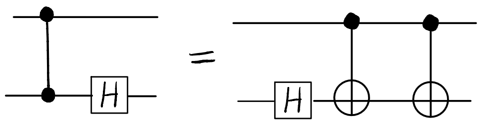
Def 3 :



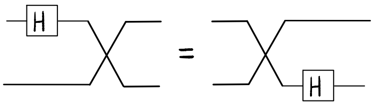
C_7: (2)



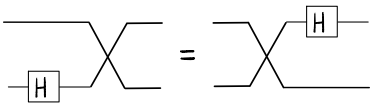
R_{32}^5 :



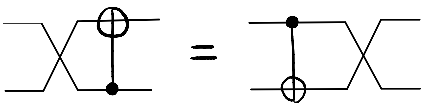
R_{19} : (1)



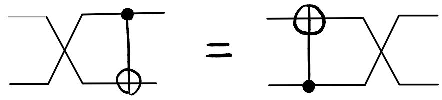
(2)



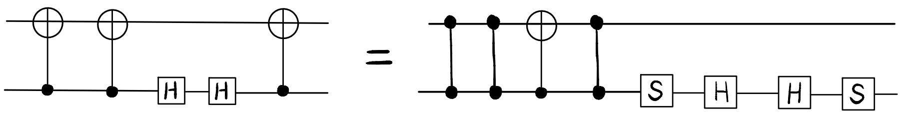
R_{31} : (1)



(2)



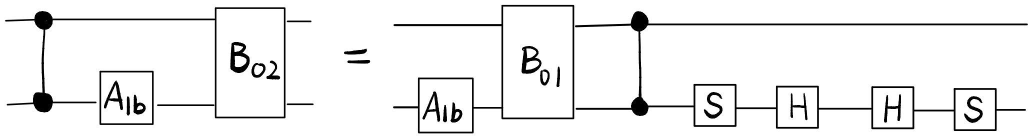
R_{33} :



$\cdot\, w$

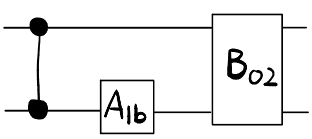
Lem 50 By Def 3, C_7, R_{19}, R_{31}, R_{32} & R_{33},

4.(e)

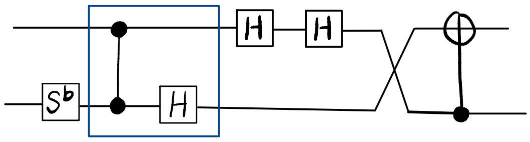


$\cdot\, w$

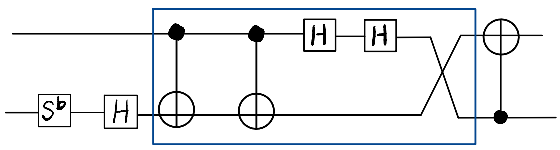
Proof: 4.(e).LHS :=



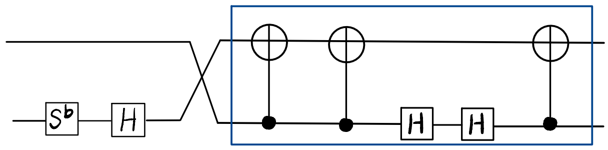
$\stackrel{C_7}{=}$



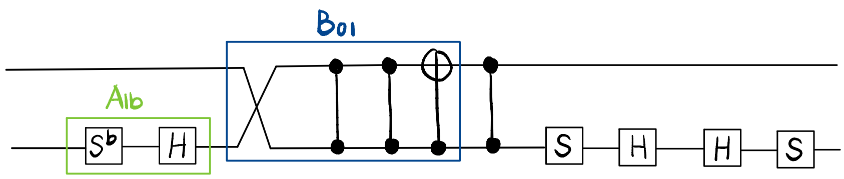
$\stackrel{R_{32}^5}{=}$



$\stackrel{R_{19}}{\underset{R_{31}}{=}}$

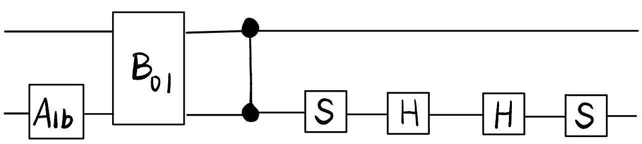


$\stackrel{R_{33}}{=}$



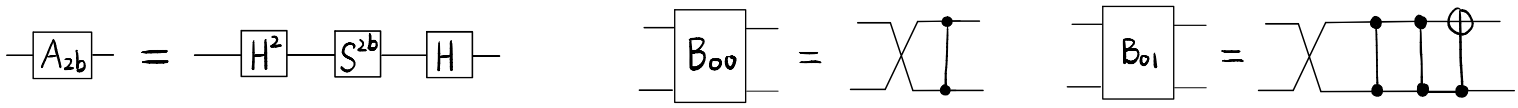
$\cdot\, w$

$\stackrel{def}{=}$

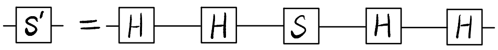


$\cdot\, w$ =: 4.(e).RHS

☐



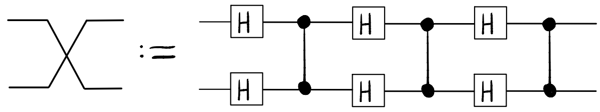
Def :



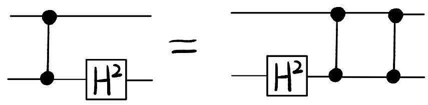
$S' := H^2 S H^2$

C5 : $SS' = S'S$ C3 : $S^3 = I$

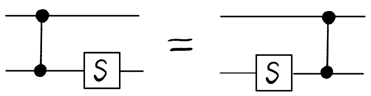
Def 3 :



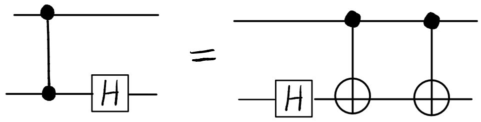
C8 : (2)



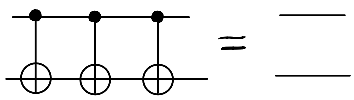
C7 : (2)



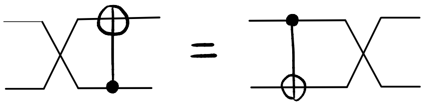
R_{32}^5 :



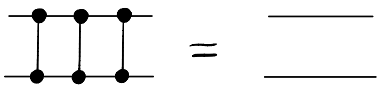
C_6' :



R_{31} : (1)

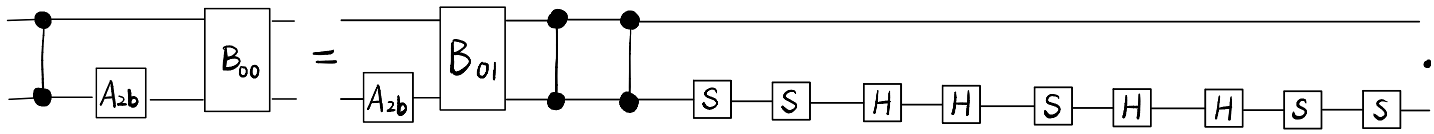


C_6 :

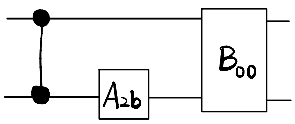


Lem 51 By Def 3, C_3, C_5, C_6, C_7, C_8, R_{15}, R_{25}, R_{31} & R_{32},

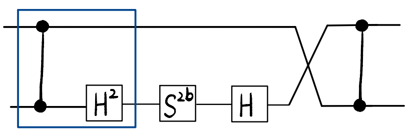
4.(f)



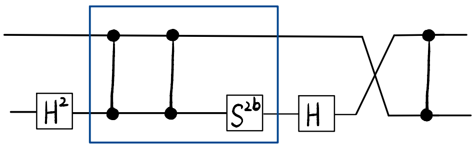
Proof: 4.(f).LHS :=



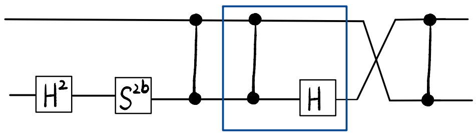
def



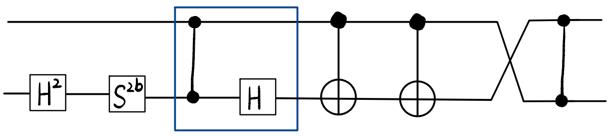
C_8



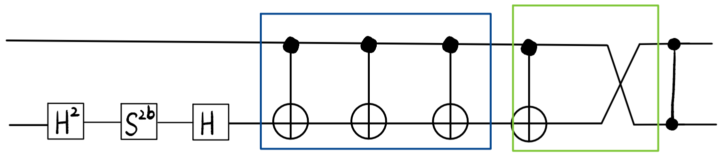
C_7



R_{32}^5

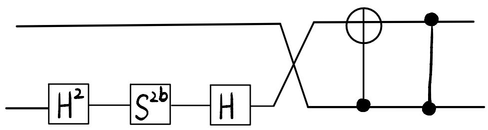


R_{32}^5

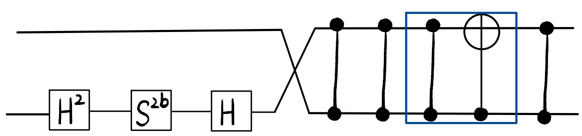


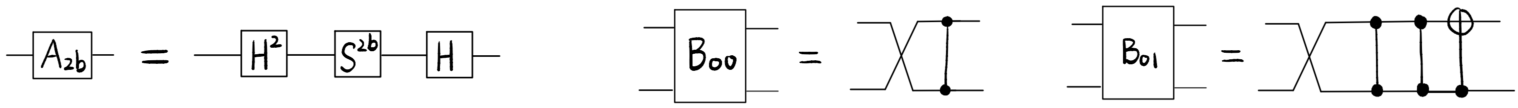
C_6'

R_{31}

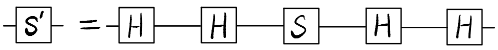


C_6





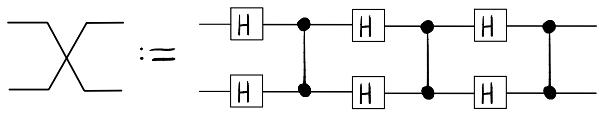
Def :



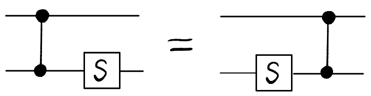
$S' := H^2 S H^2$

C5 : $SS' = S'S$ C3 : $S^3 = I$

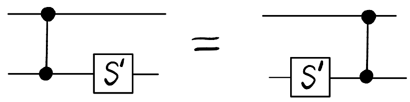
Def 3 :



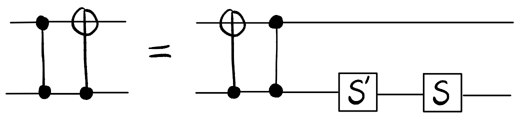
C7 : (2)



R15 : (2)

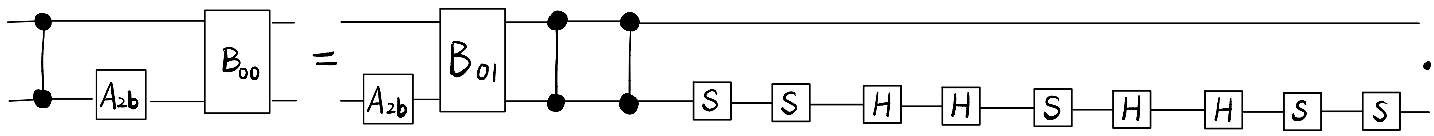


R^1_{25} :



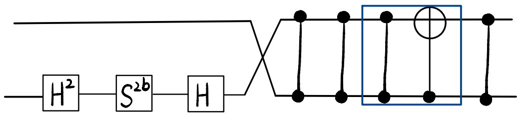
$\cdot w$

4.(f)

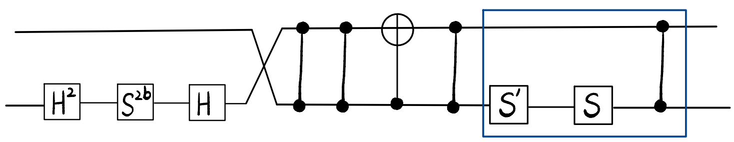


$\cdot w$

Proof cont.

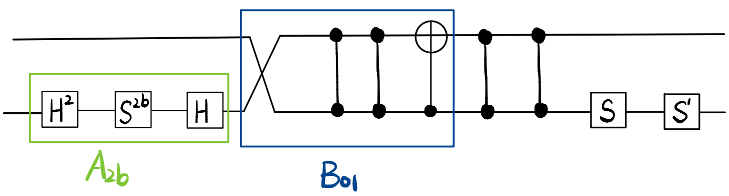


$\overset{C'_{25}}{=}$



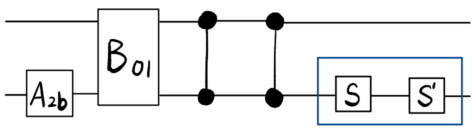
$\cdot w$

$\overset{C_5, C_7}{\underset{R_{15}}{=}}$



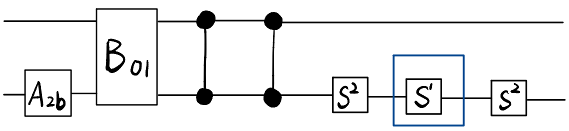
$\cdot w$

$\overset{\text{def}}{=}$



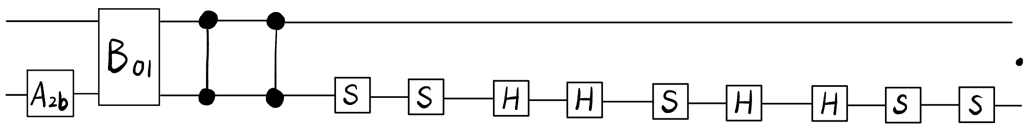
$\cdot w$

$\overset{C_3}{\underset{C_5}{=}}$



$\cdot w$

$\overset{\text{def}}{=}$



$\cdot w$ =: 4.(f).RHS

☑