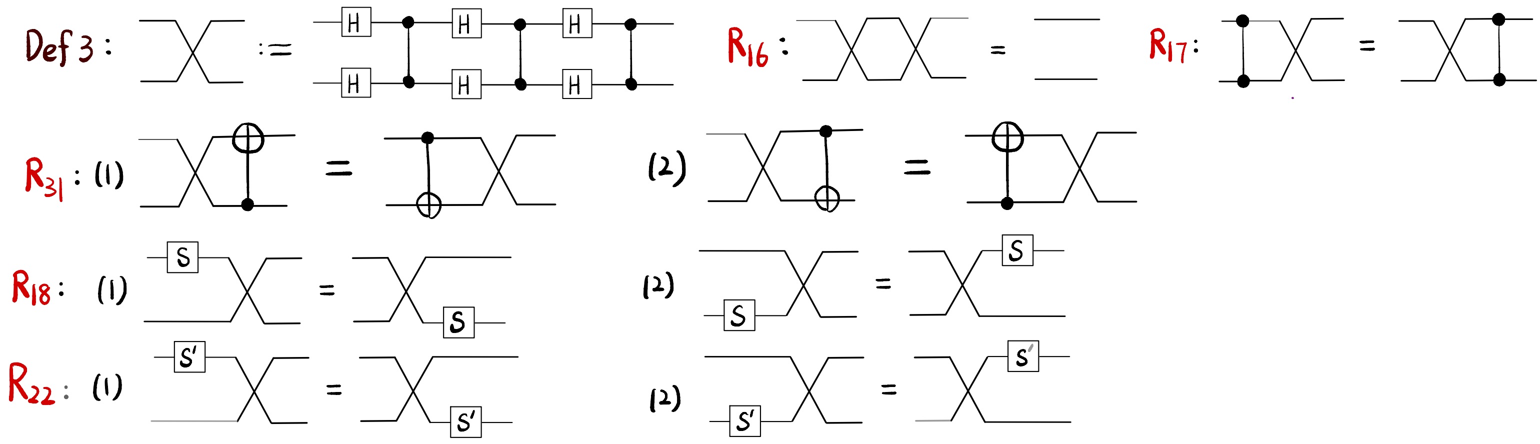
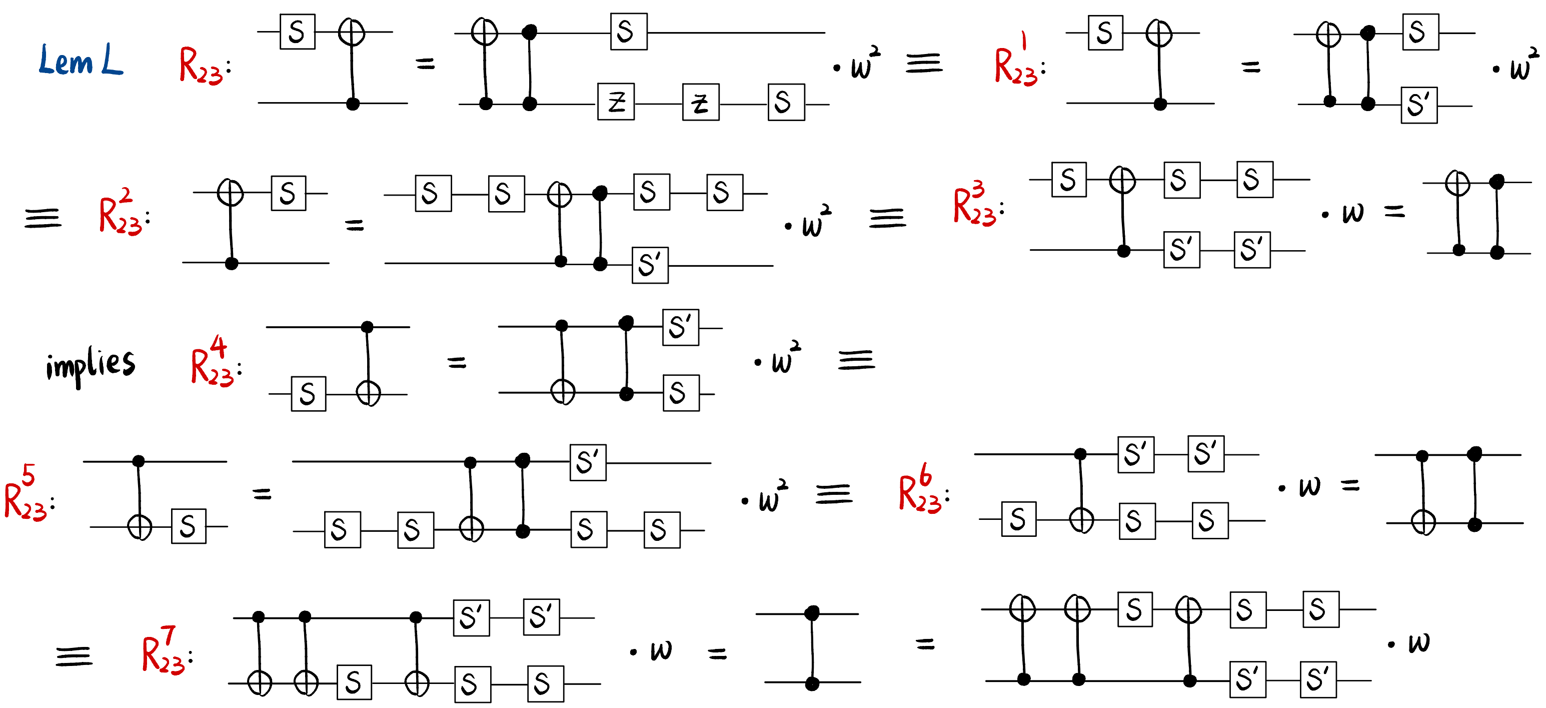
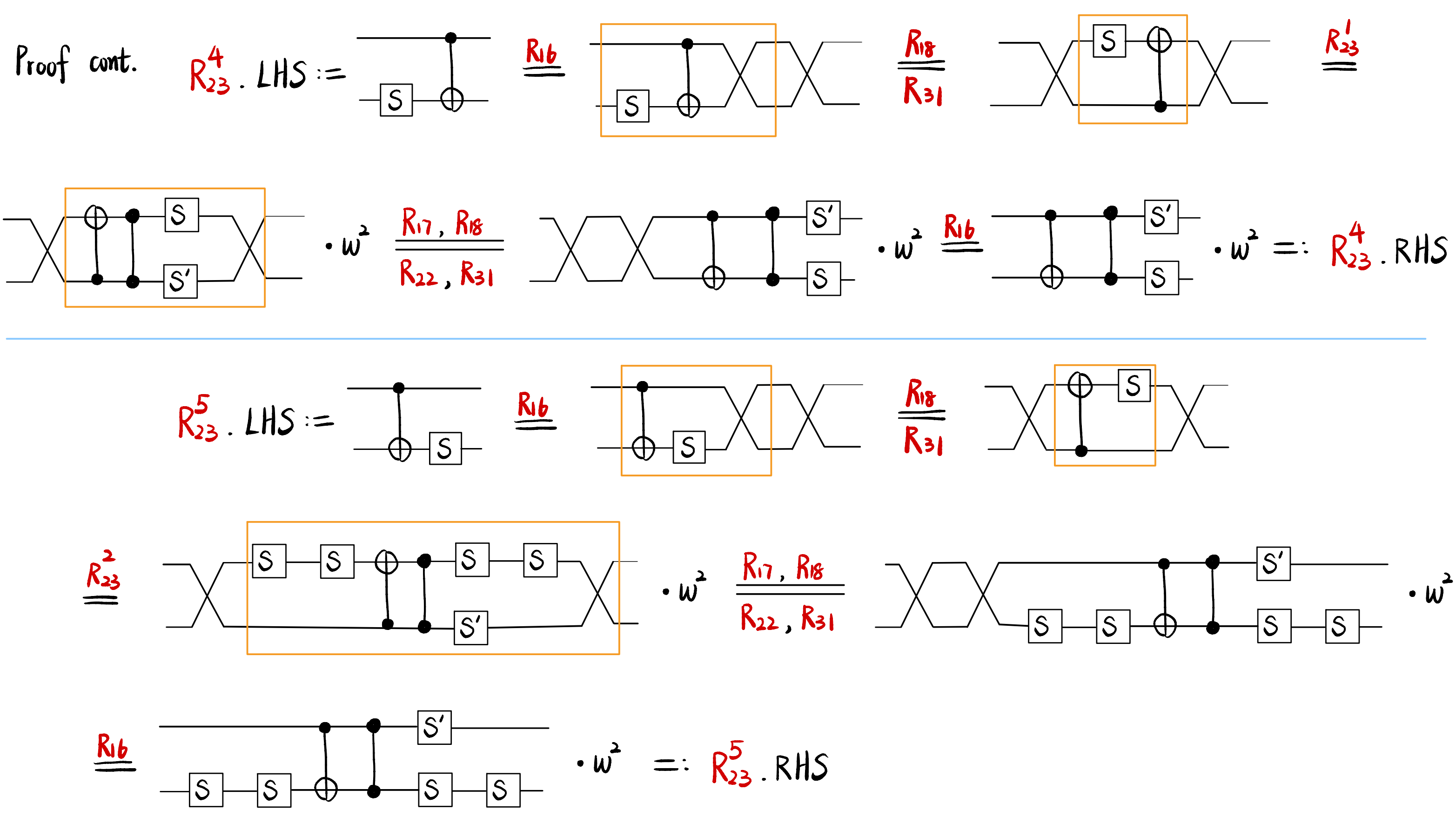


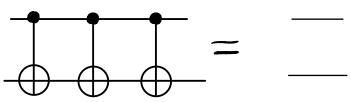
Def 3 : :=
H H H H H H
R_{16} : =
R_{17} : =
R_{31} : (1) =
(2) =
R_{18} : (1) =
S S
(2) =
S S
R_{22} : (1) =
S′ S′
(2) =
S′ S′

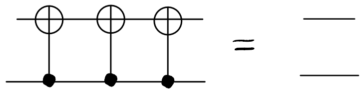


Lem L
R_{23}: = $\cdot w^2$ ≡ R^1_{23}: = $\cdot w^2$
S S Z Z S
≡ R^2_{23}: = $\cdot w^2$ ≡ R^3_{23}: $\cdot w$ =
implies R^4_{23}: = $\cdot w^2$ ≡
R^5_{23}: = $\cdot w^2$ ≡ R^6_{23}: $\cdot w$ =
≡ R^7_{23}: $\cdot w$ = = $\cdot w$

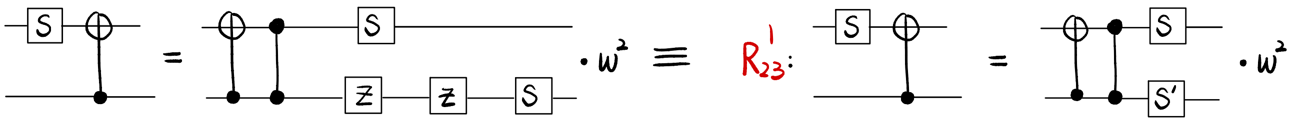


Proof cont.
R^4_{23} . LHS :=
R_{16}
R_{18} / R_{31}
R^1_{23}
$\cdot w^2$
R_{17} , R_{18} / R_{22} , R_{31}
$\cdot w^2$
R_{16}
$\cdot w^2$ =: R^4_{23} . RHS
R^5_{23} . LHS :=
R_{16}
R_{18} / R_{31}
R^2_{23}
$\cdot w^2$
R_{17} , R_{18} / R_{22} , R_{31}
$\cdot w^2$
R_{16}
$\cdot w^2$ =: R^5_{23} . RHS

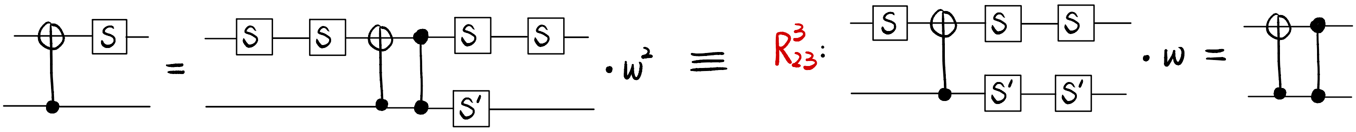
C_6^1: 

C_6^2: 

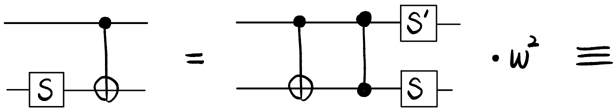
Lem L R_{23}:



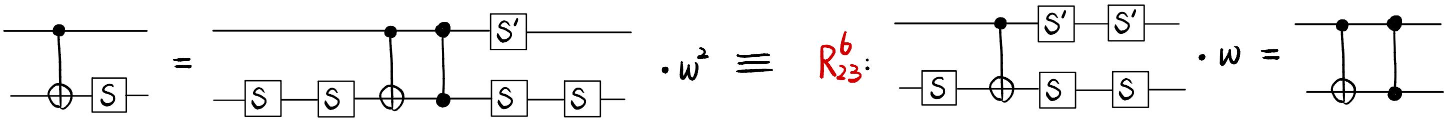
$\equiv$ R_{23}^2:



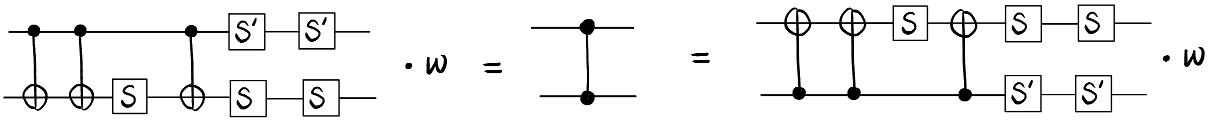
implies R_{23}^4:



R_{23}^5:

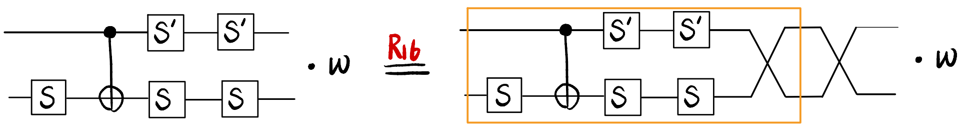


$\equiv$ R_{23}^7:

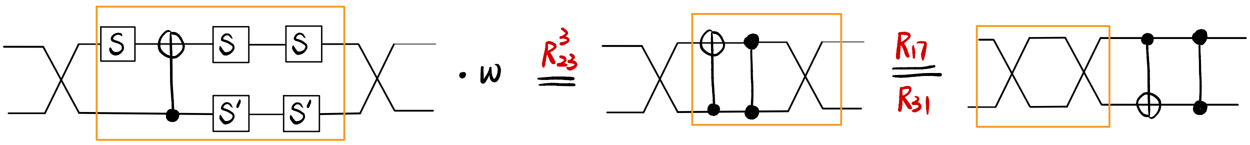


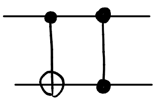
Proof cont.

R_{23}^6 . LHS :=

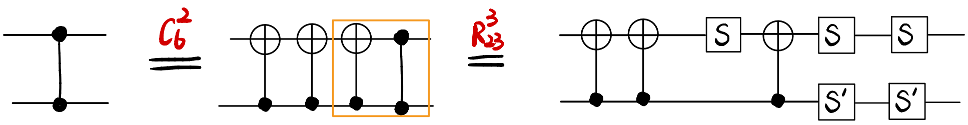


$\frac{R_{17},\ R_{18}}{R_{22},\ R_{31}}$



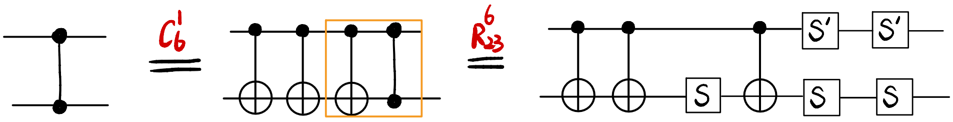
R_{16}  $=:$ R_{23}^6 . RHS

R_{23}^7 . MID :=



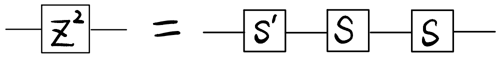
$=:$ R_{23}^7 . RHS

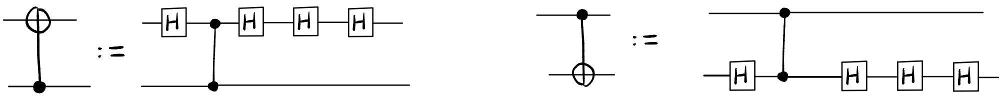
R_{23}^7 . MID :=



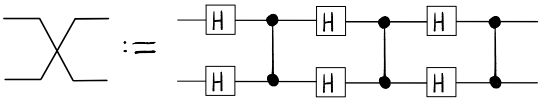
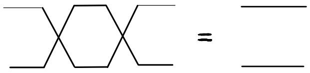
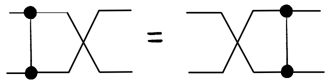
$=:$ R_{23}^7 . LHS

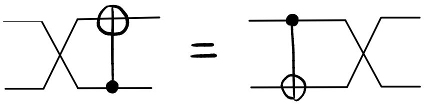
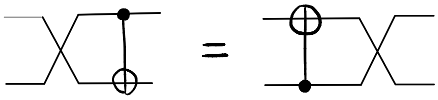
∎

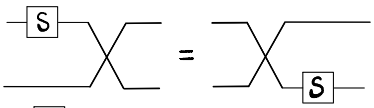
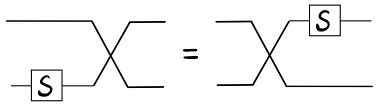
C1: $w^3 = 1$ C2: $H^4 = I$ C3: $S^3 = I$ R11: 

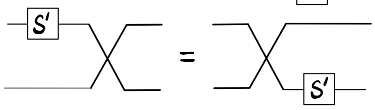
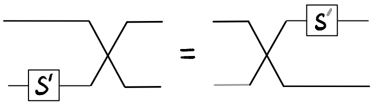
Def 2: 

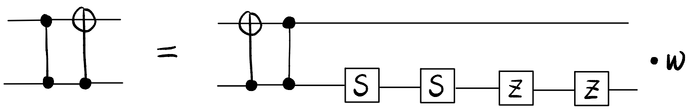
C5: $SH^2SH^2 = H^2SH^2S$ $SS' = S'S$

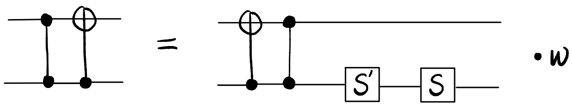
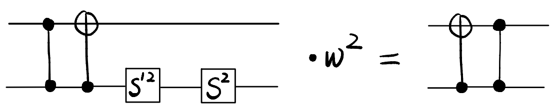
Def 3:  R_{16}:  R_{17}: 

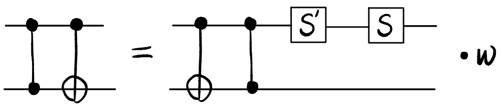
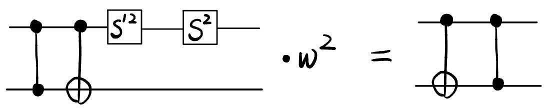
R_{31}: (1)  (2) 

R_{18}: (1)  (2) 

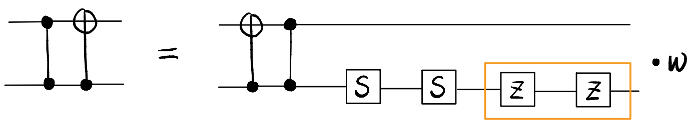
R_{22}: (1)  (2) 

Lem M R_{25}: 

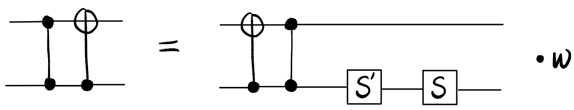
$\equiv R^1_{25}$:  $\equiv R^2_{25}$: 

R^3_{25}:  $\equiv R^4_{25}$: 

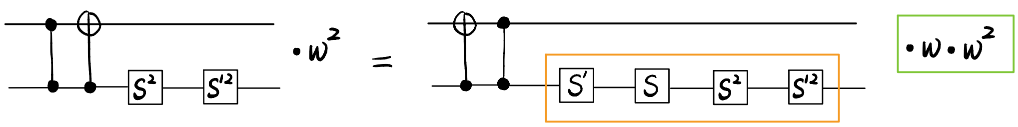
Proof:

R_{25}: 

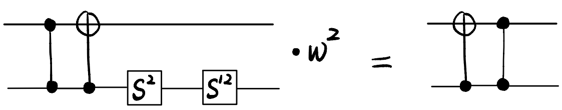
C_5 ||| R_{11} & C_3 $S^2(S'S^2) = S'S$

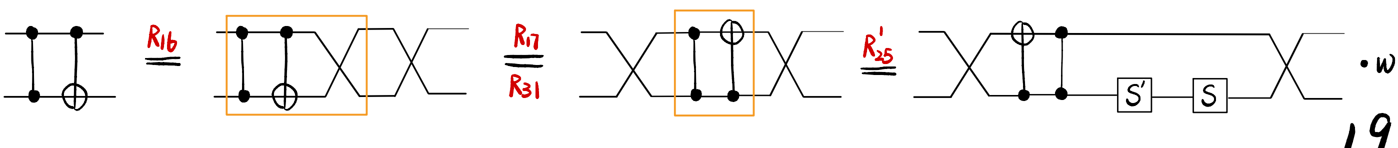
R^1_{25}: 

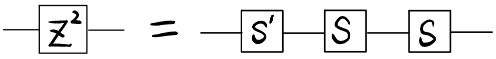
For both sides of R^1_{25}, right-appending them by $I \otimes S^2S'^2$ and multiplying them by w^2 yields

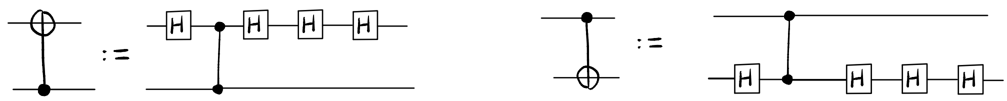
R^1_{25}: 

C_1 & C_2 ||| C_3 & C_5

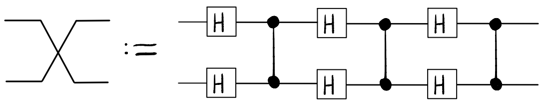
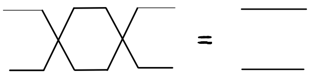
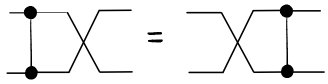
R^1_{25}:  : R^2_{25}

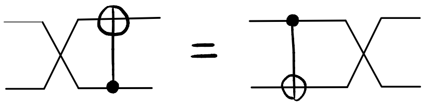
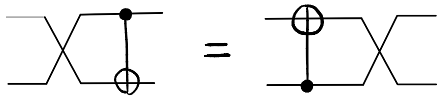
R^3_{25}. LHS := 

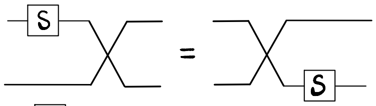
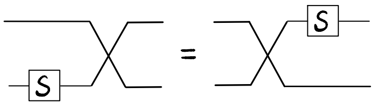
C1: $w^3=1$ C2: $H^4=I$ C3: $S^3=I$ R11: 

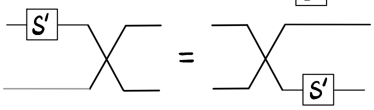
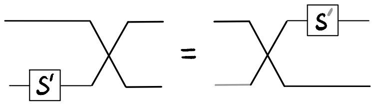
Def 2: 

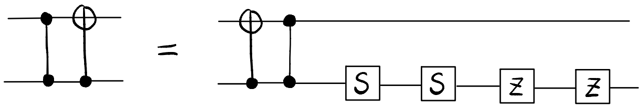
C5: $SH^2SH^2 = H^2SH^2S$ $SS' = S'S$

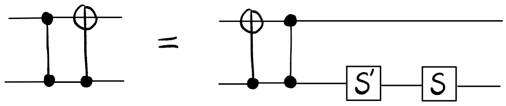
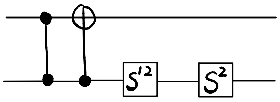
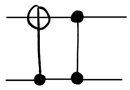
Def 3:  R16:  R17: 

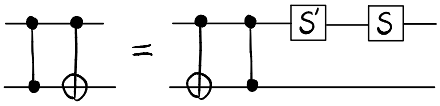
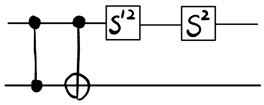
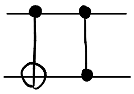
R_{31}: (1)  (2) 

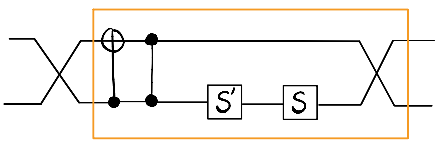
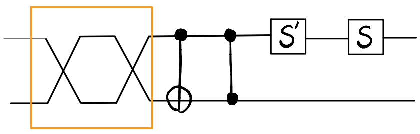
R_{18}: (1)  (2) 

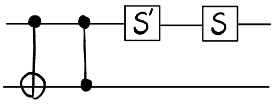
R_{22}: (1)  (2) 

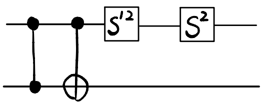
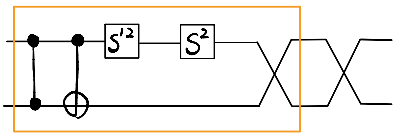
Lem M R_{25}:  $\cdot w$

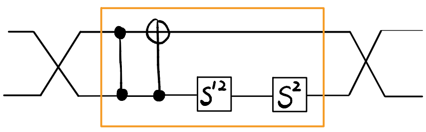
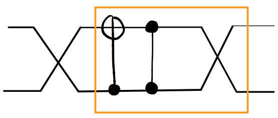
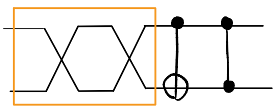
$\equiv R_{25}^1$:  $\cdot w$ $\equiv R_{25}^2$:  $\cdot w^2$ = 

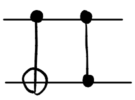
R_{25}^3:  $\cdot w$ $\equiv R_{25}^4$:  $\cdot w^2$ = 

Proof cont.  $\cdot w$ $\overset{R_{17},R_{18}}{\underset{R_{22},R_{31}}{=}}$  $\cdot w$

$\overset{R_{16}}{=}$  $\cdot w$ =: R_{25}^3. RHS.

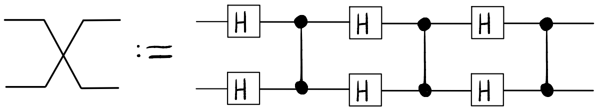
R_{25}^4. LHS :=  $\cdot w^2$ $\overset{R_{16}}{=}$  $\cdot w^2$ $\overset{R_{17},R_{18}}{\underset{R_{22},R_{31}}{=}}$

 $\cdot w^2$ $\overset{R_{25}^2}{=}$  $\overset{R_{17}}{\underset{R_{31}}{=}}$  $\overset{R_{16}}{=}$

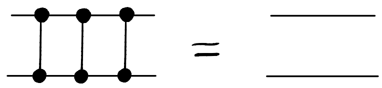
 =: R_{25}^4. RHS.

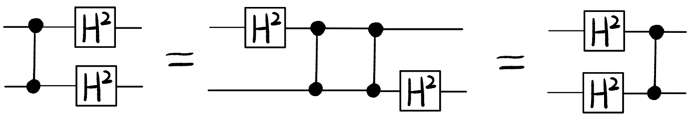
∎

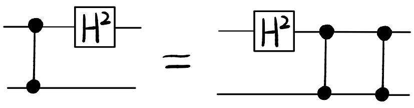
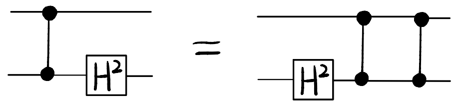
Def 2: 

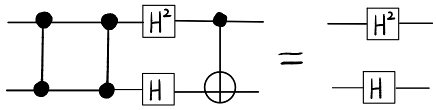
Def 3: 

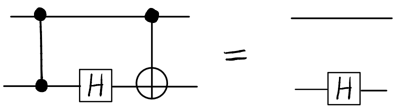
$C2: H^4 = I$

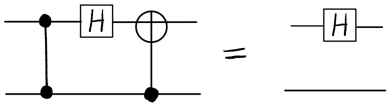
C_6: 

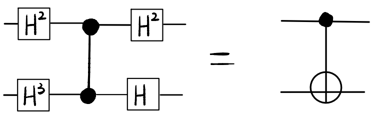
C_8^3: 

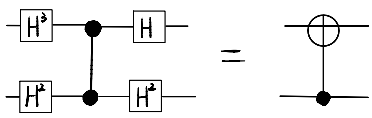
C_8: (1)  (2) 

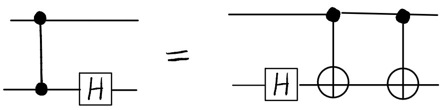
Lem N R_{32}:  ✓

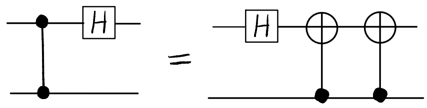
R'_{32}:  ✓

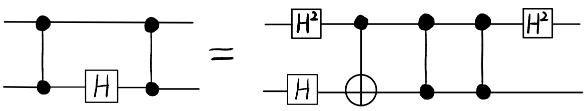
R^2_{32}: 

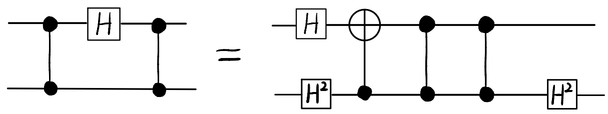
R^3_{32}: 

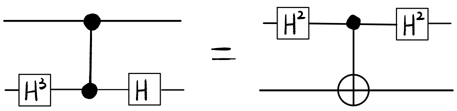
R^4_{32}: 

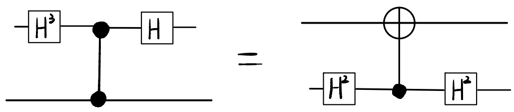
R^5_{32}: 

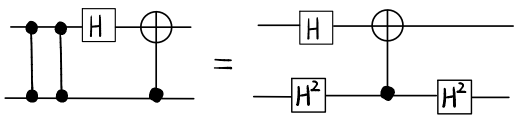
R^6_{32}: 

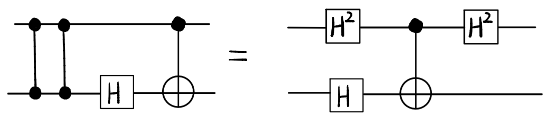
R^7_{32}: 

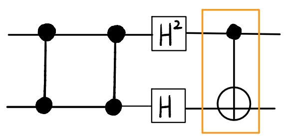
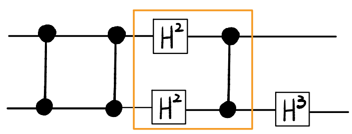
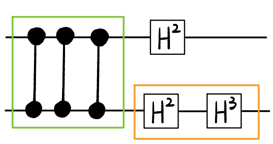
R^8_{32}: 

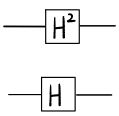
R^9_{32}: 

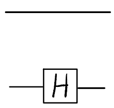
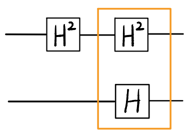
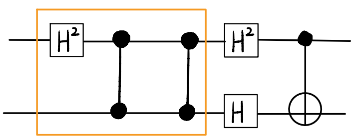
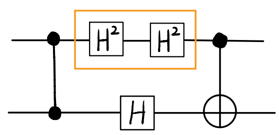
R^{10}_{32}: 

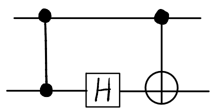
R^{11}_{32}: 

R^{12}_{32}: 

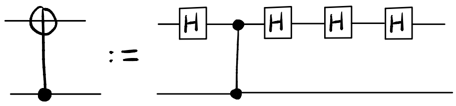
Proof: R_{32}. LHS :=  $\underset{\text{Def 2}}{=}$  $\underset{C_8^3}{=}$ 

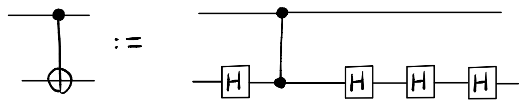
$\underset{C_2, C_6}{=}$  =: R_{32}. RHS

R'_{32}. RHS :=  $\underset{C_2}{=}$  $\underset{R_{32}}{=}$  $\underset{C_8}{=}$ 

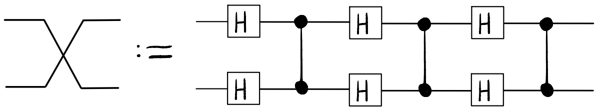
$\underset{C_2}{=}$  =: R'_{32}. LHS

Def 2 :

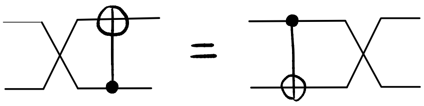




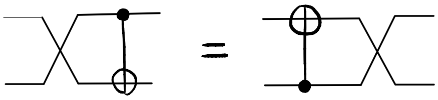
Def 3 :



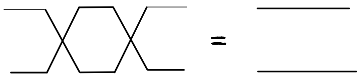
R_{31} : (1)



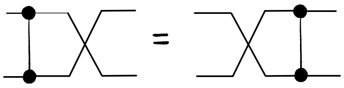
(2)



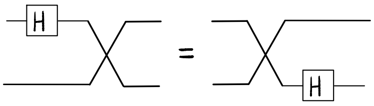
R_{16} :



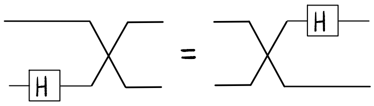
R_{17} :



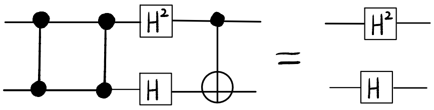
R_{19} : (1)



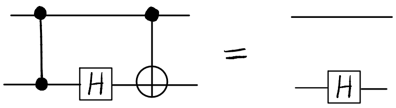
(2)



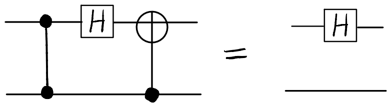
Lem N R_{32} :



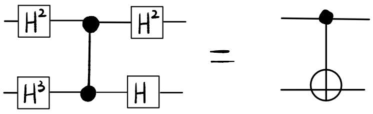
R^1_{32} :



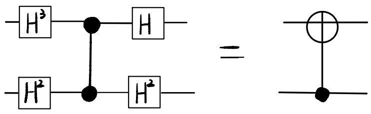
R^2_{32} :



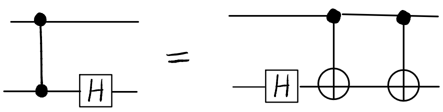
R^3_{32} :



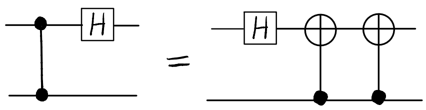
R^4_{32} :



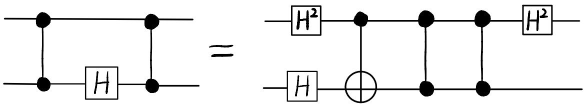
R^5_{32} :



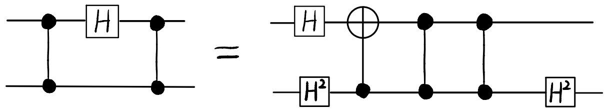
R^6_{32} :



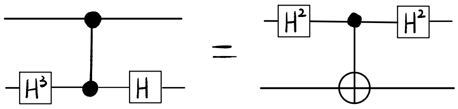
R^7_{32} :



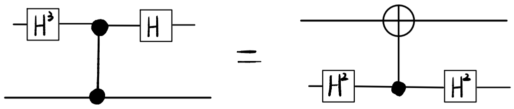
R^8_{32} :



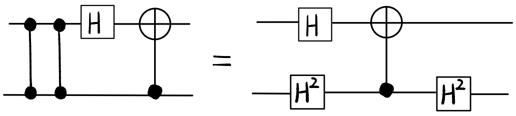
R^9_{32} :



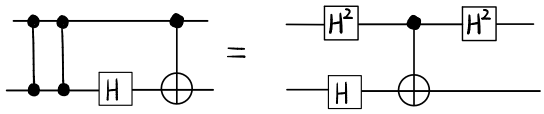
R^{10}_{32} :



R^{11}_{32} :

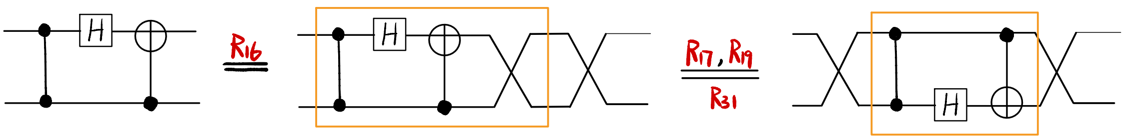


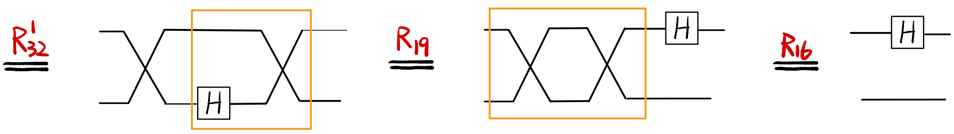
R^{12}_{32} :



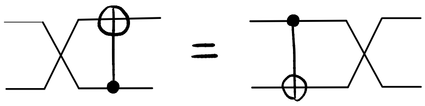
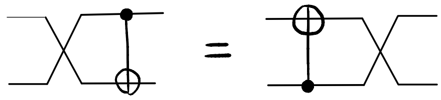
Proof cont.

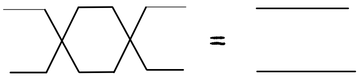
R^2_{32} . LHS :=

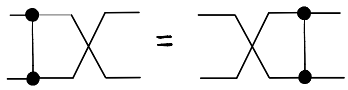




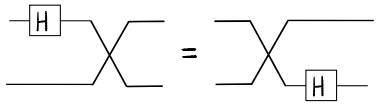
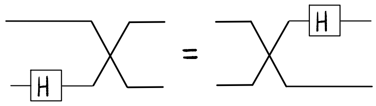
=: R^2_{32} . RHS

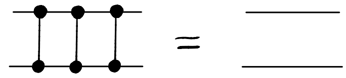
R_{31} : (1)  (2) 

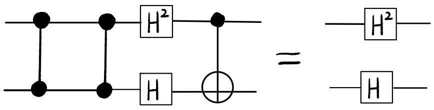
R_{16} : 

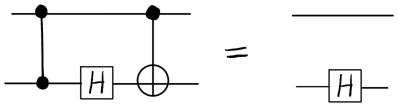
R_{17} : 

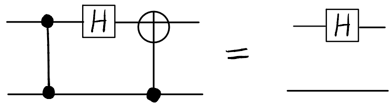
$C2 : H^4 = I$

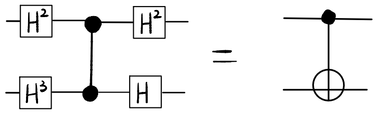
R_{19} : (1)  (2) 

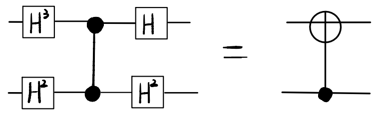
C_6 : 

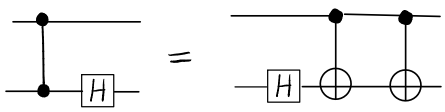
Lem N R_{32} :  ✓

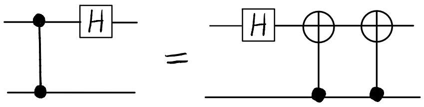
R_{32}^1 :  ✓

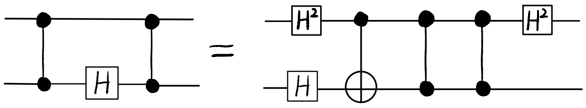
R_{32}^2 :  ✓

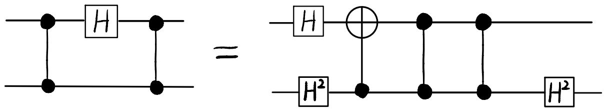
R_{32}^3 :  ✓

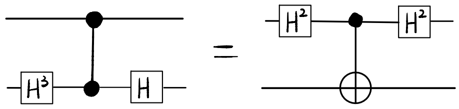
R_{32}^4 :  ✓

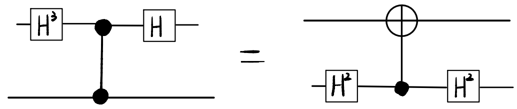
R_{32}^5 : 

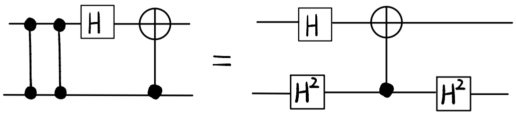
R_{32}^6 : 

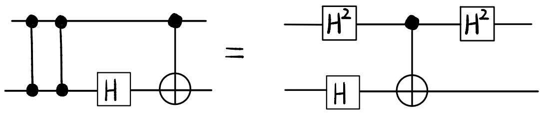
R_{32}^7 : 

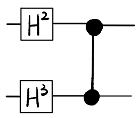
R_{32}^8 : 

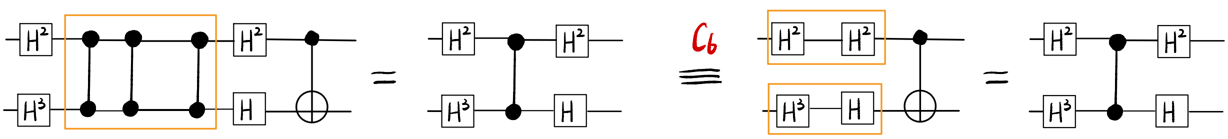
R_{32}^9 : 

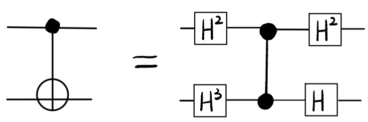
R_{32}^{10} : 

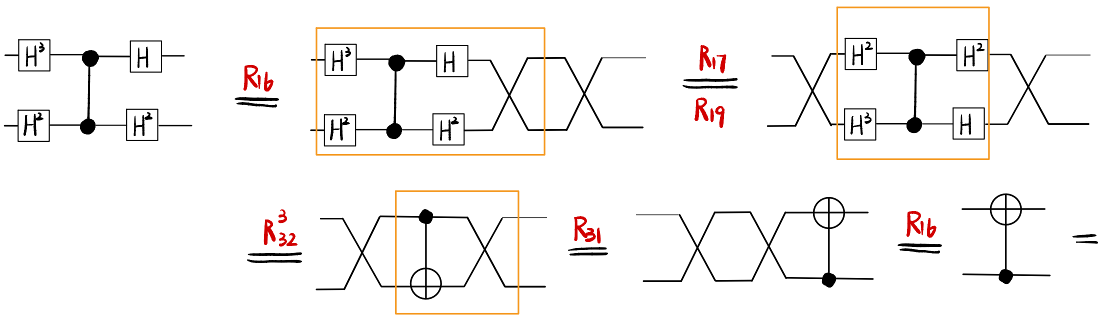
R_{32}^{11} : 

R_{32}^{12} : 

Proof cont. Left-appending both sides of R_{32} by  yields

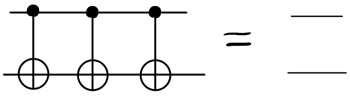


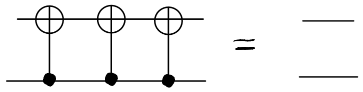
$\overset{C_2}{\equiv}$  : R_{32}^3

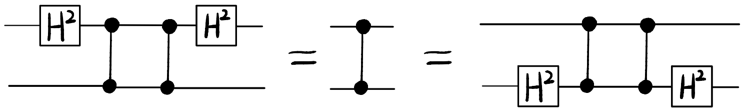
R_{32}^4 . LHS := 

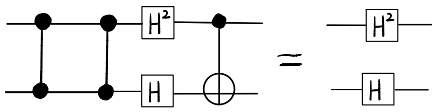
=: R_{32}^4 . RHS

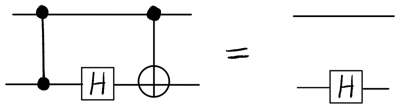
$C2: H^4 = I$

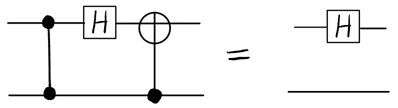
C_6^1: 

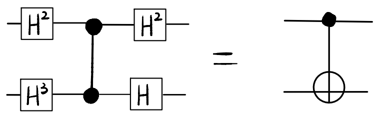
C_6^2: 

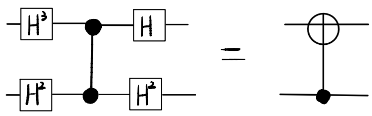
C_8^2: 

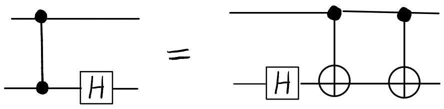
Lem N R_{32}:  ✓

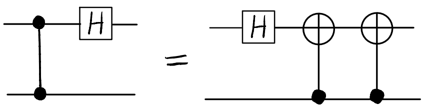
R_{32}^1:  ✓

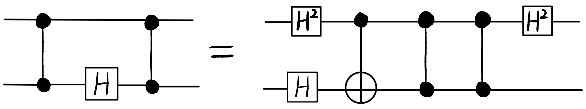
R_{32}^2:  ✓

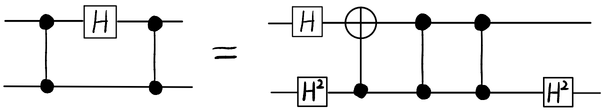
R_{32}^3:  ✓

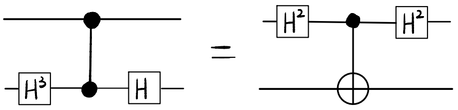
R_{32}^4:  ✓

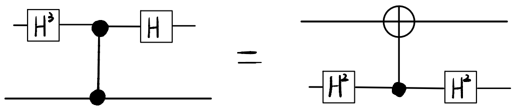
R_{32}^5:  ✓

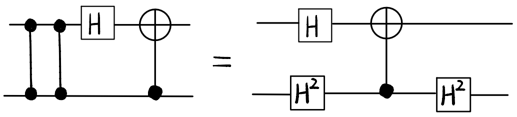
R_{32}^6:  ✓

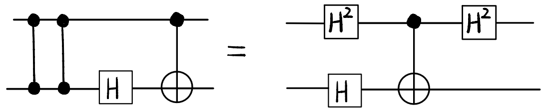
R_{32}^7:  ✓

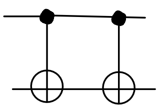
R_{32}^8: 

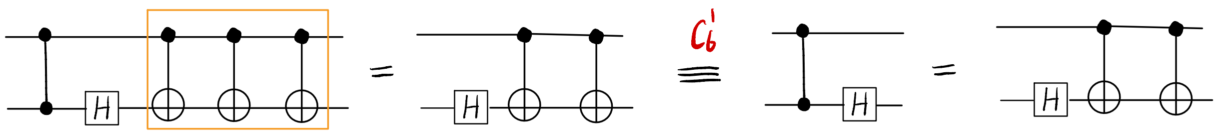
R_{32}^9: 

R_{32}^{10}: 

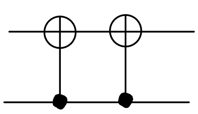
R_{32}^{11}: 

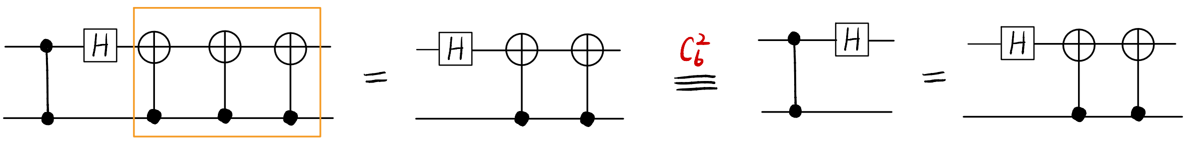
R_{32}^{12}: 

Proof cont. Right-appending both sides of R_{32}^1 by  yields

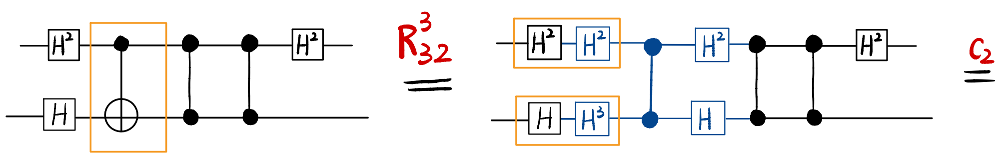


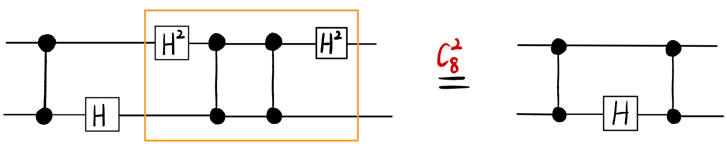
: R_{32}^5

Right-appending both sides of R_{32}^2 by  yields



: R_{32}^6

R_{32}^7.RHS := 



=: R_{32}^7.LHS