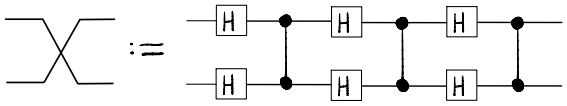
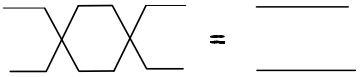
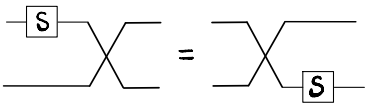
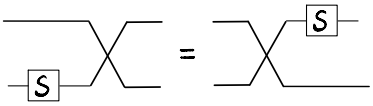
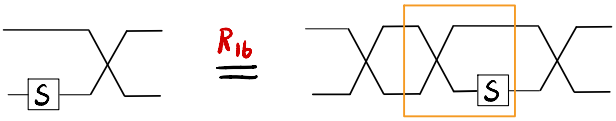
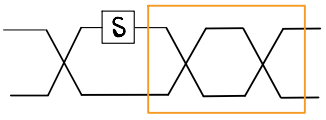
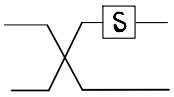
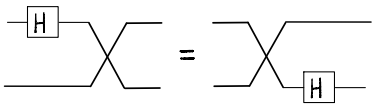
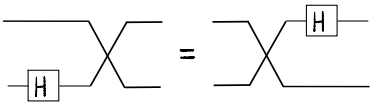
Def 3 :  R_{16} : 

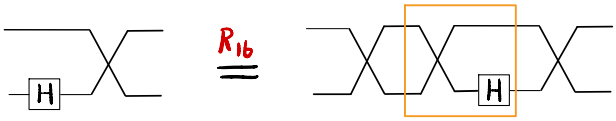
Lem A By Def 3 & R_{16}, R_{18} : (1)  implies R_{18} : (2) 

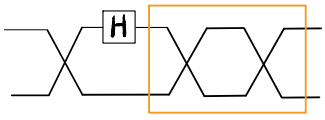
Proof: R_{18} : (2) . LHS := 

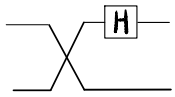
R_{18} : (1) 

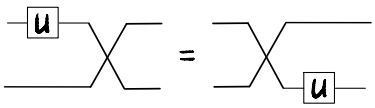
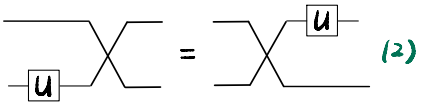
R_{16}  =: R_{18} : (2) . RHS ☒

Lem B By Def 3 & R_{16}, R_{19} : (1)  implies R_{19} : (2) 

Proof: R_{19} : (2) . LHS := 

R_{19} : (1) 

R_{16}  =: R_{19} : (2) . RHS ☒

Prop 1 Let $\mathcal{C}_1 := \langle H, S, -w \rangle$. $\forall U \in \mathcal{C}_1$  (1) and  (2)

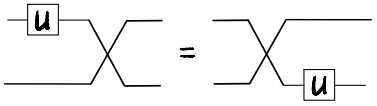
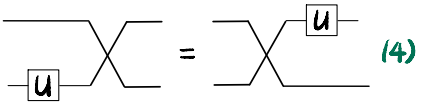
Proof: $\forall U \in \mathcal{C}_1$, $\exists\, t \in \mathbb{Z}_4$ and $m \in \mathbb{N}$ s.t. $U = (-w)^t H^{a_0} S^{b_0} H^{a_1} S^{b_1} \cdots H^{a_m} S^{b_m}$, composition in diagrammatic order, $a_i, b_i \in \mathbb{Z}_2$, $0 \le i \le m$. We proceed by induction on m.

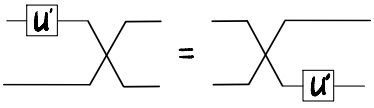
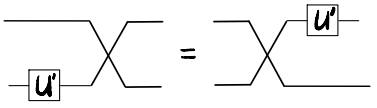
Base Case: ① $m=0$, $a_0 = b_0 = 0$. $U = (-w)^t$ is a scalar. (1) & (2) hold trivially.

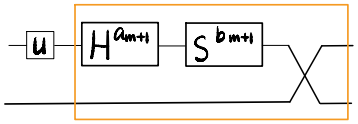
② $m=0$, $a_0 = 1$ and $b_0 = 0$. $U = (-w)^t H$. By Lem A, (1) & (2) hold.

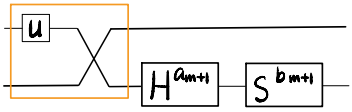
③ $m=0$, $a_0 = 0$ and $b_0 = 1$. $U = (-w)^t S$. By Lem B, (1) & (2) hold.

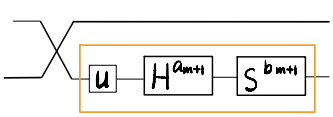
Induction Hypothesis: (1) & (2) hold for $m \ge 0$. That is, when $U = (-w)^t H^{a_0} S^{b_0} H^{a_1} S^{b_1} \cdots H^{a_m} S^{b_m}$

 (3) and  (4)

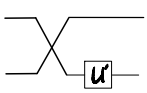
Induction Step: When $U' = U H^{a_{m+1}} S^{b_{m+1}}$, $a_{m+1}, b_{m+1} \in \mathbb{Z}_2$ WTS  (5) &  (6).

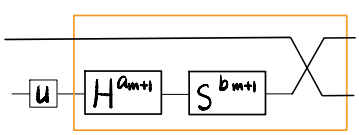
(5). LHS := 

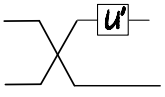
Lem A / Lem B 

IH 

def

 =: (5). RHS

(6). LHS := 

Reasoning analogously as before  =: (6). RHS

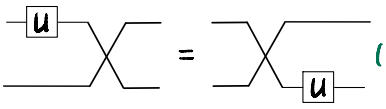
This completes the proof. ☒

Def 1 : $S' := HHSHH$

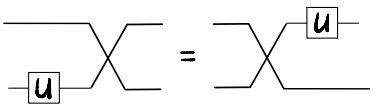
R5 : $X = HSHHSSH$

R10 : $Z = HHSSHHS = S'S'S$

Prop 1 Let $\mathcal{C}_1 := \langle H, S, -w \rangle$. $\forall U \in \mathcal{C}_1$



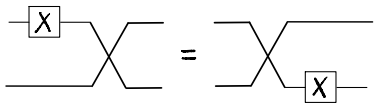
(1) and



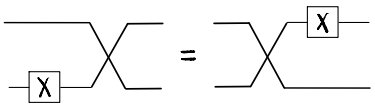
(2)

Cor 1

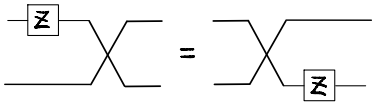
R_{20}: (1)



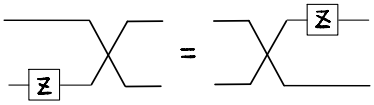
(2)



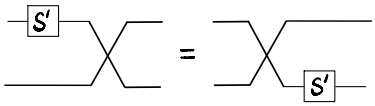
R_{21}: (1)



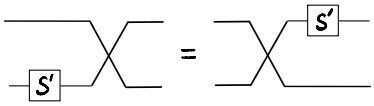
(2)



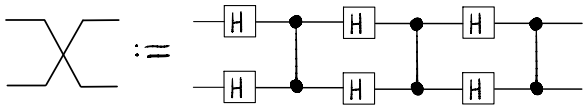
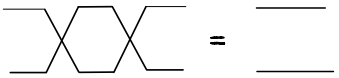
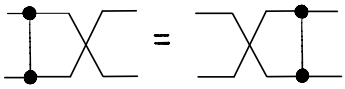
R_{22}: (1)

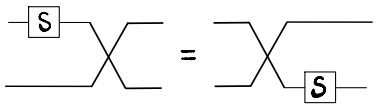
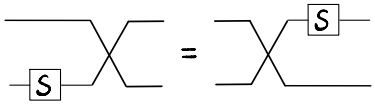


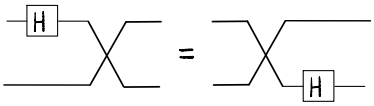
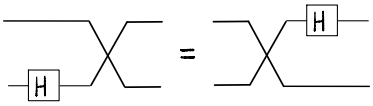
(2)

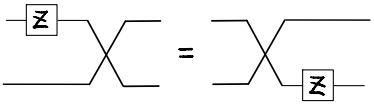
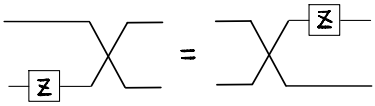


Proof : By Def 1, R_5, R_{10} & Prop 1. ☑

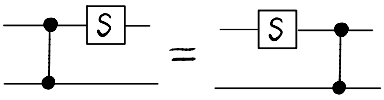
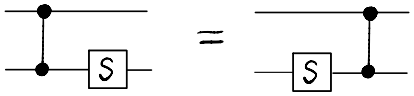
Def 3 :  R_{16} :  R_{17} : 

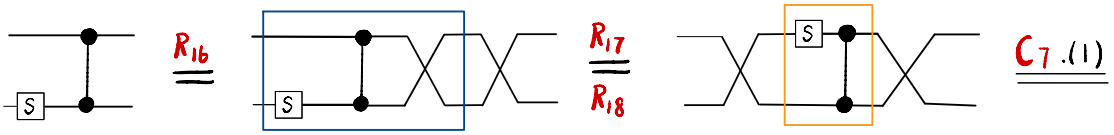
R_{18} : (1)  (2) 

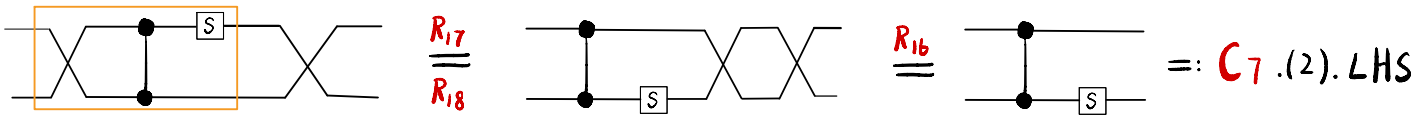
R_{19} : (1)  (2) 

R_{21} : (1)  (2) 

Lem C By Def 3, R_{16}, R_{17} & R_{18},

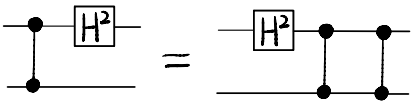
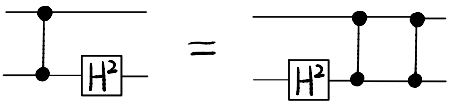
C_7 : (1)  implies (2) 

Proof: C_7 .(2). RHS := 

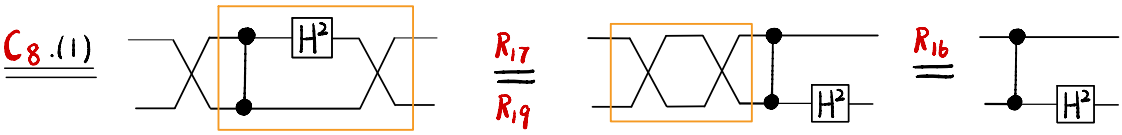


=: C_7 .(2). LHS ▨

Lem D By Def 3, R_{16}, R_{17} & R_{19},

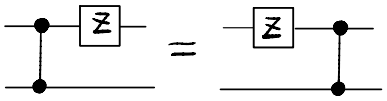
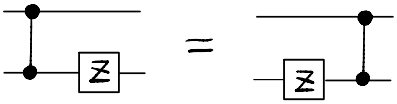
C_8 : (1)  implies (2) 

Proof: C_8 .(2). RHS := 

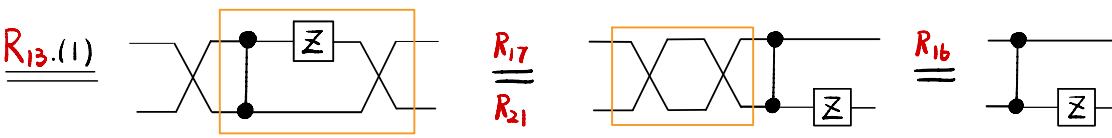


=: C_8 .(2). LHS ▨

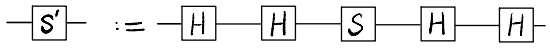
Lem E By Def 3, R_{16}, R_{17} & R_{21},

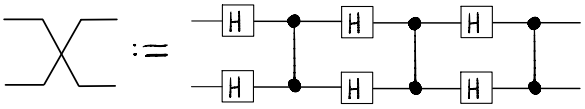
R_{13} : (1)  implies (2) 

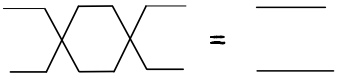
Proof: R_{13} .(2). RHS := 

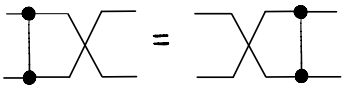


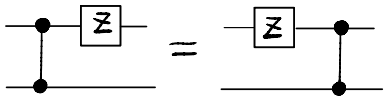
=: R_{13} .(2). LHS ▨

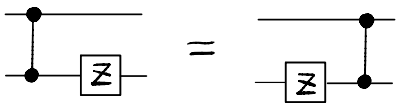
Def 1 : 

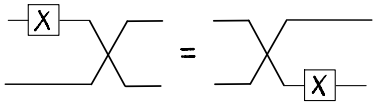
Def 3 : 

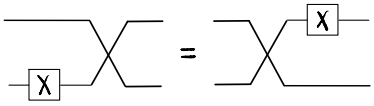
R_{16} : 

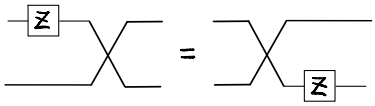
R_{17} : 

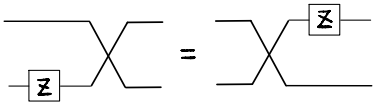
R_{13} : (1) 

(2) 

R_{20} : (1) 

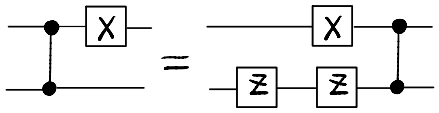
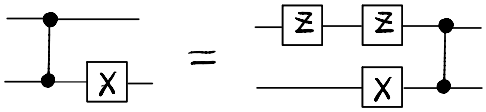
(2) 

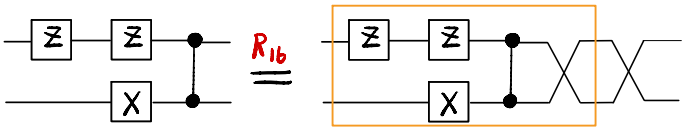
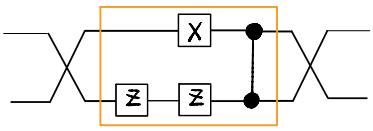
R_{21} : (1) 

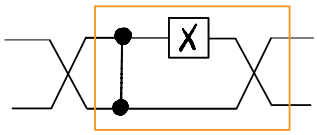
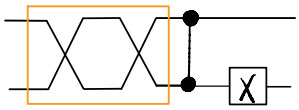
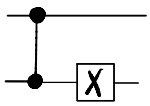
(2) 

R_{12} : $Z^3 = I$

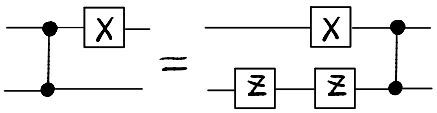
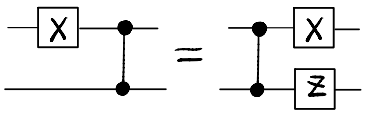
Lem F By Def 3, R_{16}, R_{17}, R_{20} & R_{21},

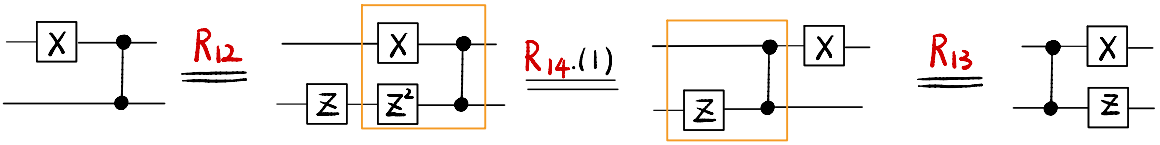
R_{14}: (1)  implies (2) 

Proof: R_{14} .(2). RHS :=  $\overset{R_{16}}{=}$ $\overset{R_{17},R_{20}}{\underset{R_{21}}{=}}$ 

R_{14}.(1)  $\overset{R_{17}}{\underset{R_{20}}{=}}$  $\overset{R_{16}}{=}$  =: R_{14} .(2). LHS ▨

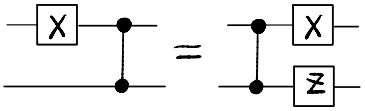
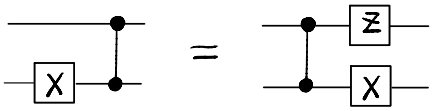
Lem G By R_{12} & R_{13},

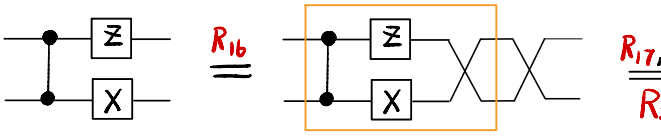
R_{14}: (1)  implies (3) 

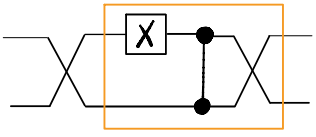
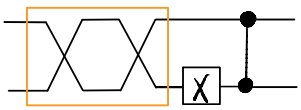
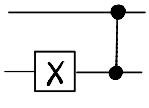
Proof: R_{14} .(3). LHS := 

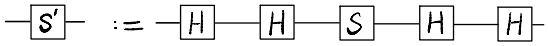
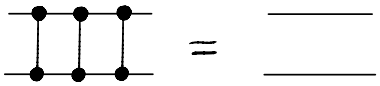
=: R_{14} .(3). RHS. ▨

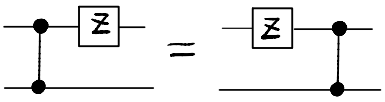
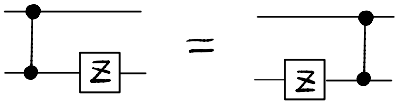
Lem H By Def 3, R_{16}, R_{17}, R_{20} & R_{21},

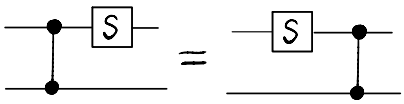
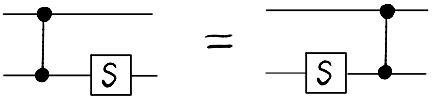
R_{14}: (3)  implies (4) 

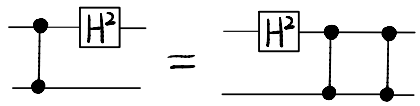
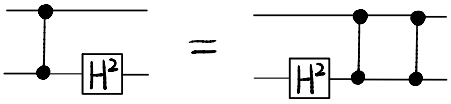
Proof: R_{14} .(4). RHS := 

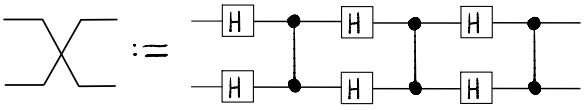
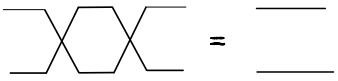
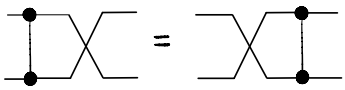
R_{14}.(3)  $\overset{R_{17}}{\underset{R_{20}}{=}}$  $\overset{R_{16}}{=}$  =: R_{14} .(4). LHS ▨

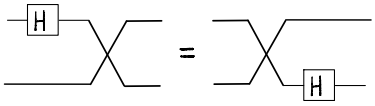
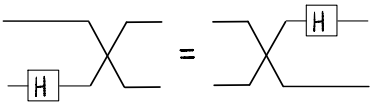
Def 1 :  C6 : 

R13 : (1)  (2) 

C7 : (1)  (2) 

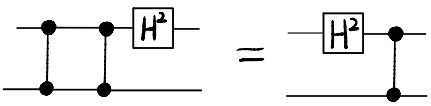
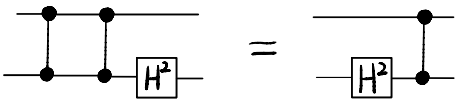
C8 : (1)  (2) 

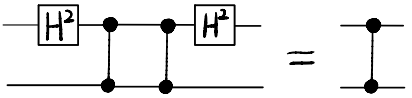
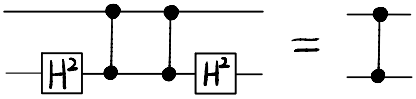
Def 3 :  R16 :  R17 : 

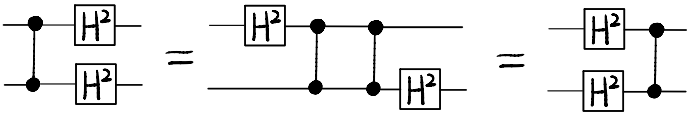
R19 : (1)  (2) 

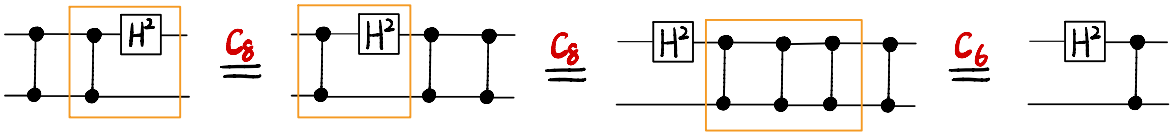
C2 : $H^4 = I$

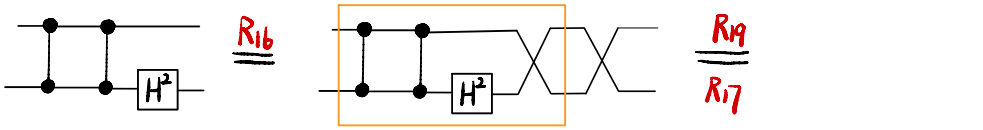
Lem K By Def3, R16, R17, R19, C6, C2 & C8,

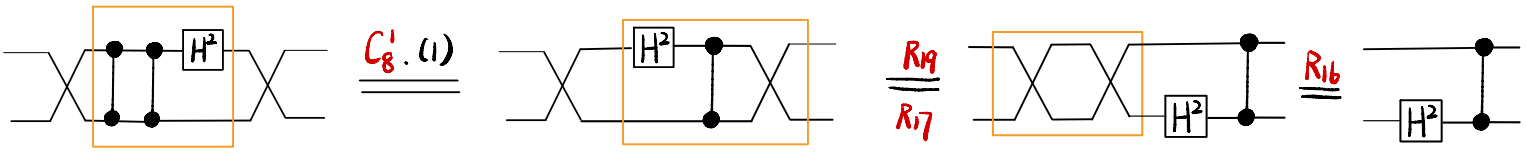
C_8^1 : (1)  (2) 

C_8^2 :  C_8^4 : 

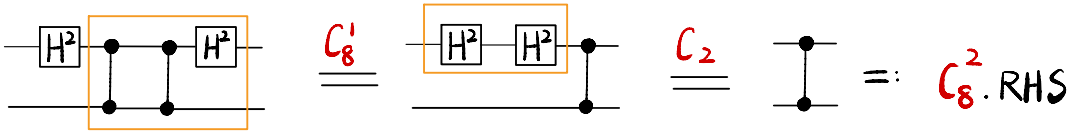
C_8^3 : 

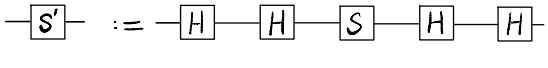
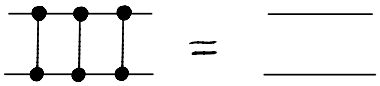
Proof : C_8^1 . (1) . LHS := 

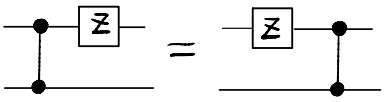
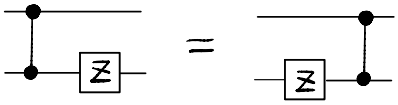
=: C_8^1 . (1) . RHS . C_8^1 . (2) . LHS := 

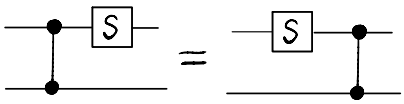
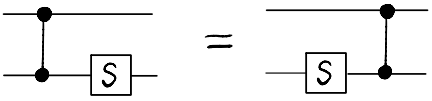


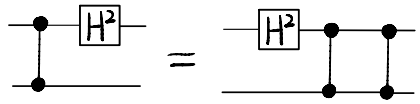
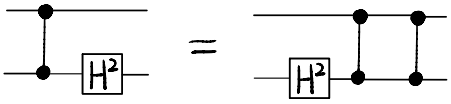
=: C_8^1 . (2) . RHS .

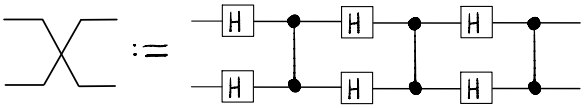
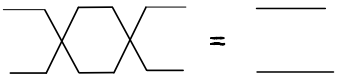
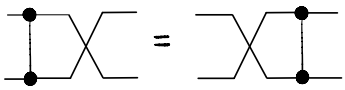
C_8^2 . LHS := 

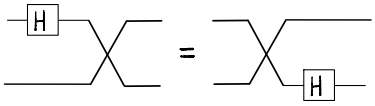
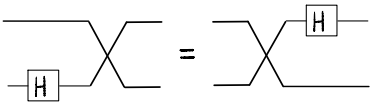
Def 1 :  C_6 : 

R_{13} : (1)  (2) 

C_7 : (1)  (2) 

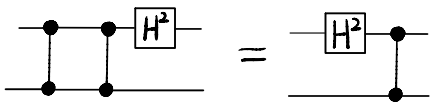
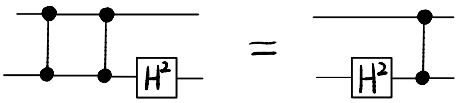
C_8 : (1)  (2) 

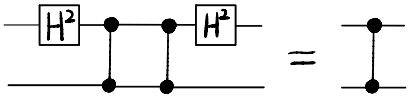
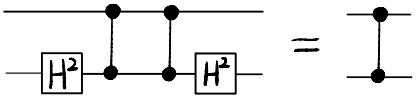
Def 3 :  R_{16} :  R_{17} : 

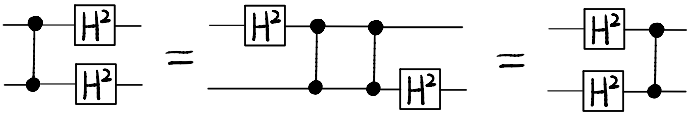
R_{19} : (1)  (2) 

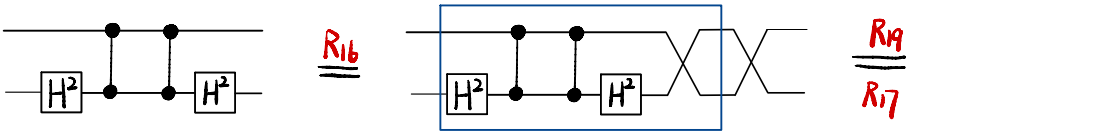
C_2 : $H^4 = I$

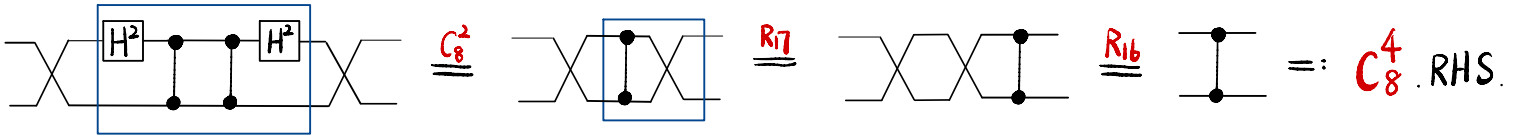
Lem K By Def 3, R_{16}, R_{17}, R_{19}, C_6, C_2 & C_8,

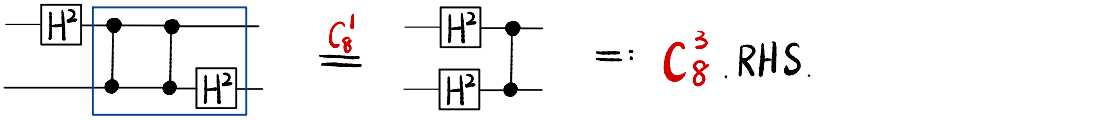
C_8^1 : (1)  (2) 

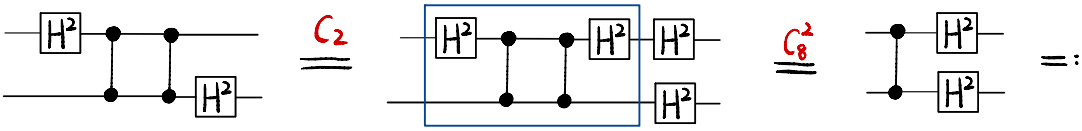
C_8^2 :  C_8^4 : 

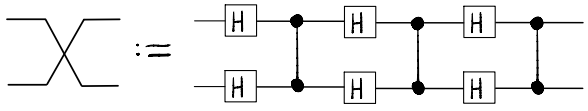
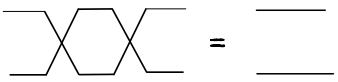
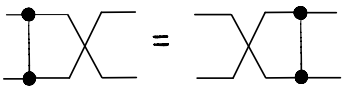
C_8^3 : 

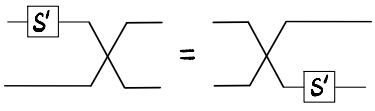
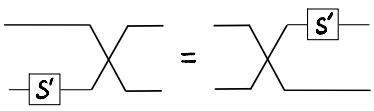
Proof cont : C_8^4 . LHS := 

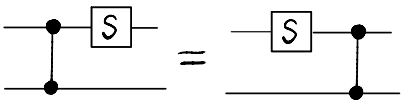
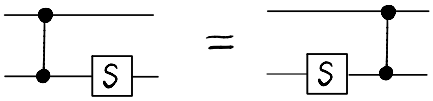


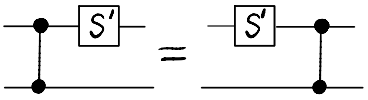
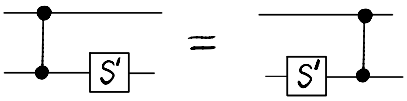
C_8^3 . MID := 

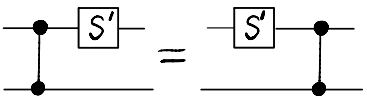
C_8^3 . MID := 

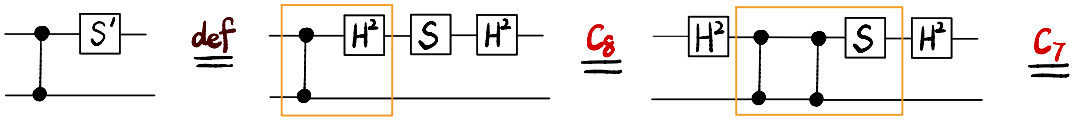
Def 3 :  R_{16} :  R_{17} : 

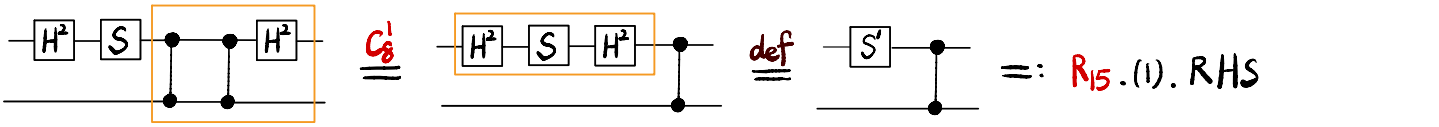
R_{22} : (1)  (2) 

C_7 : (1)  (2) 

R_{15} : (1)  (2) 

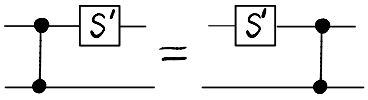
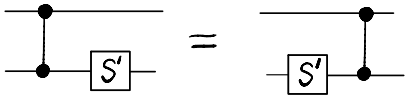
Lem I By C_7 & C_8, R_{15} : (1) 

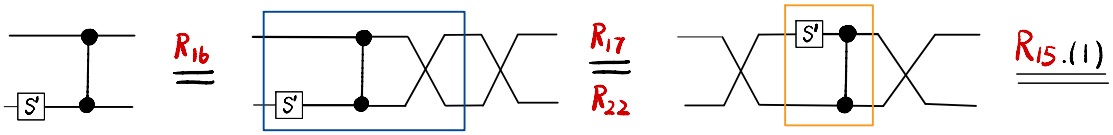
Proof : R_{15} . (1) . LHS := 



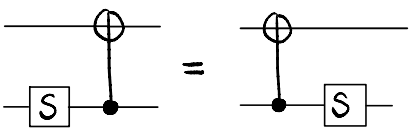
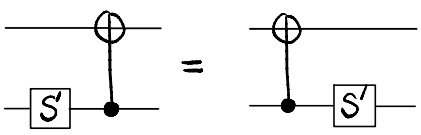
=: R_{15} . (1) . RHS

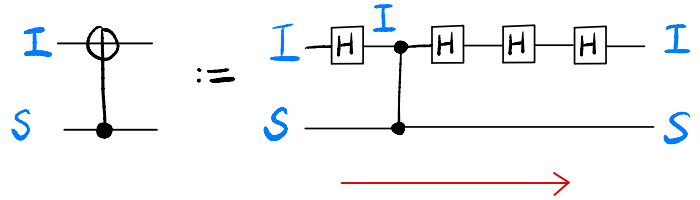
Lem J By Def 3, R_{16}, R_{17}, R_{22},

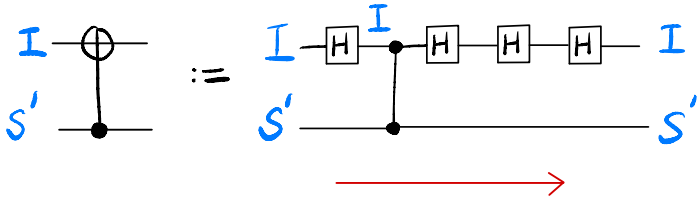
R_{15} : (1)  implies (2) 

Proof : R_{15} . (2) . RHS := 

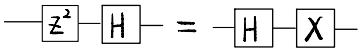
=: R_{15} . (2) . LHS ▨

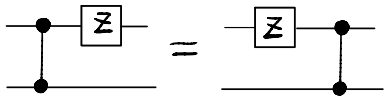
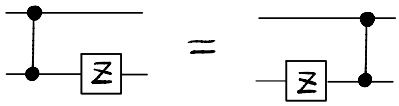
Lem L By C_7 & R_{15}, R_{24} :  & $R_{24}^{!}$: 

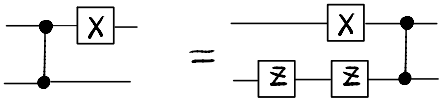
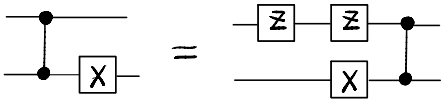
Proof : 

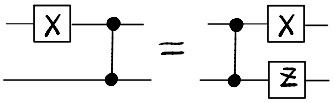
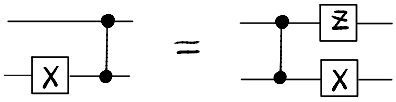


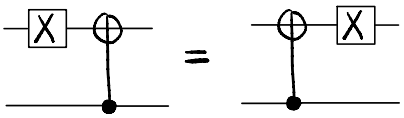
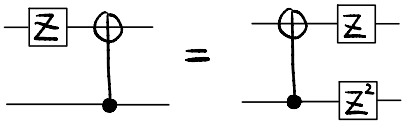
▨

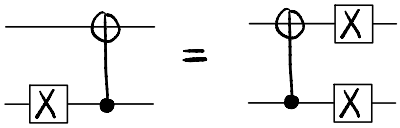
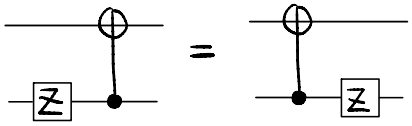
R4 : $HZ^2H^\dagger = X$ 

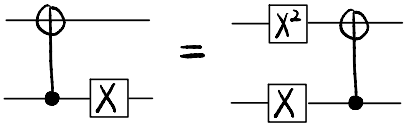
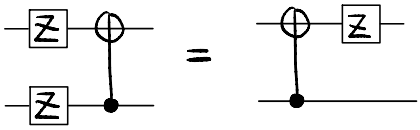
R13 : (1)  (2) 

R14 : (1)  (2) 

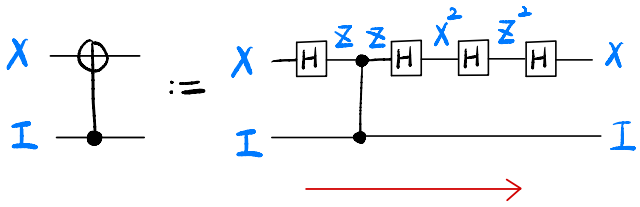
(3)  (4) 

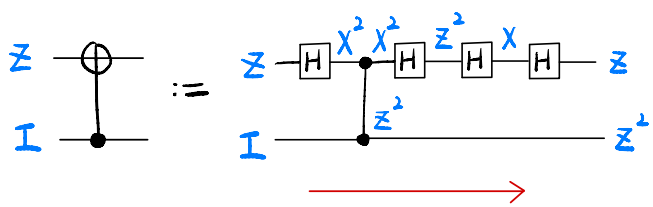
Lem M R26 : (1)  (2) 

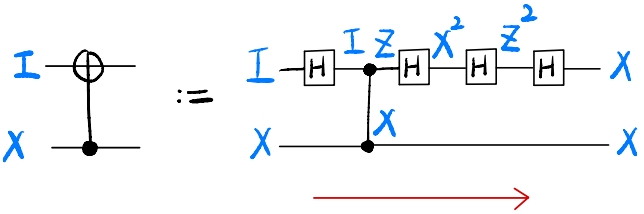
(3)  (4) 

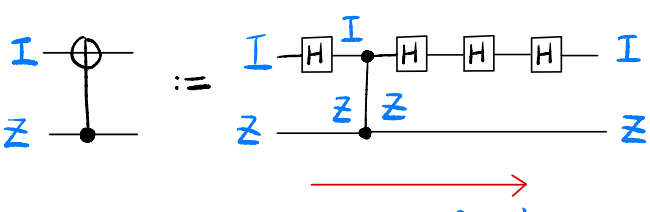
(5)  (6) 

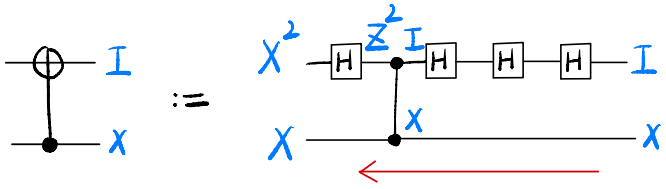
Proof : By R4 , R13 & R14 ,

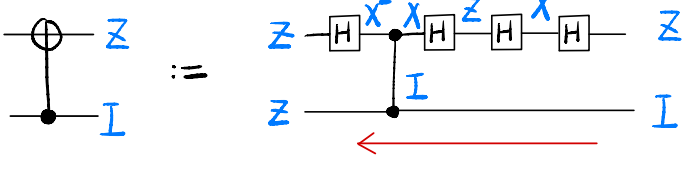












∎