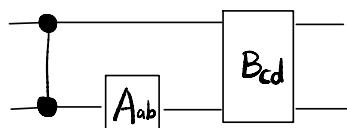
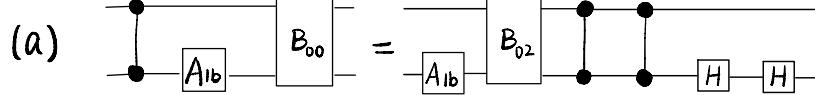


For 4.(3) - 4.(8) : $a \neq 0, b \in \mathbb{Z}_3$



Type

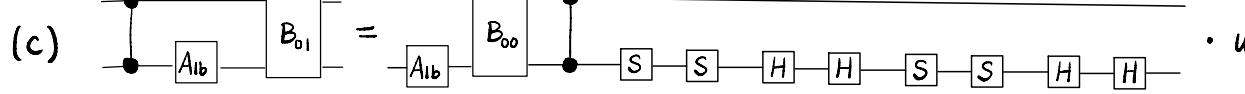
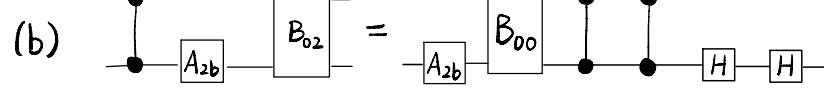
Count



✓

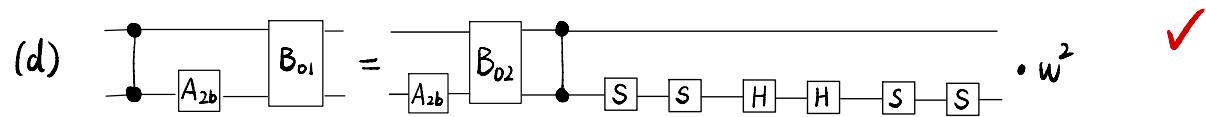
$b \in \mathbb{Z}_3$

$3 \times 2 = 6$



w^2

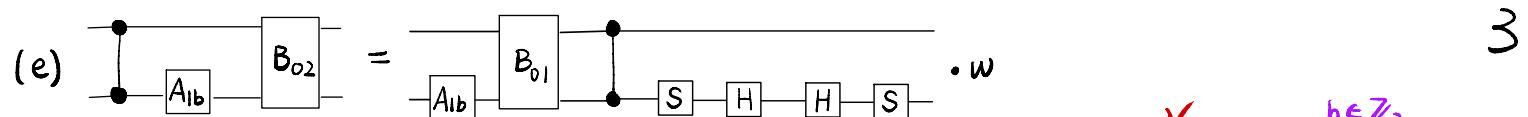
3



✓

$b \in \mathbb{Z}_3$

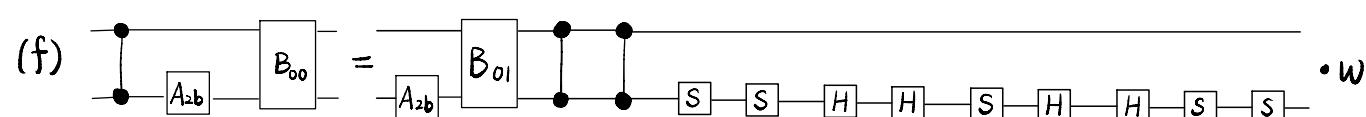
3



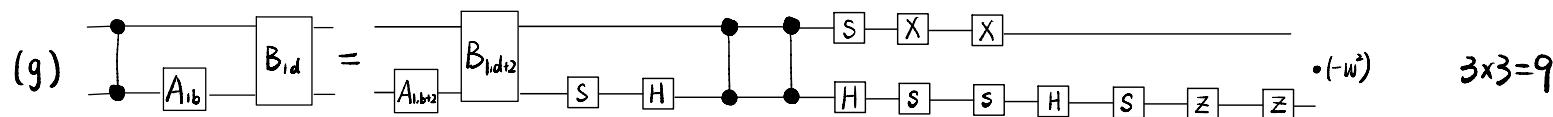
✓

$b \in \mathbb{Z}_3$

3



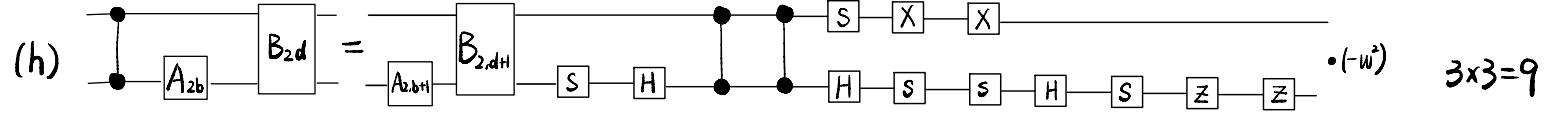
3



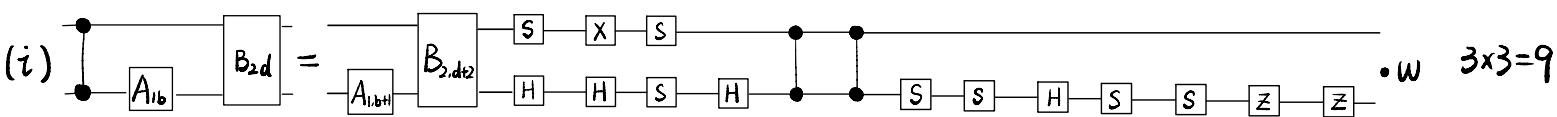
✓

$b, d \in \mathbb{Z}_3$

$3 \times 3 = 9$



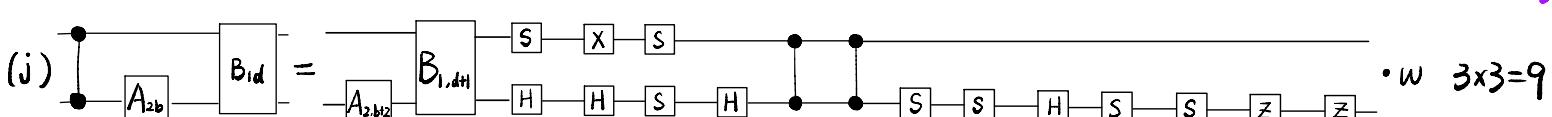
$3 \times 3 = 9$



✓

$b, d \in \mathbb{Z}_3$

$3 \times 3 = 9$



✓

$b, d \in \mathbb{Z}_3$

$3 \times 3 = 9$

Total

54

$$A_{1b} = S^b H$$

$$B_{00} = \text{X}$$

$$B_{02} = H H \text{X} \oplus$$

Def 3: $\text{X} := H \cdot H \cdot H$

R₁₇: $\text{X} = \text{X}$

R₁₉: (1) $H \text{X} = \text{X} H$

(2) $H \text{X} = \text{X} H$

R₃₁: (1) $\text{X} \oplus = \text{X} \oplus$

(2) $\text{X} \oplus = \oplus \text{X}$

C₇: (1) $S = S$

(2) $S = S$

R₃₂⁷: $H \text{X} = H \text{X}$

Lem 46 By Def 3, C₇, R₁₇, R₁₉, R₃₁ & R₃₂,

4. (a) $A_{1b} B_{00} = A_{1b} B_{02} H H$

Proof: 4.(a).LHS := $A_{1b} B_{00}$ def $\boxed{S^b H \text{X}}$

C₇
R₁₇ $\boxed{S^b H \text{X}}$

R₃₂⁷ $\boxed{H H \text{X} \oplus}$

R₁₇, R₁₉
R₃₁ $\boxed{S^b H \text{X}}$ $\boxed{H H \text{X} \oplus}$
A_{1b} B₀₂

def $A_{1b} B_{02} H H =: 4.(a).RHS$

$$A_{2b} = H^2 S^{2b} H$$

$$B_{00} = \text{X}$$

$$B_{02} = H H \text{X} \oplus$$

Def 3: $\text{X} := H H H H$ $C_6 := \text{X} \text{X} = \text{X}$

$C_8 : (1) H^2 = H^2$ $(2) H^2 = H^2$

$R_{19} : (1) H \text{X} = \text{X} H$ $(2) H \text{X} = \text{X} H$

$C_7 : (1) S = S$ $(2) S = S$

$R_{32} : \text{H}^2 \text{X} \oplus = \text{H}^2$ $R_{31} : (1) \text{X} \oplus = \text{X} \oplus$

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

4.(b) $A_{2b} B_{02} = A_{2b} B_{00} H H$

Proof: 4.(b).LHS := $A_{2b} B_{02}$ def $\boxed{H^2 S^{2b} H} \text{X} \oplus$

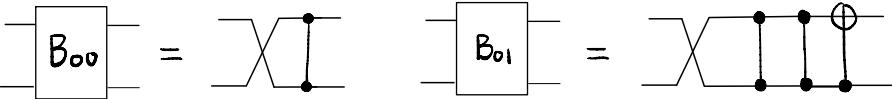
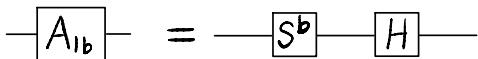
$\stackrel{C_8}{=} \boxed{H^2 S^{2b} H} \text{X} \oplus$

$\stackrel{C_7}{=} \boxed{H^2 S^{2b} H} \text{X} \oplus \stackrel{R_{32}}{=} \boxed{H^2 S^{2b} H} \text{X}$

$\stackrel{R_{19}}{=} \boxed{H^2 S^{2b} H} H^2$

$\stackrel{C_6}{=} \boxed{H^2 S^{2b} H} \text{X} \oplus \boxed{H^2 S^{2b} H} H H$

def $A_{2b} B_{00} H H =: 4.(b).\text{RHS}$



Def: $S' = HSHH$ $S'^2 = (HSHH)(H^2SH^2) = H^2S^2H^2$

Def 3: $\text{X} := HHHH$ $R_{31}: (1) \quad \text{X} \oplus \text{I} = \text{X}$

$C_7: (2)$ $R_{15}: (2)$ $C_5: SS' = S'S$

$R_{25}^1:$ $R_{32}^1:$

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

4. (c) $A_{1b} B_{01} = A_{1b} B_{00} SSSHHHHSSSSHHHH \cdot w^2$

Proof: 4. (c). LHS := $A_{1b} B_{01}$ def $\text{S}^b \text{H} \text{X} \oplus \text{I} S' S S$

$\underline{\underline{C_7}}$ $\underline{\underline{R_{25}}}$ $\text{S}^b \text{H} \text{X} \oplus \text{I} S' S S \cdot w$

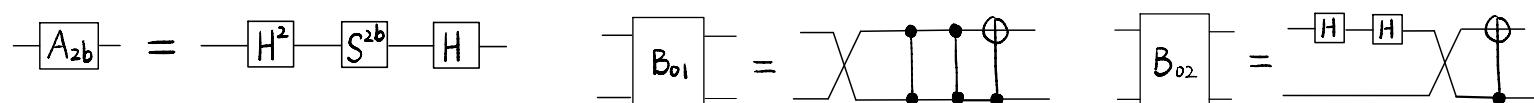
$\underline{\underline{R_{25}}} \quad \text{S}^b \text{H} \text{X} \oplus \text{I} S' S S \cdot w^2$

$\underline{\underline{C_5, C_7}}$ $\underline{\underline{R_{15}, R_{31}}}$ $\text{S}^b \text{H} \text{X} \oplus \text{I} S' S S' S' S' \cdot w^2$

$\underline{\underline{R_{32}^1}}$ $\text{A}_{1b} \text{S}^b \text{H} \text{X} \oplus \text{I} S' S' \cdot w^2$

def $\text{A}_{1b} B_{00} SSSHHHHSSSSHHHH \cdot w^2$

def $\text{A}_{1b} B_{00} SSSHHHHSSSSHHHH \cdot w^2 =: 4.(\text{c}).\text{RHS}$



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

Def 3: $\text{CNOT}_1 := H H H H$ $R_{17}: \text{CNOT}_1 \text{CNOT}_2 = \text{CNOT}_2 \text{CNOT}_1$

$R_{25}^1: \text{CNOT}_1 \text{S}' \text{S}' = \text{S}' \text{S}' \text{CNOT}_1 \cdot w$ $C_7: (1) \text{S} = \text{S}' \text{S}$

$C_8: (1) \text{H}^2 = \text{H}^2 \text{H}^2$ $(2) \text{H}^2 = \text{H}^2 \text{H}^2$ $C_5: SS' = S'S$

$R_{19}: (1) \text{H} \text{CNOT}_1 = \text{CNOT}_1 \text{H}$ $(2) \text{H} \text{CNOT}_1 = \text{CNOT}_1 \text{H}$

$R_{15}: (2) \text{S}' = \text{S}' \text{S}$ $R_{32}^6: \text{H} \text{S}' \text{H} \oplus = \text{H} \oplus \text{H}^2$

Lem 4.9 By Def 3, C₂, C₅, C₇, C₈, R₁₅, R₁₇, R₁₉, R₂₅ & R₃₂.

4. (d) $A_{2b} B_{01} = A_{2b} B_{02} \text{S} \text{S} \text{H} \text{H} \text{S} \text{S} \cdot w^2$

Proof: 4. (d). LHS := $A_{2b} B_{01}$ def $= \boxed{H^2 S^{2b} H} \text{CNOT}_1 \text{CNOT}_2 \text{CNOT}_3 \oplus$

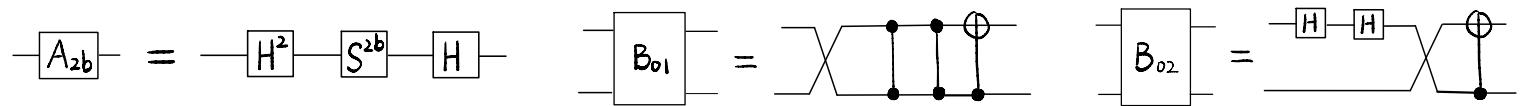
C₇ $\text{H}^2 S^{2b} H \text{CNOT}_1 \text{CNOT}_2 \text{CNOT}_3 \oplus$

R₁₇ $\text{H}^2 S^{2b} \text{CNOT}_1 \text{CNOT}_2 \text{CNOT}_3 \oplus$

R₂₅ $\text{H}^2 S^{2b} \text{CNOT}_1 \text{CNOT}_2 \text{CNOT}_3 \oplus \text{S}' \text{S} \cdot w$

R₂₅ $\text{H}^2 S^{2b} \text{CNOT}_1 \text{CNOT}_2 \text{CNOT}_3 \oplus \text{S}' \text{S} \text{S}' \text{S} \cdot w^2$

R₁₅ $\text{H}^2 S^{2b} \text{CNOT}_1 \text{CNOT}_2 \text{CNOT}_3 \oplus \text{S}'^2 \text{S}^2 \cdot w^2$



Def: $S' = H H S H H$ $S' S' = H H S S H H$ $C_2: H^4 = I$
 $S' = H^2 S H^2$ $S'^2 = (H^2 S H^2)(H^2 S H^2) = H^2 S^2 H^2$

$C_8: (1)$ =

(2) =

$R_{19}: (1)$ =

(2) =

$R_{32}^6:$ =

Proof cont. • w^2

$\underline{\underline{R_{32}^6}}$ • w^2

$\underline{\underline{R_{19}}}$ • w^2

$\underline{\underline{C_8}}$ • w^2

def • w^2

def A_{2b} • $w^2 =: 4(d). \text{RHS}$

□



$$\text{Def 3 : } \text{X} := \begin{array}{c} \text{H} \\ \text{H} \end{array} \quad \begin{array}{c} \text{H} \\ \text{H} \end{array} \quad \begin{array}{c} \text{H} \\ \text{H} \end{array}$$

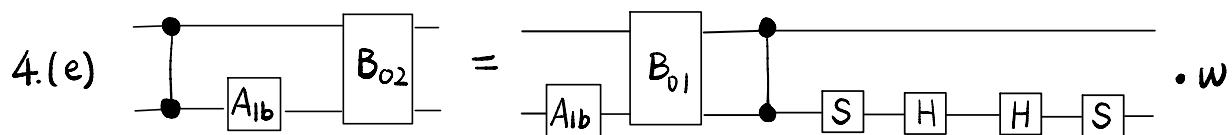
$$C_7: (2) \quad \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \quad = \quad \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

$$R_{19} : (1) \quad \begin{array}{c} \text{H} \\ \boxed{\text{H}} \end{array} \quad = \quad \begin{array}{c} \text{H} \\ \boxed{\text{H}} \end{array}$$

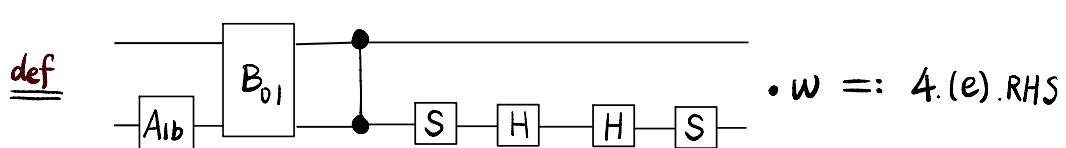
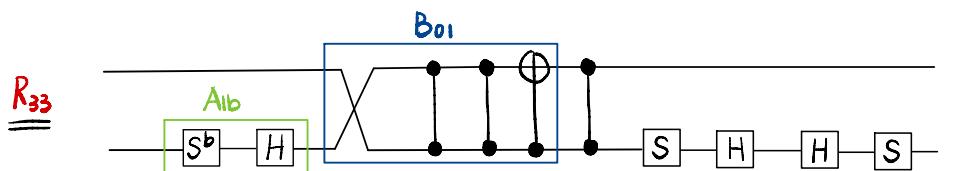
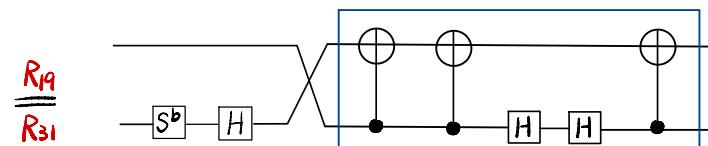
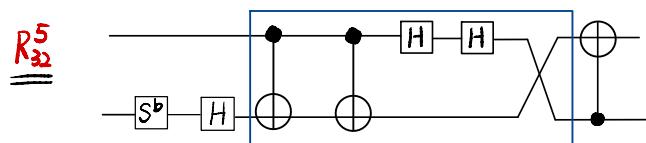
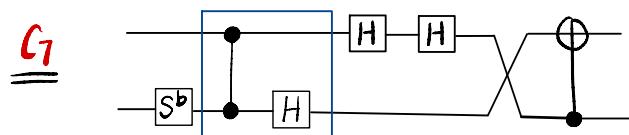
$$\textcolor{red}{R_{3|}} : (1) \quad \text{Diagram} = (2) \quad \text{Diagram} = \text{Diagram}$$

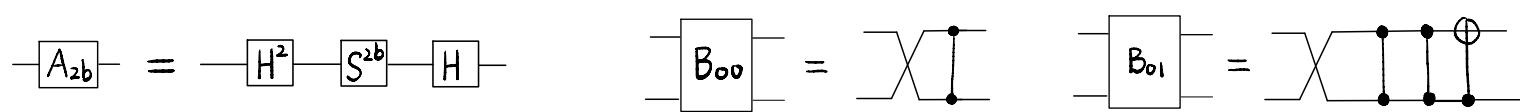
$$R_{33} : \quad \begin{array}{c} \text{Diagram of } R_{33} \text{ showing three vertical lines with circles at top and dots at bottom, connected by horizontal lines.} \\ = \end{array} \quad \begin{array}{c} \text{Diagram of } R_{33} \text{ transformed into a } 3 \times 3 \text{ grid with specific symbols (circle, dot, S, H) placed on some intersections.} \\ \cdot w \end{array}$$

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



Proof: 4.(e). LHS :=  def 





Def: $s' = H \otimes H \otimes S \otimes H \otimes H$ $C_5: ss' = s's$ $C_3: S^3 = I$
 $s' := H^2 S H^2$

Def 3: $\text{CNOT} := H \otimes H \otimes H \otimes H \otimes H$ $C_8: (2) \text{CNOT} = H^2$

$C_7: (2) S = S$ $R_{32}^5: H \otimes H = H \otimes \text{CNOT} \otimes \text{CNOT}$

$C_6': \text{CNOT} \otimes \text{CNOT} \otimes \text{CNOT} = \text{CNOT}$ $R_{31}: (1) \text{CNOT} \otimes \text{CNOT} = \text{CNOT} \otimes \text{CNOT}$

$C_6: \text{CNOT} \otimes \text{CNOT} \otimes \text{CNOT} = \text{CNOT}$

Lem 5.1 By Def 3, $C_3, C_5, C_6, C_7, C_8, R_{15}, R_{25}, R_{31}$ & R_{32} ,

4.(f) $A_{2b} \otimes B_{00} = A_{2b} \otimes B_{01} \otimes S \otimes S \otimes H \otimes H \otimes S \otimes H \otimes S \otimes S$ • w

Proof: 4.(f).LHS := $A_{2b} \otimes B_{00}$ def $\text{H}^2 \otimes S^{2b} \otimes H \otimes \text{CNOT}$

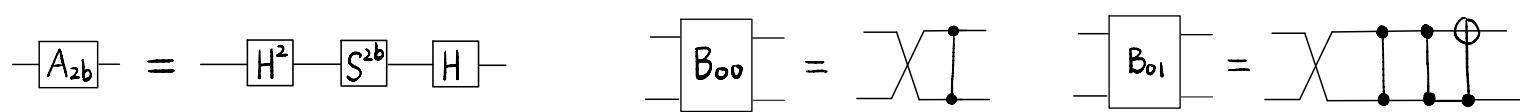
$\stackrel{C_8}{=} \text{H}^2 \otimes S^{2b} \otimes H \otimes \text{CNOT} \stackrel{C_7}{=} \text{H}^2 \otimes S^{2b} \otimes H \otimes \text{CNOT}$

$\stackrel{R_{32}^5}{=} \text{H}^2 \otimes S^{2b} \otimes H \otimes \text{CNOT}$

$\stackrel{R_{32}^5}{=} \text{H}^2 \otimes S^{2b} \otimes H \otimes \text{CNOT} \otimes \text{CNOT} \otimes \text{CNOT}$

$\stackrel{C_6'}{=} \text{H}^2 \otimes S^{2b} \otimes H \otimes \text{CNOT} \otimes \text{CNOT} \otimes \text{CNOT}$

$\stackrel{C_6}{=} \text{H}^2 \otimes S^{2b} \otimes H \otimes \text{CNOT} \otimes \text{CNOT} \otimes \text{CNOT}$



Def: $s' = H \otimes H \otimes S \otimes H \otimes H$ $C_5: ss' = s's$ $C_3: S^3 = I$
 $s' := H^2 S H^2$

Def 3: $\text{X} := H \otimes H \otimes H \otimes H \otimes H$

$C_7: (2)$ $\begin{array}{c} \bullet \\ \text{---} \\ \bullet \\ \text{---} \\ \bullet \end{array} \otimes S = \begin{array}{c} \bullet \\ \text{---} \\ \bullet \\ \text{---} \\ \bullet \end{array} \otimes S$ $R_{15}: (2)$ $\begin{array}{c} \bullet \\ \text{---} \\ \bullet \\ \text{---} \\ \bullet \end{array} \otimes S' = \begin{array}{c} \bullet \\ \text{---} \\ \bullet \\ \text{---} \\ \bullet \end{array} \otimes S'$

$R_{25}^1:$ $\begin{array}{c} \bullet \\ \text{---} \\ \bullet \\ \text{---} \\ \bullet \end{array} \otimes \oplus = \begin{array}{c} \oplus \\ \text{---} \\ \bullet \\ \text{---} \\ \bullet \end{array} \otimes S' \otimes S$ • w

4.(f) $A_{2b} \otimes B_{00} = A_{2b} \otimes B_{01} \otimes \dots \otimes S \otimes S \otimes H \otimes H \otimes S \otimes H \otimes H \otimes S \otimes S$ • w

Proof cont.

C_{25}^l

C_5, C_7
 $\underline{\underline{R_{15}}}$

def

C_3
 $\underline{\underline{C_5}}$

def
 $=: 4.(f).RHS$

□