

$$D_{0b} = \text{CNOT}_{b \in \mathbb{Z}_3} CZ^{2b}$$

Def 3: $\text{CNOT} :=$

$C_7: (1)$ (2)

$R_{18}: (1)$ (2)

Lem 11 By Def 3, C_7 & R_{18} , 19. (1)

(2)

(3)

Proof: 19. (1)/(2)/(3). LHS :=

R_{18}

C_7

$\stackrel{\text{def}}{=} D_{0b} = 19. (1)/(2)/(3). \text{ RHS. } \square$

$$\begin{array}{c} \text{---} \boxed{D_{ab}} \text{---} \\ a \neq 0 \end{array} = \begin{array}{c} \text{---} \boxed{A_{ab}} \text{---} \end{array} \begin{array}{c} \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \bullet \quad \bullet \\ \bullet \quad \bullet \end{array}$$

Def 3: $\begin{array}{c} \text{---} \diagdown \quad \diagup \text{---} \\ \text{---} \end{array} := \begin{array}{c} \text{---} \boxed{H} \bullet \text{---} \boxed{H} \bullet \text{---} \boxed{H} \bullet \text{---} \\ \text{---} \boxed{H} \bullet \text{---} \boxed{H} \bullet \text{---} \boxed{H} \bullet \text{---} \end{array}$

C_7 : (1) $\begin{array}{c} \bullet \text{---} \boxed{S} \text{---} \\ \bullet \text{---} \end{array} = \begin{array}{c} \text{---} \boxed{S} \text{---} \bullet \\ \text{---} \bullet \end{array}$ (2) $\begin{array}{c} \bullet \text{---} \\ \bullet \text{---} \boxed{S} \end{array} = \begin{array}{c} \text{---} \bullet \\ \text{---} \boxed{S} \bullet \end{array}$

R_{18} : (1) $\begin{array}{c} \boxed{S} \text{---} \diagdown \quad \diagup \\ \text{---} \end{array} = \begin{array}{c} \diagdown \quad \diagup \\ \text{---} \boxed{S} \end{array}$ (2) $\begin{array}{c} \diagdown \quad \diagup \\ \boxed{S} \text{---} \end{array} = \begin{array}{c} \diagdown \quad \diagup \\ \text{---} \boxed{S} \end{array}$

Lem 12 By Def 3, C_7 & R_{18} ,

19. (4) $\begin{array}{c} \boxed{S} \text{---} \boxed{D_{10}} \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \boxed{D_{10}} \text{---} \boxed{S} \\ \text{---} \end{array}$

(7) $\begin{array}{c} \boxed{S} \text{---} \boxed{D_{20}} \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \boxed{D_{20}} \text{---} \boxed{S} \\ \text{---} \end{array}$

(5) $\begin{array}{c} \boxed{S} \text{---} \boxed{D_{11}} \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \boxed{D_{11}} \text{---} \boxed{S} \\ \text{---} \end{array}$

(8) $\begin{array}{c} \boxed{S} \text{---} \boxed{D_{21}} \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \boxed{D_{21}} \text{---} \boxed{S} \\ \text{---} \end{array}$

(6) $\begin{array}{c} \boxed{S} \text{---} \boxed{D_{12}} \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \boxed{D_{12}} \text{---} \boxed{S} \\ \text{---} \end{array}$

(9) $\begin{array}{c} \boxed{S} \text{---} \boxed{D_{22}} \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \boxed{D_{22}} \text{---} \boxed{S} \\ \text{---} \end{array}$

Proof: 19. (4)-(9). LHS := $\begin{array}{c} \boxed{S} \text{---} \boxed{D_{ab}} \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \boxed{A_{ab}} \text{---} \end{array} \begin{array}{c} \boxed{S} \text{---} \diagdown \quad \diagup \\ \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \bullet \quad \bullet \end{array}$

$\stackrel{R_{18}}{=} \begin{array}{c} \text{---} \diagdown \quad \diagup \\ \boxed{A_{ab}} \text{---} \end{array} \begin{array}{c} \boxed{S} \text{---} \bullet \text{---} \bullet \\ \bullet \text{---} \bullet \end{array}$

$\stackrel{C_7}{=} \begin{array}{c} \text{---} \diagdown \quad \diagup \\ \boxed{A_{ab}} \text{---} \end{array} \begin{array}{c} \bullet \text{---} \bullet \\ \bullet \text{---} \bullet \end{array} \boxed{S}$

$\stackrel{\text{def}}{=} \begin{array}{c} \text{---} \boxed{D_{ab}} \text{---} \\ \text{---} \boxed{S} \end{array} = 19. (4)-(9). \text{ RHS.}$

