

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

R_{24} : $\text{S} \oplus \text{I} = \text{S}$

R_{18} : (1) $\text{S} \text{---} \text{X} = \text{X} \text{---} \text{S}$ (2) $\text{S} \text{---} \text{X} = \text{X} \text{---} \text{S}$

C_7 : (1) $\text{S} \text{---} \text{S} = \text{S} \text{---} \text{S}$ (2) $\text{S} \text{---} \text{S} = \text{S} \text{---} \text{S}$

Lem 23 By Def 3, C_7 , R_{18} & R_{24} ,

$$6. (1) \quad \text{S} \text{---} \boxed{B_{00}} = \boxed{B_{00}} \text{---} \text{S}$$

$$(2) \quad \text{S} \text{---} \boxed{B_{01}} = \boxed{B_{01}} \text{---} \text{S}$$

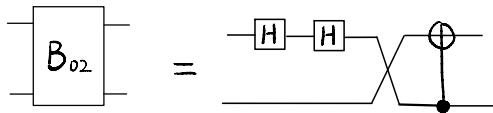
$$\text{Proof: } 6.(1).LHS := \text{S} \text{---} \boxed{B_{00}} \stackrel{\text{def}}{=} \text{S} \text{---} \text{X} \stackrel{R_{18}}{=} \text{X} \text{---} \text{S}$$

$$\stackrel{C_7}{=} \text{X} \text{---} \text{S} \stackrel{\text{def}}{=} \boxed{B_{00}} \text{---} \text{S} =: 6.(1).RHS$$

$$6.(1).LHS := \text{S} \text{---} \boxed{B_{01}} \stackrel{\text{def}}{=} \text{S} \text{---} \text{X} \stackrel{R_{18}}{=} \text{X} \text{---} \text{S} \oplus \text{I}$$

$$\stackrel{C_7}{=} \text{X} \text{---} \text{S} \oplus \text{I} \stackrel{R_{24}}{=} \text{X} \text{---} \text{S} \oplus \text{I}$$

$$\stackrel{\text{def}}{=} \boxed{B_{01}} \text{---} \text{S} =: 6.(2).RHS$$



R2 : $S \quad H \quad H = H \quad H \quad S \quad Z^2$

R₁₈ : (1) = (2) =

R₂₁ : (1) = (2) =

R₂₄ : =

R₂₆ : (1) = (2) =

(3) = (4) =

(5) = (6) =

Def 3 : :=

Lem 24 By Def 3, R₂, R₁₈, R₂₁, R₂₄ & R₂₆,

6.(3) =

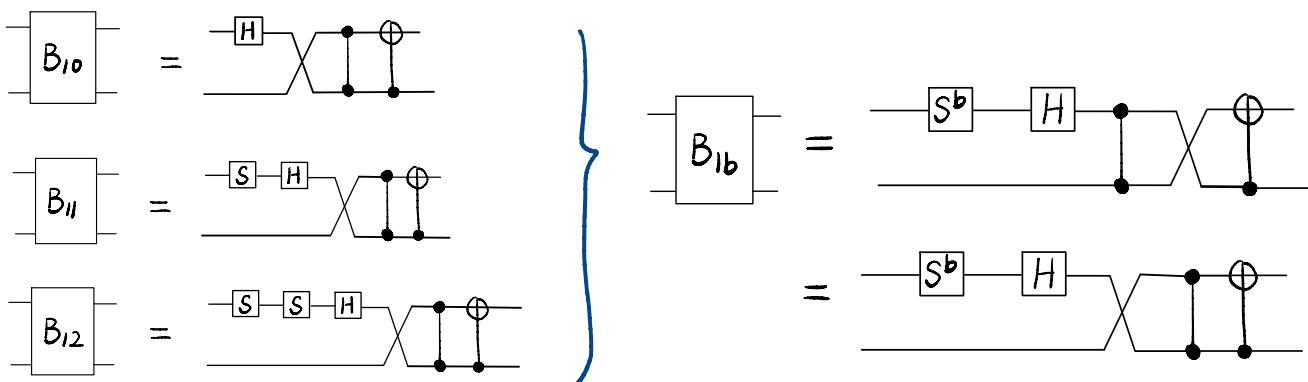
Proof: 6.(3). RHS := $\stackrel{\text{def}}{=}$

$\frac{R_{24}}{R_{26}}$

$\frac{R_{18}}{R_{21}}$

$\frac{R_2}{R_2}$

$\stackrel{\text{def}}{=} 6.(3). \text{LHS}$



$$C_3 : S^3 = I$$

Lem 25 By C_3 , 6. (4)

$$\begin{array}{c} S \\ \hline \end{array} \boxed{B_{10}} = \boxed{B_{11}}$$

$$(5) \quad \begin{array}{c} S \\ \hline \end{array} \boxed{B_{11}} = \boxed{B_{12}}$$

$$(6) \quad \begin{array}{c} S \\ \hline \end{array} \boxed{B_{12}} = \boxed{B_{10}}$$

Proof: 6. (4)/(5)/(6). LHS :=

$$\begin{array}{c} S \\ \hline \end{array} \boxed{B_{1b}} \stackrel{\text{def}}{=} \boxed{S S^b H} \text{---} \text{CNOT with control on top wire, target on bottom wire, followed by a measurement}$$

$$\stackrel{C_3}{=} \boxed{S^b H S \text{---} \text{CNOT with control on top wire, target on bottom wire, followed by a measurement}}$$

$$\stackrel{\text{def}}{=} \boxed{B_{1,1+b}} = 6. (4)/(5)/(6). \text{RHS}$$

III

$$\begin{array}{c}
 B_{20} = \text{Circuit Diagram} \\
 B_{21} = \text{Circuit Diagram} \\
 B_{22} = \text{Circuit Diagram}
 \end{array}
 \quad \left\{ \quad \begin{array}{c}
 B_{2b} = \text{Circuit Diagram} \\
 = \text{Circuit Diagram}
 \end{array} \right.$$

$$\text{Lem 10} \quad \boxed{S} - \boxed{H^2} - \boxed{S^{2b}} - \boxed{H} = -\boxed{H^2} - \boxed{S^{2b+1}} - \boxed{H} - \boxed{X}$$

$$R_{20}: \begin{array}{l} (1) \quad \text{Diagram showing } X \text{ gate on top wire and CNOT gate on bottom wire} \\ (2) \quad \text{Diagram showing } X \text{ gate on bottom wire and CNOT gate on top wire} \end{array} = \boxed{\text{Diagram showing CNOT gate on top wire and } X \text{ gate on bottom wire}} \quad \text{Def 3: } \text{Diagram showing two CNOT gates with control on top wire and target on bottom wire} := \text{Diagram showing sequence of four } H \text{ gates: first two on top wire, last two on bottom wire}$$

$$R_{14}: (1) \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \quad \boxed{X} \quad = \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \quad \boxed{X} \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \quad (2) \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \quad \boxed{Y} \quad = \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array} \quad \boxed{Z} \quad \begin{array}{c} \text{---} \\ | \\ \bullet \\ | \\ \text{---} \end{array}$$

$$(3) \quad \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{X} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{X} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{Z}$$

$$R_{26}: (2) \quad \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{Z} \text{---} \oplus = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \oplus \text{---} \boxed{Z} = (3) \quad \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \oplus \text{---} \boxed{X} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \oplus \text{---} \boxed{X}$$

Lem 26 By Def 3, Lem 10, R₁₄, R₂₀ & R₂₆, 6.17.

$$(7) \quad \boxed{S} - \boxed{B_{20}} = \boxed{B_{22}} - \boxed{X} - \boxed{Z}$$

$$(8) \quad \boxed{S} - \boxed{B_{21}} = \boxed{B_{20}} - \boxed{X} \boxed{Z}$$

$$(19) \quad \begin{array}{c} S \\ \hline \end{array} \quad \boxed{B_{22}} = \boxed{B_{21}} \quad \begin{array}{c} X \\ \hline Z \end{array}$$

$$\text{Proof: } 6.(7)/(8)/(9). \text{ LHS} := \boxed{\text{S}} \quad \boxed{B_{2b}} \quad \stackrel{\text{def}}{=} \quad \boxed{\text{S} - \text{H}^2 - \text{S}^{20} - \text{H}} \quad \times \quad \begin{array}{c} \bullet \\ \text{X} \\ \bullet \end{array} \quad \text{Lem 10}$$

R_{20} R_{14}

The diagram illustrates two equivalent quantum circuit representations for the operator R_{2b} . Both circuits begin with a sequence of three operations: H^2 , S^{2b+1} , and H . The second wire (control wire) starts with a X gate. The third wire (target wire) starts with a Z gate. The circuit then branches into two parallel paths. The first path consists of a CNOT gate with control on the second wire and target on the third wire, followed by a \oplus gate (addition mod 2) with inputs from both wires. The second path consists of a CNOT gate with control on the second wire and target on the third wire, followed by a Z gate with input from the third wire. The entire sequence is enclosed in a blue box.

$2(b+2) = 2b + 4 = 2b + 1$

def $B_{2,b+2}$

$=: 6 \cdot (7)/(8)/(9) \cdot \text{RHS}$