

$$-C_0- = -$$

$$-C_1- = -H-S-H-H-S-S-H-$$

$$-C_2- = -H-S-S-H-H-S-H-$$

$$C_1: w^3 = 1$$

$$R_5: -X- = -H-S-H-H-S-S-H- =: -C_1-$$

$$R_6: -S-X- = -X-S-Z- \cdot w^2$$

$$R_7: -X^2- = -H-S-S-H-H-S-H- =: -C_2-$$

$$R_8: XZ = w^2 ZX \quad -Z-X- = -X-Z- \cdot w^2$$

**Lem5** By definition,  $C_1$ ,  $R_5$ ,  $R_6$ ,  $R_7$  &  $R_8$ , we have

$$15. (1) -S-C_0- = -C_0-S-$$

$$(2) -S-C_1- = -C_1-S-Z- \cdot w^2$$

$$(3) -S-C_2- = -C_2-S-Z-Z-$$

**Proof:** 15. (1). LHS :=  $-S-$  =: 15. (1). RHS

$$15. (2). \text{LHS} := -S- \boxed{H-S-H-H-S-S-H} - \stackrel{R_5}{=} -S-X- \stackrel{R_6}{=} -$$

$$\boxed{X}-S-Z- \cdot w^2 \stackrel{R_5}{=} -C_1-S-Z- \cdot w^2 = 15. (2). \text{RHS}$$

$$15. (3). \text{LHS} := -S- \boxed{H-S-S-H-H-S-H} - \stackrel{R_7}{=} -\boxed{S-X}-X-$$

$$\stackrel{R_6}{=} -X-S-\boxed{Z-X} \cdot w^2 \stackrel{R_8}{=} -X-S-X-Z- \cdot w^2 \cdot w^2$$

$$\stackrel{C_1}{=} -X-\boxed{S-X}-Z- \cdot w \stackrel{R_6}{=} -X-X-S-Z-Z- \cdot w \cdot w^2$$

$$\stackrel{C_1}{=} -X-X-S-Z-Z- \stackrel{R_7}{=} -C_2-S-Z-Z-$$

$$= 15. (3). \text{RHS}$$