C_0 = ——

C_1 = H S H H S S H

C_2 = H S S H H S H

C1: $w^3 = 1$

R5 : X = H S H H S S H =: C_1

R7: X^2 = H S S H H S H =: C_2

R8: $XZ = w^2ZX$ Z X = X Z · w^2

Lem 6 By definition, R5, R7 & R8, we have 16. Z C_c

(1) Z C_0 = C_0 Z

(2) Z C_1 = C_1 Z · w^2

(3) Z C_2 = C_2 Z · w

Proof: 16.(1). LHS := Z =: 16.(1). RHS

16.(2). LHS := Z H S H H S S H $\overset{R5}{=}$ Z X

$\overset{R8}{=}$ X Z · w^2 $\overset{R5}{=:}$ C_1 Z · w^2 = 16.(2). RHS

16.(3). LHS := Z H S S H H S H $\overset{R7}{=}$ Z X X

$\overset{R8}{=}$ X Z X · w^2 $\overset{R8}{=}$ X X Z · w^2 · w^2

$\overset{C_1}{=}$ X X Z · w $\overset{R7}{=:}$ C_2 Z · w = 16.(3). RHS

//