The University of Alabama in Huntsville
Electrical and Computer Engineering
Homework #3 Solution
CPE 633 01
Spring 2008

Chapter 2: Complete the Byzantine(7,2) example (35 points)
Chapter 3: Problems 4(10 points), 6(15 points), 7(20 points), 9(20 points)

Byzantine(7, 2)

Let N = 7, m = 2. We have S, R_1, R_2, R_3, R_4, R_5, R_6. R_1 and R_6 are faulty.

Byz(7,2)

$S.R_1(1)$, $IC(R_1, S) = 1$ $S.R_2(1)$, $IC(R_2, S) = 1$ $S.R_3(1)$, $IC(R_3,S) = 1$
$S.R_4(1)$, $IC(R_4, S) = 1$ $S.R_5(1)$, $IC(R_5, S) = 1$ $S.R_6(1)$, $IC(R_6, S) = 1$

R_1 Byz(6,1)

$S.R_1.R_2(1)$, $IC(R_2, S.R_1) = 1$, $S.R_1.R_3(2)$, $IC(R_3, S.R_1) = 2$,
$S.R_1.R_4(3)$, $IC(R_4, S.R_1) = 3$, $S.R_1.R_5(4)$, $IC(R_5, S.R_1) = 4$,
$S.R_1.R_6(0)$, $IC(R_6, S.R_1) = 0$,

R_2 Byz(5, 0)

$S.R_1.R_2.R_3(1)$, $IC(R_3, S.R_1.R_2) = 1$, $S.R_1.R_2.R_4(1)$, $IC(R_4, S.R_1.R_2) = 1$
$S.R_1.R_2.R_5(1)$, $IC(R_5, S.R_1.R_2) = 1$, $S.R_1.R_2.R_6(1)$, $IC(R_6, S.R_1.R_2) = 1$

R_3 Byz(5, 0)

$S.R_1.R_3.R_2(2)$, $IC(R_2, S.R_1.R_3) = 2$, $S.R_1.R_3.R_4(2)$, $IC(R_4, S.R_1.R_3) = 2$,
$S.R_1.R_3.R_5(2)$, $IC(R_5, S.R_1.R_3) = 2$, $S.R_1.R_3.R_6(2)$, $IC(R_6, S.R_1.R_3) = 2$,

R_4 Byz(5, 0)

$S.R_1.R_4.R_2(3)$, $IC(R_2, S.R_1.R_4) = 3$, $S.R_1.R_4.R_3(3)$, $IC(R_3, S.R_1.R_4) = 3$,
$S.R_1.R_4.R_5(3)$, $IC(R_5, S.R_1.R_4) = 3$, $S.R_1.R_4.R_6(3)$, $IC(R_6, S.R_1.R_4) = 3$,

R_5 Byz(5, 0)

$S.R_1.R_5.R_2(4)$, $IC(R_2, S.R_1.R_5) = 4$, $S.R_1.R_5.R_3(4)$, $IC(R_3, S.R_1.R_5) = 4$,
$S.R_1.R_5.R_4(4)$, $IC(R_4, S.R_1.R_5) = 4$, $S.R_1.R_5.R_6(4)$, $IC(R_6, S.R_1.R_5) = 4$,

R_6 Byz(5, 0)

$S.R_1.R_6.R_2(1)$, $IC(R_2, S.R_1.R_6) = 1$, $S.R_1.R_6.R_3(8)$, $IC(R_3, S.R_1.R_6) = 8$,
$S.R_1.R_6.R_4(0)$, $IC(R_4, S.R_1.R_6) = 0$, $S.R_1.R_6.R_5(\varphi)$,$IC(R_5, S.R_1.R_6) = 0$,

$ICV_{S.R_1}(R_2) = (1, 2, 3, 4, 1)$, $IC(R_2, S.R_1) = 0$
$ICV_{S.R_1}(R_3) = (1, 2, 3, 4, 8)$, $IC(R_3, S.R_1) = 0$
$ICV_{S.R_1}(R_4) = (1, 2, 3, 4, 0)$, $IC(R_4, S.R_1) = 0$
$ICV_{S.R_1}(R_5) = (1, 2, 3, 4, 0)$, $IC(R_5, S.R_1) = 0$
$ICV_{S.R_1}(R_6) = (1, 2, 3, 4, 0)$, $IC(R_6, S.R_1) = 0$

R_2 Byz(6,1)

$S.R_2.R_1(1)$, $IC(R_1, S.R_2) = 1$, $S.R_2.R_3(1)$, $IC(R_3, S.R_2) = 1$,
$S.R_2.R_4(1)$, $IC(R_4, S.R_2) = 1$, $S.R_2.R_5(1)$, $IC(R_5, S.R_2) = 1$,
$S.R_2.R_6(1)$, $IC(R_6, S.R_2) = 1$,

R_1 Byz(5, 0)

$S.R_2.R_1.R_3(1)$, $IC(R_3, S.R_2.R_1) = 1$, $S.R_2.R_1.R_4(3)$, $IC(R_4, S.R_2.R_1) = 3$

$S.R_2.R_1.R_5(4)$, $IC(R_5, S.R_2.R_1) = 4$, $S.R_2.R_1.R_6(0)$, $IC(R_6, S.R_2.R_1) = 0$

R_3 Byz(5, 0)

$S.R_2.R_3.R_1(1)$, $IC(R_1, S.R_2.R_3) = 1$, $S.R_2.R_3.R_4(1)$, $IC(R_4, S.R_2.R_3) = 1$,

$S.R_2.R_3.R_5(1)$, $IC(R_5, S.R_2.R_3) = 1$, $S.R_2.R_3.R_6(1)$, $IC(R_6, S.R_2.R_3) = 1$,

R_4 Byz(5, 0)

$S.R_2.R_4.R_1(1)$, $IC(R_1, S.R_2.R_4) = 1$, $S.R_2.R_4.R_3(1)$, $IC(R_3, S.R_2.R_4) = 1$,

$S.R_2.R_4.R_5(1)$, $IC(R_5, S.R_2.R_4) = 1$, $S.R_2.R_4.R_6(1)$, $IC(R_6, S.R_2.R_4) = 1$,

R_5 Byz(5, 0)

$S.R_2.R_5.R_1(1)$, $IC(R_1, S.R_2.R_5) = 1$, $S.R_2.R_5.R_3(1)$, $IC(R_3, S.R_2.R_5) = 1$,

$S.R_2.R_5.R_4(1)$, $IC(R_4, S.R_2.R_5) = 1$, $S.R_2.R_5.R_6(1)$, $IC(R_6, S.R_2.R_5) = 1$,

R_6 Byz(5, 0)

$S.R_2.R_6.R_1(1)$, $IC(R_1, S.R_2.R_6) = 1$, $S.R_2.R_6.R_3(8)$, $IC(R_3, S.R_2.R_6) = 8$,

$S.R_2.R_6.R_4(0)$, $IC(R_4, S.R_2.R_6) = 0$, $S.R_2.R_6.R_5(\varphi)$,$IC(R_5, S.R_2.R_6) = 0$,

$ICV_{S.R_2}(R_1) = (1, 1, 1, 1, 1)$, $IC(R_1, S.R_2) = 1$

$ICV_{S.R_2}(R_3) = (1, 1, 1, 1, 8)$, $IC(R_3, S.R_2) = 1$

$ICV_{S.R_2}(R_4) = (3, 1, 1, 1, 0)$, $IC(R_4, S.R_2) = 1$

$ICV_{S.R_2}(R_5) = (4, 1, 1, 1, 0)$, $IC(R_5, S.R_2) = 1$

$ICV_{S.R_2}(R_6) = (0, 1, 1, 1, 1)$, $IC(R_6, S.R_2) = 1$

R_3 Byz(6,1)

$S.R_3.R_1(1)$, $IC(R_1, S.R_3) = 1$, $S.R_3.R_2(1)$, $IC(R_2, S.R_3) = 1$,

$S.R_3.R_4(1)$, $IC(R_4, S.R_3) = 1$, $S.R_3.R_5(1)$, $IC(R_5, S.R_3) = 1$,

$S.R_3.R_6(1)$, $IC(R_6, S.R_3) = 1$,

R_1 Byz(5, 0)

$S.R_3.R_1.R_2(1)$, $IC(R_2\ S.R_3.R_1) = 1$, $S.R_3.R_1.R_4(3)$, $IC(R_4, S.R_3.R_1) = 3$

$S.R_3.R_1.R_5(4)$, $IC(R_5, S.R_3.R_1) = 4$, $S.R_3.R_1.R_6(0)$, $IC(R_6, S.R_3.R_1) = 0$

R_2 Byz(5, 0)

$S.R_3.R_2.R_1(1)$, $IC(R_1, S.R_3.R_2) = 1$, $S.R_3.R_2.R_4(1)$, $IC(R_4, S.R_3.R_2) = 1$,

$S.R_3.R_2.R_5(1)$, $IC(R_5, S.R_3.R_2) = 1$, $S.R_3.R_2.R_6(1)$, $IC(R_6, S.R_3.R_2) = 1$,

R_4 Byz(5, 0)

$S.R_3.R_4.R_1(1)$, $IC(R_1, S.R_3.R_4) = 1$, $S.R_3.R_4.R_2(1)$, $IC(R_2, S.R_3.R_4) = 1$,

$S.R_3.R_4.R_5(1)$, $IC(R_5, S.R_3.R_4) = 1$, $S.R_3.R_4.R_6(1)$, $IC(R_6, S.R_3.R_4) = 1$,

R_5 Byz(5, 0)

$S.R_3.R_5.R_1(1)$, $IC(R_1, S.R_3.R_5) = 1$, $S.R_3.R_5.R_2(1)$, $IC(R_2, S.R_3.R_5) = 1$,

$S.R_3.R_5.R_4(1)$, $IC(R_4, S.R_3.R_5) = 1$, $S.R_3.R_5.R_6(1)$, $IC(R_6, S.R_3.R_5) = 1$,

R_6 Byz(5, 0)

$S.R_3.R_6.R_1(5)$, $IC(R_1, S.R_3.R_6) = 5$, $S.R_3.R_6.R_2(8)$, $IC(R_2, S.R_3.R_6) = 8$,

$S.R_3.R_6.R_4(0)$, $IC(R_4, S.R_3.R_6) = 0$, $S.R_3.R_6.R_5(6)$,$IC(R_5, S.R_3.R_6) = 6$,

$ICV_{S.R_3}(R_1) = (1, 1, 1, 1, 5)$, $IC(R_1, S.R_3) = 1$

$ICV_{S.R_3}(R_2) = (1, 1, 1, 1, 8)$, $IC(R_2, S.R_3) = 1$

$ICV_{S.R_3}(R_4) = (3, 1, 1, 1, 0)$, $IC(R_4, S.R_3) = 1$

$ICV_{S.R_3}(R_5) = (4, 1, 1, 1, 6)$, $IC(R_5, S.R_3) = 1$

$ICV_{S.R_3}(R_6) = (0, 1, 1, 1, 1)$, $IC(R_6, S.R_3) = 1$

R_4 Byz(6,1)

$S.R_4.R_1(1)$, $IC(R_1, S.R_4) = 1$, $S.R_4.R_2(1)$, $IC(R_2, S.R_4) = 1$,
$S.R_4.R_3(1)$, $IC(R_3, S.R_4) = 1$, $S.R_4.R_5(1)$, $IC(R_5, S.R_4) = 1$,
$S.R_4.R_6(1)$, $IC(R_6, S.R_4) = 1$,

R_1 Byz(5, 0)

$S.R_4.R_1.R_2(1)$, $IC(R_2\ S.R_4.R_1) = 1$, $S.R_4.R_1.R_3(2)$, $IC(R_3, S.R_4.R_1) = 2$
$S.R_4.R_1.R_5(4)$, $IC(R_5, S.R_4.R_1) = 4$, $S.R_4.R_1.R_6(0)$, $IC(R_6, S.R_4.R_1) = 0$

R_2 Byz(5, 0)

$S.R_4.R_2.R_1(1)$, $IC(R_1, S.R_4.R_2) = 1$, $S.R_4.R_2.R_3(1)$, $IC(R_3, S.R_4.R_2) = 1$,
$S.R_4.R_2.R_5(1)$, $IC(R_5, S.R_4.R_2) = 1$, $S.R_4.R_2.R_6(1)$, $IC(R_6, S.R_4.R_2) = 1$,

R_3 Byz(5, 0)

$S.R_4.R_3.R_1(1)$, $IC(R_1, S.R_4.R_3) = 1$, $S.R_4.R_3.R_2(1)$, $IC(R_2, S.R_4.R_3) = 1$,
$S.R_4.R_3.R_5(1)$, $IC(R_5, S.R_4.R_3) = 1$, $S.R_4.R_3.R_6(1)$, $IC(R_6, S.R_4.R_3) = 1$,

R_5 Byz(5, 0)

$S.R_4.R_5.R_1(1)$, $IC(R_1, S.R_4.R_5) = 1$, $S.R_4.R_5.R_2(1)$, $IC(R_2, S.R_4.R_5) = 1$,
$S.R_4.R_5.R_3(1)$, $IC(R_3, S.R_4.R_5) = 1$, $S.R_4.R_5.R_6(1)$, $IC(R_6, S.R_4.R_5) = 1$,

R_6 Byz(5, 0)

$S.R_4.R_6.R_1(7)$, $IC(R_1, S.R_4.R_6) = 7$, $S.R_4.R_6.R_2(9)$, $IC(R_2, S.R_4.R_6) = 9$,
$S.R_4.R_6.R_3(0)$, $IC(R_3, S.R_4.R_6) = 0$, $S.R_4.R_6.R_5(4)$,$IC(R_5, S.R_4.R_6) = 4$,

$ICV_{S.R_4}(R_1) = (1, 1, 1, 1, 7)$, $IC(R_1, S.R_4) = 1$
$ICV_{S.R_4}(R_2) = (1, 1, 1, 1, 9)$, $IC(R_2, S.R_4) = 1$
$ICV_{S.R_4}(R_3) = (2, 1, 1, 1, 0)$, $IC(R_3, S.R_4) = 1$
$ICV_{S.R_4}(R_5) = (4, 1, 1, 1, 4)$, $IC(R_5, S.R_4) = 1$
$ICV_{S.R_4}(R_6) = (0, 1, 1, 1, 1)$, $IC(R_6, S.R_4) = 1$

R_5 Byz(6,1)

$S.R_5.R_1(1)$, $IC(R_1, S.R_5) = 1$, $S.R_5.R_2(1)$, $IC(R_2, S.R_5) = 1$,
$S.R_5.R_3(1)$, $IC(R_3, S.R_5) = 1$, $S.R_5.R_4(1)$, $IC(R_4, S.R_5) = 1$,
$S.R_5.R_6(1)$, $IC(R_6, S.R_5) = 1$,

R_1 Byz(5, 0)

$S.R_5.R_1.R_2(1)$, $IC(R_2, S.R_5.R_1) = 1$, $S.R_5.R_1.R_3(3)$, $IC(R_3, S.R_5.R_1) = 2$
$S.R_5.R_1.R_4(4)$, $IC(R_5, S.R_5.R_1) = 4$, $S.R_5.R_1.R_6(0)$, $IC(R_6, S.R_5.R_1) = 0$

R_2 Byz(5, 0)

$S.R_5.R_2.R_1(1)$, $IC(R_1, S.R_5.R_2) = 1$, $S.R_5.R_2.R_3(1)$, $IC(R_3, S.R_5.R_2) = 1$,
$S.R_5.R_2.R_4(1)$, $IC(R_5, S.R_5.R_2) = 1$, $S.R_5.R_2.R_6(1)$, $IC(R_6, S.R_5.R_2) = 1$,

R_3 Byz(5, 0)

$S.R_5.R_3.R_1(1)$, $IC(R_1, S.R_5.R_3) = 1$, $S.R_5.R_3.R_2(1)$, $IC(R_2, S.R_5.R_3) = 1$,
$S.R_5.R_3.R_4(1)$, $IC(R_5, S.R_5.R_3) = 1$, $S.R_5.R_3.R_6(1)$, $IC(R_6, S.R_5.R_3) = 1$,

R_4 Byz(5, 0)

$S.R_5.R_4.R_1(1)$, $IC(R_1, S.R_5.R_5) = 1$, $S.R_5.R_4.R_2(1)$, $IC(R_2, S.R_5.R_5) = 1$,
$S.R_5.R_4.R_3(4)$, $IC(R_3, S.R_5.R_5) = 1$, $S.R_5.R_4.R_6(1)$, $IC(R_6, S.R_5.R_5) = 1$,

R_6 Byz(5, 0)

$S.R_5.R_6.R_1(1)$, $IC(R_1, S.R_5.R_6) = 7$, $S.R_5.R_6.R_2(8)$, $IC(R_2, S.R_5.R_6) = 9$,
$S.R_5.R_6.R_4(0)$, $IC(R_3, S.R_5.R_6) = 0$, $S.R_5.R_6.R_5(4)$,$IC(R_5, S.R_5.R_6) = 4$,

$ICV_{S.R_5}(R_1) = (1, 1, 1, 1, 7)$, $IC(R_1, S.R_5) = 1$
$ICV_{S.R_5}(R_2) = (1, 1, 1, 1, 9)$, $IC(R_2, S.R_5) = 1$
$ICV_{S.R_5}(R_3) = (2, 1, 1, 1, 0)$, $IC(R_3, S.R_5) = 1$
$ICV_{S.R_5}(R_4) = (4, 1, 1, 1, 4)$, $IC(R_4, S.R_5) = 1$
$ICV_{S.R_5}(R_6) = (0, 1, 1, 1, 1)$, $IC(R_6, S.R_5) = 1$

R_6 Byz(6,1)

$S.R_6.R_1(8)$, $IC(R_1, S.R_6) = 8$, $S.R_6.R_2(5)$, $IC(R_2, S.R_6) = 5$,
$S.R_6.R_3(2)$, $IC(R_3, S.R_6) = 2$, $S.R_6.R_4(6)$, $IC(R_4, S.R_6) = 6$
$S.R_6.R_5(1)$, $IC(R_5, S.R_6) = 1$,

R_1 Byz(5, 0)

$S.R_6.R_1.R_2(8)$, $IC(R_2, S.R_6.R_1) = 8$, $S.R_6.R_1.R_3(4)$, $IC(R_3, S.R_6.R_1) = 4$
$S.R_6.R_1.R_4(1)$, $IC(R_5, S.R_6.R_1) = 1$, $S.R_6.R_1.R_5(3)$, $IC(R_5, S.R_6.R_1) = 3$

R_2 Byz(5, 0)

$S.R_6.R_2.R_1(5)$, $IC(R_1, S.R_6.R_2) = 5$, $S.R_6.R_2.R_3(5)$, $IC(R_3, S.R_6.R_2) = 5$,
$S.R_6.R_2.R_4(5)$, $IC(R_5, S.R_6.R_2) = 5$, $S.R_6.R_2.R_5(5)$, $IC(R_5, S.R_6.R_2) = 5$,

R_3 Byz(5, 0)

$S.R_6.R_3.R_1(2)$, $IC(R_1, S.R_6.R_3) = 2$, $S.R_6.R_3.R_2(2)$, $IC(R_2, S.R_6.R_3) = 2$,
$S.R_6.R_3.R_4(2)$, $IC(R_5, S.R_6.R_3) = 2$, $S.R_6.R_3.R_5(2)$, $IC(R_5, S.R_6.R_3) = 2$,

R_4 Byz(5, 0)

$S.R_6.R_4.R_1(6)$, $IC(R_1, S.R_6.R_4) = 6$, $S.R_6.R_4.R_2(6)$, $IC(R_2, S.R_6.R_4) = 6$,
$S.R_6.R_4.R_3(6)$, $IC(R_3, S.R_6.R_4) = 6$, $S.R_6.R_4.R_5(6)$, $IC(R_5, S.R_6.R_4) = 6$,

R_5 Byz(5, 0)

$S.R_6.R_5.R_1(1)$, $IC(R_1, S.R_6.R_5) = 1$, $S.R_6.R_5.R_2(1)$, $IC(R_2, S.R_6.R_5) = 1$,
$S.R_6.R_5.R_3(1)$, $IC(R_3, S.R_6.R_5) = 1$, $S.R_6.R_5.R_4(1)$,$IC(R_4, S.R_6.R_5) = 1$

$ICV_{S.R_6}(R_1) = (8, 5, 2, 6, 1)$, $IC(R_1, S.R_6) = 0$
$ICV_{S.R_6}(R_2) = (8, 5, 2, 6, 1)$, $IC(R_2, S.R_6) = 0$
$ICV_{S.R_6}(R_3) = (4, 5, 2, 6, 1)$, $IC(R_3, S.R_6) = 0$
$ICV_{S.R_6}(R_4) = (1, 5, 2, 2, 1)$, $IC(R_4, S.R_6) = 0$
$ICV_{S.R_6}(R_5) = (3, 5, 2, 6, 1)$, $IC(R_5, S.R_6) = 0$

$ICV_S(R_1) = (1, 1, 1, 1, 1, 0)$
$ICV_S(R_2) = (0, 1, 1, 1, 1, 0)$
$ICV_S(R_3) = (0, 1, 1, 1, 1, 0)$
$ICV_S(R_4) = (0, 1, 1, 1, 1, 0)$
$ICV_S(R_5) = (0, 1, 1, 1, 1, 0)$
$ICV_S(R_6) = (0, 1, 1, 1, 1, 1)$

R_1, R_2, R_3, R_4, R_5, R_6 all vote and get 1

4. Compare two parity codes for data words consisting of 64 data bits: (1) A (72; 8) Hamming code; (2) A single parity bit per byte. Both codes require 8 check bits. Indicate the error correction and detection capabilities, the expected overhead, and list the types of multiple errors that are detectable by these two codes.

Code (1) can correct a single bit error while (2) can not. The overhead, in terms of hardware and delay, of code (1) is expected to be higher than that of (2). (1) can detect 2 bit errors any where in the word while (2) can detect most 2-bit errors except those that fall within a single byte. (1) may generate for some 3-bit errors a single bit error syndrome leading to an erroneous correction of that bit, while all 3-bit errors will be correctly detected by (2).

6. A communication channel has a probability of 10^{-3} that a bit transmitted is erroneous. The data rate is 12000 bits per second (bps). Data packets contain 240 information bits, a 32-bit CRC for error detection, and 0, 8, or 16 bits for error correction coding (ECC). Assume that if 8 ECC bits are added all single bit errors can be corrected, and if 16 ECC bits are added all double bit errors can be corrected.
   (a) Find the throughput in information bits per second of a scheme consisting of error detection with retransmission of bad packets (i.e., no error correction).
   (b) Find the throughput if 8 ECC check bits are used, so that single bit errors can be corrected. Uncorrectable packets must be retransmitted.
   (c) Finally find the throughput if 16 ECC check bits are appended, so that two bit errors can be corrected. As in (b), uncorrectable packets must be retransmitted. Would you recommend increasing the number of ECC check bits from 8 to 16?

   (a) Each packet contains 272 bits. If any error occurs, it is detected (assuming that the CRC always works) and the packet is discarded. The probability that a packet has no errors is $(272!/(272!0!))(1 - 10^{-3})^{272} = 0.762$. The data rate of the code is 240/272 = 0.882. Thus, the throughput in bits per second is 0.762 *0.882 * 12000 = 8065.
   (b) With the addition of 8 ECC check bits, each packet contains 280 bits. The probability that a packet has at most one error is $(280!(280!0!))(1 - 10^{-3})^{280} + (280!(279!1!)) * 10^{-3}(1 - 10^{-3})^{279} = 0.968$. The rate of the code is now 240/280 = 0.857. Thus, the throughput with single bit error correction is 0.968 * 0.857 * 12000 = 9955.
   (c) The second ECC byte increases the packet size to 288. The probability that a packet of 288 bits has no more than two errors is $(288!(288!0!))(1 - 10^{-3})^{288} + (288!/(287!1!))(10^{-3}(1 - 10^{-3})^{287} + (288!(286!2!))(10^{-3})^2(1 - 10^{-3})^{286} = 0.997$. The code rate is now 240/288 = 0.833, so the throughput is 0.997 * 0.833 * 12000 = 9966. Increasing the error correction capability in this case resulted in only a marginal increase in the throughput.

7. Derive all codewords for the separable 5-bit cyclic code based on the generating polynomial X + 1 and compare the resulting codewords to those for the non-separable code.

Data Word	Non-Separable	Separable		Data Word	Non-Separable	Separable
0000	00000	00000		1000	11000	10001
0001	00011	00011		1001	11011	10010
0010	00110	00101		1010	11110	10100
0011	00101	00110		1011	11101	10111
0100	01100	01001		1100	10100	11000
0101	01111	01010		1101	10111	11011
0110	01010	01100		1110	10010	11101
0111	01001	01111		1111	10001	11110

9. Given that $X^7 - 1 = (X + 1)g_1(X)g_2(X)$ where $g_1(X) = X^3 + X + 1$
(a) Calculate $g_2(X)$.
(b) Identify all the (7, k) cyclic codes that can be generated based on the factors of X^7-1. How many different such cyclic codes exist?
(c) Show all the codewords generated by $g_1(X)$ and their corresponding data words.

(a) $g_2(X) = X^3 + X^2 + 1$.

$(X^7 - 1)/(X + 1)$

$= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$

```
          01111111
      11 10000001
         11
          10
          11
           10
           11
            10
            11
             10
             11
              11
              11
               00
```

$g_2(X) = (X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)/(X^3 + X + 1)$

$= X^3 + X^2 + 1$

```
          0001101
    1011 1011111
         1011
          1001
          1011
           1011
           1011
            0000
```

(b) Any single factor or product of two factors (out of three) of $X^7 - 1$ will yield a cyclic code: $(X + 1)$ will yield a (7, 6) code, $g_1(X)$ a (7, 4) code, $g_2(X)$ another (7, 4) code, $(X + 1)g_1(X)$ a (7, 3) code, $(X + 1)g_2(X)$ another (7, 3) code, $g_1(X)g_2(X)$ a (7, 1) code.

(c) $g_1(X) = X^3 + X + 1$ For data 0001, code word is

```
    0001
    1011
    0001
   0001
  0000
   0001
  0001011
```

Data Word	Non Separable Code Word	Separable Code Word		Data Word	Non Separable Code Word	Separable Code Word
0000	0000000	0000000		1000	1011000	1000101
0001	0001011	0001011		1001	1010011	1001110
0010	0010110	0010110		1010	1001110	1010011
0011	0011101	0011101		1011	1000101	1011000
0100	0101100	0100111		1100	1110100	1100010
0101	0100111	0101100		1101	1111111	1101001
0110	0111010	0110001		1110	1100010	1110100
0111	0110001	0111010		1111	1101001	1111111