

1. Consider the first order Reed-Muller code  $R(1, 2)$  with generator matrix  $G(1, 2) = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$ .

- (a) What are the parameters of  $R(1, 2)$  (so  $n$ ,  $k$  and  $d$ )?
- (b) Codewords of  $R(1, 2)$  are of the form  $x_1x_2x_3x_4 = [a_2 \ a_1 \ a_0] G(1, 2)$ . Set up parity check equations for  $a_1$  and  $a_2$ .
- (c) Decode 1001.
- (d) Decode 1011.

*Solution :* (a) It follows from the definition of Reed-Muller codes and Proposition 4.4 that

$$n = 2^m = 2^2 = 4 \quad , \quad k = \binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r} = \binom{2}{0} + \binom{2}{1} = 1 + 2 = 3 \quad \text{and} \quad d = 2^{m-r} = 2^{2-1} = 2$$

(b) We get that

$$x_1x_2x_3x_4 = [a_2 \ a_1 \ a_0] \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

So

$$\begin{cases} x_1 = a_0 \\ x_2 = a_1 + a_0 \\ x_3 = a_2 + a_0 \\ x_4 = a_2 + a_1 + a_0 \end{cases}$$

Hence

$$a_1 = x_1 + x_2 = x_3 + x_4 \quad \text{and} \quad a_2 = x_1 + x_3 = x_2 + x_4$$

(c) We calculate the parity check sums for  $a_1$  and  $a_2$ :

$$\begin{array}{ll} a_1 & \{1, 1\} \quad \text{so } a_1 = 1 \\ a_2 & \{1, 1\} \quad \text{so } a_2 = 1 \end{array}$$

We easily get that

$$[a_2 \ a_1 \ 0] G(1, 2) = [1 \ 1 \ 0] \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} = 0110$$

Since  $1001 - 0110 = 1111$ , we get that  $a_0 = 1$ . So we decode 1001 as

$$0110 + 1111 = 1001$$

(d) When calculating the parity check sums for  $a_1$ , we find  $\{1, 0\}$ . So we can not make a decision based on majority. Hence too many errors occurred and we declare a decoding error.

Note that  $d(C) = 2$ . So this code can not correct any errors. It is however one-error correcting : the code will detect if one error occurs. □

2. This exercise is about field extensions containing an element of order 7.

- (a) What is the smallest field extension of  $GF(2)$  that contains an element of order 7?
- (b) What is the smallest field extension of  $GF(4)$  that contains an element of order 7?

*Solution :* (a) We are looking for the smallest  $r \geq 1$  such that  $2^r \equiv 1 \pmod{7}$ . We easily get that  $r = 3$ . So  $GF(2^3) = GF(8)$  is the smallest field extension of  $GF(2)$  that contains an element of order 7.

(b) We are looking for the smallest  $r \geq 1$  such that  $4^r \equiv 1 \pmod{7}$ . We easily get that  $r = 3$ . So  $GF(4^3) = GF(64)$  is the smallest field extension of  $GF(4)$  that contains an element of order 7.  $\square$

---

3. Let  $\alpha$  be a primitive element of  $GF(64)$ . So  $GF(64) = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{61}, \alpha^{62}\}$ . Identify all the subfields of  $GF(64)$  (in terms of powers of  $\alpha$ ).

*Solution :* We first give a general method. Suppose we are given a finite field  $GF(p^s)$  where  $p$  is a prime. When is  $GF(p^r)$  a subfield of  $GF(p^s)$ ? The multiplicative group  $GF(p^r)^*$  of  $GF(p^r)$  is a cyclic group of order  $p^r - 1$  while the multiplicative group  $GF(p^s)^*$  of  $GF(p^s)$  is a cyclic group of order  $p^s - 1$ .  $GF(p^r)$  is a subfield of  $GF(p^s)$  if and only if  $GF(p^r)^*$  is a subgroup of  $GF(p^s)^*$ . Since these groups are cyclic, we get that  $GF(p^r)^* \leq GF(p^s)^*$  iff and only if  $|GF(p^r)^*|$  divides  $|GF(p^s)^*|$ . So

$$GF(p^r) \text{ is a subfield of } GF(p^s) \text{ if and only if } p^r - 1 \text{ divides } p^s - 1.$$

Here we need to find all  $r$  such that  $2^r - 1$  divides  $64 - 1 = 63$ . We easily get that  $r \in \{1, 2, 3, 6\}$ . So  $GF(2)$ ,  $GF(4)$ ,  $GF(8)$  and  $GF(64)$  are the subfields of  $GF(64)$ .

To identify these subfields in terms of powers of  $\alpha$ , recall that

$$|\alpha^k| = \frac{|\alpha|}{\gcd(k, |\alpha|)} = \frac{63}{\gcd(k, 63)}$$

Since  $GF(4)$  is generated by an element of order 3 (namely if  $\beta$  is an element of order 3 then  $GF(4) = \{0, 1, \beta, \beta^2\}$ ), we are looking for  $k$  such that  $\frac{63}{\gcd(k, 63)} = 3$ .  $k = 21$  does the job.

Since  $GF(8)$  is generated by an element of order 7 (namely if  $\gamma$  is an element of order 7 then  $GF(8) = \{0, 1, \gamma, \gamma^2, \dots, \gamma^6\}$ ), we are looking for  $k$  such that  $\frac{63}{\gcd(k, 63)} = 7$ .  $k = 9$  does the job.

$$\begin{array}{l} GF(2) = \{0, 1\} \\ GF(4) = \{0, 1, \alpha^{21}, \alpha^{42}\} \\ GF(8) = \{0, 1, \alpha^9, \alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54}\} \\ GF(64) = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{62}\} \end{array}$$

4. Complete the table for  $GF(16)$  given below.

**Table for  $GF(16) = GF(2)(\alpha)$  where  $\alpha^4 + \alpha^3 + 1 = 0$**

binary	$GF(16)$	Polynomial in $\alpha$
0000	0	0
0001	1	1
0010	$\alpha$	$\alpha$
0100	$\alpha^2$	$\alpha^2$
1000	$\alpha^3$	$\alpha^3$
	$\alpha^4$	
	$\alpha^5$	
	$\alpha^6$	
	$\alpha^7$	
1110	$\alpha^8$	$\alpha^3 + \alpha^2 + \alpha$
	$\alpha^9$	
1010	$\alpha^{10}$	$\alpha^3 + \alpha$
	$\alpha^{11}$	
0011	$\alpha^{12}$	$\alpha + 1$
0110	$\alpha^{13}$	$\alpha^2 + \alpha$
1100	$\alpha^{14}$	$\alpha^3 + \alpha^2$

*Solution* : Since  $\alpha^4 + \alpha^3 + 1 = 0$ , we get

$$\begin{aligned}
 \alpha^4 &= \alpha^3 + 1 = 1001 \\
 \alpha^5 &= \alpha\alpha^4 = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = \alpha^3 + 1 + \alpha = \alpha^3 + \alpha + 1 = 1011 \\
 \alpha^6 &= \alpha\alpha^5 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + 1 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 = 1111 \\
 \alpha^7 &= \alpha\alpha^6 = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + 1 + \alpha^3 + \alpha^2 + \alpha = \alpha^2 + \alpha + 1 = 0111 \\
 \alpha^9 &= \alpha\alpha^8 = \alpha(\alpha^3 + \alpha^2 + \alpha) = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + 1 + \alpha^3 + \alpha^2 = \alpha^2 + 1 = 0101 \\
 \alpha^{11} &= \alpha\alpha^{10} = \alpha(\alpha^3 + \alpha) = \alpha^4 + \alpha^2 = \alpha^3 + 1 + \alpha^2 = \alpha^3 + \alpha^2 + 1 = 1101
 \end{aligned}$$

So the complete table is

binary	$GF(16)$	Polynomial in $\alpha$
0000	0	0
0001	1	1
0010	$\alpha$	$\alpha$
0100	$\alpha^2$	$\alpha^2$
1000	$\alpha^3$	$\alpha^3$
1001	$\alpha^4$	$\alpha^3 + 1$
1011	$\alpha^5$	$\alpha^3 + \alpha + 1$
1111	$\alpha^6$	$\alpha^3 + \alpha^2 + \alpha + 1$
0111	$\alpha^7$	$\alpha^2 + \alpha + 1$
1110	$\alpha^8$	$\alpha^3 + \alpha^2 + \alpha$
0101	$\alpha^9$	$\alpha^2 + 1$
1010	$\alpha^{10}$	$\alpha^3 + \alpha$
1101	$\alpha^{11}$	$\alpha^3 + \alpha^2 + 1$
0011	$\alpha^{12}$	$\alpha + 1$
0110	$\alpha^{13}$	$\alpha^2 + \alpha$
1100	$\alpha^{14}$	$\alpha^3 + \alpha^2$

5. Let  $C$  be a linear code of length  $n$  over  $\mathbb{F}$ .

(a) Define the dual code  $C^\perp$ .

(b) Suppose that  $C$  is cyclic. Prove (using the definition of the dual code and a cyclic code) that  $C^\perp$  is cyclic.

*Solution :* (a) The dual code  $C^\perp$  is the set of all words that are orthogonal to all codewords. So

$$C^\perp = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{x} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C\}$$

(b) Let  $\mathbf{x} \in C^\perp$ . To prove that  $C^\perp$  is cyclic, we have that show that  $\mathbf{x}' \in C^\perp$ . So we need to show that

$$\mathbf{x}' \cdot \mathbf{c} = 0 \quad \text{for all } \mathbf{c} \in C$$

Let  $\mathbf{c} \in C$ . Put  $\mathbf{x} = x_1x_2 \dots x_n$  and  $\mathbf{c} = c_1c_2 \dots c_n$ . Then  $\mathbf{x}' = x_nx_1x_2 \dots x_{n-1}$  and so

$$\mathbf{x}' \cdot \mathbf{c} = x_nc_1 + x_1c_2 + \dots + x_{n-1}c_n = x_1c_2 + x_2c_3 + \dots + x_{n-1}c_n + x_nc_1$$

Note that  $c_2c_3 \dots c_nc_1 = \mathbf{c}^{(n-1)} \in C$  since  $C$  is cyclic. So  $\mathbf{x}' \cdot \mathbf{c} = 0$ . Hence  $\mathbf{x}' \in C^\perp$  and  $C^\perp$  is cyclic.  $\square$

1. This exercise is related to  $x^{10} - 1$  over  $GF(3)$

- (a) What are the degrees of the irreducible factors of  $x^{10} - 1$  over  $GF(3)$ ?
- (b) How many ternary cyclic codes of length 10 are there?
- (c) Is there a ternary cyclic code of length 10 of dimension 7?
- (d) What are the irreducible factors of  $x^{10} - 1$  over  $GF(3)$ ? Use  $GF(3) = \{0, 1, -1\} \pmod 3$ . You do not need a table for this!

*Solution :* (a) The cyclotomic cosets depending on  $n = 10$  and  $q = 3$  are

$$\{0\} , \{1, 3, 9, 7\} , \{2, 6, 8, 4\} \text{ and } \{5\}$$

Since the sizes of the cyclotomic cosets are the degrees of the irreducible factors of  $x^{10} - 1$  over  $GF(3)$ , we get that there are two factors of degree one and two factors of degree four.

(b) Since  $x^{10} - 1$  has four different irreducible factors over  $GF(3)$ , we get that  $x^{10} - 1$  has  $2^4 = 16$  monic divisors (indeed, if  $g_1(x), g_2(x), g_3(x), g_4(x)$  are the four irreducible factors of  $x^{10} - 1$  then each monic divisor of  $x^{10} - 1$  is of the form  $g_1(x)^{\alpha_1} g_2(x)^{\alpha_2} g_3(x)^{\alpha_3} g_4(x)^{\alpha_4}$  where  $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \{0, 1\}$ ). Since each monic divisor of  $x^{10} - 1$  corresponds to a ternary cyclic code of length 10, we get that there are 16 ternary cyclic codes of length 10.

(c) Since  $x^{10} - 1$  has two factors of degree one and two factors of degree four, we can easily write down the degrees of all monic divisors of  $x^{10} - 1$  (which are the generator polynomials of all ternary cyclic codes of length 10) :

$$0, 1, 1, 2, 4, 4, 5, 5, 5, 5, 6, 6, 8, 9, 9, 10$$

If there was a ternary cyclic code  $C$  of length 10 and dimension 7, then its generator polynomial would have degree  $10 - 7 = 3$ . But there are no monic divisors of  $x^{10} - 1$  of degree 3. Hence there are no ternary cyclic codes of length 10 and dimension 7.

(d) The following is true over  $\mathbb{R}$  :

$$x^{10} - 1 = (x^5)^2 - 1^2 = (x^5 - 1)(x^5 + 1)$$

Since  $x = 1$  is a root of  $x^5 - 1$ , we know that  $x - 1$  is a factor of  $x^5 - 1$ . Using long division or synthetic division if needed, we get that

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

Since  $x = -1$  is a root of  $x^5 + 1$ , we know that  $x + 1$  is a factor of  $x^5 + 1$ . Using long division or synthetic division if needed, we get that

$$x^5 + 1 = (x + 1)(x^4 - x^3 + x^2 - x + 1)$$

So over  $\mathbb{R}$ , we get that

$$x^{10} - 1 = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$$

Since this factorization uses only integral coefficients, it still holds over  $GF(3)$ . In general, it could be that  $x^4 + x^3 + x^2 + x + 1$  and/or  $x^4 - x^3 + x^2 - x + 1$  are not irreducible over  $GF(3)$ . However, using the cyclotomic cosets, we concluded that  $x^{10} - 1$  has four irreducible factors over  $GF(3)$  : two of degree one and two of degree four. Since we have a factorization over  $GF(3)$  of  $x^{10} - 1$  into two factors of degree one and two factors of degree four, these factors must be irreducible. So the factorization into irreducible factors over  $GF(3)$  of  $x^{10} - 1$  is

$$\boxed{x^{10} - 1 = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)}$$

2. Find the minimal polynomial over  $GF(4)$  of some primitive 21-th root of unity (in some field extension of  $GF(4)$ ).

*Solution :* Let  $\beta$  be an element of order 21 in some field extension of  $GF(4)$ . The cyclotomic coset containing  $s = 1$  and depending on  $n = 21$  and  $q = 4$  is

$$\{1, 4, 16\}$$

Hence it follows from Theorem 5.4 that the minimal polynomial  $m_\beta(x)$  of  $\beta$  over  $GF(4)$  is

$$m_\beta(x) = (x - \beta)(x - \beta^4)(x - \beta^{16})$$

To practically find this polynomial, we need to use a table. The smallest field extension of  $GF(4)$  containing an element of order 21 is  $GF(64)$ . Let  $\alpha$  be a primitive element in  $GF(64)$ . So  $\alpha$  has order 63. Hence we can put  $\beta = \alpha^3$ . Note that  $GF(4) = \{0, 1, \alpha^{21}, \alpha^{42}\}$ . Using the table, we get that

$$\begin{aligned} m_\beta(x) &= (x - \beta)(x - \beta^4)(x - \beta^{16}) \\ &= (x - \alpha^3)(x - \alpha^{12})(x - \alpha^{48}) \\ &= x^3 + (\alpha^3 + \alpha^{12} + \alpha^{48})x^2 + (\alpha^3\alpha^{12} + \alpha^{12}\alpha^{48} + \alpha^{48}\alpha^3)x + \alpha^3\alpha^{12}\alpha^{48} \\ &= x^3 + (\alpha^3 + \alpha^{12} + \alpha^{48})x^2 + (\alpha^{15} + \alpha^{60} + \alpha^{51})x + \alpha^{63} \\ &= x^3 + \alpha^{42}x + 1 \end{aligned}$$

since

$$\begin{aligned} \alpha^3 + \alpha^{12} + \alpha^{48} &= 001000 + 000101 + 001101 = 000000 = 0 \\ \alpha^{15} + \alpha^{60} + \alpha^{51} &= 101000 + 111001 + 101011 = 111010 = \alpha^{42} \end{aligned}$$

$$\boxed{x^3 + \alpha^{42}x + 1}$$

Remark : There are other correct answers. Since  $\beta^2$  is also an element of order 21, one could calculate the minimal polynomial over  $GF(4)$  of  $\beta^2$ . But the minimal polynomial of  $\beta^3$  would be incorrect as  $\beta^3$  is an element of order 7.

3. Find all the binary cyclic codes of length 7 that contain the word 0001111.

*Solution :* Recall that there are eight binary cyclic codes of length 7 and that we know their generator polynomial.

If  $C$  is a binary cyclic code of length 7 with generator polynomial  $g(x)$  then

$$0001111 \in C \iff 1111000 \in C \iff g(x) \text{ divides } 1 + x + x^2 + x^3$$

Clearly, 1 divides  $1 + x + x^2 + x^3$ . Recall that  $x^7 - 1$  has three irreducible factors over  $GF(2)$  :  $x + 1$ ,  $x^3 + x + 1$  and  $x^3 + x^2 + 1$ . First we check if any of these factors divide  $1 + x + x^2 + x^3$ . We get

$$\begin{aligned} x^3 + x^2 + x + 1 &= (x + 1)(x^2 + 1) \\ x^3 + x^2 + x + 1 &= (x^3 + x + 1) \cdot 1 + x^2 \\ x^3 + x^2 + x + 1 &= (x^3 + x^2 + 1) \cdot 1 + x \end{aligned}$$

So  $x + 1$  divides  $1 + x + x^2 + x^3$  but neither  $1 + x + x^3$  nor  $1 + x^2 + x^3$  divide  $1 + x + x^2 + x^3$ . Hence the only monic divisors of  $x^7 - 1$  that divide  $1 + x + x^2 + x^3$  are 1 and  $1 + x$ . So there are only two binary cyclic codes of length 7 that contain the word 0001111 (see page 42):  $C_0$  (with generator polynomial 1) and  $C_1$  (with generator polynomial  $1 + x$ ).  $\square$

4. Let  $m \geq 1$  and  $\mathbf{c} \in R(1, m) \setminus \{\mathbf{0}, \mathbf{1}\}$  where  $\mathbf{1} = \underbrace{11 \dots 11}_{2^m \text{ times}}$ . Prove that  $w(\mathbf{c}) = 2^{m-1}$ .

*Proof* : The proof is by induction on  $m$ .

Suppose first that  $m = 1$ . Since

$$R(1, m) = R(1, 1) = \{0, 1\}^{2^m} = \{0, 1\}^2 = \{00, 01, 10, 11\}$$

and  $w(01) = w(10) = 1 = 2^{1-1} = 2^{m-1}$ , we get that  $w(\mathbf{c}) = 2^{m-1}$  for all  $\mathbf{c} \in R(1, m) \setminus \{\mathbf{0}, \mathbf{1}\}$  if  $m = 1$ .

Suppose next that  $w(\mathbf{c}) = 2^{j-1}$  for all  $\mathbf{c} \in R(1, j) \setminus \{\mathbf{0}, \mathbf{1}\}$  if  $1 \leq j \leq m-1$  for some  $m \geq 2$ . Recall that  $R(1, m) = R(1, m-1) \otimes R(0, m-1)$ . So

$$R(1, m) = \{(\mathbf{x}, \mathbf{x} + \mathbf{y}) : \mathbf{x} \in R(1, m-1), \mathbf{y} \in R(0, m-1)\}$$

But  $R(0, m-1) = \{\mathbf{0}, \mathbf{1}\}$  and has length  $2^{m-1}$ . So let  $\mathbf{c} \in R(1, m) \setminus \{\mathbf{0}, \mathbf{1}\}$ . Then there are two possibilities:

- (a)  $\mathbf{c} = (\mathbf{x}, \mathbf{x})$  for some  $\mathbf{x} \in R(1, m-1)$ .

Note that  $\mathbf{x} \neq \mathbf{0}$  since  $\mathbf{c} \neq \mathbf{0}$  and  $\mathbf{x} \neq \mathbf{1}$  since  $\mathbf{c} \neq \mathbf{1}$ . Then  $w(\mathbf{x}) = 2^{(m-1)-1} = 2^{m-2}$  by induction. Hence

$$w(\mathbf{c}) = w(\mathbf{x}, \mathbf{x}) = 2w(\mathbf{x}) = 2 \cdot 2^{m-2} = 2^{m-1}$$

- (b)  $\mathbf{c} = (\mathbf{x}, \mathbf{x} + \mathbf{1})$  for some  $\mathbf{x} \in R(1, m-1)$

In general, if  $\mathbf{y}$  is a binary word of length  $n$ , then  $w(\mathbf{y} + \mathbf{1}) = n - w(\mathbf{y})$ . Indeed, if  $\mathbf{y} + \mathbf{1} = z_1 z_2 \dots z_n$  then  $z_i = 1 \iff y_i = 0$ . So

$$w(\mathbf{y} + \mathbf{1}) = |\{1 \leq i \leq n : z_i = 1\}| = |\{1 \leq i \leq n : y_i = 0\}| = n - |\{1 \leq i \leq n : y_i = 1\}| = n - w(\mathbf{y})$$

Hence we get that

$$w(\mathbf{c}) = w(\mathbf{x}, \mathbf{x} + \mathbf{1}) = w(\mathbf{x}) + w(\mathbf{x} + \mathbf{1}) = w(\mathbf{x}) + 2^{m-1} - w(\mathbf{x}) = 2^{m-1}$$

This completes the proof by induction. □

5. Let  $C_1$  and  $C_2$  be cyclic codes of length  $n$  over  $GF(q)$  with generator polynomials  $g_1(x)$  and  $g_2(x)$ . Prove that  $C_1 \cap C_2$  is a cyclic code with generator polynomial  $\text{lcm}(g_1(x), g_2(x))$  (the least common multiple of  $g_1(x)$  and  $g_2(x)$ ).

*Proof* : First, we prove that  $C_1 \cap C_2$  is cyclic. Note that  $C_1 \cap C_2$  is a linear code of length  $n$ . Let  $\mathbf{x} \in C_1 \cap C_2$ . Then  $\mathbf{x} \in C_1$ . Since  $C_1$  is cyclic, we get that  $\mathbf{x}' \in C_1$ . Similarly,  $\mathbf{x}' \in C_2$ . Hence  $\mathbf{x}' \in C_1 \cap C_2$ . So  $C_1 \cap C_2$  is cyclic.

Let  $g(x)$  be the generator polynomial of  $C_1 \cap C_2$ .

Since  $g_1(x)$  and  $g_2(x)$  are monic divisors of  $x^n - 1$ , we have that  $\text{lcm}(g_1(x), g_2(x))$  is a monic divisor of  $x^n - 1$ . Hence  $\text{lcm}(g_1(x), g_2(x))$  is the generator polynomial of some cyclic code  $C^*$ .

Since  $C_1 \cap C_2 \subseteq C_1$ , it follows from Ex#6 that  $g_1(x)$  divides  $g(x)$ . Similarly,  $g_2(x)$  divides  $g(x)$ . So  $g(x)$  is a common multiple of  $g_1(x)$  and  $g_2(x)$ . Hence  $\text{lcm}(g_1(x), g_2(x))$  divides  $g(x)$ . Again by Ex#6, we get that  $C_1 \cap C_2 \subseteq C^*$ .

Clearly,  $g_1(x)$  divides  $\text{lcm}(g_1(x), g_2(x))$ . Hence it follows from Ex#6 that  $C^* \subseteq C_1$ . Similarly, we get that  $C^* \subseteq C_2$ . So  $C^* \subseteq C_1 \cap C_2$ .

Hence  $C_1 \cap C_2 = C^*$ . So the generator polynomial of  $C_1 \cap C_2$  is equal to the generator polynomial of  $C^*$ , namely  $\text{lcm}(g_1(x), g_2(x))$ . □