

MATH 4450/6450
HOMEWORK 10 SOLUTIONS AND COMMENTS

Extra Problem 1: (a) Let α be an element of \mathbb{F}_{q^k} . Let f be a monic polynomial in $\mathbb{F}_q[x]$ such that $f(\alpha) = 0$. Show that f is the minimal polynomial of α (in the sense defined in class) if and only if f is irreducible. (We've pretty much proved this in class, so I want you to write it down.)

(b) Let q, d, k be positive integers, $q \geq 2$. Show that $q^d - 1 | q^k - 1$ if and only if $d | k$. In fact, better yet: show that the gcd of $q^a - 1$ and $q^b - 1$ is $q^d - 1$, where $d = \gcd(a, b)$.

(c) For any positive integer d , let $S_{q,d}$ be the set of monic irreducible polynomials of degree d in $\mathbb{F}_q[x]$. Show that the following identity holds in $\mathbb{F}_q[x]$:

$$x^{q^k} - x = \prod_{d|k} \prod_{f \in S_{q,d}} f(x).$$

(Hint: show that every element of \mathbb{F}_{q^k} is a root of both sides! Think about orders. You'll want to use part (b).)

(d) Let $\nu_2(k)$ be the number of irreducible polynomials of degree k in $\mathbb{F}_2[x]$. Compute the sequences $\nu_2(k)$ and $k\nu_2(k)$ for $1 \leq k \leq 10$. (Hint: use part (c) and count degrees.)

Remark: If you know Möbius inversion, you can apply it to the degrees of both sides of part (c), and estimate the right side, and conclude that there always is at least one irreducible polynomial of degree k over \mathbb{F}_q ; this is a fact that we have alluded to but not proved.

Remark: If you wanted to cheat a little when you started to do part (d), you could have tried the following link, which I recommend wholeheartedly:

<http://www.research.att.com/~njas/sequences/>

Solution: (a) If f is the minimal polynomial of α , then suppose $f(x) = g(x)h(x)$, where g and h both have smaller degree. Since α is a root of f , it's a root of g or h , which contradicts the minimality of α . So f is irreducible. Conversely, if f is irreducible, and $f(\alpha) = 0$, then suppose $g(\alpha) = 0$. Write $g(x) = f(x)q(x) + r(x)$, where $\deg(r) < \deg(f)$ or $r = 0$. Clearly $r(\alpha) = 0$, so the only possibility is that r is the zero polynomial, so $f | g$, so f divides any polynomial which has α as a root, so its degree is minimal. \square

(b) The first statement clearly follows from the second. To see the second, let $d = \gcd(a, b)$. Clearly $q^d - 1 | q^a - 1$ and $q^d - 1 | q^b - 1$ (you can look at it mod $q^d - 1$, or long divide, or whatever). So $(q^d - 1) | \gcd(q^a - 1, q^b - 1)$. Now let $r = \gcd(q^a - 1, q^b - 1)$. So $q^a \equiv 1 \pmod r$, and $q^b \equiv 1 \pmod r$. Write $d = ax + by$ for some integers x, y , and then note that $q^{ax+by} \equiv q^{ax}q^{by} \equiv 1 \pmod r$. So $r | q^d - 1$. Together, these facts show that $r = q^d - 1$. \square

(c) We prove the result by induction. Suppose it is proved for all $\ell < k$.

Clearly every element of \mathbb{F}_{q^k} is a root of the right side, by Euler's theorem. And the right side has no repeated roots (because it has no repeated factors over \mathbb{F}_q , it satisfies the gcd

criterion from the last problem set, so it has no repeated factors over any \mathbb{F}_{q^k} , either). So we just need to show that every element of \mathbb{F}_{q^k} is a root of the right side.

Let α be an element of \mathbb{F}_{q^k} . First I argue that the degree of the minimal polynomial of α is $\leq k$. Note that the elements $1, \alpha, \dots, \alpha^k$ must be linearly dependent over \mathbb{F}_q (because the dimension of \mathbb{F}_{q^k} as a vector space over \mathbb{F}_q is k). The dependence relation gives a polynomial over \mathbb{F}_q of which α is a root, so its minimal polynomial must have degree $\leq k$.

Now if the minimal polynomial has degree k , then α is a root of the right side. If its minimal polynomial has degree $\ell < k$, then α is a root of $x^{q^\ell} - x$, by the inductive hypothesis. Since α is also a root of $x^{q^k} - x$, it's a root of

$$\begin{aligned} \gcd(x^{q^\ell} - x, x^{q^k} - x) &= x \cdot \gcd(x^{q^\ell-1} - 1, x^{q^k-1} - 1) \\ &= x(x^{\gcd(q^\ell-1, q^k-1)} - 1) \\ &= x(x^{q^m-1} - 1) = x^{q^m} - x \end{aligned}$$

where $m = \gcd(\ell, k)$. So this implies (again by the inductive hypothesis) that the minimal polynomial of α has degree dividing m , so $\ell|m$, so it must be the case that $\ell = m$, i.e. $\ell|k$. So α is a root of the right side in any case. \square

(d) Count degrees on either side of the equation in part (c) to get that

$$q^k = \sum_{d|k} d\nu_q(d).$$

So we can use this recursively to get a formula for $\nu_q(d)$, starting with the knowledge that $\nu_q(1) = q$ (there are q monic linear polynomials over \mathbb{F}_q , all of which are irreducible). For instance,

$$\begin{aligned} 2^2 &= 1 \cdot 2 + 2\nu_2(2) \Rightarrow \nu_2(2) = 1 \\ 2^3 &= 1 \cdot 2 + 3\nu_2(3) \Rightarrow \nu_2(3) = 2 \\ 2^4 &= 1 \cdot 2 + 2 \cdot 1 + 4\nu_2(4) \Rightarrow \nu_2(4) = 3 \end{aligned}$$

etc. We get

$$\begin{aligned} (\nu_2(k))_{k=1}^{10} &= (2, 1, 2, 3, 6, 9, 18, 30, 56, 99) \\ (k\nu_2(k))_{k=1}^{10} &= (2, 2, 6, 12, 30, 54, 126, 240, 504, 990) \end{aligned}$$

By the way, I definitely cheated by going to the URL above after I got the first six or seven terms. Try it yourself. \square

Extra Problem 2: (QR codes) Let p be a prime congruent to $\pm 1 \pmod 8$. Let Q_p be the set of nonzero quadratic residues in \mathbb{Z}_p . Let N_p be the set of nonzero quadratic nonresidues in \mathbb{Z}_p . Define the following polynomials in $\mathbb{F}_2[x]$:

$$\begin{aligned} e_1(x) &= \sum_{i \in Q_p} x^i \\ e_2(x) &= \sum_{j \in N_p} x^j \\ h(x) &= 1 + x + \dots + x^{p-1} = 1 + e_1(x) + e_2(x) \end{aligned}$$

(a) Show that $e_1(x)$, $e_2(x)$, $1 + e_1(x)$, and $1 + e_2(x)$ are p -idempotents.

(b) Let $f(x)$ be any polynomial of degree $< p$. Suppose $f(x)$ has ℓ nonzero terms. Show that

$$f(x)h(x) \equiv \begin{cases} 0 \pmod{x^p - 1} & \text{if } \ell \text{ is even} \\ h(x) \pmod{x^p - 1} & \text{if } \ell \text{ is odd} \end{cases}$$

(c) Show that if $p \equiv -1 \pmod{8}$, then $e_1(x)h(x) \equiv h(x) \pmod{x^p - 1}$, and conclude that $e_1(x)e_2(x) \equiv h(x) \pmod{x^p - 1}$. Also show that if $p \equiv 1 \pmod{8}$, then $(1 + e_1(x))h(x) \equiv h(x) \pmod{x^p - 1}$, and conclude that $(1 + e_1(x))(1 + e_2(x)) \equiv h(x) \pmod{x^p - 1}$.

Remark: A code whose p -idempotent generator is one of the four given in part (a) is called a *QR code*.

Solution: (a) Since we're working mod 2, we have

$$e_1(x)^2 \equiv e_1(x^2) \equiv \sum_{i \in Q_p} x^{2i \pmod{p}} \pmod{x^p - 1}$$

and the point is that $2i$ is a square mod p if and only if i is a square mod p , because $p \equiv \pm 1 \pmod{8}$, so $\left(\frac{2}{p}\right) = 1$. So the right side equals $\sum_{i \in Q_p} x^i$, which is $e_1(x)$. The exact same proof works for $e_2(x)$. And

$$(1 + e_i(x))^2 \equiv 1 + e_i(x)^2 \equiv 1 + e_i(x) \pmod{x^p - 1}$$

for $i = 1, 2$, so $1 + e_i(x)$ is also a p -idempotent. \square

(b) Obviously any nonzero monomial times $h(x) \pmod{x^p - 1}$ equals $h(x)$. Since $f(x)$ is a sum of ℓ nonzero monomials, we have that $f(x)h(x) \equiv \ell h(x) \pmod{x^p - 1}$, which breaks down as 0 or $h(x)$ depending on whether ℓ is even or odd, respectively. \square

(c) The number of nonzero monomials in $e_1(x)$ is $\frac{p-1}{2}$, and this is odd if $p \equiv -1 \pmod{8}$, so $e_1(x)h(x) \equiv h(x) \pmod{x^p - 1}$ in this case by part (b). Then we get

$$\begin{aligned} e_1(x)h(x) &\equiv h(x) \pmod{x^p - 1} \\ e_1(x)(1 + e_1(x) + e_2(x)) &\equiv h(x) \pmod{x^p - 1} \\ e_1(x) + e_1(x) + e_1(x)e_2(x) &\equiv h(x) \pmod{x^p - 1} \\ e_1(x)e_2(x) &\equiv h(x) \pmod{x^p - 1} \end{aligned}$$

as desired.

On the other hand, we get $(1 + e_1(x))h(x) \equiv h(x) \pmod{x^p - 1}$ by part (b) if $p \equiv 1 \pmod{8}$, because $1 + e_1(x)$ has $\frac{p+1}{2}$ nonzero monomials, which is odd. Since $(1 + e_1(x))e_1(x) \equiv 0 \pmod{x^p - 1}$, this reduces to $(1 + e_1(x))(1 + e_2(x)) \equiv h(x) \pmod{x^p - 1}$ as desired. \square

Extra Problem 3: (QR codes continued!) All notation as in Extra Problem 2.

(a) Suppose $p \equiv -1 \pmod{8}$. Let C_1 be the code with p -idempotent generator $e_1(x)$, and let C_2 be the code with p -idempotent generator $e_2(x)$. Show that $C_1 \cap C_2$ is the binary p -repetition code, and that $C_1 + C_2 = \mathbb{F}_2^p$. (Use results from last week's problem set.)

(b) Conclude that C_1 and C_2 are $[p, (p+1)/2]$ codes.

(c) Show that C_1 and C_2 are equivalent. (Hint: choose $n \in N_p$. Then consider the permutation of the columns that sends the column corresponding to i to the column corresponding to $ni \pmod{p}$; show that it sends the codeword corresponding to $f(x)$ to the codeword corresponding to $f(x^n) \pmod{x^p - 1}$. Show that this permutation sends C_1 to C_2 .)

(d) Repeat parts (a)-(c) when $p \equiv 1 \pmod{8}$, except that C_1 should be the code with p -idempotent generator $1 + e_1(x)$, and C_2 should be the code with p -idempotent generator $1 + e_2(x)$.

Remark: One can prove much much more about these things; for instance, their duals are QR codes (what do you think their idempotent generators are?)

Solution: (a) The p -idempotent generator of $C_1 \cap C_2$ is $e_1(x)e_2(x)$, by a result on last week's problem set. This equals $h(x)$ if $p \equiv -1 \pmod{8}$. It's easy to see that $h(x)$ is the p -idempotent generator of the binary $[p, 1, p]$ repetition code. On the other hand, by a result on last week's problem set, the p -idempotent generator of $C_1 + C_2$ is $e_1(x) + e_2(x) - e_1(x)e_2(x)$, which is 0. This corresponds to the entire space \mathbb{F}_2^p . \square

(b) Hm, I think I actually needed part (c) here. Linear algebra says that $\dim(C_1) + \dim(C_2) - \dim(C_1 \cap C_2) = \dim(C_1 + C_2)$, from which we can conclude that $\dim(C_1) + \dim(C_2) = p + 1$. To get that they have the same dimension, which must be $(p+1)/2$, I need to see that they're equivalent. So I'll put a \square here pending the answer to part (c).

(c) The permutation sending the column corresponding to i to the column corresponding to ni clearly has the effect of sending the codeword corresponding to x^i to the codeword corresponding to x^{ni} . So it sends the codeword corresponding to $f(x)$ to the codeword corresponding to $f(x^n)$ in general. Note that $e_1(x^n) = e_2(x)$ because $j \in Q_p$ if and only if $nj \in N_p$. So it's clear that the permutation sends C_1 to C_2 . \square

(d) I'll leave this to you; the work is exactly the same. \square

Extra Problem 4: Here we will show that the BCH bound is not sharp.

(a) Consider the polynomial $x^{17} - 1$ in $\mathbb{F}_2[x]$, which factors as

$$(x + 1)(x^8 + x^5 + x^4 + x^3 + 1)(x^8 + x^7 + x^6 + x^4 + x^2 + x + 1).$$

Show that these factors are irreducible. (Hint: let $h(x)$ be an irreducible factor of degree d ; a root of it lies in \mathbb{F}_{2^d} ; show that $17 \mid (2^d - 1)$.)

(b) Let α be a root of the second factor, which we'll call $g(x)$. Which powers of α are also roots of $g(x)$? Write them all down. Show that if C_g is the cyclic code with generating polynomial $g(x)$, then the best that the BCH bound can do is to show $d \geq 3$.

(c) Show that C_g has p -idempotent generator equal to $1 + e_2(x)$, where e_2 is defined as in Extra Problems 2 and 3. Conclude that C_g is a QR code.

(d) Suppose that C_g has minimum distance 3. Derive a contradiction as follows: take a polynomial $f_1(x)$ corresponding to a codeword of weight 3 in C_g , and take a polynomial $f_2(x)$ corresponding to a codeword of weight 3 in the equivalent QR code to C_g guaranteed by Extra Problem 3(d). Show that $f_1(x)f_2(x)$ is nonzero mod $x^{17} - 1$ (hint: 3 is odd), so that it must be congruent to $h(x)$ mod $x^{17} - 1$ (why?), which is visibly impossible.

Remark: One can actually show that the minimum distance of C_g is 5.

Solution: (a) Let's use the hint. Let α be a root of $h(x)$, an irreducible factor of one of the factors of degree 8 on the right side. Then $\alpha^{17} = 1$, and note that α is a root of $x^{2^d} - x$ as well, where d is the degree of h , by Extra Problem 1(c). So $\alpha^{2^d} = \alpha$, so $\alpha^{2^d - 1} = 1$. Now the order of α has to be a divisor of 17, and since $\alpha \neq 1$, it must equal 17. So $17 | 2^d - 1$. Since the order of 2 mod 17 is 8, we must have that $8 | d$. But $d \leq 8$, so $d = 8$. This shows that the factors of degree 8 on the right side can't have any irreducible factors of lower degree, so they are themselves irreducible. \square

(b) We've done this sort of thing in class. The roots of $g(x)$ are

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{15}, \alpha^{13}, \alpha^9.$$

(The exponents are of course just the powers of 2 mod 17.) The maximum number of consecutive powers of α that vanish is 2, so the BCH bound can only show that $d \geq 3$ (one more than the number of consecutive powers that vanish). \square

(c) In fact we can follow the recipe of Extra Problem 3 on the last homework; that is, factor

$$x^{17} - 1 = (x^8 + x^5 + x^4 + x^3 + 1)(x^9 + x^6 + x^5 + x^4 + x^3 + 1),$$

and set $h(x)$ to be the second factor, and then write

$$(x^6 + x^4 + 1)g(x) + (x^5 + x^3)h(x) = 1,$$

and then we get that our p -idempotent generator for C_g is

$$(x^6 + x^4 + 1)g(x) \equiv x^{14} + x^{12} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^3 + 1 \equiv 1 + e_2(x) \pmod{x^{17} - 1}.$$

So C_g is a QR code. \square

(d) The product of two polynomials over \mathbb{F}_2 with an odd number of nonzero terms can never be 0, because the product will have an odd number of nonzero terms. Some of these may sum to 0, but this will remove 2 of the terms at a time. Try it and see! (Modding out by $x^{17} - 1$ will never change the number of terms, because the effect of modding out by $x^{17} - 1$ is to replace any nonzero monomial x^i by $x^{i \bmod 17}$, which is still a nonzero monomial.)

So suppose C_g has minimum weight 3, and take a polynomial $f_1(x)$ corresponding to a codeword in C_g of weight 3, and a polynomial $f_2(x)$ corresponding to a codeword in C'_g of weight 3, where C'_g is the equivalent QR code whose p -idempotent generator is $1 + e_1(x)$. (There will be a codeword of weight 3 in this code if there's one in C_g , because the codes are equivalent.) Then $f_1(x)f_2(x)$ is a multiple of $(1 + e_1(x))(1 + e_2(x)) \equiv h(x)$, so it's either $h(x)$ or 0, but it can't be 0, so it must be $h(x)$. But $f_1(x)f_2(x)$ has at most 9 nonzero terms,

so there's no way it can equal $h(x)$. This is a contradiction. Therefore the minimum weight of C_g is at least 4. \square

Extra Problem 5: If you didn't like the example in Extra Problem 4, try this one:

(a) Consider the polynomial $x^{23} - 1$ in $\mathbb{F}_2[x]$, which factors as

$$(x + 1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1).$$

Show that these factors are irreducible. (Hint: same as Extra Problem 4.)

(b) Let α be a root of the second factor, which we'll call $g(x)$. Which powers of α are also roots of $g(x)$? Write them all down. Show that if C_g is the cyclic code with generating polynomial $g(x)$, then the best that the BCH bound can do is to show $d \geq 5$.

(c) (Extra credit!) Show that C_g is equivalent to \mathcal{G}_{23} , so that its minimum distance is actually 7.

Solution: (a) This really is the same as Extra Problem 4. The point here is that the order of 2 mod 23 is 11. I'll let you fill in the details. \square

(b) Here we get

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^9, \alpha^{18}, \alpha^{13}, \alpha^3, \alpha^6, \alpha^{12}.$$

The maximum number of consecutive powers of α that are roots is 4, so the BCH bound at its best says that $d \geq 5$. \square

(c) If it's extra credit, I don't have to give you the solution. It's in my contract. If you don't like it, take it up with my agent.