

MATH 4450/6450
HOMEWORK 10
DUE 4/20/07

No book problems this time; we've run out!

Your instructions for the extra problems this week are: 4450 students should do Extra Problems 1, 2, 4ab, and 5ab. As usual, 6450 students have to do everything (except for 5c, which is extra credit).

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/>

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 $\mathbb{F}_2[x]$:

$$e_1(x) = \sum_{i \in Q_p} x^i$$

$$e_2(x) = \sum_{j \in N_p} x^j$$

$$h(x) = 1 + x + \cdots + x^{p-1} = 1 + e_1(x) + e_2(x)$$

(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*.

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?)

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.

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.