AM 106/206: Applied Algebra **Prof. Salil Vadhan**

Problem Set 8

Assigned: Wed. Dec. 2, 2009 Due: Wed. Dec. 9, 2009 (1:10 PM sharp)

- You may submit your problem sets in the AM106 in the Maxwell–Dworkin basement, or electronically by email to `am106-hw@seas.harvard.edu`.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details.
- If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`). Name your files `PS8-yourlastname`.
- AM206 students should do the problems marked [AM206-X], and need not do the ones marked [AM106-X]. AM106 students need not do the problems marked [AM206-X], but may do so in place of the corresponding [AM106-X] problem (but not [AM106-Y] for Y $\neq X$) if desired.

Problem 1. (Gallian 20.34, Splitting Fields) Find a splitting field E for the $f(x) = (x^2 + x + 2)(x^2 + 2x + 2)$ over $F = \mathbb{Z}_3$. Write F as a product of linear factors in E. What is $[E : F]$?

Problem 2. (Density of Irreducible Polynomials) Let $F = \mathrm{GF}(q)$, and $E = \mathrm{GF}(q^n)$ for some prime power q.

1. Show that every element $a \in E$ is the zero of an irreducible polynomial in $F[x]$ of degree dividing n. (Hint: consider $[F(a) : F]$.)
2. [AM106-A] Deduce that the number of monic irreducible polynomials in $F[x]$ of degree at most n is at least q^n/n, and the number of monic irreducible polynomials of degree exactly n is at least $q^n/n - q^{n/2}$.
3. [AM206-A] Prove that the number of monic irreducible polynomials in $F[x]$ of degree exactly n is at least $(q^n - 2q^{n/2})/n$. You may use the Möbius inversion formula, which says that if $f, g : \mathbb{N} \to \mathbb{R}$ satisfy $g(n) = \sum_{d|n} f(d)$ for all $n \geq 1$, then $f(n) = \sum_{d|n} \mu(d) g(n/d)$, where $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined as follows:

$$\mu(d) = \begin{cases} 1 & \text{if } d \text{ square-free with an even number of prime factors} \\ -1 & \text{if } d \text{ square-free with an odd number of prime factors} \\ 0 & \text{if } d \text{ not square-free} \end{cases}$$

where a number d is *square free* if $d = p_1 p_2 \cdots p_k$ for distinct primes $p_1, \ldots, p_k$.

Problem 3. (Codes over small alphabets, extra credit) The q-ary *Hadamard code* is the mapping $\mathrm{Had} : \mathrm{GF}(q)^k \to \mathrm{GF}(q)^{q^k}$ taking each $m \in \mathrm{GF}(q)^k$ to the tuple $(\langle m, v_1\rangle, \langle m, v_2\rangle, \ldots, \langle m, v_{q^k}\rangle)$, where $v_1, \ldots, v_{q^k}$ are a list of all elements of $\mathrm{GF}(q)^k$ and $\langle u, v\rangle = \sum_i u_i v_i$. That is, we view m as describing a linear function from $\mathrm{GF}(q)^k \to \mathrm{GF}(q)$ and the codeword is the evaluation of this linear function at all points. This code has very poor rate ($k/2^k$), but it has very good distance (as you will show) and can use very small alphabet sizes (even $q = 2$).

1. Show that the minimum distance of Had is $1 - 1/q$.

2. Combine a Reed-Solomon code over $\mathrm{GF}(2^\ell)$ for some ℓ and a Hadamard code to construct, for every $k = 2^\ell \geq 4$, an error-correcting code $\mathrm{Enc} : \{0,1\}^k \to \{0,1\}^{k^2}$ with minimum distance at least $1/4$. (Hint: view elements of $\{0,1\}^k$ as elements of $(\mathrm{GF}(2^\ell))^{\lceil k/\ell \rceil}$, encode these in a Reed-Solomon code, and then encode each resulting symbol in a Hadamard code.)

The above code has much better rate ($1/k$) than the Hadamard code, but still not constant. Nevertheless, this same approach of combining two codes ("code concatenation") is very widely used, and has been used to construct codes in which the rate, distance, and alphabet size are all constants independent of the message length k.