Mathematics 392 – Seminar in Coding Theory
Final Problem Set
April 26, 2002

Ground Rules

The problems below form the final problem set announced in the course syllabus. This is an open book, open notes, open Swords 335 assignment. You must work *independently* on these problems, and you may not consult with other faculty members or students. You may consult other sources in the library, on the Internet, etc. but if you find something relevant there, please *footnote it*. When you have finished your solutions, please write out a short statement that you have abided by these ground rules, sign it, and return it with your solutions.

This assignment is due no later than *5:00pm on Saturday, May 4*.

I. (20) In class, we stated that if F_1 and F_2 are finite fields of the same size 2^r, then F_1 and F_2 are *isomorphic* – that is, there exists a one-to-one, onto mapping $\phi : F_1 \to F_2$ such that

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b), \text{ and} \\ \phi(a \cdot b) &= \phi(a) \cdot \phi(b) \end{aligned} \tag{1}$$

for all $a, b \in F_1$. (Such a mapping is, in particular, a group homomorphism for the additive groups, so $\phi(0) = 0$ will always be true.) In this problem, you will exhibit such a mapping ϕ explicitly if F_1 is the field of size 8 constructed using the irreducible polynomial $h_1(x) = x^3 + x + 1$ and F_2 is the field of size 8 constructed using the irreducible polynomial $h_2(y) = y^3 + y^2 + 1$.

A) (5) Call the primitive element $x \bmod h_1(x) = \alpha$ in F_1. Show that if ϕ satisfies (1), then $\phi(\alpha)$ must be a root of $x^3 + x + 1 = 0$ in F_2. What choices does this give for $\phi(\alpha)$? To standardize notation, write $\beta = y \bmod h_2(y)$ for the primitive element in F_2, and write the nonzero elements of F_2 as powers of β.
B) (5) If ϕ satisfies the second equation in (1), show that the choice of $\phi(\alpha)$ determines $\phi(\alpha^j)$ for all j.
C) (10) Find a choice of $\phi(\alpha)$ so that both parts of (1) hold for all $a, b \in F_1$.

II. Let C be a binary linear code of block length n and dimension k. The *weight enumerator* of C is the polynomial $W_C(t) = \sum_{i=0}^{n} A_i t^i$ where $A_i = |\{c \in C : \mathrm{wt}(c) = i\}|$. ($W_C(t)$ is the *generating function* of the weight sequence A_i, and is important for more refined study of decoding error probabilities.)

A) (10) Show that the weight enumerator of the binary cyclic code C with $n = 7$ and $g(x) = x^3 + x + 1$ is $W_C(t) = 1 + 7t^3 + 7t^4 + t^7$.

B) (10) Recall that the dual code $C^\perp$ of C is

$$C^\perp = \{y \in \mathbf{F}_2^n : x \cdot y = 0 \bmod 2 \text{ for all } x \in C\}.$$

It is a famous theorem of MacWilliams that the weight enumerators of C and $C^\perp$ are related by the *MacWilliams identity*:

$$2^k W_{C^\perp}(t) = (1+t)^n W_C\left(\frac{1-t}{1+t}\right).$$

Use the MacWilliams identity to find the weight enumerator of the dual of the code from part A.

C) (10) Show that the dual code of the code from part A is also a cyclic code and find its generator polynomial.

III. In this problem you will justify our alternate construction of the Reed-Solomon code $RS(2^r, \delta)$ ($k = 2^r - \delta$), via the evaluation mapping. Let β be a primitive element of $\mathbf{F}_{2^r}$, and define

$$\begin{aligned} ev : \mathrm{Span}\{1, t, \ldots, t^{k-1}\} &\to \mathbf{F}_{2^r}^{2^r-1} \\ p(t) &\mapsto (p(1), p(\beta), \ldots, p(\beta^{2^r-2})) \end{aligned}$$

A) (5) Show that the image of ev is a cyclic code of length $n = 2^r - 1$. (Recall that question B from Discussion 4 gives a criterion for when a code is cyclic.)

B) (5) What happens if you multiply $1 + x + x^2 + \cdots + x^{2^r-2}$ times $x+1$ (mod 2)? What are the roots of $1 + x + x^2 + \cdots + x^{2^r-2} = 0$ in $\mathbf{F}_{2^r}$?

C) (10) The codeword polynomial corresponding to $ev(t^j)$ is $1 + \beta^j x + (\beta^j x)^2 + \cdots + (\beta^j x)^{2^r-2}$. What are the roots of this polynomial in $\mathbf{F}_{2^r}$?

D) (10) Using part C, deduce that the common roots of the codeword polynomials corresponding to $ev(1), ev(t), \ldots, ev(t^{k-1})$ are $\beta, \beta^2, \ldots, \beta^{2^r-2-k+1}$, and explain why this shows that the image of the evaluation map equals the Reed-Solomon code $RS(2^r, \delta)$. (Hint: What is the generator polynomial of this code?)

IV. Let β be a primitive element for $\mathbf{F}_{2^r}$. In the derivation of the Key Equation for decoding of Reed-Solomon codes, we introduced the *set of error locations*, L, the *error values* e_i, the *error locator polynomial*: $\sigma(x) = \prod_{i \in L}(1 - \beta^i x)$ whose roots are β^{-i} for $i \in L$, and the *error evaluator polynomial*: $\omega(x) = \sum_{i \in L} e_i \beta^i \prod_{j \in L, j \neq i}(1 - \beta^j x)$. In this problem, you will prove two important steps in the connection between the Key Equation and decoding.

A) (10) (Lemma 1 from class on 4/19) Show that $\sigma(x)$ and $\omega(x)$ have gcd equal to 1 in $\mathbf{F}_{2^r}[x]$. (Hint: $\sigma(x)$ is given in factored form so we know what its divisors and roots are.)

B) (10) (Lemma 2 from class on 4/19) Show that if the roots of $\sigma(x) = 0$ are known, then we can get the error values by "Forney's formula": For all $\ell \in L$,

$$e_\ell = \frac{\omega(\beta^{-\ell})}{\beta^\ell \prod_{j \in L, j \neq \ell}(1 - \beta^{j-\ell})}.$$

Have an enjoyable, productive summer, and best wishes to the graduating seniors!