MAT 3343, APPLIED ALGEBRA, FALL 2003

Problem Set 6, due Nov 28, 2003

Peter Selinger

Problem 1. Consider the polynomial (7,4)-code with generating polynomial $x^3 + x + 1$ over $\mathbb{Z}_2$.

(a) Make a list of all 16 codewords for this code. Represent them in binary; for instance, $x^6 + x^4 + x^3$ is represented as 1011000.

(b) Encode the message 0011, 1011, 1110.

(c) How many single-bit errors does this code detect? How many does it correct?

(d) Calculate the syndromes for the received codewords 0110110, 1110000, 0110100. Correct all single-bit errors and decode.

(e) Find a generator matrix and a parity check matrix for this code.

Problem 2. Find all the primitive elements in $\mathrm{GF}(16) = \mathbb{Z}_2(\alpha)$, where $\alpha^4 + \alpha + 1 = 0$. [See Handout 5 for a representation of $\mathrm{GF}(16)$].

Problem 3. Let α be a primitive element in $\mathrm{GF}(32)$, where $\alpha^5 = 1 + \alpha^2$. Find irreducible polynomials $p_3(x)$ and $p_5(x)$ in $\mathbb{Z}_2[x]$ such that α^3 is a root of $p_3(x)$, and α^5 is a root of $p_5(x)$. [Note: it might help to first make a table for $\mathrm{GF}(32)$ similar to Handout 5].

Problem 4. Find the generator polynomials of the two- and three-error-correcting BCH codes of length 15 by starting with the primitive element β in $\mathrm{GF}(16)$ where $\beta^4 = 1 + \beta^3$ [NOTE: β is not the same as the element α from Handout 5. There are two ways of approaching this problem. Either find the element β in the table of Handout 5 (hint: $\beta = \alpha^j$ for some j). Or else, make a new representation of $\mathrm{GF}(16)$ based on β.]

Problem 5. Find the generator polynomial of a 2-error-correcting BCH code of length 31.