Math 350
Spring, 2003

Review for the final

Five of these problems will appear in one section of the final, and you will have to do three of them.

1. Construct a Linear Feedback Shift Register of length 4 using the polynomial $g(x) = x^4 + x + 1$, and show how it encodes the message $x^{10} + x^8 + x^7 + x^6 + x^3 + x + 1$.

2. Use induction to prove that $W_{2^n} = \begin{pmatrix} W_{2^{n-1}} & W_{2^{n-1}} \\ W_{2^{n-1}} & -W_{2^{n-1}} \end{pmatrix}$ is a Hadamard matrix for all n ($W_1 = (1)$).

3. Use the $(11, 5, 2)$ design constructed early this semester to construct a Hadamard matrix with 12 rows and columns.

4. The dual of the Hamming code C of length $2^r - 1$ was shown in homework 6 to have a weight enumerator of $W_{C^\perp} = 1 + (2^r - 1)x^{2^{r-1}}$. Use the MacWilliams identities to show that the minimum weight of the Hamming code is $d = 3$ (you need to show that the coefficient on the z and z^2 terms are 0).

5. Construct 3 Latin squares of order 5 that are pairwise Mutually Orthogonal. More points if you can show how to use this to construct a code with length 5, minimum distance 4 (explain how you know your code has this property!).

6. Work through a few steps of a genetic algorithm with a 10 percent mutation rate.

7. Consider the vector space of dimension 5 over the field with 7 elements in it. Let the points of the design be the 1-dimensional subspaces and the lines be the 2-dimensional subspaces. How many points are there? How many lines? How many points per line? How many lines per point? How many lines is each pair of points contained in?

8. Find a minimum weight codeword in the code $RS_3(2, 13)$.

9. Describe your strategy in the game of NIM if you are player 1 and the piles are 5,9, and 13. Explain what this has to do with coding theory.

10. Construct $M_8^{(3)}$, the matrix used in the Green machine to decode the first order Reed-Muller code.

11. Decode 10111100 using the Green machine given in class. Explain how it works.

12. Construct a binary Huffman code for the following frequency chart: A,23; B,11; C,15; D,16; E,26; F,18. Explain how this type of coding is different from the coding we did this semester.

13. Construct the Nordstrom-Robinson code, which is a length 16, $M = 256$, and $d = 6$ binary code, using cyclic codes over Z_4.

14. Describe why there does not exist a $[90, 78, 5]$ linear binary code.

15. Reconstruct the table method decoding procedure for cyclic redundancy check polynomials for length 3.

16. Construct a quadratic residue code of length 31, and explain why it is important to have length that is $\pm 1 \bmod 8$.

17. Calculate the entropy for the discrete random variable X taking on values $0, 1, 2$ or 3 with probabilities $1/8, 1/8, 1/4$, and $1/2$ respectively. Interpret what that number means.

18. Explain why no linear $[12, 5, 5]$ code can exist using the approach of Gilbert-Varshamov.