Math 350
Spring, 2003

HOMEWORK #8

Do 100 points of the following problems (due 4/10/03).

20 pts. **1** Which binary cyclic codes of length 7 contain the vector $(0,1,0,0,1,1,1)$?

$\star$ 50 pts. **2** The Vandermonde matrix has entries $a_{i,j} = b_j^{i-1}$ for $1 \leq i,j \leq n$. Show that the determinant of this matrix is the product $\Pi_{i>j}(b_i - b_j)$. You can get 25 points but no star credit for showing that this works in the $n = 5$ case, but you must do this by hand (no cheating and using Mathematica!).

25 pts. **3** Let $1 + x + x^3$ generate the binary Hamming code of length 7. Use the decoding algorithm discussed in class to decode $1 + x + x^3 + x^4 + x^6$.

25 pts. **4** Let $1 + x + x^4$ generate the binary Hamming code of length 15. Use the decoding algorithm discussed in class to decode $x+x^3+x^5+x^7+x^9+x^{11}$.

30 pts. **5** Find all binary cyclic codes of length 5 by (a) factoring $x^5 + 1$ and (b) computing all idempotents.

30 pts. **6** Use the following Mathematica code to show that the binary cyclic code of length 31 generated by $1+x^3+x^5+x^6+x^8+x^9+x^{10}$ has a minimum distance of at least 5.

```
PolynomialMod[PolynomialRemainder[(y + x)*(y + x^2)*(y + x^(4))*
(y + x^(8))*(y + x^(16)), x^5 + x^2 + 1, x], 2]
```

Make sure you explain why this code helps answer that question! a cyclic code of length 31 with a minimum distance of at least 5. This problem is worth 50 points and $\star$ credit if you can find a binary cyclic code of length 31 and minimum distance at least 7.

20 pts. **7.** A discrete random variable is a variable X that takes a finite number of values, and the probability that it takes those values is predetermined. For example, flipping a coin takes the value 0 for heads with probability 1/2 and the value 1 for tails with probability 1/2. The entropy of a discrete random variable is defined as $\Sigma_X plog(1/p)$ (note: we will only use the logarithm base 2). Calculate the entropy for the discrete random variable described above.