M 375 53420 Final Exam

name:
ssn:
signature:

1. Show that the polynomial \( x^5 + x^2 + 1 \) in \( \mathbb{F}_2[x] \) is irreducible.

1st. Solution:
   If the polynomial \( x^5 + x^2 + 1 \) factors then, looking at the irreducible factor of lowest degree, we see that \( x^5 + x^2 + 1 \) has an irreducible factor of degree at most two. The irreducible polynomials of degree at most two over \( \mathbb{F}_2 \) are \( x, x + 1, x^2 + x + 1 \) and by direct inspection we can see that none of these polynomials divide \( x^5 + x^2 + 1 \), so this polynomial does not factor.

2nd Solution:
   Applying the algorithm taught in class we need to verify that \( x^5 + x^2 + 1 \) is relatively prime with \( x^2 - x \) and \( x^4 - x \) and direct calculation of the gcd’s shows this.
2. Consider the code $C$ over $\mathbb{F}_4 = \mathbb{F}_2[t]/(t^2 + t + 1)$ given as the image in $\mathbb{F}_4^3$ of the linear map $(a, b, c) \mapsto (a, b, c, a + b + c, t^2a + tb + c, ta + t^2b + c)$. Write down a generator matrix, a parity check matrix for $C$ and compute the dimension and minimal distance of $C$.

Solution:

The generator matrix can be obtained by looking at the images of $(100), (010), (001)$ which form a basis for $\mathbb{F}_4^3$, so the matrix is:

$$
\begin{pmatrix}
1 & 0 & 0 & 1 & t^2 & t \\
0 & 1 & 0 & 1 & t & t^2 \\
0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}
$$

The parity check matrix can be obtained by looking at the description of the code, so the 4th entry is the sum of the first three, giving a parity check formula $c_4 = c_1 + c_2 + c_3$ and so on, giving the matrix:

$$
\begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 \\
t^2 & t & 1 & 0 & 1 & 0 \\
t & t^2 & 1 & 0 & 0 & 1
\end{pmatrix}
$$

The dimension is clearly 3.

To compute the minimal distance consider, given $a, b, c$, the polynomial $f(x) = ax^2 + bx + c$. The last four entries in the codeword corresponding to $a, b, c$ are $f(0), f(1), f(t), f(t^2)$. At most two of those can be zero, so we are done unless one of $a, b$ is zero, but then $f(x)$ is linear or the square of a linear polynomial so can have only one zero and again the minimal weight of the codeword is at least 4. Alternatively the minimal distance can be obtained from the parity check matrix.
3. Find all binary linear cyclic codes of length 9.
   Solution:
   It is enough to find the generator polynomials which are divisors of \(x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)\). The polynomials on the left are irreducible (because, for instance 2 has order 2 mod 3 and 6 mod 9). So the factors of \(x^9 - 1\) are 1, \(x - 1\), \(x^2 + x + 1\), \(x^6 + x^3 + 1\), \((x - 1)(x^2 + x + 1)\), \((x^2 + x + 1)(x^6 + x^3 + 1)\), \((x - 1)(x^6 + x^3 + 1)\), \(x^9 - 1\), which give all eight possible binary linear cyclic codes of length 9.
4. Construct a binary linear code of length 5, dimension 2 and minimal distance 3. Show that there does not exist a binary linear code of length 5, dimension 3 and minimal distance 3. Show also that there does not exist a binary linear code of length 5, dimension 2 and minimal distance 4.

Solution:

The code \{((00000), (11100), (00111), (11011))\} is a binary linear code of length 5, dimension 2 and minimal distance 3.

If a binary linear code of length 5, dimension 3 and minimal distance 3 exists, then there is one such in standard form and so it has a generator matrix of the form

$$
\begin{pmatrix}
1 & 0 & 0 & a_{11} & a_{12} \\
0 & 1 & 0 & a_{21} & a_{22} \\
0 & 0 & 1 & a_{31} & a_{32}
\end{pmatrix}
$$

but for it to have minimal distance 3 we need all \(a_{ij} = 1\) but then \((11000) = (10011) + (01011)\) is on the code, contradiction. Alternatively, the sphere packing bound can be used.

The other problem is similar. This time the generator matrix looks like

$$
\begin{pmatrix}
1 & 0 & a_{11} & a_{12} & a_{13} \\
0 & 1 & a_{21} & a_{22} & a_{23}
\end{pmatrix}
$$

Again need all \(a_{ij} = 1\) but then \((11000) = (10111) + (01111)\) is on the code, contradiction.
5. I have encrypted a message with the RSA method using the modulus 100001 and the encryption exponent 85553. The encrypted message is 43603. Using the factorization 100001 = 11 \times 9091 find the decryption exponent and the original message. Read the message using a = 01, b = 02, etc.

Solution:
To find the decryption exponent d we use that 85553d \equiv 1 \pmod{\varphi(100001)} and that 
\varphi(100001) = (11 - 1)(9091 - 1) = 90900. We get that d = 17. So the message is 43603^{17} \pmod{100001} which can be computed by successive squaring. The result is 22505, that is, “bye”.