PROBLEM SET 2: FINITE FIELDS AND LINEAR CODES

HARM DERKSEN

Due, Monday Feb 18.

1. Let $\mathbb{F}_3 = \mathbb{Z}/3$ be the field with 3 elements. The elements of $\mathbb{F}_3$ are represented by 0, 1 and 2.
   (a) Prove that the polynomial $x^2 + 1 \in \mathbb{F}_3[x]$ is irreducible.
   (b) Now $\mathbb{F}_9 := \mathbb{F}_3[x]/(x^2 + 1)$ is a field whose 9 = 3^2 elements can be represented by $a + bx$ with $a, b \in \{0, 1, 2\}$. Fill out the addition and multiplication table below. The entries in the table should be of the form $ax + b$ with $a, b \in \{0, 1, 2\}$.

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>x</th>
<th>x + 1</th>
<th>x + 2</th>
<th>2x</th>
<th>2x + 1</th>
<th>2x + 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>1</td>
<td>2</td>
<td>x</td>
<td>x + 1</td>
<td>x + 2</td>
<td>2x</td>
<td>2x + 1</td>
<td>2x + 2</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x + 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x + 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2x + 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2x + 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. (a) Show that if $C$ is a perfect 1-error correcting $q$-ary code of length $n$, then $n$ must be of the form

$$\frac{q^k - 1}{q - 1}$$

for some $k$.

(b) Suppose that $C$ is a perfect 2-error correcting binary code of length $n$. Show that $n^2 + n + 2$ must be a power of 2.

(c) * Can you find all $n$ for which $n^2 + n + 2$ is a power of 2? (or, say, all $n \leq 100$ for which $n^2 + n + 2$ is a power of 2?) (There are no interesting examples of 2-error correcting perfect binary codes, though.)

3. Show that for every $k$ there exists a binary self-dual $[2k, k]$-code (with minimum distance 2). (Think repeatedly.)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>$x$</th>
<th>$x + 1$</th>
<th>$x + 2$</th>
<th>$2x$</th>
<th>$2x + 1$</th>
<th>$2x + 2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x + 1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x + 2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2x$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2x + 1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2x + 2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(c) For example by using your table, find representants of the form $ax + b$ for the multiplicative inverses of $x^{-1}$, $(x + 1)^{-1}$, $(x + 2)^{-1}$, $(2x)^{-1}$, $(2x + 1)^{-1}$ and $(2x + 2)^{-1}$.

(d) Let $\mathbb{F}_9 := \mathbb{F}_9 \setminus \{0\}$ be the set of nonzero elements of $\mathbb{F}_9$. For which $y \in \mathbb{F}_9$ is it true that

$$\mathbb{F}_9 = \{1, y, y^2, y^3, \ldots, y^8\}?$$

(Such an element is called a generator of the multiplicative group $\mathbb{F}_9$.)
4. (a) Write down the $2 \times 6$ parity check matrix for the $[6, 4]$-Hamming code over $\mathbb{F}_5 := \mathbb{Z}/5$.
   (b) Write down the $4 \times 6$ generator matrix of this code.
5. Recall the field $\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2 + x + 1)$, whose elements can be represented by $\{0, 1, x, x+1\}$. Write down the parity check matrix of the Hamming code over $\mathbb{F}_4$ of wordlength 21.
6. Consider the binary Hamming code with parity check matrix
   $$\begin{pmatrix}
   0 & 0 & 0 & 1 & 1 & 1 \\
   0 & 1 & 1 & 0 & 0 & 1 \\
   1 & 0 & 1 & 0 & 1 & 0
   \end{pmatrix}$$
   Decode the following words
   (a) 1101101
   (b) 1101111
   (c) 0001111