Coding Theory Prelim, May 30, 2009

In $\mathbf{F}_2[x]$,

$$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

$$\begin{aligned} \mathbf{F}_{16} &:= \mathbf{F}_2[\gamma]/\langle 1+\gamma+\gamma^4 \rangle \\ &= \{c_0 + c_1\gamma + c_2\gamma^2 + c_3\gamma^3 : c_i \in \mathbf{F}_2\} \\ &= \{0\} \cup \{\gamma^i : 0 \le i < 15\} \end{aligned}$$

i	c_0	c_1	c_2	c_3
$15 \equiv 0$	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	1	0	0
5	0	1	1	0
6	0	0	1	1
7	1	1	0	1
8	1	0	1	0
9	0	1	0	1
10	1	1	1	0
11	0	1	1	1
12	1	1	1	1
13	1	0	1	1
14	1	0	0	1

In $\mathbf{F}_2[x]$,

$x^{31} - 1 = (x+1)(x^5+x^2+1)(x^5+x^3+1)(x^5+x^4+x^3+x^2+1)\cdot$
$(x^5+x^4+x^3+x+1)(x^5+x^4+x^2+x+1)(x^5+x^3+x^2+x+1)$.

$$\begin{aligned}\mathbf{F}_{32} &:= \mathbf{F}_2[\delta]/\langle 1+\delta^2+\delta^5\rangle \\ &= \{c_0 + c_1\delta + c_2\delta^2 + c_3\delta^3 + c_4\delta^4 : c_i \in \mathbf{F}_2\} \\ &= \{0\} \cup \{\delta^i : 0 \le i < 31\}\end{aligned}$$

i	c_0	c_1	c_2	c_3	c_4
$31 \equiv 0$	1	0	0	0	0
1	0	1	0	0	0
2	0	0	1	0	0
3	0	0	0	1	0
4	0	0	0	0	1
5	1	0	1	0	0
6	0	1	0	1	0
7	0	0	1	0	1
8	1	0	1	1	0
9	0	1	0	1	1
10	1	0	0	0	1
11	1	1	1	0	0
12	0	1	1	1	0
13	0	0	1	1	1
14	1	0	1	1	1
15	1	1	1	1	1
16	1	1	0	1	1
17	1	1	0	0	1
18	1	1	0	0	0
19	0	1	1	0	0
20	0	0	1	1	0
21	0	0	0	1	1
22	1	0	1	0	1
23	1	1	1	1	0
24	0	1	1	1	1
25	1	0	0	1	1
26	1	1	1	0	1
27	1	1	0	1	0
28	0	1	1	0	1
29	1	0	0	1	0
30	0	1	0	0	1

1. Explain, using some reasonable notation how the error e, the syndrome power series s, the error-locator polynomial σ, and the error-evaluator polynomial ρ are related. Include a proof that the error-locator polynomial actually locates error positions.

   Which of these show up where in the following Berlekamp-Massey computation over $\mathbf{F}_{16}$?

0							–	4	–	9	5	4		0	0	–
1						–	4	–	9	5	4		0		2	–
2					–	4	–	9	5	4		0			1	1
3				–	8	–	13	9	8		4				3	1
4			–	12	–	–	13	2		8	–	13			4	3
5		–	10	6	–	–	9		6	2	11				5	4
6	–	8	12	–	–	–		4	8	9	7				6	5

2. Assume λ is a *primitive* $(q-1)$-st *root of 1* in $\mathbf{F}_q$ (and hence generates an index table for $\mathbf{F}_q$).

   (a) Define a *Reed-Solomon code* $RS(q, \delta)$ over $\mathbf{F}_q$ with (*designed*) *minimum distance* δ, by describing a *generator polynomial* $g(x)$ for it, and give its other parameters n, the *wordlength* and k, the *dimension*. Justify these and the fact that $d = \delta$ is the actual minimum distance.

   (b)

$$g(x) := (x-1)(x-\gamma)(x-\gamma^2)(x-\gamma^3)(x-\gamma^4) | m_{\gamma^0}(x) m_{\gamma}(x) m_{\gamma^3}(x)$$

$$= (x+1)(x^4+x+1)(x^4+x^3+x^2+x+1) =: G(x).$$

   Since $G(x) \in \mathbf{F}_2[x]$, it generates a cyclic (sub)code over $\mathbf{F}_2$. What are the parameters (n, k, d) of this code?

3. One of the following matrices generates a *catastrophic convolutional code* and one does not.

$$G_1 := \begin{pmatrix} 1 & 1+x & x \\ 1+x & x & 1 \end{pmatrix}, \quad G_2 := \begin{pmatrix} 1 & 1+x & 0 \\ 1+x & x & 1+x \end{pmatrix}$$

   (a) For the catastrophic code, find a message $\underline{m}$ of infinite weight with corresponding codeword $\underline{c}$ of finite weight.

(b) For the other, produce a finite state table and compute its *minimum free distance.*

4. $x^5 + x^2 + 1 \in \mathbf{Z}_2[x]$ was used to produce the index table for $\mathbf{F}_{32}$ above. Lift this from $\mathbf{F}_2[x]$ to one in $\mathbf{Z}_4[x]$. And lift the corresponding *index table* for $\mathbf{F}_{32}$ to an "index table" over $\mathbf{Z}_4$ as well.

5. State and prove at least one good upper bound and one good lower bound on the size of a linear code – the sphere-packing bound and the Gilbert-Varshamov bound being perhaps the most obvious choices.

6. Given a curve defined by the equation $x^2y+y^2+x=0$ in characteristic 2, find the divisors $div(y)$ and $div(x)$. Pick a point P_∞ at which both have poles, and find as many rational functions (in y and x) that have only poles at P_∞ and with different pole orders there as you can. Make a guess at the genus (that is, the number of "missing" pole orders) based on what you found.

7. Finish the following Berlekamp-Massey-Sakata type row-reduction and shifiting computation ($22 \leq m \leq 26$) relative to the Hermitian curve above and an error of weight 6, and produce a Gröbner basis for the error-locator ideal computed by it. Make sure you explain how you chose the unknown syndrome values.

$$s := \left(\begin{array}{ccccccc}
\gamma^6 & \gamma^7 & \gamma^8 & \gamma^9 & \gamma^{10} & \gamma^{11} & s(x^6) \\
\gamma^9 & \gamma^{13} & \gamma^0 & \gamma^3 & \gamma^8 & s(yx^5) & \\
\gamma^8 & \gamma^4 & \gamma^4 & \gamma^{12} & s(y^2x^4) & & \\
\gamma^{10} & \gamma^{10} & \gamma^7 & & & & \\
\hline
\gamma^{11}+\gamma^9 & s(x^6)+\gamma^{13} & & & & & \\
s(yx^5)+\gamma^8 & & & & & &
\end{array}\right)$$

0	:	γ^0				γ^6		
4	:	γ^1	γ^0			0	0	
						γ^9		
5	:	γ^3	0			0	γ^9	
		γ^0						
8	:	γ^{10}	γ^3	γ^0		0	0	0
		0				0	γ^8	
9	:	γ^3	γ^5			0	0	γ^8
		γ^9	γ^0			0	0	
10	:	γ^0	0	0		0	0	0
		γ^5	0			0	0	
		γ^0				0		
12	:	γ^{12}	γ^{13}	γ^9	γ^0	0	0	0
		0	0			0	0	
		0				0		
13	:	γ^2	γ^6	γ^5	0	0	0	0
		γ^{11}	γ^3	γ^0		0		
		0						