Coding Theory

Sheet 3 Solutions

Spring and Summer 2010

1. Let $\mathbf{F}_4 = \{0, 1, \omega, \bar{\omega} = \omega^2 = \omega + 1\}$.

$+$	0	1	ω	$\bar{\omega}$
0	0	1	ω	$\bar{\omega}$
1	1	0	$\bar{\omega}$	ω
ω	ω	$\bar{\omega}$	0	1
$\bar{\omega}$	$\bar{\omega}$	ω	1	0

$\times$	0	1	ω	$\bar{\omega}$
0	0	0	0	0
1	0	1	ω	$\bar{\omega}$
ω	0	ω	$\bar{\omega}$	1
$\bar{\omega}$	0	$\bar{\omega}$	1	ω

2. An element is primitive in $\mathbf{F}_q$ if it generates the cyclic group; that is, it has order $q-1$. Note, also, that the order of x divides $q-1$ and the order of x^{-1} is the same as the order of x. As a check, the number of generators of a cyclic group of order $q-1$ is $\phi(q-1)$, where $\phi(n)$ is the Euler function that counts the number of positive integers coprime to n.

   (a) In $\mathbf{F}_5$,

x	1	2	-2	-1
order of x	1	4	4	2

   So the primitive elements are $2, -2$.

   (b) In $\mathbf{F}_7$,

x	1	2	3	-3	-2	-1
order of x	1	3	6	3	6	2

   So the primitive elements are $3, -2$.

   (c) In $\mathbf{F}_{13}$,

x	1	2	3	4	5	6	-6	-5	-4	-3	-2	-1
order of x	1	12	3	6	4	12	12	4	3	6	12	2

   So the primitive elements are $2, 6, -6, -2$.

   (d) In $\mathbf{F}_{17}$,

x	1	2	3	4	5	6	7	8	-8	-7	-6	-5	-4	-3	-2	-1
order of x	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

   So the primitive elements are $\pm 3, \pm 5, \pm 6, \pm 7$.

3. By the Binomial Theorem,

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{r} x^{p-r} y^r + \cdots + \binom{p}{p-1} x y^{p-1} + y^p.$$

For $1 \le r \le p-1$,

$$\binom{p}{r} = \frac{p(p-1)\cdots(p-r+1)}{r(r-1)\cdots 3\cdot 2}.$$

As p is prime and $p > r$, so none of $r, r-1, \ldots, 2$ divide p. Hence p divides $\binom{p}{r}$, which is therefore zero in $\mathbf{F}_p$ and $\mathbf{F}_q$. So

$$(x+y)^p = x^p + y^p.$$

4. A monic quadratic in $\mathbf{F}_3[X]$ is $X^2 + bX + c$ with $b, c \in \{0, 1, -1\}$. The reducible ones are

$$\begin{array}{l} X^2,\ (X-1)^2 = X^2 + X + 1,\ (X+1)^2 = X^2 - X + 1, \\ X(X-1) = X^2 - X,\ X(X+1) = X^2 + X,\ (X-1)(X+1) = X^2 - 1. \end{array}$$

This leaves the $9 - 6 = 3$ irreducibles:

$$X^2 + 1,\ X^2 - X - 1,\ X^2 - X + 1.$$

Take $X^2 + 1$ and let $\tau^2 + 1 = 0$; then $\tau^2 = -1$, and $\tau^4 = 1$. So $X^2 + 1$ is not primitive since the order of τ is not 8.

Take $X^2 - X - 1$ and let $\sigma^2 - \sigma - 1 = 0$. Then the elements of $\mathbf{F}_9$ are $0, 1, \sigma$,

$$\begin{array}{l} \sigma^2 = \sigma + 1, \quad \sigma^3 = \sigma^2 + \sigma = -\sigma + 1, \\ \sigma^4 = -\sigma^2 + \sigma = -1, \quad \sigma^5 = -\sigma, \quad \sigma^6 = -\sigma^2 = -\sigma - 1, \\ \sigma^7 = -\sigma^2 - \sigma = \sigma - 1, \quad \sigma^8 = \sigma^2 - \sigma = 1. \end{array}$$

So $X^2 - X - 1$ is primitive. Similarly, $X^2 + X - 1$ is primitive.

(a)

x	1	σ	σ^2	σ^3	$-\sigma^3$	$-\sigma^2$	$-\sigma$	-1
order of x	1	8	4	8	8	4	8	2

(b)

x	1	-1	τ	$-\tau$	$1+\tau$	$1-\tau$	$-1+\tau$	$-1-\tau$
order of x	1	2	4	4	8	8	8	8

(c) From Theorem 3.9, the automorphisms of $\mathbf{F}_9$ are the identity and $x \mapsto x^3$. The zeros of $X^2 - X - 1$ are σ, σ^3. For an automorphism of $\mathbf{F}_9$, the element σ must map to another element that has order 8 and is a zero of $X^2 - X - 1$. Now,

$$(-1+\tau)^2 = 1 - 2\tau + \tau^2 = \tau = (-1+\tau) + 1.$$

So $-1+\tau$ is a zero of X^2-X-1; the other is therefore $-1-\tau$.

Therefore an isomorphism between these two representations of $\mathbf{F}_9$ is either $\sigma \mapsto -1+\tau$ or $\sigma \mapsto -1-\tau$.

If in (a) the polynomial X^2-X+1 is chosen, let a zero be ρ. Then an isomorphism would be $\rho \mapsto 1+\tau$ or $\rho \mapsto 1-\tau$.

5. A cubic in $\mathbf{F}_2[X]$ is X^3+bX^2+cX+d with $b,c,d \in \{0,1\}$. Recall that the only irreducible quadratic is X^2+X+1. Hence the reducible cubics are

$$X^3,\ (X+1)^3 = X^3+X^2+X+1,\ X^2(X+1) = X^3+X^2,\ X(X+1)^2 = X^3+X,$$
$$X(X^2+X+1) = X^3+X^2+X,\ (X+1)(X^2+X+1) = X^3+1$$

This leaves the $8-6=2$ irreducibles:

$$X^3+X+1, \quad X^3+X^2+1.$$

As 7 is a prime, a zero of one of these can only have order 7. So, both are primitive.

6. Since X^4+1 has no zeros in $\mathbf{F}_3$, it has no linear factors. So, if it is reducible it can only be the product of two irreducible quadratics; the latter were found in Question 3. In fact,

$$X^4+1 = (X^2+X-1)(X^2-X-1)$$

7. Similarly to Question 4, there are three irreducible quartics in $\mathbf{F}_2[X]$:

$$X^4+X+1, \quad X^4+X^3+1, \quad X^4+X^3+X^2+X+1.$$

The first two are primitive; the third is not. With $\alpha^4+\alpha+1=0$, the elements of $\mathbf{F}_{16}$ are $0,1,\alpha,\alpha^2,\alpha^3$,

$$\begin{aligned}
\alpha^4 &= \alpha+1,\\
\alpha^5 &= \alpha^2+\alpha,\\
\alpha^6 &= \alpha^3+\alpha^2,\\
\alpha^7 &= \alpha^4+\alpha^3 = \alpha^3+\alpha+1,\\
\alpha^8 &= \alpha^4+\alpha^2+\alpha = \alpha^2+1,\\
\alpha^9 &= \alpha^3+\alpha,\\
\alpha^{10} &= \alpha^4+\alpha^2 = \alpha^2+\alpha+1,\\
\alpha^{11} &= \alpha^3+\alpha^2+\alpha,\\
\alpha^{12} &= \alpha^4+\alpha^3+\alpha^2 = \alpha^3+\alpha^2+\alpha+1,\\
\alpha^{13} &= \alpha^4+\alpha^3+\alpha^2+\alpha = \alpha^3+\alpha^2+1,\\
\alpha^{14} &= \alpha^4+\alpha^3+\alpha = \alpha^3+1,\\
\alpha^{15} &= \alpha^4+\alpha = 1.
\end{aligned}$$

8. (i) Any monic quadratic in $\mathbf{F}_q[X]$ has the form $X^2 + bX + c$; so there are q^2 of them. If it is reducible, it has the form

$$(X - \alpha)(X - \beta).$$

If $\alpha \neq \beta$, there are $\binom{q}{2}$ of them. If $\alpha = \beta$, there are q of them. So the number of reducibles is

$$\tfrac{1}{2}q(q-1) + q = \tfrac{1}{2}q(q+1),$$

and so the number of irreducibles is

$$q^2 - \tfrac{1}{2}q(q+1) = \tfrac{1}{2}q(q-1).$$

Alternatively, the elements of $\mathbf{F}_{q^2} \backslash \mathbf{F}_q$ split into $\frac{1}{2}(q^2 - q)$ pairs of zeros of irreducible quadratics in $\mathbf{F}_q[X]$.

(ii) This is a similar argument. The number of monic cubics is q^3. The number reducible to three linear factors is

$$\begin{array}{llll} q & \text{like} & (X-\alpha)^3, & \\ q(q-1) & \text{like} & (X-\alpha)(X-\beta)^2 & \text{with } \alpha \neq \beta, \\ q(q-1)(q-2)/6 & \text{like} & (X-\alpha)(X-\beta)(X-\gamma) & \text{with } \alpha, \beta, \gamma \text{ distinct,} \end{array}$$

totalling $\frac{1}{6}q(q^2 + 3q + 2)$.

The number of cubics that are the product of a linear factor and an irreducible quadratic is

$$q \times \tfrac{1}{2}q(q-1) = \tfrac{1}{2}q^2(q-1).$$

Hence the number of irreducible cubics is

$$q^3 - \tfrac{1}{6}q(q^2 + 3q + 2) - \tfrac{1}{2}q^2(q-1) = \tfrac{1}{3}(q^3 - q).$$

9. (i) $x_1 \ldots x_{10} = 3411021756$ implies that

$$\begin{aligned} \sum ix_i &= 3 + 8 + 3 + 4 + 0 + 12 + 7 + 56 + 45 + 60 \\ &= 3 - 3 + 3 + 4 + 0 + 1 - 4 + 1 + 1 + 5 = 0 \text{ in } \mathbf{F}_{11}. \end{aligned}$$

So, it is an ISBN.

(ii) $x_1 \ldots x_{10} = 285036008X$ implies that

$$\begin{aligned} \sum ix_i &= 2 + 16 + 15 + 0 + 15 + 36 + 0 + 0 + 72 + 100 \\ &= 2 + 5 + 4 + 4 + 3 + 6 + 1 = 25 = 3 \text{ in } \mathbf{F}_{11}. \end{aligned}$$

So, it is not an ISBN-10.

10. $x_1 \ldots x_{10} = 0521283t87$ implies that

$$\begin{aligned} \sum ix_i &= 0 + 10 + 6 + 4 + 10 + 48 + 21 + 8t + 72 + 70 \\ &= 8t - 1 \text{ in } \mathbf{F}_{11}. \end{aligned}$$

So, if it is an ISBN-10, then $8t - 1 = 0$, whence $t = 7$.

11. As 9 digits determine the tenth in an ISBN-10, the minimum distance is greater than 1. If one of the first nine digits in an ISBN-10 is changed, then the check digit can be calculated to make a new ISBN-10; so the minimum distance of the ISBN-10 code is 2. Alternatively, $00\ldots0$ and $150\ldots0$, say, are at distance 2.

12.

$$\begin{array}{ccccccccccccccc} 9 & 7 & 8 & 8 & 8 & 4 & 7 & 0 & 0 & 5 & 3 & 9 & 6 & \\ 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & \\ \hline 9 & 1 & 8 & 4 & 8 & 2 & 7 & 0 & 0 & 5 & 3 & 7 & 6 & = 60 \end{array}$$

So it is a valid ISBN-13.

13. (i)

$$\begin{array}{cccccccccccccccc} 4 & 5 & 3 & 9 & 2 & 7 & 8 & 6 & 4 & 1 & 3 & 2 & 1 & 2 & 7 & x \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ \hline 8 & 5 & 6 & 9 & 4 & 7 & 6 & 6 & 8 & 1 & 6 & 2 & 2 & 2 & 4 & x \end{array}$$

Positions $7, 15$ have digits at least 5. So

$$76 + x + 2 \equiv 0 \pmod{10} \Rightarrow x = 2.$$

So the codabar number is 4539 2786 4132 1272.

(ii)

$$\begin{array}{cccccccccccccccc} 4 & 9 & 2 & 9 & x & 4 & 6 & 2 & 7 & 3 & 4 & 1 & 3 & 4 & 7 & 8 \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ \hline 8 & 9 & 4 & 9 & 2x & 4 & 2 & 2 & 4 & 3 & 8 & 1 & 6 & 4 & 4 & 8 \end{array}$$

Positions $7, 9, 15$ have digits at least 5. There are two possibilities:

(a) The fifth digit is at least 5; in this case,

$$76 + 2x + 4 \equiv 0 \pmod{10} \Rightarrow x = 5.$$

(b) The fifth digit is at most 4; in this case,

$$76 + 2x + 3 \equiv 0 \pmod{10}, \quad \text{impossible}.$$

So the codabar number is 4929 5462 7341 3478.