C&O 331: Assignment #2 solutions

---

1. Without loss of generality, let the alphabet be $A = \mathbb{Z}_q$ (the set of integers modulo q).

   (a) Since codewords are n-tuples over $\mathbb{Z}_q$, and there are q^n n-tuples in total, the number of codewords in any code of length n over $\mathbb{Z}_q$ is at most q^n. Hence $T_q(n,d) \le q^n$.

   (b) The code consisting of all the n-tuples over $\mathbb{Z}_q$ has distance $d = 1$; hence $T_q(n,1) \ge q^n$. By (a), we have $T_q(n,1) \le q^n$. Thus $T_q(n,1) = q^n$.

   (c) The code consisting of the q codewords $(0,0,0,\ldots,0)$, $(1,1,1,\ldots,1)$, $(2,2,2,\ldots,2)$, $\ldots(q-1,q-1,q-1,\ldots,q-1)$ has distance n, so $T_q(n,n) \ge q$.
   Suppose now that $c_1, c_2, \ldots c_{q+1}$ are pairwise distinct words of length n over $\mathbb{Z}_q$. Consider the symbols in the first coordinate position in each of these words. Since there are q symbols in $\mathbb{Z}_q$, at least two of the words must have the same symbol in the first coordinate position; without loss of generality, suppose that c_1 and c_2 have the same symbol in the first coordinate position. Then $d(c_1, c_2) \le n-1$. This shows that any code over $\mathbb{Z}_q$ having more than q codewords has distance at most $n-1$.
   Hence $T_q(n,n) = q$.

2. (a) $q = 5^5 = 3125$.

   (b) The polynomials in $\mathbb{Z}_5[x]$ of degree less than 5.

   (c) 5.

   (d) $2x^4 + 4x^3 + x + 4$.

   (e) Consider a as a polynomial $a(x)$. We need to find a solution to the polynomial Diophantine equation $f(x)s(x) + a(x)t(x) = 1$. Using the Extended Euclidean Algorithm, we get a table of the form

$s(x)$	$t(x)$	$f(x)s(x) + a(x)t(x)$
1	0	$x^5 + 4x + 2$
0	1	$2x^2 + 3$
1	$2x^3 + 2x$	2
$4x^2 + 1$	$3x^5 + 2x + 1$	0

   Multiplying the second-last row by 3 gives the solution $s(x) = 3$ and $t(x) = x^3 + x$, from which we see that $a^{-1} = t = x^3 + x$.

   (f) By the Freshman's dream, $(x+4)^5 = (x^5+4) = x+2$. Since $6249 = q + (q-1)$, it follows that

$$(4x^3+2x^2+x+4)^{6249} = (4x^3+2x^2+x+4)^{3125}(4x^3+2x^2+x+4)^{3124} = (4x^3+2x^2+x+4)(1) = 4x^3+2x^2+x+4$$

   Hence the answer is $(x+2)(4x^3+2x^2+x+4) = 4x^4 + x + 3$.

3. (a) Long division of $f(x)$ by $(x-a)$ yields polynomials $l(x), r(x) \in F[x]$ such that

$$f(x) = l(x)(x-a) + r(x), \text{ where } \deg(r) < 1, \tag{1}$$

   i.e., $r(x)$ is a constant polynomial, say $r(x) = c$. Now, substituting $x = a$ in (1) yields $f(a) = c$. Hence $f(a) = 0 \Leftrightarrow c = 0 \Leftrightarrow (x-a) | f(x)$.

(b) Degree 1: x, $x+1$.
Degree 2: x^2+x+1.
Degree 3: x^3+x+1, x^3+x^2+1.
Degree 4: x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$.

4. (a) Since f has degree 3, it is irreducible if and only if it has a linear factor. From part 2a), it has a linear factor if and only if $f(a)=0$ for some $a=0,1,2$. But $f(0)=2$, $f(1)=2$, and $f(2)=2$. Hence, f is irreducible.

(b) A primitive element in $GF(3^3)$ has order 26. We are given that x has order 13. Also, $-1=2$ has order 2. Since 2 and 13 are coprime, $2x$ must have order $2\cdot 13=26$ and hence is primitive.

(c)

Order	# of Elements
1	1
2	1
13	12
26	12

5. (a) Assume that $\alpha^i=\alpha^j$ for $0\le i<j\le t-1$. Then $\alpha^{j-i}=1$. But $0<j-i\le t-1$, which contradicts $\mathrm{ord}(\alpha)=t$. Hence $\alpha^0,\alpha^1,\ldots,\alpha^{t-1}$ are pairwise distinct.

(b) By the division algorithm, we can write $s=qt+r$ where $q,r\in\mathbb{Z}$ and $0\le r<t$. We have

$$\alpha^s=\alpha^{qt+r}=(\alpha^t)^q\alpha^r=1^q\alpha^r=\alpha^r.$$

Now, if $\alpha^s=1$, then $\alpha^r=1$. If $r\neq 0$ then $\alpha^r=1$ and $0<r<t$ would contradict the definition of t. Thus $r=0$ and so $t\mid s$.
Conversely, suppose that $t\mid s$. Then $r=0$ so $\alpha^s=\alpha^0=1$.

(c) Let $t=\mathrm{ord}(\alpha)$ and $s=\mathrm{ord}(\alpha^{-1})$. Now,

$$\alpha^s=(\alpha^{-1})^{-s}=\frac{1}{(\alpha^{-1})^s}=\frac{1}{1}=1.$$

Hence $t\mid s$. Similarly, $(\alpha^{-1})^t=\alpha^{-t}=1/\alpha^t=1/1=1$; hence $s\mid t$. We conclude that $t=s$.