ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

Handout 20 Introduction to Communication Systems

Solutions to Homework 13 December 24, 2008

PROBLEM 1. (a) $5^0 \equiv 1 \pmod 7$, $5^1 \equiv 5 \pmod 7$, $5^2 \equiv 4 \pmod 7$, $5^3 \equiv 6 \pmod 7$, $5^4 \equiv 2 \pmod 7$, $5^5 \equiv 3 \pmod 7$. Since $\phi(7) = 6$ and $\gcd(5, 7) = 1$, from the Euler's theorem we have,

$$5^6 \equiv \quad \pmod 7$$

(b) One can see from the previous part that $5^k \not\equiv 1 \pmod 7$ for $0 < k < 6$. Since $\phi(7) = 6$, and $\gcd(5^k, 7) = 1$ for any k we have from the Euler's theorem,

$$5^{6k} = (5^k)^6 \equiv 1 \pmod 7$$

(c) Clearly,

$$\begin{aligned}(5^k - 1)(1 + 5^k + 5^{2k} + 5^{3k} + 5^{4k} + 5^{5k}) &= 5^k(1 + 5^k + 5^{2k} + 5^{3k} + 5^{4k} + 5^{5k}) \\ &\quad - (1 + 5^k + 5^{2k} + 5^{3k} + 5^{4k} + 5^{5k}) \\ &= 5^{6k} - 1 = 0\end{aligned}$$

The last equality follows from the previous part. This implies that

$$(5^k - 1)\sum_{i=0}^{5} 5^{ki} = 0$$

Again, from the previous part we know that $5^k \not\equiv 1 \pmod 7$ for $0 < k < 6$, this implies that

$$\sum_{i=0}^{5} 5^{ki} = 0$$

for $0 < k < 6$. For $k = 0$ we have

$$\sum_{i=0}^{5} 5^{ki} = 1 + 1 + 1 + 1 + 1 + 1 \equiv 6 \pmod 7$$

(e) From the definition of Fourier transform we have,

$$\hat{u}_i = \sum_{l=0,1,\ldots,5} u_l 3^{il}$$

Performing all computations modulo 7, we have

$$\begin{aligned}
\hat{u}_0 &= \sum_{l=0,1,\ldots,5} u_l 3^{0l} = \sum_{l=0,1,\ldots,5} u_l = 0 \\
\hat{u}_1 &= \sum_{l=0,1,\ldots,5} u_l 3^{1l} = 3 \\
\hat{u}_2 &= \sum_{l=0,1,\ldots,5} u_l 3^{2l} = 6 \\
\hat{u}_3 &= \sum_{l=0,1,\ldots,5} u_l 3^{3l} = 4 \\
\hat{u}_4 &= \sum_{l=0,1,\ldots,5} u_l 3^{4l} = 2 \\
\hat{u}_5 &= \sum_{l=0,1,\ldots,5} u_l 3^{5l} = 5
\end{aligned}$$

(f) From the definition of the inverse Fourier transform we have

$$u_j = 6 \sum_{i=0,1,\ldots,5} \hat{u}_i 5^{ij}$$

Since $\hat{u}_i$ is the i^{th} component of the Fourier transform of u, we use the its definition to get

$$u_j = 6 \sum_{i=0,1,\ldots,5} \sum_{l=0,1,\ldots,5} u_l 3^{il} 5^{ij}$$

Since $5 \cdot 3 \equiv 1 \pmod 7$, 3 is the inverse of 5, i.e. $3 = 5^{-1}$ modulo 7. Thus we have

$$\begin{aligned}
u_j = 6 \sum_{i=0,1,\ldots,5} \sum_{l=0,1,\ldots,5} u_l 5^{-il} 5^{ij} &= 6 \sum_{i=0,1,\ldots,5} \sum_{l=0,1,\ldots,5} u_l 5^{i(j-l)} \\
= \sum_{l=0,1,\ldots,5} u_l 6 \sum_{i=0,1,\ldots,5} (5^{(j-l)})^i &
\end{aligned}$$

where in the last equality we exchanged the order of two summations.

Now using the results of part (c) we know that $j = l$ implies $\sum_{i=0,1,\ldots,5} (5^{(j-l)})^i = 6 \pmod 7$ and $6 \cdot 6 = 36 \equiv 1 \pmod 7$. Also for $j \neq l$ we have

$$\sum_{i=0,1,\ldots,5} (5^{(j-l)})^i = \sum_{i=0,1,\ldots,5} (5^{ki})$$

where $0 < |k| < 6$. Thus if $k > 0$ then from the results of part (c) we have that

$$\sum_{i=0,1,\ldots,5} (5^{ki}) = 0$$

if $k < 0$, then we know that $5^{-1} = 3$, thus

$$\sum_{i=0,1,\ldots,5} (5^{ki}) = \sum_{i=0,1,\ldots,5} (3^{-ki})$$

Here $0 < -k < 6$. One can easily verify that the results of part (c) are valid if we replace 5 by 3, thus we get

$$\sum_{i=0,1,\ldots,5} (3^{-ki}) = 0$$

and hence

$$u_j = \sum_{l=0,1,\ldots,5} u_l 6 \sum_{i=0,1,\ldots,5} (5^{(j-l)})^i = u_j$$

(g) (i) Cyclic convolution y, of two vectors u, v is given by,

$$y[n] = \sum_{m=0,1,\ldots,5} u[m]v[n-m \pmod 6]$$

Note that here the signals are periodic with period 6. Thus we have

$$\begin{aligned}
y[0] &= \sum_{m=0,1,\ldots,5} u[m]v[-m \pmod 6] \\
&= u[0]v[0] + u[1]v[5] + u[2]v[4] + u[3]v[3] + u[4]v[2] + u[5]v[1] = 5 \\
y[1] &= \sum_{m=0,1,\ldots,5} u[m]v[1-m \pmod 6] \\
&= u[0]v[1] + u[1]v[0] + u[2]v[5] + u[3]v[4] + u[4]v[3] + u[5]v[2] = 2 \\
y[2] &= \sum_{m=0,1,\ldots,5} u[m]v[2-m \pmod 6] \\
&= u[0]v[2] + u[1]v[1] + u[2]v[0] + u[3]v[5] + u[4]v[4] + u[5]v[3] = 5 \\
y[3] &= \sum_{m=0,1,\ldots,5} u[m]v[3-m \pmod 6] \\
&= u[0]v[3] + u[1]v[2] + u[2]v[1] + u[3]v[0] + u[4]v[5] + u[5]v[4] = 2 \\
y[4] &= \sum_{m=0,1,\ldots,5} u[m]v[4-m \pmod 6] \\
&= u[0]v[4] + u[1]v[3] + u[2]v[2] + u[3]v[1] + u[4]v[0] + u[5]v[5] = 5 \\
y[5] &= \sum_{m=0,1,\ldots,5} u[m]v[5-m \pmod 6] \\
&= u[0]v[5] + u[1]v[4] + u[2]v[3] + u[3]v[2] + u[4]v[1] + u[5]v[0] = 2 \qquad (1)
\end{aligned}$$

(ii) Fourier transform of u is given by

$$\begin{aligned}
\hat{u}_0 &= \sum_{l=0,1,\ldots,5} u_l 3^{0l} = \sum_{l=0,1,\ldots,5} u_l = 0 \\
\hat{u}_1 &= \sum_{l=0,1,\ldots,5} u_l 3^{1l} = 3 \\
\hat{u}_2 &= \sum_{l=0,1,\ldots,5} u_l 3^{2l} = 6 \\
\hat{u}_3 &= \sum_{l=0,1,\ldots,5} u_l 3^{3l} = 4 \\
\hat{u}_4 &= \sum_{l=0,1,\ldots,5} u_l 3^{4l} = 2 \\
\hat{u}_5 &= \sum_{l=0,1,\ldots,5} u_l 3^{5l} = 5
\end{aligned}$$

The Fourier transform of v is given by

$$\begin{aligned}
\hat{v}_0 &= \sum_{l=0,1,\ldots,5} v_l 3^{0l} = \sum_{l=0,1,\ldots,5} v_l = 2 \\
\hat{v}_1 &= \sum_{l=0,1,\ldots,5} v_l 3^{1l} = 0 \\
\hat{v}_2 &= \sum_{l=0,1,\ldots,5} v_l 3^{2l} = 0 \\
\hat{v}_3 &= \sum_{l=0,1,\ldots,5} v_l 3^{3l} = 4 \\
\hat{v}_4 &= \sum_{l=0,1,\ldots,5} v_l 3^{4l} = 0 \\
\hat{v}_5 &= \sum_{l=0,1,\ldots,5} v_l 3^{5l} = 0
\end{aligned}$$

Multiplying $\hat{u}$ and $\hat{v}$ component wise we get

$$\begin{aligned}
\hat{w}_0 &= \hat{u}_0\hat{v}_0 = 0 \\
\hat{w}_1 &= \hat{u}_1\hat{v}_1 = 0 \\
\hat{w}_2 &= \hat{u}_2\hat{v}_2 = 0 \\
\hat{w}_3 &= \hat{u}_3\hat{v}_3 = 16 = 2 \pmod 7 \\
\hat{w}_4 &= \hat{u}_4\hat{v}_4 = 0 \\
\hat{w}_5 &= \hat{u}_5\hat{v}_5 = 0
\end{aligned}$$

We take the inverse Fourier transform of $\hat{w} = (000200)$ is given by $w = (525252)$ which matches the original calculation in equation (1).

(h) (a) For the canonical definition of RS codes, we consider n non-zero distinct elements $(a_0, a_1, \ldots, a_{n-1})$ of the field F_q where $n < q$. Then we consider all polynomials $A(x)$ of degree at most $k-1$ and then evaluate $(A(a_0), A(a_1), \ldots, A(a_{n-1}))$ to form the code of length n and dimension k. Here $n = 6$ and $q = 7$. Thus clearly the only 6 non-zero distinct elements are $1, 2, 3, 4, 5, 6$. Also since $k = 2$ we have that $A(x) = c_1 + c_2 x$ where both $c_1, c_2 \in F_7$. Thus there are 49 codewords.

Now we know from the previous part (a) that 3 is a *generator* of the field F_7, i.e. 3^i for $0 \leq i \leq 5$ covers all the non-zero elements of the field F_7. Indeed this is easily checked: $3^0 \equiv 1 \pmod 7, 3^1 \equiv 3 \pmod 7, 3^2 \equiv 2 \pmod 7, 3^3 \equiv 6 \pmod 7, 3^4 \equiv 4 \pmod 7, 3^5 \equiv 5 \pmod 7$.

Now consider the Fourier transform of the set $\hat{c} = (c_1, c_2, 0, 0, 0)$ for $c_1, c_2 \in F_7$. We have

$$\begin{aligned}\hat{\hat{c}}_i &= \sum_{j=0,1,\ldots,5} \hat{c}_j 3^{ij} \\ &= c_1 + c_2 3^i\end{aligned}$$

The equivalence of the definitions is now got as follows: let the 6 distinct, non-zero elements required for the canonical definition of RS codes be given by

$$a_0 = 3^0 \equiv 1; a_1 = 3^1 \equiv 3; a_2 = 3^2 \equiv 2; a_3 = 3^3 \equiv 6; a_4 = 3^4 \equiv 4; a_5 = 3^5 \equiv 5.$$

Thus according to the canonical definition of RS codes, a codeword is given by

$$y_i = c_1 + c_2 3^i$$

which is exactly the Fourier transform of the set $\hat{c} = (c_1, c_2, 0, 0, 0, 0)$.

(b) Code is generated by the generator matrix G as follows: consider the vector $u = (u_1, \ldots, u_k)$, where k is the dimension of the code and each $u_i \in F_q$. Then a codeword x is given by $u \cdot G$. Here $k = 2, q = 7$. Thus we have $u = (u_1, u_2)$ and the codeword x is given by

$$x_i = u_1 g_{1i} + u_2 g_{2i} \pmod 7 \tag{2}$$

where (g_{1i}, g_{2i}) is the i^{th} column of the matrix G.

From the Fourier transform definition of the RS code, we see that

$$x_i = u_1 + u_2 3^i$$

where $u_1, u_2 \in F_7$. Thus together with equation (2), this implies that the i^{th} column of G is given by $(1, 3^i)$. One easily verifies that G is thus given by

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}.$$

(c) The codeword is given by

$$x_i = 1 + 4 \cdot 3^i \pmod 7$$

Thus

$$x_0 = 5; x_1 = 6; x_2 = 2; x_3 = 4; x_4 = 3; x_5 = 0$$

Thus the transmitted codeword is given by $(5, 6, 2, 4, 3, 0)$.

(d) Let us denote the codeword by $x = (x_0, x_1, x_2, x_3, x_4, x_5)$. Using the generator matrix definition of the code we get,

$$c_1 + 3c_2 = 4 \quad (3)$$
$$c_1 + 6c_2 = 6 \quad (4)$$
$$c_1 + 4c_2 = 0 \quad (5)$$

Solving equation (1), (2) we get $c_1 = 2, c_2 = 3$. Thus the transmitted codeword is given by (541603).

PROBLEM 2 (HAMMING BOUND). (i) If we take a codeword c and flip its values at some j positions, we get a word which is at a Hamming distance j from the codeword c. There are $\binom{n}{j}$ ways of selecting j positions amongst n positions. Thus the number of words at a Hamming distance j from the codeword c is given by $\binom{n}{j}$. Thus the number of words contained in a sphere of radius i around c is given by

$$\sum_{j=0}^{i} \binom{n}{j}$$

(ii) If suppose the spheres of radius $t = \lfloor\frac{d-1}{2}\rfloor$ around two codewords x, y overlap, then there exists a word z such that $d(x,z) \leq \lfloor\frac{d-1}{2}\rfloor$ and $d(y,z) \leq \lfloor\frac{d-1}{2}\rfloor$. Since Hamming distance is a true distance, from the triangle inequality for distances we have

$$d(x,y) \leq d(x,z) + d(y,z) \leq \lfloor\frac{d-1}{2}\rfloor + \lfloor\frac{d-1}{2}\rfloor \leq d-1$$

But this is a contradiction, since the minimum distance between any two codewords is d.

(iii) & (iv) Consider sphere of radius $t = \lfloor\frac{d-1}{2}\rfloor$ around all codewords. From the answer to the above part, we have that none of these spheres overlap. As a result the total number of words contained in all the spheres must be less than the total words of length n possible. The total words of length n are 2^n. Let $A(n,d)$ be the total number of codewords. Since $\sum_{i=0}^{t} \binom{n}{i}$ is the total number of words in a sphere of radius t, we get

$$A(n,d) \sum_{i=0}^{t} \binom{n}{i} \leq 2^n$$
$$A(n,d) \leq \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}}$$

proving the Hamming bound.