ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 23 Introduction to Communication Systems
Graded Homework 4. **Due Date: Before 12:00pm (lunch-time), Friday, December 19, 2008** December 4, 2008

PROBLEM 1 (ALMOST EVERYTHING YOU LEARNED IN THIS COURSE IN ONE EXAMPLE). In this example you will use almost everything you learned in this class, signal processing, number theory, and last but not least channel coding.

In the first module of this course we have introduced the convolution of two signals as the fundamental operation which computes the effect of passing a signal through a filter. Recall that if we have a signal $x[n]$ and the filter is given by $h[n]$, then the output of the filter is given by the convolution,

$$y[n] = \sum_m x[m]h[n-m].$$

Since convolutions are such basic operations, they are used very frequently. It is therefore important to find an efficient method to compute them. In this exercise we will learn the *Fourier transform* which is one of the most fundamental techniques in signal processing. It allows for an efficient implementation of convolutions and much more. The reason we have not introduced Fourier transforms in the signal processing module is that we need to be well familiar with complex numbers. But over finite fields it is much easier. We will also see that Reed-Solomon are most easily defined in terms of the Fourier transform. We will consider a very specific case but the same principle applies to any finite field.

(a) Consider the field F_7. Compute explicitly the set $\{5^i \pmod 7\}, i = 0, 1, \ldots, 5$. What is $5^6 \pmod 7$? A field element a such that its power $a^i, i = 0, 1, \ldots, |F| - 2$ covers all the non-zero elements of the field is called a *generator*.

(b) Using your mastery of number theory (and the result in (a)), show that

$$\begin{aligned} 5^k &\equiv 1 \pmod 7, \quad k = 0, \\ 5^k &\not\equiv 1 \pmod 7, \quad 0 < k < 6, \\ 5^{6k} = (5^k)^6 &\equiv 1 \pmod 7, \quad k \in \mathbb{Z}. \end{aligned}$$

(c) Show that for any integer k

$$(5^k - 1)\sum_{i=0}^{5} 5^{ki} = (5^k - 1)(1 + 5^k + 5^{2k} + 5^{3k} + 5^{4k} + 5^{5k}) = 5^{6k} - 1 = 0.$$

Argue that this implies that $\sum_{i=0}^{5} 5^{ki} \equiv 0 \pmod 7$ for $0 < k < 6$ and that $\sum_{i=0}^{5} 5^{ki} \equiv 6 \pmod 7$ for $k = 0$.

(d) Consider a vector u of length 6 whose components are elements of F_7. Define the following *Fourier transform* pair between the vectors $u, \hat{u}$ of length 6 with components in F_7. We have

$$\begin{aligned} \hat{u}_i &= \sum_{l=0,1,\ldots,5} u_l 3^{il}, \quad \text{Fourier Transform} \\ u_j &= 6 \sum_{i=0,1,\ldots,5} \hat{u}_i 5^{ij}, \quad \text{Inverse Fourier Transform} \end{aligned}$$

where all computations are done in F_7. Note that 5 is the multiplicative inverse of 3.

(e) Start with $u = (123456)$. Compute $\hat{u}$. Then verify that you get back u by computing the inverse transform.

(f) Show that in general if you start with u and compute first $\hat{u}$ by applying the Fourier transform and then compute the inverse Fourier transform of $\hat{u}$, you get back u?

To accomplish this, verify the following steps by using the results of (b) and (c):

$$\begin{aligned} u_j &= 6 \sum_{i=0,1,\ldots,5} \hat{u}_i 5^{ij} \\ &= 6 \sum_{i=0,1,\ldots,5} \sum_{l=0,1,\ldots,5} u_l 3^{il} 5^{ij} \\ &= \sum_{l=0,1,\ldots,5} u_l \; 6 \sum_{i=0,1,\ldots,5} 5^{i(j-l)} \\ &= \sum_{l=0,1,\ldots,5} u_l \; 6 \sum_{i=0,1,\ldots,5} (5^{(j-l)})^i \\ &= u_j. \end{aligned}$$

(g) Here is how you can use the Fourier transform to compute the convolution. Assume you have a signal $x[n]$ and a filter with impulse response $h[n]$. Assume you want to compute the *cyclic* convolution. This cyclic convolution differs slightly from the regular convolution in that we consider the signals to be periodic with period 7. In more detail, we have

$$y[n] = \sum_{m=0,\ldots,6} x[m]h[n-m \pmod 7)].$$

(i) Compute the cyclic convolution of the two vectors $u = (123456)$ and $v = (121212)$.

(ii) Compute the Fourier transform of u and v. Multiply the two resulting signals $\hat{u}$ and $\hat{v}$ componentwise, call the result $\hat{w}$. Take the inverse Fourier transform of $\hat{w}$. Hopefully, you get the same result as in (i). Indeed, this is the standard way a computer would compute the convolution.

In this example we considered a very simple example of a field with 7 elements. In practice you would use a much larger field, lets say of size N. In this case the Fourier transform can be used to compute the cyclic convolution of periodic signals of period N. With a proper implementation of the Fourier transform (called the Fast Fourier transform) it is possible to compute the convolution in roughly $N \log N$ operations. A brute force implementation of the convolution on the other hand would require N^2 operations. This is a siginificant saving.

(h) Now we will see how to define Reed-Solomon codes in terms of this Fourier transform. Define a RS code of length $n = 6$ with $k = 2$ and $d_{\min} = 5$ as follows. Consider the set of vectors $\hat{c}$ of length 6 of the form $\hat{c} = (c_1, c_2, 0, 0, 0, 0)$, where $c_1, c_2 \in F_7$. The RS code is then the set of Fourier transforms of this set.

(a) Show that this definition is equal to the definition we gave in class for the *canonical* Reed-Solomon code.

(b) Check that the following is a generator matrix for this code:

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

(c) Assume that you want to transmit the information vector $u = (14)$. What is the corresponding codeword?

(d) Assume you received the word (?4?60?). You want to determine the received codeword. Write down the corresponding system of equations. Now use the Gaussian elimination algorithm to recover the transmitted information. What was the transmitted codeword?

PROBLEM 2 (HAMMING BOUND). Consider a binary linear code C of length n and dimension k. This means that C is a subspace of $\{0,1\}^n$ of dimension k. Let d be the minimum Hamming distance of C. Let $A(n,d)$ be the maximum number of codewords in a code over F_2 of length n and minimum distance at least d. Let $t = \lfloor \frac{(d-1)}{2} \rfloor$. Prove the following fundamental inequality called the Hamming bound,

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

To prove the above bound we proceed as follows:

(i) Consider a "sphere" around a codeword c of radius i. This "sphere" of radius i contains all the words which have a Hamming distance less than or equal to i from c. In more detail: the sphere of radius 1 around a codeword c of length n consists of the codeword c itself together with the n words c' which have Hamming distance exactly 1 from c.

Let $\binom{n}{i}$ denote the number of ways of selecting i positions from n positions. It can be shown that the number of ways to choose i positions out of n positions is given by $\binom{n}{i} = \frac{n!}{(n-i)!i!}$, where $n! = n(n-1)(n-2)\cdots 1$.

Show that the number of words contained in the sphere of radius i around a codeword c is equal to $\sum_{j=0}^{i} \binom{n}{j}$?

(ii) Consider two codewords x, y. Consider a sphere of radius $t = \lfloor \frac{(d-1)}{2} \rfloor$ around both x and y. Using the fact that the Hamming distance is a true distance, show that the two spheres do not overlap, i.e., show that there is no word z such that z belongs to both spheres.

(iii) Consider a sphere of radius $t = \lfloor \frac{(d-1)}{2} \rfloor$ around each codeword. Show that the total number of words contained in all the spheres is not more than the total number of binary words of length n, i.e., show that

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

(iv) By putting all previous results together, conclude the Hamming bound.