ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 21 — Introduction to Communication Systems
Homework 12 — December 4, 2008

PROBLEM 1 (ARITHMETIC OVER FINITE FIELDS). Let $F = F_7$. Consider the system of linear equations

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= 2, \\ 2x_1 + 2x_2 + 2x_3 &= 1, \\ 3x_1 + 3x_2 + x_3 &= 0. \end{aligned}$$

(a) Write this system in matrix form as $\mathbf{A}\mathbf{x}^{\mathbf{T}} = \mathbf{u}^{\mathbf{T}}$. What are $\mathbf{A}, \mathbf{x}, \mathbf{u}$, and what are their dimensions ?

(b) Consider the matrix $\mathbf{A}$ first as a matrix over the integers. You can check that it has determinant equal to 4. What is the determinant of $\mathbf{A}$ if you consider it as a matrix over F_7?

(c) Show that the system can be solved uniquely over F_7.

(d) Solve the system over F_7 using Gaussian elimination.

(e) If you had to solve a $n \times n$ system. How complex is Gaussian elimination, i.e., how many elementary operations (addition, multiplication, etc.) will you need ?

PROBLEM 2 (HAMMING DISTANCE IS TRUE DISTANCE). The Hamming distance between two vectors u, v of length n, belonging to the space $\{0,1\}^n$ is defined as the number of positions at which u, v differ. More precisely

$$d(u, v) = \sum_{i=1}^{n} (u_i + v_i)$$

where all operations are done in the field F_2. Prove that the Hamming distance is indeed a true distance. I.e. prove that

(a) $d(u, v) \geq 0$ for any u, v and $d(u, v) = 0$ if and only if $u = v$.

(b) $d(u, v) = d(v, u)$.

(c) $d(u, v) \leq d(u, w) + d(w, v)$.

PROBLEM 3 (DUAL SPACES). Let S be a subspace of the vector space W over the field F. The set

$$S^{\perp} = \{w \in W : w \cdot s = 0 \text{ for all } s \in S\}$$

is called the *dual space*. Here, $w \cdot s$ is defined as $\sum_i w_i s_i$, where all computations are done in F.

(a) Show that $S^\perp$ is a subspace.

(b) Show that if S is a subspace of dimension k, then $S^\perp$ is a subspace of dimension $n-k$.

(c) Take $F = F_2$ and $S = \{0000, 0011, 1100, 1111\}$. Determine the dual space $S^\perp$.

Problem 4 (Parity Check Matrix as Dual of Generator Matrix). We consider a binary code generated by the matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

This means that

$$C = \{x : x = uG, u \in F_2^4\}.$$

(a) Is the word $(1, 0, 1, 0, 1, 0, 1)$ a codeword?

(b) How many codewords are generated by this code? Give a list of them.

(c) The first two bits of the word $(x, x, 0, 1, 1, 0, 1)$ were deleted. What was the transmitted word ? What is the maximum number of binary symbols which can be removed while still being able to find the transmitted codeword?

(d) Let C be the vector space of the words generated by this code, $C^\perp$ its dual. Find $C^\perp$ (give the list of all its elements).

(e) Give a basis for the vector space, $C^\perp$. Such a basis is usually denoted by the matrix H. It is called the parity check matrix of the code C.

(f) Let $\hat{y}$ be the received word. The vector given by $s = \hat{y}H^T$ is called the *syndrome*. If the received word is $(0, 0, 0, 1, 0, 0, 1)$, what is the resulting syndrome? What is the word which was most likely transmitted if we knew that there was only one error?

(g) What is the smallest number of errors (Hamming distance) which could change one codeword into another codeword?

Problem 5 (Singleton 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. Prove the following fundamental inequality due to Singleton.

$$d \leq n - k + 1$$

Hint: Write down the 2^k codewords in a $(2^k) \times n$ binary matrix. Delete all except the first k columns of the matrix. Note that the distance between two codewords is the sum of the difference among the first k components and the difference among the last $(n - k)$ components.