ASSIGNMENT 2 - MATH 251, WINTER 2008

Submit by Monday, January 28, 12:00

1. Let $\mathcal{B} = \{(1,1),(4,5)\}$ and $\mathcal{C} = \{(2,1),(1,1)\}$ be bases of $\mathbb{R}^2$. Find the change of basis matrices ${}_{\mathcal{B}}M_{\mathcal{C}}$ and ${}_{\mathcal{C}}M_{\mathcal{B}}$ between the bases $\mathcal{B}$ and $\mathcal{C}$. Let $v = \binom{8}{28}$ with respect to the standard basis. Find $[v]_{\mathcal{B}}$ and $[v]_{\mathcal{C}}$.

2. Which of the following functions is a linear map? (provide proof):
   (1) $T : \mathbb{R}^2 \to \mathbb{R}^2, \quad T(x,y) = (3x - 2y, x + y)$.
   (2) $T : \mathbb{R}^2 \to \mathbb{R}^2, \quad T(x,y) = (x^2 - y, x + y + 1)$.
   (3) $T : \mathbb{R}[x]_3 \to \mathbb{R}^2, \quad T(f(x)) = (f(1), f'(1))$.
   (4) $T : \mathbb{R}[x]_3 \to \mathbb{R}[x]_4, \quad T(f(x)) = xf(x) + f(1)$.

In each case where T is a linear map, find its kernel.

3. Prove the following Proposition.

Proposition 0.1. *Let V and W be vector spaces over $\mathbb{F}$. Let $B = \{b_1, \ldots, b_n\}$ be a basis for V and let $t_1, \ldots, t_n$ be any elements of W. There is a unique linear map*

$$T : V \to W,$$

such that

$$T(b_i) = t_i, \qquad i = 1, \ldots, n.$$

5. Consider the following subspaces of $\mathbb{R}^3$:

$$U = \{(x,y,z) \in \mathbb{R}^3 : x + y - z = 0; x - 2y + z = 0;\}, \quad W = \{(x,y,z) \in \mathbb{R}^3 : x + y + z = 0\}.$$

Answer the following questions.
   (1) Find the dimensions of U and W.
   (2) Find a linear map $T : \mathbb{R}^3 \to \mathbb{R}^3$ such that $U = \mathrm{Ker}(T)$, $W = \mathrm{Im}(T)$.
   (3) Find a linear map $S : \mathbb{R}^3 \to \mathbb{R}^3$ such that $W = \mathrm{Ker}(S), U = \mathrm{Im}(S)$.
   (4) Find $\mathrm{Im}(T^2), \mathrm{Im}(S^2), \mathrm{Im}(S \circ T)$ and $\mathrm{Im}(T \circ S)$ (hint: it is possible to do that without any calculations).

7. **Graphs.** A graph G consists of a finite set of vertices $V(G)$ and a set of edges $E(G) \subset V(G) \times V(G)$. Thus, a vertex u is connected to a vertex v precisely if $(u,v) \in E(G)$. We assume that the graph is non-oriented, meaning $(u,v) \in E(G) \Leftrightarrow (v,u) \in E(G)$. Note that by our definition there is at most one edge between any two vertices. We shall also assume, for simplicity, that the graph has no loops. Namely, $(v,v) \notin E(G)$ for all $v \in V(G)$.

Suppose that the vertices are labeled $1, 2, \ldots, n$. We may encode the graph by a symmetric matrix A, called the **adjacency matrix** of the graph. We define

$$A = (a_{ij}), \quad a_{ij} = \begin{cases} 1 & (i,j) \in E(G) \\ 0 & \text{else.} \end{cases}$$

A. Write the adjacency matrix of the graph whose vertices are $\{0, \ldots, 6\}$ where any i is connected to $i + 1 \pmod 7$ and $i + 2 \pmod 7$. Draw the graph as well.

Let k be an integer. A graph is called **k-regular** if from every vertex there are exactly k edges.

B. Show that the above graph is 4-regular. Prove that a graph is k-regular if and only if the sum of the coefficients of every row (every column) of its adjacency matrix is k.

A graph is called **bipartite** if we can divide its vertices into two disjoint sets L and R such that vertices from L are only connected to vertices in R and vertices in R are only connected to vertices in L. We shall say that a bipartite graph is regular if for some d_L, d_R, every vertex in L connects to exactly d_L vertices in R and any vertex in R connects to exactly d_R vertices in L.

C. Prove that in this case $|L| \cdot d_L = |R| \cdot d_R$. Is our example above bipartite?

D. For a bipartite graph G, with $L = \{\ell_1, \ldots, \ell_n\}, R = \{r_1, \ldots, r_m\}$ define an $m \times n$ matrix M whose ij entry is one if r_i is connected to ℓ_j and zero otherwise. How can we write the adjacency matrix of G in terms of M? How can we determine in terms of M whether the graph is regular?

Binary codes. A **binary linear code**, or just a **code** for us, is a subspace of $\mathbb{F}_2^n$. The elements of $\mathbb{F}_2^n$ are referred to as "words" and those of C as "code words". Codes are used in order to send messages over noisy channels in such a way that the receiver can detect transmission errors and correct them, to some extent. Here is a basic example, called a **parity check code**: Suppose we wish to send one of the following four datum $\{(0,0),(0,1),(1,0),(1,1)\}$. If we just send the data and there is error in the transmission, for example $(0,0)$ is sent but $(1,0)$ is received due to error in the transmission of the first digit, then the receiver cannot know that an error has occurred, let alone correct the error. If instead of sending the vector (x,y) we sent $(x,y,x+y \mod 2)$ (thus, instead of $(1,0)$ we send $(1,0,1)$ and instead of $(1,1)$ we send $(1,1,0)$), then if a single error occurs then the receiver will receive three digits such that the last digit is not the sum of the first two. Thus, the receiver can recognize that an error has occurred, though not correct it. Thus, by adding redundancy (sending 3 digits instead of 2) we are gaining ability to detect errors. The code in this example is the subspace of $\mathbb{F}_2^3$ defined by $x+y+z=0$.

In general, we are having some collection of messages (or data) we want to send, for example a blocks of $0,1$ bits of length k, namely elements of $\mathbb{F}_2^k$. We are looking for a k-dimensional subspace C of $\mathbb{F}_2^n$ and we fix an isomorphism of $\mathbb{F}_2^k \cong C$, thus translating each original sequence of k bits into a code word, an element of C. We transmit the element of C and not the original sequence of k-bits.

The receiver knows the code C - our goals is to transmit information overcoming errors, not to hide it - and thus looks for the code word closest (relative to the Hamming distance) to the received message. Here are some definitions:

The **Hamming distance** on $\mathbb{F}_2^n$ is

$$d(x,y) = \text{ number of digits in which } x \text{ and } y \text{ differ.}$$

This is a distance function ("metric"), i.e., (i) $d(x,y)=0$ iff $x=y$; (ii) $d(x,y)=d(y,x)$; (iii) $d(x,z) \leq d(x,y)+d(y,z)$. Note also the easy identity

$$d(x,y) = d(x-y,0).$$

Let $C \subseteq \mathbb{F}_2^n$ be a code (i.e., a subspace). The **distance** of C is

$$d(C) = \min_{c \in C, c \neq 0} d(c,0).$$

We say that a code **detects k errors**, if given an element $v \in C$ there is no element $w \in C$ such that $d(v,w) \leq k$, except v itself. The idea that is that more than k errors must occur in the transmission of a code word v so that the received message is not detected as an error (namely, is also an element of C).

We say that a code **corrects k errors**, if for $v \in \mathbb{F}_2^n$ and $u, w \in C$ the inequalities $d(v,u) \leq k$ and $d(v,w) \leq k$ imply that $u = w$. Namely, as long as no more than k errors have occurred there is a unique way to retrieve the original code word, there is a unique element of C in distance at most k from the received message.

E. Prove the following: Let $C \subseteq \mathbb{F}_2^n$ be a linear code. One can detect $d(C)-1$ errors and correct $(d(C)-1)/2$ errors if $d(C)$ is odd and $(d(C)-2)/2$ errors if $d(C)$ is even.

F. Let H_7 the **Hamming code** of length 7. It's defined as the subspace of $\mathbb{F}_2^7$ generated by

$$(1,1,0,1,0,0,0),(0,1,1,0,1,0,0),(0,0,1,1,0,1,0),(0,0,0,1,1,0,1).$$

Prove that it's a four dimensional code with distance 3.

If $C \subset \mathbb{F}^n$ is a linear code, we define its **rate** to be

$$r(C) = \dim(C)/n.$$

This magnitude measures the efficiency of the code. Note that $0 \leq r(C) \leq 1$.

Now take the matrix M we have constructed in the context of bipartite graphs and consider it as a linear map

$$T : \mathbb{F}_2^n \to \mathbb{F}_2^m, \qquad T(v) := Mv,$$

(we think of the vectors as column vectors). Define a linear code by taking the kernel of this linear transformation. For future reference we denote this code by C_G,

$$C_G := \{v \in \mathbb{F}^n : Mv = 0\}.$$

G. Prove that the rate of C_G is at least $\frac{n-m}{n}$.

H. Consider the following example. Let $R = \{1, 2, \ldots, n\}$ and let L the set whose elements are subsets of order k of R. Thus, L has $\binom{n}{k}$-elements. An element a of R is connected to an element S of L if and only if $a \in S$. Show that this gives a regular bipartite graph. Find the rate and distance of the linear code for $n = 4$ and $k = 2$.