ASSIGNMENT 1 - MATH 251, WINTER 2007

Submit by Monday, January 22, 12:00

1. Consider the following vector spaces (you do not need to prove those are vector spaces, unless specified):

(1) The vector space V_1 of continuous functions $f : [0, 1] \to \mathbb{R}$, where we define $f+g$ to be the function $(f+g)(x) = f(x)+g(x)$ and αf to be the function $(\alpha f)(x) = \alpha f(x)$.

(2) The vector space V_2 of polynomials over a field $\mathbb{F}$ with the usual addition of polynomials and multiplication by a scalar (which is a special case of multiplying two polynomials).

(3) The vector space $V_3 = \{(x_1, x_2, x_3, \dots) : x_i \in \mathbb{F}\}$, where we define

$$(x_1, x_2, x_3, \dots) + (y_1, y_2, y_3, \dots) = (x_1 + y_1, x_2 + y_2, x_3 + y_3, \dots),$$

and

$$\alpha(x_1, x_2, x_3, \dots) = (\alpha x_1, \alpha x_2, \alpha x_3, \dots).$$

(4) Fix scalars $A, B \in F$. Prove that the vectors $(x_1, x_2, x_3, \dots)$ of V_3 that satisfy:

$$x_n = Ax_{n-1} + Bx_{n-2}, \quad n \geq 3$$

form a subspace V_4.

(5) The vector space of functions $f : \{1, 2, \dots, n\} \to \mathbb{R}$, where again $(f + g)(x) = f(x) + g(x)$ and $(\alpha f)(x) = \alpha f(x)$.

In each case determine whether the vector space is finite dimensional or infinite dimensional. In case it is finite dimensional, give a basis. In case it is infinite dimensional, prove that by providing an explicit infinite set of linearly independent vectors.

2. Let V be an n-dimensional vector space over a field $\mathbb{F}$. Let $T = \{t_1, \dots, t_m\} \subset V$ be a linearly independent set. Let $W = \text{Span}(T)$. Prove:

$$\dim(W) = m.$$

3. Let V_1, V_2 be finite dimensional vector spaces over a field $\mathbb{F}$. Prove that

$$\dim(V_1 \oplus V_2) = \dim(V_1) + \dim(V_2).$$

4. Let V be a vector space over $\mathbb{F}$ and let $S \subset V$ be a non-empty set. Let $v \in V$. Prove that

$$\text{Span}(S \cup \{v\}) = \text{Span}(S) \iff v \in \text{Span}(S).$$

5. Find which two of the following sets of vectors in $\mathbb{R}^3$ have the same span:
(i) $\{(1,0,1),(2,3,2),(-1,-3,-1)\}$;
(ii) $\{(3,-2,3),(1,1,1)\}$;
(iii) $\{(1,0,0),(0,0,1),(0,1,0)\}$.

6. Let $\mathbb{F}$ be a finite field with q elements.
(1) Show that the kernel of the ring homomorphism
$$\mathbb{Z} \to \mathbb{F}$$
defined by $n \mapsto n \cdot 1 = 1 + \cdots + 1$ (n times) is of the form $p\mathbb{Z}$ for some prime p. Conclude that we may assume that $\mathbb{F} \supseteq \mathbb{Z}/p\mathbb{Z}$ for some prime p.
(2) Prove that $\mathbb{F}$ is a vector space of finite dimension over $\mathbb{Z}/p\mathbb{Z}$ and if this dimension is n then $\mathbb{F}$ has p^n elements[1].

7. **Rudiments of Coding Theory I.** In this exercise $\mathbb{F}$ is a finite field having q elements, for example $\mathbb{Z}/p\mathbb{Z}$ that has p elements.[2] Let $V = \mathbb{F}^n$. Thus, an element of V is just an n-tuple $(x_1, \ldots, x_n)$ where each coordinate x_i is an element of $\mathbb{F}$. Define a distance function $d(x,y)$ on V as follows. If x and y are vectors
$$d(x,y) = \text{the number of coordinates in which } x \text{ and } y \text{ differ.}$$
For example: if $n = 6$, $x = (1,1,0,0,1,0)$ and $y = (1,1,1,0,0,0)$ then $d(x,y) = 2$. This distance is called the *Hamming distance*[3]. Prove that:
(1) $d(x,y) \geq 0$ with equality holding if and only if $x = y$;
(2) $d(x,y) \leq d(x,z) + d(z,y)$ for every $x, y, z \in V$ (the *Triangle Inequality*).
We also call $d(x,0)$, where 0 is the zero vector, the *Hamming weight of* x; it is equal to the number of non zero coordinates of x.

Coding theory has nothing to do with concealing information. It is rather the science of transmitting information over noisy, or defective, channels. Those could be your telephone line when you connect to the internet, or a rover transmitting to NASA from Mars, etc.. They are used in CD and DVD readers, in barcodes, in cellphones and numerous other everyday life applications. The purpose in each case is to find some means to ensure that the receiving side either receives the correct information or is able to reconstruct it from the information it received, at least if it is not too corrupted. Assume that the original message, that consists of "words" (or chunks of information) of some fixed length, is written

[1]Note: at this point you've proven that every finite field has cardinality p^n for some prime p.
[2]We use the notation $\mathbb{Z}/n\mathbb{Z}$ for the ring of integers (mod n), which some denote by $\mathbb{Z}_n$. A good case to keep in mind in this exercise is $\mathbb{F} = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$.
[3]After the scientist Richard W. Hamming.

as a string of zeros and ones. For example, suppose that $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$. We might be interested in sending the following information, already cut into chunks,

$$01 \quad 11 \quad 01 \quad 10 \quad 00\ldots$$

(This might mean "all is well, tell mom I'll be back for supper"). To do that we have a "code". A code is like a dictionary that substitutes for each original word a longer word and it is that longer word that is being transmitted. The receiving side has the same code (or "dictionary") and has no problem translating longer words back into the original words. The logic is, in a sense, that longer words are more "robust" and can be recognized even if distorted.

For example, our code could be the subspace of $\mathbb{F}^3$ consisting of all vectors (x_1, x_2, x_3) such that $x_1 + x_2 + x_3 = 0$. There are 4 such code words in this code. We translate each original word (i.e., $00, 01, 10, 11$) to a code word by adding the unique third digit that makes the sum zero. Therefore, our original message is now written as

$$011 \quad 110 \quad 011 \quad 101 \quad 000\ldots$$

This code is called a *parity check* code. The receiver gets the message and checks if every word belongs to the code by checking in this example that the sum of digits is zero. Thus, if 111 is received, we know there is an error because the digits sum up to 1 in the field $\mathbb{Z}/2\mathbb{Z}$.

Definition 0.1. Let $\mathbb{F}$ be a field with q elements. An (n, k) linear code C is a subspace of $\mathbb{F}^n$ having q^k elements.

Show that the minimal distance between two distinct elements of a code C is the minimal weight of a non-zero vector. Namely:

$$\min\{d(x, y) : x \neq y,\ x \in C, y \in C\} = \min\{d(x, 0) : x \in C,\ x \neq 0\}.$$

The procedure of coding continues as follows. The transmitting side is sending words that belong to an (n, k) code C that is known to the receiving side and sends only such words. The receiving side receives vectors of $\mathbb{F}^n$. Each such vector may be in C (i.e., if no errors occurred, or if errors did occur but the erroneous vector happens to belong to C as well). In case it isn't, the receiving side looks for the word in C that is closest to the vector that was received.

We say that a linear code *corrects t errors* if for every code word that is transmitted with t or less errors the original code word is the *unique* element of the code C which is the nearest to it. We say that a linear code *detects t errors* if every received word with at least one, but no more that t errors, is not a code word. Prove the following Theorem

Theorem 0.2. *A linear code C corrects t errors if and only if the Hamming distance of every two distinct elements of C is at least $2t + 1$.*

A linear code C detects t errors if and only if the Hamming distance between any two elements of C is at least $t + 1$.

For example, in the parity check code, the Hamming distance of every non zero vector is precisely 2. Thus, the code detects single errors and corrects none. This illustrate the fact that we can tell that 111 is an error, but cannot determine if the original word was 101 or 011.

Prove the following theorem.

Theorem 0.3. *Let $\mathbb{F}$ be a finite field of q elements. Let $V = \mathbb{F}^n$ and let C be a code (= a subspace) of dimension k, hence having q^k elements. Let d be the minimal Hamming weight of a non zero element of C. Prove that*

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