ASSIGNMENT 6 - MATH 251, WINTER 2008

Submit by Monday, March 3, 16:00

The maximal grade you can get for this assignment is 200 (relative to 100).

(1) Let $A = (a_{ij})$ be a matrix in REF with the special columns being $i_1, \dots, i_r$ (so that A looks like

$$\begin{pmatrix} 0 & \dots & 0 & a_{1i_1} & \dots & 0 & 0 & \dots & 0 & 0\dots \\ 0 & \dots & \dots & \dots & \dots & 0 & a_{2i_2} & \dots & 0 & 0\dots \\ 0 & \dots & \dots & \dots & \dots & & \dots & \dots & 0 & a_{3i_3}\dots \\ \vdots & & & & & & & & & \end{pmatrix},$$

where the $a_{ji_j} = 1$ and possibly the lower rows are all zeros.) Let W be the solutions to the homogenous system. Prove that the map

$$W \to \mathbb{F}^{n-r}, \qquad (x_1, \dots, x_n) \mapsto (x_1, \dots, \widehat{x_{i_1}}, \dots, \widehat{x_{i_2}}, \dots, \widehat{x_{i_r}}, \dots, x_n),$$

is an isomorphism. Explain also in words what that means as to finding all the solutions of the homogenous system.

(2) Find all the solutions to the following system of linear equations

$$Ax = b,$$

where

$$A = \begin{pmatrix} 0 & 2 & 4 & 1 & 1 & 0 \\ 0 & -1 & -2 & 0 & -1 & 1 \\ 0 & 5 & 10 & 0 & 5 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 3 \\ -1 \\ 10 \end{pmatrix}.$$

(3) Let $T : V \to W$ be a linear map and define $T^* : W^* \to V^*$ by $(T^*(g))(v) := g(Tv)$. Prove the following lemma:

LEMMA **1.** (a) *T^* is a well-defined linear map.*

(b) *Let B, C be bases to V, W, respectively. Let $A = {}_C[T]_B$ be the $m \times n$ matrix representing T, where $n = \dim(V), m = \dim(W)$. Then the matrix representing T^* with respect to the dual bases B^*, C^* is the transpose of A:*

$$_{B^*}[T^*]_{C^*} = ({}_C[T]_B)^t.$$

(c) *If T is injective then T^* is surjective. (Do NOT use Proposition 7.2.9 in the notes).*

(d) *If T is surjective then T^* is injective.*

(4) Let $V = \mathbb{R}[t]_n$ be the space of polynomials with real coefficients of degree at most n. Let $r_0 < r_1 < \dots < r_n$ be $n+1$ distinct real numbers. We have seen that

$$f_i : \mathbb{R}[t]_n \to \mathbb{R}, \qquad f_i(g(t)) = g(r_i),$$

is a linear map and so is a linear functional. Prove that

$$B^* = \{f_0, \dots, f_n\}$$

is a basis for V^*. Find the basis $B = \{g_0, g_1, \dots, g_n\}$ of V dual to it. Prove that if $g \in V$ then

$$g(t) = \sum_{i=0}^{n} g(r_i) \cdot g_i(t).$$

(5) **Latin Squares.** Wikipedia has an entry for Latin squares which you may find interesting, but it is not needed to solve the exercise. (`http://en.wikipedia.org/wiki/Latin_square`)

A Latin square is, for us, an $n \times n$ matrix all whose entries are integers belonging to $\{1, 2, \dots, n\}$ in such a way that every row and every column contain every number exactly once. For example,

1	2
2	1

1	2	3
3	1	2
2	3	1

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

Such matrices are important for group theory, experimental designs and linear algebra; there are many open questions. It is a hard theorem that there are more than $(n!)^{2n}/n^{n^2}$ Latin squares of order n (this is more than exponential in n). One way to construct Latin squares is as multiplication tables for groups. If G is a group of order n we write its elements as $a_1, \dots, a_n$ and the ij entry of the table is k if $a_i a_j = a_k$. I'll let you ponder why this gives a Latin square.

Here is an interesting way to construct Latin squares that has to do with linear algebra. Let $\mathbb{F}$ be a field with q elements and choose in $\mathbb{P}^2(\mathbb{F})$ three distinct points x, y, z lying on a line ℓ. Enumerate the lines through x, besides the line ℓ, by the numbers $1, \dots, q$ (can we do that?). Do the same for y and z. Define a matrix $M = (m_{ij})$ as follows. Let t be the intersection point of the i-th line through x and the j-th line through y. The line connecting t to z is different from ℓ (why?) and so has a certain number k. Let $m_{ij} = k$. Prove that this works. Namely that this is a well-defined process yielding a Latin square for $\{1, 2, \dots, q\}$.

(6) **Cellular automata.** We are taking here a very simplified point of view. To have a better picture you can read the Wiki entry `http://en.wikipedia.org/wiki/Cellular_automaton`, but it is not needed to solve the exercise.

In this exercise a cellular automaton refers to a finite set of cells, each of which can be in one of two states: black, or white (or, if you wish, off and on). At each time increment the whole collection of cells changes state as a function of all the states of all the cells. If we number the cells by $1, 2, \dots, n$ then we can think about the state of the system as an element of $\mathbb{F}_2^n$, where 1 means black and 0 means white, say. The change then is a function $f : \mathbb{F}^n \to \mathbb{F}^n$.

As a simple example of a cellular automaton, let f be defined by

$$f(x_1, \dots, x_n) = (x_n + x_2, x_1 + x_3, \dots, x_{n-2} + x_n, x_{n-1} + x_n);$$

namely the state of the i-th cell becomes 0 if both its neighbors are in the same state and becomes 1 if its neighbors are in opposite states. In this case the function f is linear, but in general it need not be and in fact the most interesting cellular automata are not linear.

One is interested in the evolution of the system as time passes. For example, is there a periodic state? Namely, a state to which the system returns eventually. Is there a graveyard state? Namely, a state that once reached the system does not leave anymore.

In this general definition of automata there is no restriction on the function f. A special class of automata are the additive automata. In this case f has the form

$$f(v) = T(v) + C,$$

where T is a linear transformation and $C \in \mathbb{F}_2^n$ is a constant vector. Thus, $f^2(v) = T^2(v) + TC + C$ and so on. Such a function f is called an affine transformation. T is called its linear part and C its constant part.

(a) Prove that an affine linear transformation is a bijection if and if its linear part is a bijection.
(b) Prove that the set of bijective affine transformations forms a group under composition of functions.

(c) Consider an automaton in which f is an invertible affine transformation. Prove that every state is periodic. (A graveyard state is periodic.)

(d) Formulate a condition that an affine transformation has a graveyard state.

(e) Suppose that f is in an affine transformation whose linear part is nilpotent. Prove that f has a graveyard state, whatever C is.

(f) To an automaton we can assign a directed graph in a natural way. The vertices are the states (i.e., the elements of $\mathbb{F}_2^n$) and we connect state a to state b if $f(a) = b$. Suppose that f is a nilpotent linear transformation ($C = 0$) such that $T^n = 0$, but $T^{n-1} \neq 0$. Prove that the graph is then a tree with a single root in which every node has precisely 2 branches, except to the root that has one branch.

(g) Conversely, if f is a linear transformation whose graph that is such a tree, prove that $T^n = 0$ and $T^{n-1} \neq 0$.

In the folowing V is an inner product space over $\mathbb{F}$, where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

(7) Prove the Parallelogram Law:

$$\|u + v\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2).$$

(8) Prove that any inner product on $\mathbb{F}^n$ arises from a positive definite Hermitian matrix.

(9) Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix of complex numbers. Prove that the function

$$\langle (x_1, x_2), (y_1, y_2) \rangle = (x_1, x_2) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \overline{y_1} \\ \overline{y_2} \end{pmatrix},$$

is an inner product on $\mathbb{C}^2$ if and only if a and d are positive real numbers, $c = \bar{b}$ and $ad - b\bar{b} > 0$. In addition, in the case of the matrix $\left(\begin{smallmatrix} 1 & 1+i \\ 1-i & 5 \end{smallmatrix}\right)$ compute $\langle (1, 2), (1, 3) \rangle$ and $\|(1 + i, 5)\|$.

(10) Let $a < b$ be real numbers. Show that the function

$$\langle f, g \rangle = \int_a^b f(x)g(x)dx$$

defines an inner product of $\mathbb{R}[x]_n$.[1] Compute the norm of the vector $f(x) = 1 + x^3$ in the case $(a, b) = (0, 1)$ and in the case $(a, b) = (0, 2)$.

[1] This is also true for $\mathbb{C}[x]_n$ if we define

$$\langle f, g \rangle = \int_a^b f(x)\overline{g(x)}dx.$$

Note that in this case one can do the integration formally because we are dealing with polynomials. Thus, for example,

$$\langle x^2, 1 + ix \rangle = \int_a^b (x^2 - ix^3)\, dx = (x^3/3 - ix^4/4)|_a^b = (b^3/3 - ib^4/4) - (a^3/3 - ia^4/4).$$