TW314 Lecture 22 (Mo 27 Mar 2017)

VECTOR SPACES OVER FINITE FIELD

For q a prime power, let $GF(q)$ denote the field with q elements.

Let $V(n,q)$ be the set of all n-tuples over $GF(q)$.

Define two operations:

1. vector addition

   If $\underline{x} = (x_1, x_2, \ldots, x_n)$ and $\underline{y} = (y_1, y_2, \ldots, y_n)$,

   then $\underline{x} + \underline{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$.

2. scalar multiplication

   If $\underline{x} = (x_1, x_2, \ldots, x_n)$ and $a \in GF(q)$,

   then $a\underline{x} = (ax_1, ax_2, \ldots, ax_n)$.

Then $V(n,q)$ is a <u>vectors space</u>; that is

1. $V(n,q)$ is an abelian group under vector addition
2. $a\underline{x} \in V(n,q)$ for any $a \in GF(q)$ and $\underline{x} \in V(n,q)$
3. $a(\underline{x} + \underline{y}) = a\underline{x} + a\underline{y}$
4. $(a+b)\underline{x} = a\underline{x} + b\underline{x}$
5. $(ab)\underline{x} = a(b\underline{x})$
6. $1\underline{x} = \underline{x}$

A subset of $V(n,q)$ is a <u>subspace</u> if it is itself a vector space.

<u>Examples:</u> $\{\underline{0}\}$ — trivial subspace

The non-trivial proper subspaces excludes $\{0\}$ and $V(n,q)$.

<u>Theorem 2.4</u>

A non-empty subset C of $V(n,q)$ is a subspace iff it is closed under vector addition and scalar multiplication, that is

1. $\underline{x}, \underline{y} \in C \implies \underline{x} + \underline{y} \in C$
2. $a \in GF(q)$ and $\underline{x} \in C \implies a\underline{x} \in C$.

<u>Definition</u> A linear combination of the vectors $\underline{x}_1, \underline{x}_2, \ldots \underline{x}_r$ in $V(n,r)$ is any vector $a_1\underline{x}_1 + a_2\underline{x}_2 + \cdots + a_r\underline{x}_r$, with $a_1, a_2, \ldots, a_r \in GF(q)$.

<u>Example:</u> For $S \subseteq V(n,r)$, the set of all linear combinations of vectors of S is a subspace of $V(n,r)$.

Definition $\{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_r\}$ is a set of linearly dependant vectors if $\exists$ scalars $a_1, a_2, \ldots, a_r$ NOT ALL ZERO such that

$$a_1\underline{x}_1 + a_2\underline{x}_2 + \cdots + a_r\underline{x}_r = \underline{0}.$$

It is linearly independent if

$$a_1\underline{x}_1 + a_2\underline{x}_2 + \cdots + a_r\underline{x}_r = \underline{0} \implies a_1 = a_2 = \cdots = a_r = 0.$$

Definition For a subspace C of $V(n,q)$, $\{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_r\}$ is a generating set of C if every vector of C can be written as a linear combination of $\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_r$.

Definition A basis of C is a generating set of C that is linearly independent.

Example: A basis for $V(n,q)$ is

$$\{(1,0,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (0,0,0,\ldots,1)\}$$

Basis for $V(3,q)$ is $\{(1,0,0), (0,1,0), (0,0,1)\}$