LINEAR VECTOR SPACES OVER FINITE FIELDS

Let q is prime consider $GF(q)$

and Z_q^n $\quad x = (x_1, \ldots, x_n) \in GF(q)$

iff $x_i \in GF(q)$

$x, y \in Z_q^n$ 1) $x + y = (x_1 + y_1, \ldots, x_n + y_n) \pmod q$

scalar $a \in GF(q)$: 2) $ax = (ax_1, ax_2, \ldots, ax_n)$

$a \in GF(q)$ 3) $a(x+y) = ax + ay$

$a, b \in GF(q)$. 4) $a(bx) = (ab)x$

Z_q^n is a n-dimensional linear vector space over $GF(q)$

Let $V \subseteq Z_q^n$ and:

1) $x, y \in V \quad x + y \in V$

2) $a \in GF(q)$, $x \in V$, $ax \in V$

the V is a <u>subspace</u> of Z_q^n

Let $v_1, v_2, \ldots, v_r \in Z_q^n$

Consider a <u>linear combination</u>

$a_1 v_1 + a_2 v_2 + \ldots + a_r v_r \quad a_i \in GF(q)$

$v_1, v_2, \ldots, v_r$ are <u>linear dependent</u>

iff $\exists\, a_1, a_2, \ldots, a_r$ not all equal 0:

$$a_1 v_1 + a_2 v_2 + \ldots + a_r v_r = 0$$

otherwise $v_1, v_2, \ldots, v_r$ are <u>linearly independent</u>

A linear independent set of vectors called <u>basis</u> iff all linear combinations of these vectors form the subspace. All these linear combinations are different

<u>Examples</u> $q=2$ $n=4$.

1) $\{0001, 0010, 0100, 1000\}$ is a basis for Z_2^4

2) $\{0011, 0010, 1100, 1000\}$ is a basis for Z_2^4

3) $\{0011, 0110, 1100, 1001\}$ is <u>not</u> a basis for Z_2^4.

Let $v_1, v_2, \ldots, v_r$ is a basis for Z_q^n then: $v_i \in Z_q^n$

1) $r = n$
2) any vector $x \in Z_q^n$ can be represented in a unique way as

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = x$$

REMARK:
Z_q^n is a n-dimensional space over $GF(q)$ iff q is prime or power of prime.

Equivalent Transformations of linear Codes

Two codes are equivalent if: they can be obtained by

1) permutation of digits
2) multiplication of all digits in the same position by a scalar

Example $q=3$, $n=3$, $k=2$

$$C_1 = \begin{matrix} 0\,0\,0 \\ 0\,1\,2 \\ 0\,2\,1 \\ 1\,0\,2 \\ 1\,1\,1 \\ 1\,2\,0 \\ 2\,0\,1 \\ 2\,1\,0 \\ 2\,2\,2 \end{matrix} \qquad C_2 = \begin{matrix} 0\,0\,0 \\ 2\,2\,0 \\ 1\,1\,0 \\ 2\,0\,1 \\ 1\,2\,1 \\ 0\,1\,1 \\ 1\,0\,2 \\ 0\,2\,2 \\ 2\,1\,2 \end{matrix}$$

C_1 and C_2 are equivalent —

(columns 1 and 3 are transposed and column 2 multiplied by 2 (mod 3))

T: Two $(k \times n)$ matrices generate equivalent (n, q^k) codes over GF(q) if one matrix can be obtained from another by the sequence of operations of the following types:

(R1) Permutation of rows

(R2) Multiplication of a row by a nonzero scalar

(R3) Addition of a scalar multiple of one row to another

(C1) Permutations of columns

(C2) Multiplication of a column by a nonzero scalar.

T. Let G be a generating matrix of (n, q^k) code

(G is a $(k \times n)$ q-ary matrix)

Then using (R1) $\div$ R(3) and (C1), (C2) G can be transformed into a

Standard form

$$G = [\, I \,\vdots\, P \,]$$

where: I $(k \times k)$ identity matrix

P $(k \times (n-k))$ matrix