Coding and Information Theory

Mathematical Fundamentals (C)

Dr. Xuejun Liang

Quick Review of Last Lecture

- Field Definition and Examples
- Extension Field
  - $Z_p[x]/(f)$: Galois field $GF(p^n)$
  - Examples
- Definition of Linear (vector) space

Linear (vector) space: Definition

A linear space V over a field F is a set whose elements are called vectors and where two operations, addition and scalar multiplication, are defined:

1. **addition**, denoted by +, such that to every pair $x, y \in V$ there correspond a vector $x + y \in V$, and
   - $x + y = y + x$,
   - $x + (y + z) = (x + y) + z$, $x, y, z \in V$;

   (V, +) is a group, with identity element denoted by 0 and inverse denoted by −, $x + (-x) = x - x = 0$.
2. **scalar multiplication** of $x \in V$ by elements $k \in F$, denoted by $kx \in V$, and
   - $k(ax) = (ka)x$,
   - $k(x + y) = kx + ky$,
   - $(k + a)x = kx + ax$, $x, y \in V$, $k, a \in F$.

   Moreover $1x = x$ for all $x \in V$, 1 being the unit in F.

Subspace and Linearly independent

- Subspace: $S \subseteq V$
  - addition and scalar multiplication are closed in S
- Linear combination
  - $a_1v_1+a_2v_2+ \ldots + a_nv_n$
  - Linearly independent of $v_1, v_2, \ldots, v_n$
    - If $a_1v_1+a_2v_2+ \ldots + a_nv_n = 0$ then $a_1=0, a_2=0, \ldots, a_n=0$.
  - Linearly dependent of $v_1, v_2, \ldots, v_n$
    - There are $a_1, a_2, \ldots, a_n$ (not all 0's) such that

$$a_1v_1+a_2v_2+ \ldots + a_nv_n = 0$$

Example: determine if the three vectors over Z_2 (GF(2)) are linearly dependent or not.

1. $\mathbf{u}_1 = (1\ 0\ 1\ 1)$, $\mathbf{u}_2 = (0\ 1\ 0\ 0)$, and $\mathbf{u}_3 = (1\ 1\ 1\ 1)$
2. $\mathbf{v}_1 = (0\ 1\ 1\ 0)$, $\mathbf{v}_2 = (1\ 0\ 0\ 1)$, and $\mathbf{v}_3 = (1\ 0\ 1\ 1)$

Basis and Dimension

- Basis (or Base)
  - Basis: independent vectors that can span the whole vector space.
  - Any vector is a linear combination of basis vectors.
- Dimension
  - Number of vectors within the basis
  - Example: V_n is n-dimension

Example: determine a basis and the dimension of the subspace S in V_4 over Z_2 consisting of vectors:

(0 0 0 0) (1 1 0 0) (1 0 1 0) (0 0 0 1)
(0 1 1 0) (1 1 0 1) (1 0 1 1) (0 1 1 1)

v_1 = (1 1 0 0), v_2 = (1 0 1 0), v_3 = (0 1 1 1) are independent and

$$a_1v_1 + a_2v_2 + a_3v_3, \text{ where } a_1, a_2, a_3 \in Z_2.$$

generates vectors in S. So v_1, v_2, v_3 is a basis of S.

$0v_1 + 0v_2 + 0v_3$	= (0 0 0 0)
$0v_1 + 0v_2 + 1v_3 = v_3$	= (0 1 1 1)
$0v_1 + 1v_2 + 0v_3 = v_2$	= (1 0 1 0)
$0v_1 + 1v_2 + 1v_3 = v_2+v_3$	= (1 1 0 1)
$1v_1 + 0v_2 + 0v_3 = v_1$	= (1 1 0 0)
$1v_1 + 0v_2 + 1v_3 = v_1+v_3$	= (1 0 1 1)
$1v_1 + 1v_2 + 0v_3 = v_1+v_2$	= (0 1 1 0)
$1v_1 + 1v_2 + 1v_3 = v_1+v_2+v_3$	= (0 0 0 1)

Orthogonality and Dual Space

- Orthogonality
  - **Inner product** of $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$:
    $$\mathbf{u} \cdot \mathbf{v} = u_0 v_0 + u_1 v_1 + \ldots, + u_{n-1} v_{n-1}$$
  - $\mathbf{u}$ and $\mathbf{v}$ are said orthogonal if $\mathbf{u} \cdot \mathbf{v} = 0$
  - Subspaces S and P of V_n are said orthogonal if for any $\mathbf{u} \in S$ and any $\mathbf{v} \in P$, we have $\mathbf{u} \cdot \mathbf{v} = 0$
- Dual Space
  - Subspace S of V_n is the dual space (null space) of another subspace P of V_n if S and P are orthogonal and
    $$\dim(S) + \dim(P) = n$$

Example: Show S and P are dual each other

S = {(0 0 0 0), (1 1 0 0), (1 0 1 1), (0 1 1 1)

P = {(0 0 0 0), (1 1 0 1), (1 1 1 0), (0 0 1 1)

Matrix

$$\mathbf{G} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{m-1,0} & g_{m-1,1} & g_{m-1,2} & \cdots & g_{m-1,n-1} \end{bmatrix}$$

- Let G be a m×n matrix
  - All linear combinations of row vectors of G is a subspace of $V_{n,}$ called **row vector space** of G.
  - All linear combinations of column vectors of G is a subspace of V_m called **column vector space** of G.
  - The dimension of row vector space is called **row rank** and the dimension of column vector space is called **column rank**.
  - Row rank and column are always equal, it is called **the rank of the matrix.**
- Elementary row operations of a matrix
  - swap two rows, multiply a row with a scalar, add multiple of a row to another
- Elementary row operations do not change the row rank.

Example: Determine the row space of matrix over Z_2

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Let $v_1 = (1\ 0\ 0\ 1\ 0\ 1)$, $v_2 = (0\ 1\ 0\ 0\ 1\ 1)$, $v_3 = (0\ 0\ 1\ 1\ 1\ 0)$, then

$$a_1v_1 + a_2v_2 + a_3v_3, \text{ where } a_1, a_2, a_3 \in Z_2.$$

generates the following vectors

$0v_1 + 0v_2 + 0v_3$	$= (0\ 0\ 0\ 0\ 0\ 0)$
$0v_1 + 0v_2 + 1v_3 = v_3$	$= (0\ 0\ 1\ 1\ 1\ 0)$
$0v_1 + 1v_2 + 0v_3 = v_2$	$= (0\ 1\ 0\ 0\ 1\ 1)$
$0v_1 + 1v_2 + 1v_3 = v_2+v_3$	$= (0\ 1\ 1\ 1\ 0\ 1)$
$1v_1 + 0v_2 + 0v_3 = v_1$	$= (1\ 0\ 0\ 1\ 0\ 1)$
$1v_1 + 0v_2 + 1v_3 = v_1+v_3$	$= (1\ 0\ 1\ 0\ 1\ 1)$
$1v_1 + 1v_2 + 0v_3 = v_1+v_2$	$= (1\ 1\ 0\ 1\ 1\ 0)$
$1v_1 + 1v_2 + 1v_3 = v_1+v_2+v_3$	$= (1\ 1\ 1\ 0\ 0\ 0)$

Example:

- Consider the G in previous example. Compute a matric G' by adding row 3 of G to row 1 of G and then interchanging rows 2 and 3 of G.
- Show that the row space of G' is the same as that generated by G.

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \Longrightarrow G' = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Let v_1 = (1 0 1 0 1 1), v_2 = (0 0 1 1 1 0), v_3 = (0 1 0 0 1 1), then

$$a_1v_1 + a_2v_2 + a_3v_3, \text{ where } a_1, a_2, a_3 \in Z_2.$$

generates the following vectors

$0v_1 + 0v_2 + 0v_3$	= (0 0 0 0 0 0)
$0v_1 + 0v_2 + 1v_3 = v_3$	= (0 1 0 0 1 1)
$0v_1 + 1v_2 + 0v_3 = v_2$	= (0 0 1 1 1 0)
$0v_1 + 1v_2 + 1v_3 = v_2+v_3$	= (0 1 1 1 0 1)
$1v_1 + 0v_2 + 0v_3 = v_1$	= (1 0 1 0 1 1)
$1v_1 + 0v_2 + 1v_3 = v_1+v_3$	= (1 1 1 0 0 0)
$1v_1 + 1v_2 + 0v_3 = v_1+v_2$	= (1 0 0 1 0 1)
$1v_1 + 1v_2 + 1v_3 = v_1+v_2+v_3$	= (1 1 0 1 1 0)

Matrix Multiplication and Transpose

Assume $A = (a_{ij})_{m\times k}$ and $B = (b_{ij})_{k\times n}$

$$c_{ij} = (a_{i1}a_{i2} \ldots a_{ik})\begin{pmatrix} b_{1j} \\ b_{2j} \\ \cdot \\ \cdot \\ b_{kj} \end{pmatrix}$$

Then, $C = AB = (c_{ij})_{m\times n}$, where

$$c_{ij} = \sum_{l=1}^{k} a_{il}b_{lj}$$

The transpose of matrix A is defined as $A^T = (a_{ji})_{k\times m}$

$$A = \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix} \qquad AB =$$

$$A^T = \qquad B^T =$$

Linear Equations and Matrix

Assume $A = (a_{ij})_{m\times n}$ and $X = \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_n \end{pmatrix}_{n\times 1}$. Then, we have

$$AX = \begin{pmatrix} a_{11}a_{12} \dots a_{1n} \\ a_{21}a_{22} \dots a_{2n} \\ \cdot \\ \cdot \\ a_{m1}a_{m2} \dots a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \cdot \\ \cdot \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix}$$

A set of *m* simultaneous linear equations have two equivalent representations

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0$$

$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0$$

$$\dots \dots \dots$$

$$a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0$$

$$\Longleftrightarrow$$

$$\begin{pmatrix} a_{11}a_{12} \dots a_{1n} \\ a_{21}a_{22} \dots a_{2n} \\ \cdot \\ \cdot \\ a_{m1}a_{m2} \dots a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$$

$$AX = 0$$