MATH 525

Sections 2.1–2.3: Basics of Linear Codes

September 14, 2020

A linear code C of length n is a nonempty subset of $K^n = \{0, 1\}^n$ such that $\mathbf{u} + \mathbf{v} \in C$ whenever $\mathbf{u}, \mathbf{v} \in C$. Using linear algebra jargon, C is a subspace of K^n.

Advantages of linear codes:

- Theoretical: In comparison with nonlinear codes:
  1. It is easier to determine the minimum distance of linear codes.
  2. It is easier to identify error patterns that are detectable/correctable.
  3. It is easier to evaluate the performance (reliability of IMLD, etc.) of linear codes.
- Practical: In comparison with nonlinear codes, linear codes use much less hardware and/or memory for encoding and decoding.

Disadvantage of linear codes:

A linear code has more structure than a general block code; as a consequence, they usually achieve lower minimum distances than non-linear codes of the same rate. Therefore, non-linear codes have higher error-correction and detection capabilities.

Key concepts from linear algebra we will use throughout the course:

1. Vector spaces
2. Linear combinations
3. Linear span of a set of vectors
4. Linearly dependent and linearly independent sets
5. Basis of a vector space
6. Dimension of a vector space
7. Subspaces
8. Matrices: Row space, column space, rank, and null space.
9. The Rank Theorem: Let A be an $m \times n$ matrix with entries in a field F. Then
$$\operatorname{rank} A + \dim \operatorname{Nul} A = n.$$

Basic definitions:

- $K = \{0, 1\}$ is the binary field. For any positive integer n, K^n is the vector space over K consisting of all binary n-tuples.
- A linear code C of length n is a subspace of K^n. Equivalently, a nonempty set $C \subseteq K^n$ is a linear code of length n if $\mathbf{u} + \mathbf{v} \in C$ whenever $\mathbf{u}, \mathbf{v} \in C$. In a linear code, the all-zero vector $\mathbf{0}$ is always a codeword. Note: A subset of K^n containing $\mathbf{0}$ may not be a linear code.
- If C is a linear code, then

$$\begin{aligned} d(C) &= \min\{d(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\} \\ &= \min\{\mathrm{wt}(\mathbf{u} + \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\} \\ &= \min\{\mathrm{wt}(\mathbf{w}) \mid \mathbf{w} \in C, \mathbf{w} \neq \mathbf{0}\} \end{aligned}$$

- In conclusion, the minimum distance of a linear code is the minimum weight of its nonzero codewords.

- $\mathbf{w} \in K^n$ is a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in K^n$ if there are scalars $a_1, a_2, \ldots, a_k \in K$ such that

$$\mathbf{w} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k.$$

- If $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\} \subseteq K^n$, then $\langle S \rangle$ denotes the subspace (or the code) generated by S:

$$\langle S \rangle = \{a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k \mid a_1, a_2, \ldots, a_k \in K\}.$$

- Let $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$ be two elements of K^n. Their dot product (or scalar product) is defined as:

$$\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n$$

  where all sums and multiplications take place in K. Note that $\mathbf{u} \cdot \mathbf{v} \in K$. Basic property: $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$ for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in K^n$.

- $\mathbf{u}$ and $\mathbf{v}$ in K^n are said to be orthogonal if $\mathbf{u} \cdot \mathbf{v} = 0$. Notation: $\mathbf{u} \perp \mathbf{v}$.

- $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\} \subseteq K^n$ is said to be linearly dependent (LD) if there are scalars $a_1, a_2, \ldots, a_k \in K$, not all zero, such that

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = \mathbf{0}.$$

  Otherwise, S is said to be linearly independent (LI). As customary, $\mathbf{0}$ denotes the all-zero vector.

- Let $C \neq \{\mathbf{0}\}$ be a subspace of the vector space K^n. An indexed set of vectors $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\} \subseteq C$ is a basis for C if:
  1. $\mathcal{B}$ is a linearly independent set, and
  2. $C = \langle \mathcal{B} \rangle$.
- From linear algebra, any set of vectors $S \neq \{\mathbf{0}\}$ contains a largest linearly independent set. This set is a basis for $\langle S \rangle$. See the next slide for an example.
- If $C = \langle S \rangle$, $S \neq \{\mathbf{0}\}$, then C has a basis, say, $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$. Any codeword $\mathbf{v} \in C$ can be written in a unique way as

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k.$$

  Hence, $|C| = 2^k$. The parameter k is known as the dimension of code C. Note that the rate of C is $R = \dfrac{\log_2 2^k}{n} = \dfrac{k}{n}$.

Example

Let $v_1 = 10100, v_2 = 10110, v_3 = 10101, v_4 = 00011$ and $S = \{v_1, v_2, v_3, v_4\} \subseteq K^5$. Write down the elements of $\langle S \rangle$.

a	b	c	d	$a \cdot v_1 + b \cdot v_2 + c \cdot v_3 + d \cdot v_4$
0	0	0	0	00000
0	0	0	1	00011
0	0	1	0	10101
0	0	1	1	10110
0	1	0	0	10110
0	1	0	1	10101
0	1	1	0	00011
0	1	1	1	00000
1	0	0	0	10100
1	0	0	1	10111
1	0	1	0	00001
1	0	1	1	00010
1	1	0	0	00010
1	1	0	1	00001
1	1	1	0	10111
1	1	1	1	10100

- $\langle S \rangle = \{00000, 00011, 101101, 10110, 10100, 10111, 00001, 00010\}$.
- A basis for $\langle S \rangle$ is $\{v_1, v_2, v_3\}$.

- For any set $S \subseteq K^n$, the orthogonal complement of S is the set

$$S^{\perp} = \{\mathbf{w} \in K^n \mid \mathbf{u} \cdot \mathbf{w} = 0 \quad \forall\, \mathbf{u} \in S\} \subseteq K^n.$$

Example

Let $S = \{1011, 0110\}$. Then $S^{\perp} = \{a \cdot (1001) + b \cdot (0111) \mid a, b \in K\}$.

- From linear algebra, $S^{\perp}$ is a subspace of K^n.
- If $C = \langle S \rangle$, then $C^{\perp}$ is called the dual code of C.
- The dual code of a linear code of length n is another linear code of length n.
- Let C be a linear code of length n. We shall prove later on that if the dimension of C is equal to k, then the dimension of $C^{\perp}$ is equal to $n - k$.