Coding Theory

Alec Zabel-Mena

February 27, 2022

Contents

1 Linear Codes. **5**

1.1 Definitions, Generator, and Check Matrices. 5

Chapter 1

Linear Codes.

1.1 Definitions, Generator, and Check Matrices.

Definition. Wed define an (n, k)**-linear code)** over a field F to be a k-dimensional subspace $\mathcal{C}$ of the n-dimensional vector space F^n over F.

Remark. We shall be focusing exclusively on the finit fields $\mathbb{F}_p$ where $p = 2, 3$. Then in this case, we can consider the vector spaces to be extension fields of $\mathbb{F}_p$. We shall prove theorems and lemmas however, for general fields, unless specified.

Definition. Let $\mathcal{C}$ be an (n, k)-linear codeover a field F. We we call a $k \times n$matrix G a **generator matrix** for $\mathcal{C}$ if its row space is $\mathcal{C}$.

Example 1.1. [1]

(1) A $(5, 1)$-linear code, $\mathcal{C}_1$, over $\mathbb{F}_2$ with generator matrix:

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

It contains the codewords 00000 and (11111); and has rate $\frac{1}{5}$. We call $\mathcal{C}_1$ the **binary repitition code**.

(2) The $(5, 3)$-code $\mathcal{C}_2$ with generator matrix:

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$\mathcal{C}_2$ has rate $\frac{3}{5}$.

(3) The $(7, 4)$**-Hamming Code**, $\mathcal{C}_3$ over $\mathbb{F}_2$ with generator matrix:

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

The $(7, 4)$-Hamming code has rate $\frac{4}{7}$.

Lemma 1.1.1. *If $\mathcal{C}$ is an (n,k)-code over a field F, and if G is a generator matrix for $\mathcal{C}$, then so is any matrix row-equivalent to G.*

Proof. Let A be an $k \times n$ matrix row-equivalent to G. Then, take $A \to G$ via the sequence of elementary matrices $\{E_i\}_{i=1}^m$. That is, $G = E_m \dots E_2 E_2 A$. Then for any $v \in F^n$. we can take $Av \to Gv$ via this same sequence; that is $Gv = E_m \dots E_2 E_1 Av$. Thus, A generates the same set of vectors as G, and hence has the same row space. ■

Remark. Thus, using this lemma, one would ideally like to find a generator matrix in Row-Reduced-Echelon form, for ease of computation.

Definition. If $\mathcal{C}$ is an (n,k)-code over a field F, we define a **check** for $\mathcal{C}$ to be the equation:

$$a_1x_1 + \cdots + a_nx_n = 0 \tag{1.1}$$

satisfied for all $x \in \mathcal{C}$. We define the **dual code** of $\mathcal{C}$ to be the orthogonal complement

$$\mathcal{C}^{\perp} = \{a \in F^n : \langle a, x\rangle = 0\} \tag{1.2}$$

Where $\langle a, x\rangle$ is the inner product of a and x.

Proof. If $\mathcal{C}$ is an $(n,k) - code$, then $\mathcal{C}^{\perp}$ is an $(n, n-k)$-linear code. ■

Proof. We have by a result from [2] (theorem $4.I$), that $F^n = \mathcal{C} \oplus \mathcal{C}^{\perp}$, ($\oplus$ the direct sum). Then $\dim F^n = \dim \mathcal{C} + \dim \mathcal{C}^{\perp}$. Therefore, $\dim \mathcal{C}^{\perp} = n - k$. ■

Definition. Let $\mathcal{C}$ be an (n,k)-linear code over a field F. We define a **check** matrix for $\mathcal{C}$ the be an $n \times (n-k)$ matrix H such that $Hx^T = 0$.

Lemma 1.1.2. *If H is a check matrix for the (n,k)-code $\mathcal{C}$, then H is a generator matrix for the dual code $\mathcal{C}^{\perp}$.*

Proof. For any $x = (x_1, \dots, x_n) \in \mathcal{C}$, we have that $Hx^T = 0$, by definition. Thus, for any row $a = (a_1, \dots, a_n)$ of H. That is, $a_1x_1 + \cdots + a_nx_n = \langle a, x\rangle = 0$, making $a \in \mathcal{C}^{\perp}$. Since a is an arbitrary row of H, this holds for every row of H. Thus the row space of H is equal to $\mathcal{C}^{\perp}$. ■

Lemma 1.1.3. *Let $\mathcal{C}$ be an (n,k)-code over a field F, and let G be a generator matrix for the code. If G has the form $G = (I_{k\times k}|A)$, then the check matrix for $\mathcal{C}$, corresponding to G has the form*

$$H = (-A^T | I_{(n-k)\times(n-k)}) \tag{1.3}$$

Example 1.2. [1] Consider the generator matrices for the codes in example 1.1, then:

(1) $H_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

(2) $H_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$

(3) $H_3 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

Theorem 1.1.4. *Let $\mathcal{C}$ be an (n, k)-code over a field F. Then there is a unique $k \times n$ Row-Reduced-Echelon matrix G such that $x \in \mathcal{C}$ if, and only if x is in the row space of G. Likewise, there exists an $(n-k) \times n$ matrix H such that $x \in \mathcal{C}$ if, and only if $Hx^T = 0$.*

Corollary. *If $\mathcal{C}$ is used on a memoryless channel, then $G = (I_{k\times k}|A)$ and $H = (-A^T|I_{(n-k)\times(n-k)})$.*

1.2 Syndrome Decoding.

Bibliography

[1] R. McEliece, *The theory of information and coding.* Cambridge: Cambridge University Press, 2001.

[2] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.

[3] D. J. Welsh, *Codes and cryptography.* Oxford Oxfordshire New York: Clarendon Press Oxford University Press, 1988.

[4] K. Hoffman and R. Kunze, *Linear algebra.* Englewood Cliffs, NJ: Prentice-Hall, 1971.

[5] J. Lint, *Introduction to coding theory.* Berlin New York: Springer, 1999.

[6] J. Justesen and T. Høholdt, *A course in error-correcting codes.* Zurich, Switzerland: European Mathematical Society, 2017.