Linear codes, generator matrices, dual codes

Mikko Korpela

mikko.korpela@tkk.fi

Contents

- Linear codes - group of codes with nice properties

Contents

- Linear codes - group of codes with nice properties
- Generator matrices - method to convert information to a linear code form

Contents

- Linear codes - group of codes with nice properties
- Generator matrices - method to convert information to a linear code form
- Dual codes - offers an easy method for checking if a word is part of a linear code

Linear Codes

Linear Codes

C is a linear code if and only if

- $C \subseteq F^n$ where F is any finite field
- $C \neq \emptyset$
- $\forall \vec{x}, \vec{y} \in C \rightarrow \vec{x} + \vec{y} \in C$
- $\forall \alpha \in F$ and $\forall \vec{x} \in C \rightarrow \alpha \vec{x} \in C$

Hamming weight

- Hamming weight of a $\vec{x}$ is the number of nonzero entries in $\vec{x}$

Hamming weight

- Hamming weight of a $\vec{x}$ is the number of nonzero entries in $\vec{x}$
- Hamming weight of a $\vec{x}$ is denoted by $w(\vec{x})$

Hamming weight

- Hamming weight of a $\vec{x}$ is the number of nonzero entries in $\vec{x}$
- Hamming weight of a $\vec{x}$ is denoted by $w(\vec{x})$
- $w(\vec{x}) = d_H(\vec{0}, \vec{x})$

Hamming weight

- Hamming weight of a $\vec{x}$ is the number of nonzero entries in $\vec{x}$
- Hamming weight of a $\vec{x}$ is denoted by $w(\vec{x})$
- $w(\vec{x}) = d_H(\vec{0}, \vec{x})$
- Minimum weight of a code C is defined as

$$w_{\min}(C) = \min_{\vec{x} \in C, \vec{x} \neq \vec{0}} \{w(\vec{x})\} \tag{1}$$

Hamming weight

- Hamming weight of a $\vec{x}$ is the number of nonzero entries in $\vec{x}$
- Hamming weight of a $\vec{x}$ is denoted by $w(\vec{x})$
- $w(\vec{x}) = d_H(\vec{0}, \vec{x})$
- Minimum weight of a code C is defined as

$$w_{\min}(C) = \min_{\vec{x}\in C, \vec{x}\neq\vec{0}} \{w(\vec{x})\} \tag{1}$$

- $w_{\min}(C) = d_{\min}(C)$ for linear codes

Generator Matrices

Generator Matrices

- Rowspace is defined as
  $RS(G) = \{\alpha_1 \vec{x}_1 + \ldots + \alpha_k \vec{x}_k | \forall i : \alpha_i \in F\} \subseteq F^n$
  where $G = (\vec{x}_1, \ldots, \vec{x}_k)^T$ and $\forall i : \vec{x}_i \in F^n$

Generator Matrices

- Rowspace is defined as $RS(G) = \{\alpha_1\vec{x}_1 + \ldots + \alpha_k\vec{x}_k | \forall i : \alpha_i \in F\} \subseteq F^n$ where $G = (\vec{x}_1, \ldots, \vec{x}_k)^T$ and $\forall i : \vec{x}_i \in F^n$
- Rowspace defines the set of vectors that can be generated with the matrix G by calculating $\vec{\alpha} \cdot G$ where $\vec{\alpha} \in F^k$

Generator Matrices

- Rowspace is defined as $RS(G) = \{\alpha_1\vec{x}_1 + \ldots + \alpha_k\vec{x}_k | \forall i : \alpha_i \in F\} \subseteq F^n$ where $G = (\vec{x}_1, \ldots, \vec{x}_k)^T$ and $\forall i : \vec{x}_i \in F^n$
- Rowspace defines the set of vectors that can be generated with the matrix G by calculating $\vec{\alpha} \cdot G$ where $\vec{\alpha} \in F^k$
- If rows of a matrix G are linearly independent vectors from F^n and the rowspace of the matrix is linear code C then the matrix is called generator matrix for the code C

Generator Matrices

- Rowspace is defined as
$RS(G) = \{\alpha_1 \vec{x}_1 + \ldots + \alpha_k \vec{x}_k | \forall i : \alpha_i \in F\} \subseteq F^n$
where $G = (\vec{x}_1, \ldots, \vec{x}_k)^T$ and $\forall i : \vec{x}_i \in F^n$
- Rowspace defines the set of vectors that can be generated with the matrix G by calculating $\vec{\alpha} \cdot G$ where $\vec{\alpha} \in F^k$
- If rows of a matrix G are linearly independent vectors from F^n and the rowspace of the matrix is linear code C then the matrix is called generator matrix for the code C
- Generator matrix offers an easy way to map information to a linear code

Dual Codes

Dual Codes

- The dual code of C, denoted $C^\perp$ is the code

$$C^\perp = \{\vec{x} \in F^n | \forall \vec{c} \in C : \vec{x} \cdot \vec{c} = 0\} \tag{2}$$

Dual Codes

- The dual code of C, denoted $C^{\perp}$ is the code

$$C^{\perp} = \{\vec{x} \in F^{n} | \forall \vec{c} \in C : \vec{x} \cdot \vec{c} = 0\} \tag{2}$$

- For a linear codes C generator matrix G it holds that $\vec{x} \in C^{\perp} \leftrightarrow G \cdot \vec{x}^{T} = \vec{0}$

Dual Codes

- The dual code of C, denoted $C^{\perp}$ is the code

(2) $$C^{\perp} = \{\vec{x} \in F^{n} | \forall \vec{c} \in C : \vec{x} \cdot \vec{c} = 0\}$$

- For a linear codes C generator matrix G it holds that $\vec{x} \in C^{\perp} \leftrightarrow G \cdot \vec{x}^{T} = \vec{0}$
- If C is a linear code then $C^{\perp}$ is a linear code and $(C^{\perp})^{\perp} = C$

Dual Codes

- The dual code of C, denoted $C^{\perp}$ is the code

$$C^{\perp} = \{\vec{x} \in F^n | \forall \vec{c} \in C : \vec{x} \cdot \vec{c} = 0\} \tag{2}$$

- For a linear codes C generator matrix G it holds that $\vec{x} \in C^{\perp} \leftrightarrow G \cdot \vec{x}^T = \vec{0}$
- If C is a linear code then $C^{\perp}$ is a linear code and $(C^{\perp})^{\perp} = C$
- Linear codes $C^{\perp}$ generator matrix H can be used to easily check if an element $\vec{x} \in F^n$ is part of the linear code or not by checking if $H \cdot \vec{x}^T = \vec{0}$ holds

Dual Codes

- The dual code of C, denoted $C^{\perp}$ is the code

(2) $$C^{\perp} = \{\vec{x} \in F^n | \forall \vec{c} \in C : \vec{x} \cdot \vec{c} = 0\}$$

- For a linear codes C generator matrix G it holds that $\vec{x} \in C^{\perp} \leftrightarrow G \cdot \vec{x}^T = \vec{0}$
- If C is a linear code then $C^{\perp}$ is a linear code and $(C^{\perp})^{\perp} = C$
- Linear codes $C^{\perp}$ generator matrix H can be used to easily check if an element $\vec{x} \in F^n$ is part of the linear code or not by checking if $H \cdot \vec{x}^T = \vec{0}$ holds
- A generator matrix H for linear code $C^{\perp}$ is called a check matrix for code C

Conclusion

- Linear codes are a set of codes that have nice properties that make it easy to manipulate them
- Many real life error checking codes are linear codes