NDMI011: Combinatorics and Graph Theory 1

Lecture #13

Linear codes

Irena Penev

January 5, 2021

This lecture consists of three parts:

- a bit of Linear Algebra;

This lecture consists of three parts:

- a bit of Linear Algebra;
- linear codes;

This lecture consists of three parts:

- a bit of Linear Algebra;
- linear codes;
- Hamming codes.

Part I: A bit of Linear Algebra

Part I: A bit of Linear Algebra

- This is essentially a review of some Linear Algebra topics, but we will use row vectors instead of column vectors, and we will swap the roles of rows and columns in matrices.
    - Reason: this is customary in coding theory.

Part I: A bit of Linear Algebra

- This is essentially a review of some Linear Algebra topics, but we will use row vectors instead of column vectors, and we will swap the roles of rows and columns in matrices.
  - Reason: this is customary in coding theory.
- For a field $\mathbb{F}$ and a positive integer n, we denote by $\mathbb{F}^n$ the set of all row vectors of length n whose entries are all in $\mathbb{F}$.

Part I: A bit of Linear Algebra

- This is essentially a review of some Linear Algebra topics, but we will use row vectors instead of column vectors, and we will swap the roles of rows and columns in matrices.
  - Reason: this is customary in coding theory.
- For a field $\mathbb{F}$ and a positive integer n, we denote by $\mathbb{F}^n$ the set of all row vectors of length n whose entries are all in $\mathbb{F}$.
- For vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in $\mathbb{F}^n$, we define $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i$, where the summation and multiplication denote the operations from the field $\mathbb{F}$.
  - So, $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{F}$.

Part I: A bit of Linear Algebra

- This is essentially a review of some Linear Algebra topics, but we will use row vectors instead of column vectors, and we will swap the roles of rows and columns in matrices.
  - Reason: this is customary in coding theory.
- For a field $\mathbb{F}$ and a positive integer n, we denote by $\mathbb{F}^n$ the set of all row vectors of length n whose entries are all in $\mathbb{F}$.
- For vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in $\mathbb{F}^n$, we define $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i$, where the summation and multiplication denote the operations from the field $\mathbb{F}$.
  - So, $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{F}$.
  - If $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, then $\mathbf{x}$ and $\mathbf{y}$ are said to be *orthogonal*.

- Instead of multiplying matrices by column vectors on the right ($A\mathbf{x}$), we will multiply matrices by row vectors on the left ($\mathbf{x}A$).

- Instead of multiplying matrices by column vectors on the right ($A\mathbf{x}$), we will multiply matrices by row vectors on the left ($\mathbf{x}A$).
- If A is an $n \times m$ matrix with entries in $\mathbb{F}$, and $\mathbf{x} \in \mathbb{F}^n$, then we can think of $\mathbf{x}$ as a $1 \times n$ matrix, and we can compute $\mathbf{x}A$ according to the usual rules of matrix multiplication.
    - We obtain a row vector of length m.

- Instead of multiplying matrices by column vectors on the right ($A\mathbf{x}$), we will multiply matrices by row vectors on the left ($\mathbf{x}A$).
- If A is an $n \times m$ matrix with entries in $\mathbb{F}$, and $\mathbf{x} \in \mathbb{F}^n$, then we can think of $\mathbf{x}$ as a $1 \times n$ matrix, and we can compute $\mathbf{x}A$ according to the usual rules of matrix multiplication.
  - We obtain a row vector of length m.
- If $\mathbf{x} = (x_1, \dots, x_n)$ and $A = \begin{bmatrix} \mathbf{r}_1 \\ \vdots \\ \mathbf{r}_n \end{bmatrix}$ (i.e. $\mathbf{r}_1, \dots, \mathbf{r}_n$ are the rows of A, from top to bottom), then $\mathbf{x}A = \sum_{i=1}^{n} x_i \mathbf{r}_i$.

- Instead of multiplying matrices by column vectors on the right ($A\mathbf{x}$), we will multiply matrices by row vectors on the left ($\mathbf{x}A$).
- If A is an $n \times m$ matrix with entries in $\mathbb{F}$, and $\mathbf{x} \in \mathbb{F}^n$, then we can think of $\mathbf{x}$ as a $1 \times n$ matrix, and we can compute $\mathbf{x}A$ according to the usual rules of matrix multiplication.
    - We obtain a row vector of length m.
- If $\mathbf{x} = (x_1, \ldots, x_n)$ and $A = \begin{bmatrix} \mathbf{r}_1 \\ \vdots \\ \mathbf{r}_n \end{bmatrix}$ (i.e. $\mathbf{r}_1, \ldots, \mathbf{r}_n$ are the rows of A, from top to bottom), then $\mathbf{x}A = \sum_{i=1}^{n} x_i \mathbf{r}_i$.
- If $\mathbf{e}_i$ is the i-th standard basis vector of $\mathbb{F}^n$, i.e. the row vector whose i-th entry is 1, and all of whose other entries are 0, then $\mathbf{e}_i A$ is equal to the i-th row of A.

- Instead of multiplying matrices by column vectors on the right ($A\mathbf{x}$), we will multiply matrices by row vectors on the left ($\mathbf{x}A$).
- If A is an $n \times m$ matrix with entries in $\mathbb{F}$, and $\mathbf{x} \in \mathbb{F}^n$, then we can think of $\mathbf{x}$ as a $1 \times n$ matrix, and we can compute $\mathbf{x}A$ according to the usual rules of matrix multiplication.
    - We obtain a row vector of length m.
- If $\mathbf{x} = (x_1, \ldots, x_n)$ and $A = \begin{bmatrix} \mathbf{r}_1 \\ \vdots \\ \mathbf{r}_n \end{bmatrix}$ (i.e. $\mathbf{r}_1, \ldots, \mathbf{r}_n$ are the rows of A, from top to bottom), then $\mathbf{x}A = \sum_{i=1}^{n} x_i \mathbf{r}_i$.
- If $\mathbf{e}_i$ is the i-th standard basis vector of $\mathbb{F}^n$, i.e. the row vector whose i-th entry is 1, and all of whose other entries are 0, then $\mathbf{e}_i A$ is equal to the i-th row of A.
- With these adjustments, all familiar theorems of Linear Algebra still hold, but with rows and columns reversed.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define
$C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

- It is easy to see that $C^\perp$ is a subspace of $\mathbb{F}^n$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

- It is easy to see that $C^\perp$ is a subspace of $\mathbb{F}^n$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proof.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

- It is easy to see that $C^\perp$ is a subspace of $\mathbb{F}^n$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proof. Set $k = \dim C$. WTS $\dim C^\perp = n - k$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

- It is easy to see that $C^\perp$ is a subspace of $\mathbb{F}^n$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proof. Set $k = \dim C$. WTS $\dim C^\perp = n - k$. If $k = 0$, then $C = \{\mathbf{0}\}$ and $C^\perp = \mathbb{F}^n$, and so $\dim C^\perp = n = n - k$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

- It is easy to see that $C^\perp$ is a subspace of $\mathbb{F}^n$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proof. Set $k = \dim C$. WTS $\dim C^\perp = n - k$. If $k = 0$, then $C = \{\mathbf{0}\}$ and $C^\perp = \mathbb{F}^n$, and so $\dim C^\perp = n = n - k$. From now on, we assume that $k \geq 1$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

- It is easy to see that $C^\perp$ is a subspace of $\mathbb{F}^n$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proof. Set $k = \dim C$. WTS $\dim C^\perp = n - k$. If $k = 0$, then $C = \{\mathbf{0}\}$ and $C^\perp = \mathbb{F}^n$, and so $\dim C^\perp = n = n - k$. From now on, we assume that $k \geq 1$. Let $\{\mathbf{c}_1, \dots, \mathbf{c}_k\}$ be a basis for C, and let $G = \begin{bmatrix} \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_k \end{bmatrix}$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

- It is easy to see that $C^\perp$ is a subspace of $\mathbb{F}^n$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proof. Set $k = \dim C$. WTS $\dim C^\perp = n - k$. If $k = 0$, then $C = \{\mathbf{0}\}$ and $C^\perp = \mathbb{F}^n$, and so $\dim C^\perp = n = n - k$. From now on, we assume that $k \geq 1$. Let $\{\mathbf{c}_1, \dots, \mathbf{c}_k\}$ be a basis for C, and let $G = \begin{bmatrix} \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_k \end{bmatrix}$. Then $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \mathbf{y}G^T = \mathbf{0}\} = \mathrm{Ker}(G^T)$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

- It is easy to see that $C^\perp$ is a subspace of $\mathbb{F}^n$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proof. Set $k = \dim C$. WTS $\dim C^\perp = n - k$. If $k = 0$, then $C = \{\mathbf{0}\}$ and $C^\perp = \mathbb{F}^n$, and so $\dim C^\perp = n = n - k$. From now on, we assume that $k \geq 1$. Let $\{\mathbf{c}_1, \dots, \mathbf{c}_k\}$ be a basis for C, and let $G = \begin{bmatrix} \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_k \end{bmatrix}$. Then $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \mathbf{y}G^T = \mathbf{0}\} = \mathrm{Ker}(G^T)$. By the Rank-nullity theorem, $\mathrm{rank}(G^T) + \dim \mathrm{Ker}(G^T) = n$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

- It is easy to see that $C^\perp$ is a subspace of $\mathbb{F}^n$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proof. Set $k = \dim C$. WTS $\dim C^\perp = n - k$. If $k = 0$, then $C = \{\mathbf{0}\}$ and $C^\perp = \mathbb{F}^n$, and so $\dim C^\perp = n = n - k$. From now on, we assume that $k \geq 1$. Let $\{\mathbf{c}_1, \dots, \mathbf{c}_k\}$ be a basis for C, and let $G = \begin{bmatrix} \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_k \end{bmatrix}$. Then $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \mathbf{y}G^T = \mathbf{0}\} = \text{Ker}(G^T)$. By the Rank-nullity theorem, $\text{rank}(G^T) + \dim \text{Ker}(G^T) = n$. But $\text{rank}(G^T) = \text{rank}(G) = k$, and it follows that $k + \dim C^\perp = n$, i.e. $\dim C^\perp = n - k$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proposition 1.2

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $(C^\perp)^\perp = C$.

Proof.

Definition

For a field $\mathbb{F}$ and a subspace C of $\mathbb{F}^n$, we define $C^\perp = \{\mathbf{y} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$.

Theorem 1.1

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $\dim C + \dim C^\perp = n$.

Proposition 1.2

Let $\mathbb{F}$ be a field, and let C be a subspace of $\mathbb{F}^n$. Then $(C^\perp)^\perp = C$.

Proof. Obviously, $C \subseteq (C^\perp)^\perp$; since C and $(C^\perp)^\perp$ are both subspaces of $\mathbb{F}^n$, it follows that C is a subspace of $(C^\perp)^\perp$. On the other hand, by Theorem 1.1, we have that

$$\dim (C^\perp)^\perp = n - \dim C^\perp = n - (n - \dim C) = \dim C,$$

and we deduce that $C = (C^\perp)^\perp$.

Part II: Linear codes

Part II: Linear codes

Definition

A *linear code* is a subspace C of a vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is a finite field of size q (here, q is a prime power).

Part II: Linear codes

Definition

A *linear code* is a subspace C of a vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is a finite field of size q (here, q is a prime power).

- Note that every linear code contains the zero vector.

Part II: Linear codes

Definition

A *linear code* is a subspace C of a vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is a finite field of size q (here, q is a prime power).

- Note that every linear code contains the zero vector.
- If a linear code C is an $(n, k, d)_q$-code, then we write that C is an $[n, k, d]_q$-code.

Part II: Linear codes

Definition

A *linear code* is a subspace C of a vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is a finite field of size q (here, q is a prime power).

- Note that every linear code contains the zero vector.
- If a linear code C is an $(n, k, d)_q$-code, then we write that C is an $[n, k, d]_q$-code.
  - Reminder:
    - $q =$ size of alphabet;
    - $n =$ length of codewords;
    - $k = \log_q |C|$;
    - $d =$ minimum distance between codewords.
  - The square brackets indicate that C is a linear code.

Part II: Linear codes

Definition

A *linear code* is a subspace C of a vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is a finite field of size q (here, q is a prime power).

- Note that every linear code contains the zero vector.
- If a linear code C is an $(n, k, d)_q$-code, then we write that C is an $[n, k, d]_q$-code.
  - Reminder:
    - $q =$ size of alphabet;
    - $n =$ length of codewords;
    - $k = \log_q |C|$;
    - $d =$ minimum distance between codewords.
  - The square brackets indicate that C is a linear code.
- An $[n, k, d]_q$-code is a subspace of $\mathbb{F}_q^n$.

Part II: Linear codes

Definition

A *linear code* is a subspace C of a vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is a finite field of size q (here, q is a prime power).

- Note that every linear code contains the zero vector.
- If a linear code C is an $(n, k, d)_q$-code, then we write that C is an $[n, k, d]_q$-code.
  - Reminder:
    - $q =$ size of alphabet;
    - $n =$ length of codewords;
    - $k = \log_q |C|$;
    - $d =$ minimum distance between codewords.
  - The square brackets indicate that C is a linear code.
- An $[n, k, d]_q$-code is a subspace of $\mathbb{F}_q^n$.

Proposition 2.1

Let C be an $[n, k, d]_q$-code. Then $\dim C = k$, i.e. the dimension of C as a vector space is k.

Proposition 2.1

Let C be an $[n, k, d]_q$-code. Then $\dim C = k$, i.e. the dimension of C as a vector space is k.

Proof.

Proposition 2.1

Let C be an $[n, k, d]_q$-code. Then $\dim C = k$, i.e. the dimension of C as a vector space is k.

Proof. Since C is an $[n, k, d]_q$-code, we know that C is a subspace of $\mathbb{F}_q^n$; set $\ell = \dim C$. WTS $\ell = k$.

Proposition 2.1

Let C be an $[n, k, d]_q$-code. Then $\dim C = k$, i.e. the dimension of C as a vector space is k.

Proof. Since C is an $[n, k, d]_q$-code, we know that C is a subspace of $\mathbb{F}_q^n$; set $\ell = \dim C$. WTS $\ell = k$.

Let $\{\mathbf{c}_1, \ldots, \mathbf{c}_\ell\}$ be a basis for C.

Proposition 2.1

Let C be an $[n, k, d]_q$-code. Then $\dim C = k$, i.e. the dimension of C as a vector space is k.

Proof. Since C is an $[n, k, d]_q$-code, we know that C is a subspace of $\mathbb{F}_q^n$; set $\ell = \dim C$. WTS $\ell = k$.

Let $\{\mathbf{c}_1, \ldots, \mathbf{c}_\ell\}$ be a basis for C. Then C is the set of all vectors of the form $\sum_{i=1}^{\ell} \alpha_i \mathbf{c}_i$, where $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_q$. There are q choices for each α_i, and so there are q^ℓ choices for the ℓ-tuple $(\alpha_1, \ldots, \alpha_\ell)$.

Proposition 2.1

Let C be an $[n, k, d]_q$-code. Then $\dim C = k$, i.e. the dimension of C as a vector space is k.

Proof. Since C is an $[n, k, d]_q$-code, we know that C is a subspace of $\mathbb{F}_q^n$; set $\ell = \dim C$. WTS $\ell = k$.

Let $\{\mathbf{c}_1, \ldots, \mathbf{c}_\ell\}$ be a basis for C. Then C is the set of all vectors of the form $\sum_{i=1}^{\ell} \alpha_i \mathbf{c}_i$, where $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_q$. There are q choices for each α_i, and so there are q^ℓ choices for the ℓ-tuple $(\alpha_1, \ldots, \alpha_\ell)$. On the other hand, since $\{\mathbf{c}_1, \ldots, \mathbf{c}_\ell\}$ is linearly independent (because it is a basis), we know that $\sum_{i=1}^{\ell} \alpha_i \mathbf{c}_i = \sum_{i=1}^{\ell} \beta_i \mathbf{c}_i$ iff $(\alpha_1, \ldots, \alpha_\ell) = (\beta_1, \ldots, \beta_\ell)$.

Proposition 2.1

Let C be an $[n, k, d]_q$-code. Then $\dim C = k$, i.e. the dimension of C as a vector space is k.

Proof. Since C is an $[n, k, d]_q$-code, we know that C is a subspace of $\mathbb{F}_q^n$; set $\ell = \dim C$. WTS $\ell = k$.

Let $\{\mathbf{c}_1, \dots, \mathbf{c}_\ell\}$ be a basis for C. Then C is the set of all vectors of the form $\sum_{i=1}^{\ell} \alpha_i \mathbf{c}_i$, where $\alpha_1, \dots, \alpha_\ell \in \mathbb{F}_q$. There are q choices for each α_i, and so there are q^ℓ choices for the ℓ-tuple $(\alpha_1, \dots, \alpha_\ell)$. On the other hand, since $\{\mathbf{c}_1, \dots, \mathbf{c}_\ell\}$ is linearly independent (because it is a basis), we know that $\sum_{i=1}^{\ell} \alpha_i \mathbf{c}_i = \sum_{i=1}^{\ell} \beta_i \mathbf{c}_i$ iff $(\alpha_1, \dots, \alpha_\ell) = (\beta_1, \dots, \beta_\ell)$. It follows that $|C| = q^\ell$, and consequently, $\ell = \log_q |C|$.

Proposition 2.1

Let C be an $[n, k, d]_q$-code. Then $\dim C = k$, i.e. the dimension of C as a vector space is k.

Proof. Since C is an $[n, k, d]_q$-code, we know that C is a subspace of $\mathbb{F}_q^n$; set $\ell = \dim C$. WTS $\ell = k$.

Let $\{\mathbf{c}_1, \ldots, \mathbf{c}_\ell\}$ be a basis for C. Then C is the set of all vectors of the form $\sum_{i=1}^{\ell} \alpha_i \mathbf{c}_i$, where $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_q$. There are q choices for each α_i, and so there are q^ℓ choices for the ℓ-tuple $(\alpha_1, \ldots, \alpha_\ell)$. On the other hand, since $\{\mathbf{c}_1, \ldots, \mathbf{c}_\ell\}$ is linearly independent (because it is a basis), we know that $\sum_{i=1}^{\ell} \alpha_i \mathbf{c}_i = \sum_{i=1}^{\ell} \beta_i \mathbf{c}_i$ iff $(\alpha_1, \ldots, \alpha_\ell) = (\beta_1, \ldots, \beta_\ell)$. It follows that $|C| = q^\ell$, and consequently, $\ell = \log_q |C|$.

Since $k = \log_q |C|$ (by definition), it follows that $\ell = k$, which is what we needed to show.

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.
- By Proposition 2.1, $\dim C = k$.

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.
- By Proposition 2.1, $\dim C = k$.
- Let G be any matrix whose rows form a basis for C (in particular, $G \in \mathbb{F}_q^{k \times n}$).

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.
- By Proposition 2.1, $\dim C = k$.
- Let G be any matrix whose rows form a basis for C (in particular, $G \in \mathbb{F}_q^{k \times n}$).
  - G is called the *generator matrix* of the linear code C.

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.
- By Proposition 2.1, $\dim C = k$.
- Let G be any matrix whose rows form a basis for C (in particular, $G \in \mathbb{F}_q^{k \times n}$).
  - G is called the *generator matrix* of the linear code C.
  - We have $C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{y}G^T = \mathbf{0}\}$.

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.
- By Proposition 2.1, $\dim C = k$.
- Let G be any matrix whose rows form a basis for C (in particular, $G \in \mathbb{F}_q^{k \times n}$).
  - G is called the *generator matrix* of the linear code C.
  - We have $C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{y}G^T = \mathbf{0}\}$.
- Suppose H is any matrix such that the rows of H^T form a basis for $C^\perp$.

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.
- By Proposition 2.1, $\dim C = k$.
- Let G be any matrix whose rows form a basis for C (in particular, $G \in \mathbb{F}_q^{k \times n}$).
  - G is called the *generator matrix* of the linear code C.
  - We have $C^{\perp} = \{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{y}G^T = \mathbf{0}\}$.
- Suppose H is any matrix such that the rows of H^T form a basis for $C^{\perp}$.
  - So, H^T is a generator matrix for $C^{\perp}$.
  - H is called a *parity check matrix* for C, and by Proposition 1.2, it satisfies $C = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H = \mathbf{0}\}$, i.e. $C = \mathrm{Ker}(H)$.

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.
- By Proposition 2.1, $\dim C = k$.
- Let G be any matrix whose rows form a basis for C (in particular, $G \in \mathbb{F}_q^{k \times n}$).
  - G is called the *generator matrix* of the linear code C.
  - We have $C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{y}G^T = \mathbf{0}\}$.
- Suppose H is any matrix such that the rows of H^T form a basis for $C^\perp$.
  - So, H^T is a generator matrix for $C^\perp$.
  - H is called a *parity check matrix* for C, and by Proposition 1.2, it satisfies $C = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H = \mathbf{0}\}$, i.e. $C = \mathrm{Ker}(H)$.
- The parity check matrix H can be used to check whether a vector $\mathbf{x} \in \mathbb{F}_q^n$ is a codeword of C.

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.
- By Proposition 2.1, $\dim C = k$.
- Let G be any matrix whose rows form a basis for C (in particular, $G \in \mathbb{F}_q^{k \times n}$).
  - G is called the *generator matrix* of the linear code C.
  - We have $C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{y}G^T = \mathbf{0}\}$.
- Suppose H is any matrix such that the rows of H^T form a basis for $C^\perp$.
  - So, H^T is a generator matrix for $C^\perp$.
  - H is called a *parity check matrix* for C, and by Proposition 1.2, it satisfies $C = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H = \mathbf{0}\}$, i.e. $C = \mathrm{Ker}(H)$.
- The parity check matrix H can be used to check whether a vector $\mathbf{x} \in \mathbb{F}_q^n$ is a codeword of C.
  - Indeed, if $\mathbf{x}H = \mathbf{0}$, then $\mathbf{x} \in C$, and otherwise, $\mathbf{x} \notin C$.

- Suppose that $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$.
- By Proposition 2.1, $\dim C = k$.
- Let G be any matrix whose rows form a basis for C (in particular, $G \in \mathbb{F}_q^{k \times n}$).
  - G is called the *generator matrix* of the linear code C.
  - We have $C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{y}G^T = \mathbf{0}\}$.
- Suppose H is any matrix such that the rows of H^T form a basis for $C^\perp$.
  - So, H^T is a generator matrix for $C^\perp$.
  - H is called a *parity check matrix* for C, and by Proposition 1.2, it satisfies $C = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H = \mathbf{0}\}$, i.e. $C = \mathrm{Ker}(H)$.
- The parity check matrix H can be used to check whether a vector $\mathbf{x} \in \mathbb{F}_q^n$ is a codeword of C.
  - Indeed, if $\mathbf{x}H = \mathbf{0}$, then $\mathbf{x} \in C$, and otherwise, $\mathbf{x} \notin C$.
- Note that, given a generator matrix for C, one can easily compute a parity check matrix for C, and vice versa.

Definition

Given a vector $\mathbf{x} \in \mathbb{F}_q^n$, the *Hamming weight* of $\mathbf{x}$, denoted by $\mathrm{wt}(\mathbf{x})$, is the number of non-zero coordinates in $\mathbf{x}$.

Definition

Given a vector $\mathbf{x} \in \mathbb{F}_q^n$, the *Hamming weight* of $\mathbf{x}$, denoted by $\mathrm{wt}(\mathbf{x})$, is the number of non-zero coordinates in $\mathbf{x}$.

Proposition 2.2

Let $C \subsetneq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$. Then $d = \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$.

Proof.

Definition

Given a vector $\mathbf{x} \in \mathbb{F}_q^n$, the *Hamming weight* of $\mathbf{x}$, denoted by $\mathrm{wt}(\mathbf{x})$, is the number of non-zero coordinates in $\mathbf{x}$.

Proposition 2.2

Let $C \subsetneq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$. Then $d = \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$.

Proof. Fix $\mathbf{x} \in C \setminus \{\mathbf{0}\}$ with minimum Hamming weight. WTS $d = \mathrm{wt}(\mathbf{x})$.

Definition

Given a vector $\mathbf{x} \in \mathbb{F}_q^n$, the *Hamming weight* of $\mathbf{x}$, denoted by $\mathrm{wt}(\mathbf{x})$, is the number of non-zero coordinates in $\mathbf{x}$.

Proposition 2.2

Let $C \subsetneq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$. Then $d = \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$.

Proof. Fix $\mathbf{x} \in C \setminus \{\mathbf{0}\}$ with minimum Hamming weight. WTS $d = \mathrm{wt}(\mathbf{x})$.

Since C is a linear code, we know that $\mathbf{0} \in C$, and so (since $\mathbf{x}$ and $\mathbf{0}$ are distinct codewords in C) we have that $d(\mathbf{x}, \mathbf{0}) \geq d$. But obviously, $d(\mathbf{x}, \mathbf{0}) = \mathrm{wt}(\mathbf{x})$, and it follows that $\mathrm{wt}(\mathbf{x}) \geq d$.

Definition

Given a vector $\mathbf{x} \in \mathbb{F}_q^n$, the *Hamming weight* of $\mathbf{x}$, denoted by $\mathrm{wt}(\mathbf{x})$, is the number of non-zero coordinates in $\mathbf{x}$.

Proposition 2.2

Let $C \subsetneq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$. Then $d = \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$.

Proof. Fix $\mathbf{x} \in C \setminus \{\mathbf{0}\}$ with minimum Hamming weight. WTS $d = \mathrm{wt}(\mathbf{x})$.

Since C is a linear code, we know that $\mathbf{0} \in C$, and so (since $\mathbf{x}$ and $\mathbf{0}$ are distinct codewords in C) we have that $d(\mathbf{x}, \mathbf{0}) \geq d$. But obviously, $d(\mathbf{x}, \mathbf{0}) = \mathrm{wt}(\mathbf{x})$, and it follows that $\mathrm{wt}(\mathbf{x}) \geq d$.

WTS $\mathrm{wt}(\mathbf{x}) \leq d$.

Definition

Given a vector $\mathbf{x} \in \mathbb{F}_q^n$, the *Hamming weight* of $\mathbf{x}$, denoted by $\mathrm{wt}(\mathbf{x})$, is the number of non-zero coordinates in $\mathbf{x}$.

Proposition 2.2

Let $C \subsetneq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$. Then $d = \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$.

Proof. Fix $\mathbf{x} \in C \setminus \{\mathbf{0}\}$ with minimum Hamming weight. WTS $d = \mathrm{wt}(\mathbf{x})$.

Since C is a linear code, we know that $\mathbf{0} \in C$, and so (since $\mathbf{x}$ and $\mathbf{0}$ are distinct codewords in C) we have that $d(\mathbf{x}, \mathbf{0}) \geq d$. But obviously, $d(\mathbf{x}, \mathbf{0}) = \mathrm{wt}(\mathbf{x})$, and it follows that $\mathrm{wt}(\mathbf{x}) \geq d$.

WTS $\mathrm{wt}(\mathbf{x}) \leq d$. Fix distinct $\mathbf{y}, \mathbf{z} \in C$ such that $d(\mathbf{y}, \mathbf{z}) = d$.

Definition

Given a vector $\mathbf{x} \in \mathbb{F}_q^n$, the *Hamming weight* of $\mathbf{x}$, denoted by $\text{wt}(\mathbf{x})$, is the number of non-zero coordinates in $\mathbf{x}$.

Proposition 2.2

Let $C \subsetneq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$. Then $d = \min\{\text{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$.

Proof. Fix $\mathbf{x} \in C \setminus \{\mathbf{0}\}$ with minimum Hamming weight. WTS $d = \text{wt}(\mathbf{x})$.

Since C is a linear code, we know that $\mathbf{0} \in C$, and so (since $\mathbf{x}$ and $\mathbf{0}$ are distinct codewords in C) we have that $d(\mathbf{x}, \mathbf{0}) \geq d$. But obviously, $d(\mathbf{x}, \mathbf{0}) = \text{wt}(\mathbf{x})$, and it follows that $\text{wt}(\mathbf{x}) \geq d$.

WTS $\text{wt}(\mathbf{x}) \leq d$. Fix distinct $\mathbf{y}, \mathbf{z} \in C$ such that $d(\mathbf{y}, \mathbf{z}) = d$. Since C is a vector space, we know that $\mathbf{y} - \mathbf{z} \in C$, and so by the choice of $\mathbf{x}$, we have that $\text{wt}(\mathbf{x}) \leq \text{wt}(\mathbf{y} - \mathbf{z})$.

Definition

Given a vector $\mathbf{x} \in \mathbb{F}_q^n$, the *Hamming weight* of $\mathbf{x}$, denoted by $\text{wt}(\mathbf{x})$, is the number of non-zero coordinates in $\mathbf{x}$.

Proposition 2.2

Let $C \subsetneq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, with $0 < k < n$. Then $d = \min\{\text{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$.

Proof. Fix $\mathbf{x} \in C \setminus \{\mathbf{0}\}$ with minimum Hamming weight. WTS $d = \text{wt}(\mathbf{x})$.

Since C is a linear code, we know that $\mathbf{0} \in C$, and so (since $\mathbf{x}$ and $\mathbf{0}$ are distinct codewords in C) we have that $d(\mathbf{x}, \mathbf{0}) \geq d$. But obviously, $d(\mathbf{x}, \mathbf{0}) = \text{wt}(\mathbf{x})$, and it follows that $\text{wt}(\mathbf{x}) \geq d$.

WTS $\text{wt}(\mathbf{x}) \leq d$. Fix distinct $\mathbf{y}, \mathbf{z} \in C$ such that $d(\mathbf{y}, \mathbf{z}) = d$. Since C is a vector space, we know that $\mathbf{y} - \mathbf{z} \in C$, and so by the choice of $\mathbf{x}$, we have that $\text{wt}(\mathbf{x}) \leq \text{wt}(\mathbf{y} - \mathbf{z})$. But now $d = d(\mathbf{y}, \mathbf{z}) = \text{wt}(\mathbf{y} - \mathbf{z}) \geq \text{wt}(\mathbf{x})$.

Part III: Hamming codes

Part III: Hamming codes

- Fix an integer $\ell \geq 2$, and set $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.

Part III: Hamming codes

- Fix an integer $\ell \geq 2$, and set $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- Our goal in this section is to construct an $[n, k, d]_2$-code, called a *Hamming code*.

Part III: Hamming codes

- Fix an integer $\ell \geq 2$, and set $n = 2^{\ell} - 1$, $k = 2^{\ell} - \ell - 1$, and $d = 3$.
- Our goal in this section is to construct an $[n, k, d]_2$-code, called a *Hamming code*.
    - It is also possible to construct "q-ary Hamming codes," which are over the (more general) field $\mathbb{F}_q$.
    - For the sake of simplicity, though, we consider only binary Hamming codes, i.e. those over the field $\mathbb{F}_2$.

Part III: Hamming codes

- Fix an integer $\ell \geq 2$, and set $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- Our goal in this section is to construct an $[n, k, d]_2$-code, called a *Hamming code*.
    - It is also possible to construct "q-ary Hamming codes," which are over the (more general) field $\mathbb{F}_q$.
    - For the sake of simplicity, though, we consider only binary Hamming codes, i.e. those over the field $\mathbb{F}_2$.
- We do this by constructing its parity check matrix H; then the code in question will simply be the subspace $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$.

- Reminder: $\ell \geq 2$, $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.

- Reminder: $\ell \geq 2$, $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- For all $i \in \{1, \ldots, n\}$, let $\mathbf{h} \in \mathbb{F}_2^\ell$ be the vector giving the binary representation of i, with zeros added to the front if necessary (so that the length of the representation is ℓ).

- Reminder: $\ell \geq 2$, $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- For all $i \in \{1, \ldots, n\}$, let $\mathbf{h} \in \mathbb{F}_2^\ell$ be the vector giving the binary representation of i, with zeros added to the front if necessary (so that the length of the representation is ℓ).
- Let $H = \begin{bmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_n \end{bmatrix}$. Note that $H \in \mathbb{F}_2^{n \times \ell}$.

- Reminder: $\ell \geq 2$, $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- For all $i \in \{1, \ldots, n\}$, let $\mathbf{h} \in \mathbb{F}_2^\ell$ be the vector giving the binary representation of i, with zeros added to the front if necessary (so that the length of the representation is ℓ).
- Let $H = \begin{bmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_n \end{bmatrix}$. Note that $H \in \mathbb{F}_2^{n \times \ell}$.
- Let $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.

- Reminder: $\ell \geq 2$, $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- For all $i \in \{1, \ldots, n\}$, let $\mathbf{h} \in \mathbb{F}_2^\ell$ be the vector giving the binary representation of i, with zeros added to the front if necessary (so that the length of the representation is ℓ).
- Let $H = \begin{bmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_n \end{bmatrix}$. Note that $H \in \mathbb{F}_2^{n \times \ell}$.
- Let $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- Obviously, C is a subspace of $\mathbb{F}_2^n$.
  - So, C is a linear code, and furthermore, n and the subscript 2 in $[n, k, d]_2$ are correct.

- Reminder: $\ell \geq 2$, $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- For all $i \in \{1, \dots, n\}$, let $\mathbf{h} \in \mathbb{F}_2^\ell$ be the vector giving the binary representation of i, with zeros added to the front if necessary (so that the length of the representation is ℓ).
- Let $H = \begin{bmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_n \end{bmatrix}$. Note that $H \in \mathbb{F}_2^{n \times \ell}$.
- Let $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- Obviously, C is a subspace of $\mathbb{F}_2^n$.
    - So, C is a linear code, and furthermore, n and the subscript 2 in $[n, k, d]_2$ are correct.
- Each of $\mathbf{e}_1^\ell, \dots, \mathbf{e}_\ell^\ell$ is a row of H, and $\{\mathbf{e}_1^\ell, \dots, \mathbf{e}_\ell^\ell\}$ is a basis for $\mathbb{F}_2^\ell$; so, $\text{rank}(H) = \ell$.

- Reminder: $\ell \geq 2$, $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- For all $i \in \{1, \dots, n\}$, let $\mathbf{h} \in \mathbb{F}_2^\ell$ be the vector giving the binary representation of i, with zeros added to the front if necessary (so that the length of the representation is ℓ).
- Let $H = \begin{bmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_n \end{bmatrix}$. Note that $H \in \mathbb{F}_2^{n \times \ell}$.
- Let $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- Obviously, C is a subspace of $\mathbb{F}_2^n$.
  - So, C is a linear code, and furthermore, n and the subscript 2 in $[n, k, d]_2$ are correct.
- Each of $\mathbf{e}_1^\ell, \dots, \mathbf{e}_\ell^\ell$ is a row of H, and $\{\mathbf{e}_1^\ell, \dots, \mathbf{e}_\ell^\ell\}$ is a basis for $\mathbb{F}_2^\ell$; so, $\text{rank}(H) = \ell$.
- By the Rank-nullity theorem, $\text{rank}(H) + \dim \text{Ker}(H) = n$.

- Reminder: $\ell \geq 2$, $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- For all $i \in \{1, \ldots, n\}$, let $\mathbf{h} \in \mathbb{F}_2^\ell$ be the vector giving the binary representation of i, with zeros added to the front if necessary (so that the length of the representation is ℓ).
- Let $H = \begin{bmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_n \end{bmatrix}$. Note that $H \in \mathbb{F}_2^{n \times \ell}$.
- Let $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- Obviously, C is a subspace of $\mathbb{F}_2^n$.
  - So, C is a linear code, and furthermore, n and the subscript 2 in $[n, k, d]_2$ are correct.
- Each of $\mathbf{e}_1^\ell, \ldots, \mathbf{e}_\ell^\ell$ is a row of H, and $\{\mathbf{e}_1^\ell, \ldots, \mathbf{e}_\ell^\ell\}$ is a basis for $\mathbb{F}_2^\ell$; so, $\operatorname{rank}(H) = \ell$.
- By the Rank-nullity theorem, $\operatorname{rank}(H) + \dim \operatorname{Ker}(H) = n$.
- So, $\dim \operatorname{Ker}(H) = n - \ell = k$.

- Reminder: $\ell \geq 2$, $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$.
- For all $i \in \{1, \ldots, n\}$, let $\mathbf{h} \in \mathbb{F}_2^\ell$ be the vector giving the binary representation of i, with zeros added to the front if necessary (so that the length of the representation is ℓ).
- Let $H = \begin{bmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_n \end{bmatrix}$. Note that $H \in \mathbb{F}_2^{n \times \ell}$.
- Let $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- Obviously, C is a subspace of $\mathbb{F}_2^n$.
    - So, C is a linear code, and furthermore, n and the subscript 2 in $[n, k, d]_2$ are correct.
- Each of $\mathbf{e}_1^\ell, \ldots, \mathbf{e}_\ell^\ell$ is a row of H, and $\{\mathbf{e}_1^\ell, \ldots, \mathbf{e}_\ell^\ell\}$ is a basis for $\mathbb{F}_2^\ell$; so, $\text{rank}(H) = \ell$.
- By the Rank-nullity theorem, $\text{rank}(H) + \dim \text{Ker}(H) = n$.
- So, $\dim \text{Ker}(H) = n - \ell = k$.
- But $C = \text{Ker}(H)$, and so $\dim C = k$.
    - So, k in $[n, k, d]_2$ is correct.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.
- By Proposition 2.2, it suffices to show that the minimum Hamming weight of a non-zero vector in C is $d = 3$.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.
- By Proposition 2.2, it suffices to show that the minimum Hamming weight of a non-zero vector in C is $d = 3$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 1 are precisely the vectors $\mathbf{e}_1^n, \ldots, \mathbf{e}_n^n$.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.
- By Proposition 2.2, it suffices to show that the minimum Hamming weight of a non-zero vector in C is $d = 3$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 1 are precisely the vectors $\mathbf{e}_1^n, \ldots, \mathbf{e}_n^n$.
  - For all $i \in \{1, \ldots, n\}$, $\mathbf{e}_i^n H = \mathbf{h}_i \neq \mathbf{0}$, and so $\mathbf{e}_i^n \notin C$.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.
- By Proposition 2.2, it suffices to show that the minimum Hamming weight of a non-zero vector in C is $d = 3$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 1 are precisely the vectors $\mathbf{e}_1^n, \dots, \mathbf{e}_n^n$.
    - For all $i \in \{1, \dots, n\}$, $\mathbf{e}_i^n H = \mathbf{h}_i \neq \mathbf{0}$, and so $\mathbf{e}_i^n \notin C$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 2 are precisely the vectors of the form $\mathbf{e}_i^n + \mathbf{e}_j^n$, with $i \neq j$.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.
- By Proposition 2.2, it suffices to show that the minimum Hamming weight of a non-zero vector in C is $d = 3$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 1 are precisely the vectors $\mathbf{e}_1^n, \dots, \mathbf{e}_n^n$.
  - For all $i \in \{1, \dots, n\}$, $\mathbf{e}_i^n H = \mathbf{h}_i \neq \mathbf{0}$, and so $\mathbf{e}_i^n \notin C$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 2 are precisely the vectors of the form $\mathbf{e}_i^n + \mathbf{e}_j^n$, with $i \neq j$.
  - For distinct $i, j \in \{1, \dots, n\}$, $(\mathbf{e}_i^n + \mathbf{e}_j^n)H = \mathbf{h}_i + \mathbf{h}_j \neq \mathbf{0}$, and so $\mathbf{e}_i^n + \mathbf{e}_j^n \notin C$.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.
- By Proposition 2.2, it suffices to show that the minimum Hamming weight of a non-zero vector in C is $d = 3$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 1 are precisely the vectors $\mathbf{e}_1^n, \ldots, \mathbf{e}_n^n$.
  - For all $i \in \{1, \ldots, n\}$, $\mathbf{e}_i^n H = \mathbf{h}_i \neq \mathbf{0}$, and so $\mathbf{e}_i^n \notin C$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 2 are precisely the vectors of the form $\mathbf{e}_i^n + \mathbf{e}_j^n$, with $i \neq j$.
  - For distinct $i, j \in \{1, \ldots, n\}$, $(\mathbf{e}_i^n + \mathbf{e}_j^n)H = \mathbf{h}_i + \mathbf{h}_j \neq \mathbf{0}$, and so $\mathbf{e}_i^n + \mathbf{e}_j^n \notin C$.
- So, C does not contain any non-zero vectors of Hamming weight at most two.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.
- By Proposition 2.2, it suffices to show that the minimum Hamming weight of a non-zero vector in C is $d = 3$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 1 are precisely the vectors $\mathbf{e}_1^n, \ldots, \mathbf{e}_n^n$.
  - For all $i \in \{1, \ldots, n\}$, $\mathbf{e}_i^n H = \mathbf{h}_i \neq \mathbf{0}$, and so $\mathbf{e}_i^n \notin C$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 2 are precisely the vectors of the form $\mathbf{e}_i^n + \mathbf{e}_j^n$, with $i \neq j$.
  - For distinct $i, j \in \{1, \ldots, n\}$, $(\mathbf{e}_i^n + \mathbf{e}_j^n)H = \mathbf{h}_i + \mathbf{h}_j \neq \mathbf{0}$, and so $\mathbf{e}_i^n + \mathbf{e}_j^n \notin C$.
- So, C does not contain any non-zero vectors of Hamming weight at most two.
- C does contain a vector of Hamming weight at most three, e.g. the vector $\mathbf{e}_1^n + \mathbf{e}_2^n + \mathbf{e}_3^n$.
  - Because: $(\mathbf{e}_1^n + \mathbf{e}_2^n + \mathbf{e}_3^n)H = \mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3 = \mathbf{0}$.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.
- By Proposition 2.2, it suffices to show that the minimum Hamming weight of a non-zero vector in C is $d = 3$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 1 are precisely the vectors $\mathbf{e}_1^n, \dots, \mathbf{e}_n^n$.
  - For all $i \in \{1, \dots, n\}$, $\mathbf{e}_i^n H = \mathbf{h}_i \neq \mathbf{0}$, and so $\mathbf{e}_i^n \notin C$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 2 are precisely the vectors of the form $\mathbf{e}_i^n + \mathbf{e}_j^n$, with $i \neq j$.
  - For distinct $i, j \in \{1, \dots, n\}$, $(\mathbf{e}_i^n + \mathbf{e}_j^n)H = \mathbf{h}_i + \mathbf{h}_j \neq \mathbf{0}$, and so $\mathbf{e}_i^n + \mathbf{e}_j^n \notin C$.
- So, C does not contain any non-zero vectors of Hamming weight at most two.
- C does contain a vector of Hamming weight at most three, e.g. the vector $\mathbf{e}_1^n + \mathbf{e}_2^n + \mathbf{e}_3^n$.
  - Because: $(\mathbf{e}_1^n + \mathbf{e}_2^n + \mathbf{e}_3^n)H = \mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3 = \mathbf{0}$.
- So, $\min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\} = 3 = d$.

- Reminder: $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}H = \mathbf{0}\}$. WTS $[n, k, d]_2$-code.
- It remains to show that the d in $[n, k, d]_2$ is correct, i.e. that the minimum distance in C is $d = 3$.
- By Proposition 2.2, it suffices to show that the minimum Hamming weight of a non-zero vector in C is $d = 3$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 1 are precisely the vectors $\mathbf{e}_1^n, \ldots, \mathbf{e}_n^n$.
  - For all $i \in \{1, \ldots, n\}$, $\mathbf{e}_i^n H = \mathbf{h}_i \neq \mathbf{0}$, and so $\mathbf{e}_i^n \notin C$.
- Vectors of $\mathbb{F}_2^n$ of Hamming weight 2 are precisely the vectors of the form $\mathbf{e}_i^n + \mathbf{e}_j^n$, with $i \neq j$.
  - For distinct $i, j \in \{1, \ldots, n\}$, $(\mathbf{e}_i^n + \mathbf{e}_j^n)H = \mathbf{h}_i + \mathbf{h}_j \neq \mathbf{0}$, and so $\mathbf{e}_i^n + \mathbf{e}_j^n \notin C$.
- So, C does not contain any non-zero vectors of Hamming weight at most two.
- C does contain a vector of Hamming weight at most three, e.g. the vector $\mathbf{e}_1^n + \mathbf{e}_2^n + \mathbf{e}_3^n$.
  - Because: $(\mathbf{e}_1^n + \mathbf{e}_2^n + \mathbf{e}_3^n)H = \mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3 = \mathbf{0}$.
- So, $\min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\} = 3 = d$.
  - So, d from $[n, k, d]_2$ is correct.

- What about error correction for the Hamming code C that we just constructed?

- What about error correction for the Hamming code C that we just constructed?
- Suppose $\mathbf{w} \in \mathbb{F}_2^n$ differs in exactly one coordinate from some codeword in C, that is, that $\mathbf{w}$ can be obtained from a codeword in C by introducing one error (i.e. by changing exactly one 1 into 0, or vice versa, in some codeword of C).

- What about error correction for the Hamming code C that we just constructed?
- Suppose $\mathbf{w} \in \mathbb{F}_2^n$ differs in exactly one coordinate from some codeword in C, that is, that $\mathbf{w}$ can be obtained from a codeword in C by introducing one error (i.e. by changing exactly one 1 into 0, or vice versa, in some codeword of C).
- Then there exist some $\mathbf{x} \in C$ and $i \in \{1, \ldots, n\}$ such that $\mathbf{w} = \mathbf{x} + \mathbf{e}_i^n$, and so

$$\mathbf{w}H \quad = \quad (\mathbf{x} + \mathbf{e}_i^n)H \quad = \quad \underbrace{\mathbf{x}H}_{=\mathbf{0}} + \underbrace{\mathbf{e}_i^n H}_{=\mathbf{h}_i} \quad = \quad \mathbf{h}_i.$$

- What about error correction for the Hamming code C that we just constructed?
- Suppose $\mathbf{w} \in \mathbb{F}_2^n$ differs in exactly one coordinate from some codeword in C, that is, that $\mathbf{w}$ can be obtained from a codeword in C by introducing one error (i.e. by changing exactly one 1 into 0, or vice versa, in some codeword of C).
- Then there exist some $\mathbf{x} \in C$ and $i \in \{1, \ldots, n\}$ such that $\mathbf{w} = \mathbf{x} + \mathbf{e}_i^n$, and so

$$\mathbf{w}H \;=\; (\mathbf{x} + \mathbf{e}_i^n)H \;=\; \underbrace{\mathbf{x}H}_{=\mathbf{0}} + \underbrace{\mathbf{e}_i^n H}_{=\mathbf{h}_i} \;=\; \mathbf{h}_i.$$

- But $\mathbf{h}_i$ is simply the integer i written in binary code!

- What about error correction for the Hamming code C that we just constructed?
- Suppose $\mathbf{w} \in \mathbb{F}_2^n$ differs in exactly one coordinate from some codeword in C, that is, that $\mathbf{w}$ can be obtained from a codeword in C by introducing one error (i.e. by changing exactly one 1 into 0, or vice versa, in some codeword of C).
- Then there exist some $\mathbf{x} \in C$ and $i \in \{1, \ldots, n\}$ such that $\mathbf{w} = \mathbf{x} + \mathbf{e}_i^n$, and so

$$\mathbf{w}H \;=\; (\mathbf{x} + \mathbf{e}_i^n)H \;=\; \underbrace{\mathbf{x}H}_{=\mathbf{0}} + \underbrace{\mathbf{e}_i^n H}_{=\mathbf{h}_i} \;=\; \mathbf{h}_i.$$

- But $\mathbf{h}_i$ is simply the integer i written in binary code!
- So, if $\mathbf{w}$ was obtained from a codeword in C by introducing exactly one error, then the coordinate of that error is the integer whose binary representation is given by the vector $\mathbf{w}H$.

- What about error correction for the Hamming code C that we just constructed?
- Suppose $\mathbf{w} \in \mathbb{F}_2^n$ differs in exactly one coordinate from some codeword in C, that is, that $\mathbf{w}$ can be obtained from a codeword in C by introducing one error (i.e. by changing exactly one 1 into 0, or vice versa, in some codeword of C).
- Then there exist some $\mathbf{x} \in C$ and $i \in \{1, \ldots, n\}$ such that $\mathbf{w} = \mathbf{x} + \mathbf{e}_i^n$, and so

$$\mathbf{w}H \;=\; (\mathbf{x} + \mathbf{e}_i^n)H \;=\; \underbrace{\mathbf{x}H}_{=\mathbf{0}} + \underbrace{\mathbf{e}_i^n H}_{=\mathbf{h}_i} \;=\; \mathbf{h}_i.$$

- But $\mathbf{h}_i$ is simply the integer i written in binary code!
- So, if $\mathbf{w}$ was obtained from a codeword in C by introducing exactly one error, then the coordinate of that error is the integer whose binary representation is given by the vector $\mathbf{w}H$.
- We can correct the error by altering the entry (from 1 to 0, or vice versa) in that one coordinate of $\mathbf{w}$.