Finite fields: An introduction

Vlad Gheorghiu

Department of Physics
Carnegie Mellon University
Pittsburgh, PA 15213, U.S.A.

July 2, 2008

Definitions

- A *field* (F,+,·) is a set F, together with two binary operations on $F \times F$ denoted by $+$ (addition) and $\cdot$ (multiplication) such that:

Definitions

- A *field* (F,+,·) is a set F, together with two binary operations on $F \times F$ denoted by $+$ (addition) and $\cdot$ (multiplication) such that:
  1) $(F,+)$ forms an Abelian group under addition. The neutral element is denoted by 0.

Definitions

- A *field* (F,+,·) is a set F, together with two binary operations on $F \times F$ denoted by $+$ (addition) and $\cdot$ (multiplication) such that:
  1) $(F,+)$ forms an Abelian group under addition. The neutral element is denoted by 0.
  2) $(F\backslash\{0\},\cdot)$ forms an Abelian group under multiplication. The neutral element is denoted by 1.

Definitions

- A *field* (F,+,·) is a set F, together with two binary operations on $F \times F$ denoted by $+$ (addition) and $\cdot$ (multiplication) such that:
  1) $(F,+)$ forms an Abelian group under addition. The neutral element is denoted by 0.
  2) $(F\backslash\{0\},\cdot)$ forms an Abelian group under multiplication. The neutral element is denoted by 1.
  3) The multiplication operation is distributive over the addition.

Definitions

- A *field* (F,+,·) is a set F, together with two binary operations on $F \times F$ denoted by $+$ (addition) and $\cdot$ (multiplication) such that:
  1) $(F,+)$ forms an Abelian group under addition. The neutral element is denoted by 0.
  2) $(F\backslash\{0\},\cdot)$ forms an Abelian group under multiplication. The neutral element is denoted by 1.
  3) The multiplication operation is distributive over the addition.

Observation

A field does not contain any divizors of zero, that is, for any $a, b \in \mathbb{F}$, $ab = 0$ implies either $a = 0$ or $b = 0$. This property is extremely important in solving systems of linear equations.

- More intuitively, a field is an algebraic structure in which the operations of addition, subtraction, multiplication and division (except division by zero) may be performed, and the familiar rules of ordinary arithmetic hold.

- More intuitively, a field is an algebraic structure in which the operations of addition, subtraction, multiplication and division (except division by zero) may be performed, and the familiar rules of ordinary arithmetic hold.
- A *finite field* is a field in which F has a finitely many elements.

- More intuitively, a field is an algebraic structure in which the operations of addition, subtraction, multiplication and division (except division by zero) may be performed, and the familiar rules of ordinary arithmetic hold.
- A *finite field* is a field in which F has a finitely many elements.
- A subset $\mathbb{K}$ of a field $\mathbb{F}$ that is itself a field under the operations of $\mathbb{F}$ is called a *subfield*.

- More intuitively, a field is an algebraic structure in which the operations of addition, subtraction, multiplication and division (except division by zero) may be performed, and the familiar rules of ordinary arithmetic hold.
- A *finite field* is a field in which F has a finitely many elements.
- A subset $\mathbb{K}$ of a field $\mathbb{F}$ that is itself a field under the operations of $\mathbb{F}$ is called a *subfield*.

Observation

If $\mathbb{K}$ is a subfield of a finite field $\mathbb{F}_p$, p prime, then $\mathbb{K}$ must contain the elements 0 and 1, and so all other elements of $\mathbb{F}_p$ by the closure of $\mathbb{K}$ under addition. Then $\mathbb{F}$ does not contain any proper subfield. We are led to the following concept.

Further definitions

- A field containing no proper subfields is called a *prime field*.

Further definitions

- A field containing no proper subfields is called a *prime field*.
- The intersection of any nonempty collection of subfields of a given field $\mathbb{F}$ is again a subfield. The intersection of *all* subfields of $\mathbb{F}$ is called the *prime subfield* of $\mathbb{F}$.

Further definitions

- A field containing no proper subfields is called a *prime field*.
- The intersection of any nonempty collection of subfields of a given field $\mathbb{F}$ is again a subfield. The intersection of *all* subfields of $\mathbb{F}$ is called the *prime subfield* of $\mathbb{F}$.
- The *characteristic* of a field $\mathbb{F}$ is the smallest integer n such that $1 + 1 + \cdots + 1(n \text{ times }) = 0$.

Examples

- The complex numbers $\mathbb{C}$, under the usual operations of addition and multiplication.

Examples

- The complex numbers $\mathbb{C}$, under the usual operations of addition and multiplication.
- The rational numbers $\mathbb{Q} = \{a/b \text{ with } a, b \in \mathbb{Z}, b \neq 0\}$ where $\mathbb{Z}$ is the set of integers. The field of rational numbers is a subfield of $\mathbb{C}$ containing no proper subfields.

Examples

- The complex numbers $\mathbb{C}$, under the usual operations of addition and multiplication.
- The rational numbers $\mathbb{Q} = \{a/b \text{ with } a, b \in \mathbb{Z}, b \neq 0\}$ where $\mathbb{Z}$ is the set of integers. The field of rational numbers is a subfield of $\mathbb{C}$ containing no proper subfields.
- For a given field $\mathbb{F}$, the set $\mathbb{F}(X)$ of rational functions in the variable X with coefficients in $\mathbb{F}$ is a field.

Examples

- The complex numbers $\mathbb{C}$, under the usual operations of addition and multiplication.
- The rational numbers $\mathbb{Q} = \{a/b \text{ with } a, b \in \mathbb{Z}, b \neq 0\}$ where $\mathbb{Z}$ is the set of integers. The field of rational numbers is a subfield of $\mathbb{C}$ containing no proper subfields.
- For a given field $\mathbb{F}$, the set $\mathbb{F}(X)$ of rational functions in the variable X with coefficients in $\mathbb{F}$ is a field.
- The set $\mathbb{Z}_p$ of integers modulo p, where p is prime. This is a finite field with p elements, usually denoted by $\mathbb{F}_p$.

Examples

- The complex numbers $\mathbb{C}$, under the usual operations of addition and multiplication.
- The rational numbers $\mathbb{Q} = \{a/b \text{ with } a, b \in \mathbb{Z}, b \neq 0\}$ where $\mathbb{Z}$ is the set of integers. The field of rational numbers is a subfield of $\mathbb{C}$ containing no proper subfields.
- For a given field $\mathbb{F}$, the set $\mathbb{F}(X)$ of rational functions in the variable X with coefficients in $\mathbb{F}$ is a field.
- The set $\mathbb{Z}_p$ of integers modulo p, where p is prime. This is a finite field with p elements, usually denoted by $\mathbb{F}_p$.
- Taking $p = 2$, we obtain the smallest field, $\mathbb{F}_2$, which has only two elements: 0 and 1. This field has important uses in computer science, especially in cryptography and coding theory.

The structure of finite fields

Lemma 1

If the characteristic of a field is nonzero, then the characteristic is prime. The characteristic of a finite field is always prime.

The structure of finite fields

Lemma 1

If the characteristic of a field is nonzero, then the characteristic is prime. The characteristic of a finite field is always prime.

Proof.

The structure of finite fields

Lemma 1

If the characteristic of a field is nonzero, then the characteristic is prime. The characteristic of a finite field is always prime.

Proof.

- Suppose the characteristic n of a field $\mathbb{F}$ factors as $n_1 n_2$, with $1 < n_1, n_2 < n$; thus $n_1 n_2 \cdot 1 = 0$.

The structure of finite fields

Lemma 1

If the characteristic of a field is nonzero, then the characteristic is prime. The characteristic of a finite field is always prime.

Proof.

- Suppose the characteristic n of a field $\mathbb{F}$ factors as $n_1 n_2$, with $1 < n_1, n_2 < n$; thus $n_1 n_2 \cdot 1 = 0$.
- Since there are no divisors of zero in $\mathbb{F}$, either $n_1 \cdot 1$ or $n_2 \cdot 1$ is zero.

The structure of finite fields

Lemma 1

If the characteristic of a field is nonzero, then the characteristic is prime. The characteristic of a finite field is always prime.

Proof.

- Suppose the characteristic n of a field $\mathbb{F}$ factors as $n_1 n_2$, with $1 < n_1, n_2 < n$; thus $n_1 n_2 \cdot 1 = 0$.
- Since there are no divisors of zero in $\mathbb{F}$, either $n_1 \cdot 1$ or $n_2 \cdot 1$ is zero.
- It follows that either $(n_1 \cdot 1)a = n_1 a = 0$ or $(n_2 \cdot 1)a = n_2 a = 0$ for all $a \in \mathbb{F}$, in contradiction to the definition of the characteristic n, hence the characteristic is zero or prime.

$\square$

The structure of finite fields

Lemma 1

If the characteristic of a field is nonzero, then the characteristic is prime. The characteristic of a finite field is always prime.

Proof.

- Suppose the characteristic n of a field $\mathbb{F}$ factors as $n_1 n_2$, with $1 < n_1, n_2 < n$; thus $n_1 n_2 \cdot 1 = 0$.
- Since there are no divisors of zero in $\mathbb{F}$, either $n_1 \cdot 1$ or $n_2 \cdot 1$ is zero.
- It follows that either $(n_1 \cdot 1)a = n_1 a = 0$ or $(n_2 \cdot 1)a = n_2 a = 0$ for all $a \in \mathbb{F}$, in contradiction to the definition of the characteristic n, hence the characteristic is zero or prime.

$\square$

Observation: The field of rational numbers, real numbers and complex numbers all have characteristic zero.

Lemma 2

Let $\mathbb{F}$ be a finite field containing a subfield $\mathbb{K}$ with q elements. Then $\mathbb{F}$ is a vector space over $\mathbb{K}$ and $|\mathbb{F}| = q^m$, where m is the dimension of $\mathbb{F}$ viwed as a vector space over $\mathbb{K}$.

Lemma 2

Let $\mathbb{F}$ be a finite field containing a subfield $\mathbb{K}$ with q elements. Then $\mathbb{F}$ is a vector space over $\mathbb{K}$ and $|\mathbb{F}| = q^m$, where m is the dimension of $\mathbb{F}$ viwed as a vector space over $\mathbb{K}$.

Proof.

Lemma 2

Let $\mathbb{F}$ be a finite field containing a subfield $\mathbb{K}$ with q elements. Then $\mathbb{F}$ is a vector space over $\mathbb{K}$ and $|\mathbb{F}| = q^m$, where m is the dimension of $\mathbb{F}$ viwed as a vector space over $\mathbb{K}$.

Proof.

- It is straightforward to verify that $\mathbb{F}$ is a vector space over $\mathbb{K}$.

Lemma 2

Let $\mathbb{F}$ be a finite field containing a subfield $\mathbb{K}$ with q elements. Then $\mathbb{F}$ is a vector space over $\mathbb{K}$ and $|\mathbb{F}| = q^m$, where m is the dimension of $\mathbb{F}$ viwed as a vector space over $\mathbb{K}$.

Proof.

- It is straightforward to verify that $\mathbb{F}$ is a vector space over $\mathbb{K}$.
- Let $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a basis for $\mathbb{F}$ over $\mathbb{K}$.

Lemma 2

Let $\mathbb{F}$ be a finite field containing a subfield $\mathbb{K}$ with q elements. Then $\mathbb{F}$ is a vector space over $\mathbb{K}$ and $|\mathbb{F}| = q^m$, where m is the dimension of $\mathbb{F}$ viwed as a vector space over $\mathbb{K}$.

Proof.

- It is straightforward to verify that $\mathbb{F}$ is a vector space over $\mathbb{K}$.
- Let $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a basis for $\mathbb{F}$ over $\mathbb{K}$.
- Every $\alpha \in \mathbb{F}$ can be written uniquely as $\alpha = a_1\beta_1 + \cdots + a_m\beta_m$, where $a_i \in \mathbb{K}$ and the sequence $a_1, a_2, \ldots, a_m$ is uniquely determined by α.

Lemma 2

Let $\mathbb{F}$ be a finite field containing a subfield $\mathbb{K}$ with q elements. Then $\mathbb{F}$ is a vector space over $\mathbb{K}$ and $|\mathbb{F}| = q^m$, where m is the dimension of $\mathbb{F}$ viwed as a vector space over $\mathbb{K}$.

Proof.

- It is straightforward to verify that $\mathbb{F}$ is a vector space over $\mathbb{K}$.
- Let $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a basis for $\mathbb{F}$ over $\mathbb{K}$.
- Every $\alpha \in \mathbb{F}$ can be written uniquely as $\alpha = a_1\beta_1 + \cdots + a_m\beta_m$, where $a_i \in \mathbb{K}$ and the sequence $a_1, a_2, \ldots, a_m$ is uniquely determined by α.
- There are $|\mathbb{K}|^m = q^m$ distinct sequences of coefficients, because there are $|\mathbb{K}| = q$ choices for each a_i.

$\square$

Lemma 2

Let $\mathbb{F}$ be a finite field containing a subfield $\mathbb{K}$ with q elements. Then $\mathbb{F}$ is a vector space over $\mathbb{K}$ and $|\mathbb{F}| = q^m$, where m is the dimension of $\mathbb{F}$ viwed as a vector space over $\mathbb{K}$.

Proof.

- It is straightforward to verify that $\mathbb{F}$ is a vector space over $\mathbb{K}$.
- Let $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a basis for $\mathbb{F}$ over $\mathbb{K}$.
- Every $\alpha \in \mathbb{F}$ can be written uniquely as $\alpha = a_1\beta_1 + \cdots + a_m\beta_m$, where $a_i \in \mathbb{K}$ and the sequence $a_1, a_2, \ldots, a_m$ is uniquely determined by α.
- There are $|\mathbb{K}|^m = q^m$ distinct sequences of coefficients, because there are $|\mathbb{K}| = q$ choices for each a_i.

$\square$

The m occuring in Lemma 2, which is the dimension of $\mathbb{F}$ as a vector space over $\mathbb{K}$, is called the *degree* of $\mathbb{F}$ over $\mathbb{K}$.

Theorem 1

The prime subfield of a finite field $\mathbb{F}$ is isomorphic to $\mathbb{F}_p$, where p is the characteristic of $\mathbb{F}$.

Theorem 1

The prime subfield of a finite field $\mathbb{F}$ is isomorphic to $\mathbb{F}_p$, where p is the characteristic of $\mathbb{F}$.

Theorem 2

Let $\mathbb{F}$ be a finite field. The cardinality of $\mathbb{F}$ is p^m, where the prime p is the characteristic of F and m is the degree of F over its prime subfield.

Theorem 1

The prime subfield of a finite field $\mathbb{F}$ is isomorphic to $\mathbb{F}_p$, where p is the characteristic of $\mathbb{F}$.

Theorem 2

Let $\mathbb{F}$ be a finite field. The cardinality of $\mathbb{F}$ is p^m, where the prime p is the characteristic of F and m is the degree of F over its prime subfield.

Proof. (of Theorem 2).

Since $\mathbb{F}$ is finite, its characteristic is prime (according to Lemma 1). Therefore the prime subfield $\mathbb{K}$ of $\mathbb{F}$ is isomorphic to $\mathbb{F}_p$, by Theorem 1. By Lemma 2, the cardinality of $\mathbb{F}$ is just $|K|^m = p^m$. $\square$

Theorem 3 (Existence of finite fields)

For every prime p and positive integer $n \geqslant 1$ there is a finite field with p^n elements. Any two finite fields with p^n elements are isomorphic.

Theorem 3 (Existence of finite fields)

For every prime p and positive integer $n \geqslant 1$ there is a finite field with p^n elements. Any two finite fields with p^n elements are isomorphic.

- The previous theorem shows that a finite field of a given order is unique up to field isomorphism.

Theorem 3 (Existence of finite fields)

For every prime p and positive integer $n \geqslant 1$ there is a finite field with p^n elements. Any two finite fields with p^n elements are isomorphic.

- The previous theorem shows that a finite field of a given order is unique up to field isomorphism.
- Thus one speaks of "the" finite field of a particular order q. It is usually denoted by $GF(q)$, where G stands for Galois (Evariste Galois, 1811-1832) and F for field.

Theorem 4 (Subfield structure)

Let $\mathbb{F}$ be a finite field with p^n elements. Every subfield of $\mathbb{F}$ has p^m elements for some integer m dividing n. Conversely, for any integer m dividing n there is a unique subfield of $\mathbb{F}$ of order p^m.

Theorem 4 (Subfield structure)

Let $\mathbb{F}$ be a finite field with p^n elements. Every subfield of $\mathbb{F}$ has p^m elements for some integer m dividing n. Conversely, for any integer m dividing n there is a unique subfield of $\mathbb{F}$ of order p^m.

Proof.

- A subfield of the finite field $GF(p^n)$ must have p^m distinct elements for some positive integer m with $m \leqslant n$.

Theorem 4 (Subfield structure)

Let $\mathbb{F}$ be a finite field with p^n elements. Every subfield of $\mathbb{F}$ has p^m elements for some integer m dividing n. Conversely, for any integer m dividing n there is a unique subfield of $\mathbb{F}$ of order p^m.

Proof.

- A subfield of the finite field $GF(p^n)$ must have p^m distinct elements for some positive integer m with $m \leqslant n$.
- By Lemma 2, p^n must be a power of p^m, so m must divide n.

$\square$

Theorem 4 (Subfield structure)

Let $\mathbb{F}$ be a finite field with p^n elements. Every subfield of $\mathbb{F}$ has p^m elements for some integer m dividing n. Conversely, for any integer m dividing n there is a unique subfield of $\mathbb{F}$ of order p^m.

Proof.

- A subfield of the finite field $GF(p^n)$ must have p^m distinct elements for some positive integer m with $m \leqslant n$.
- By Lemma 2, p^n must be a power of p^m, so m must divide n.

$\square$

Theorem 5 (Multiplicative group structure)

For every finite field $\mathbb{F}$, the multiplicative group $(F\backslash\{0\}, \cdot)$ is cyclic.

Introduction

- In practice, all communication channels are noisy.

Introduction

- In practice, all communication channels are noisy.
- One of the main problems in algebraic coding theory is to make the errors, which occur for instance because of noisy channels, extremely improbable.

Introduction

- In practice, all communication channels are noisy.
- One of the main problems in algebraic coding theory is to make the errors, which occur for instance because of noisy channels, extremely improbable.
- A basic idea is to transmit redundant information together with the original message one wants to communicate.

Introduction

- In practice, all communication channels are noisy.
- One of the main problems in algebraic coding theory is to make the errors, which occur for instance because of noisy channels, extremely improbable.
- A basic idea is to transmit redundant information together with the original message one wants to communicate.
- In common applications, a message is considered to be a fixed finite word on a fixed finite alphabet.

- A code is an injection from a set of messages to a set of words on a fixed finite alphabet. The words in the range of this function are called codewords.

- A code is an injection from a set of messages to a set of words on a fixed finite alphabet. The words in the range of this function are called codewords.
- One requires a code to be injective so that one can decode the sequence that is receive.

- A code is an injection from a set of messages to a set of words on a fixed finite alphabet. The words in the range of this function are called codewords.
- One requires a code to be injective so that one can decode the sequence that is receive.
- Main goal: detect and correct the errors.

- A code is an injection from a set of messages to a set of words on a fixed finite alphabet. The words in the range of this function are called codewords.
- One requires a code to be injective so that one can decode the sequence that is receive.
- Main goal: detect and correct the errors.
- Usually the detection of errors is accomplished by noticing that the received sequence is not a codeword.

- For some codes, it is possible for the receiver to determine, with high probability, the intended message when the received sequence is not a codeword.

- For some codes, it is possible for the receiver to determine, with high probability, the intended message when the received sequence is not a codeword.
- Such codes are called *error-correcting codes*.

- For some codes, it is possible for the receiver to determine, with high probability, the intended message when the received sequence is not a codeword.
- Such codes are called *error-correcting codes*.
- Error-correcting codes are often called *algebraic codes* because they are usually constructed using some algebraic system, very often a finite field.

Linear codes: basic properties

Definition

Let $\mathbb{F}_q^n$ denote the set of all n-tuples over a finite field $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(a_1, \ldots, a_n) \,|a_i \in \mathbb{F},\ i = 1, \ldots, n\}.$$

Linear codes: basic properties

Definition

Let $\mathbb{F}_q^n$ denote the set of all n-tuples over a finite field $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(a_1, \ldots, a_n) \,|a_i \in \mathbb{F},\ i = 1, \ldots, n\}.$$

- $\mathbb{F}_q^n$ is a vector space over the field $\mathbb{F}_q$, of dimension n.

Linear codes: basic properties

Definition

Let $\mathbb{F}_q^n$ denote the set of all n-tuples over a finite field $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(a_1, \ldots, a_n) \,|a_i \in \mathbb{F},\ i = 1, \ldots, n\}.$$

- $\mathbb{F}_q^n$ is a vector space over the field $\mathbb{F}_q$, of dimension n.
- The messages are assumed to be elements of $\mathbb{F}_q^k$ for some $k \geqslant 1$.

Linear codes: basic properties

Definition

Let $\mathbb{F}_q^n$ denote the set of all n-tuples over a finite field $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(a_1, \ldots, a_n) \,|a_i \in \mathbb{F},\ i = 1, \ldots, n\}.$$

- $\mathbb{F}_q^n$ is a vector space over the field $\mathbb{F}_q$, of dimension n.
- The messages are assumed to be elements of $\mathbb{F}_q^k$ for some $k \geqslant 1$.
- There are q^k distinct messages that can be sent.

Linear codes: basic properties

Definition

Let $\mathbb{F}_q^n$ denote the set of all n-tuples over a finite field $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(a_1, \ldots, a_n) \,|a_i \in \mathbb{F},\ i = 1, \ldots, n\}.$$

- $\mathbb{F}_q^n$ is a vector space over the field $\mathbb{F}_q$, of dimension n.
- The messages are assumed to be elements of $\mathbb{F}_q^k$ for some $k \geqslant 1$.
- There are q^k distinct messages that can be sent.
- The codewords are assumed to be elements of $\mathbb{F}_q^n$ for some $n \geqslant k$.

- A code is an injective function from $\mathbb{F}_q^k$ to $\mathbb{F}_q^n$. The codewords are the range of this function.

- A code is an injective function from $\mathbb{F}_q^k$ to $\mathbb{F}_q^n$. The codewords are the range of this function.
- We are particularly interested in those codes for which the range is a subspace of $\mathbb{F}_q^n$, for then we can use results of linear algebra to analyze the code.

- A code is an injective function from $\mathbb{F}_q^k$ to $\mathbb{F}_q^n$. The codewords are the range of this function.
- We are particularly interested in those codes for which the range is a subspace of $\mathbb{F}_q^n$, for then we can use results of linear algebra to analyze the code.

Definition

A linear code C is a subspace of the vector space $\mathbb{F}_q^n$. Such a code is called a q-ary code; the code is *binary* if $q = 2$ and *ternary* if $q = 3$. The number n is the length of the code.

- Since a linear code C is a subspace of $\mathbb{F}_q^n$, it will contain q^k distinct codewords for some k with $0 \leqslant k \leqslant n$. The integer k is called the dimension of the linear code C.

- Since a linear code C is a subspace of $\mathbb{F}_q^n$, it will contain q^k distinct codewords for some k with $0 \leqslant k \leqslant n$. The integer k is called the dimension of the linear code C.
- One can also regard k as the length of each uncoded message, for our messages will be elements from the set $\mathbb{F}_q^k$. We denote such a code C as an [n,k] linear code.

- Since a linear code C is a subspace of $\mathbb{F}_q^n$, it will contain q^k distinct codewords for some k with $0 \leqslant k \leqslant n$. The integer k is called the dimension of the linear code C.
- One can also regard k as the length of each uncoded message, for our messages will be elements from the set $\mathbb{F}_q^k$. We denote such a code C as an [n,k] linear code.
- Example 1: the q-ary repetition code which acts by repeating the message $a \in \mathbb{F}_q$ that is to be encoded a total of n times: $a \to a \ldots a$. This is an $[n, 1]$ linear code.

- Since a linear code C is a subspace of $\mathbb{F}_q^n$, it will contain q^k distinct codewords for some k with $0 \leqslant k \leqslant n$. The integer k is called the dimension of the linear code C.
- One can also regard k as the length of each uncoded message, for our messages will be elements from the set $\mathbb{F}_q^k$. We denote such a code C as an [n,k] linear code.
- Example 1: the q-ary repetition code which acts by repeating the message $a \in \mathbb{F}_q$ that is to be encoded a total of n times: $a \to a \ldots a$. This is an $[n, 1]$ linear code.
- Example 2: The binary $parity - check$ code over $\mathbb{F}_2$: $(a_1, \ldots, a_n) \to (a_1, \ldots, a_n, \sum_{i=1}^n a_i)$. This is an $[n, n-1]$ linear code, but with no error-correcting ability.

Encoding methods

- There are two well known matrix encoding techniques: the parity-check matrix and the generator matrix.

Encoding methods

- There are two well known matrix encoding techniques: the parity-check matrix and the generator matrix.

Parity chech matrix

Let H be a $(n-k) \times n$ matrix over $\mathbb{F}_q$ of rank $n-k$. Then $C = \{\mathbf{c} \in \mathbb{F}_q^n \,|H\mathbf{c}^T = 0\}$ is a linear $[n, k]$ code.

Encoding methods

- There are two well known matrix encoding techniques: the parity-check matrix and the generator matrix.

Parity chech matrix

Let H be a $(n-k) \times n$ matrix over $\mathbb{F}_q$ of rank $n-k$. Then $C = \{\mathbf{c} \in \mathbb{F}_q^n \,|H\mathbf{c}^T = 0\}$ is a linear $[n, k]$ code.

Generator matrix

Let G be a $k \times n$ matrix over $\mathbb{F}_q$. The set $C = \{\mathbf{a}G \,|\mathbf{a} \in \mathbb{F}_q^k\}$ is a linear code, of dimension k equal to the rank of G.

Hamming distance as a metric

Definition

The Hamming distance $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^n$ is defined as the number of coordinates where the vectors differ. The Hamming weight $wt(\mathbf{x})$ of a vector $\mathbf{x}$ is the number of coordinates where the vector is nonzero.

Hamming distance as a metric

Definition

The Hamming distance $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^n$ is defined as the number of coordinates where the vectors differ. The Hamming weight $wt(\mathbf{x})$ of a vector $\mathbf{x}$ is the number of coordinates where the vector is nonzero.

Proposition

The Hamming distance function is a metric. That is, for all vectors $\mathbf{u}, \mathbf{v}$ and $\mathbf{w}$:

1. $d(\mathbf{u}, \mathbf{v}) \geqslant 0$.

Hamming distance as a metric

Definition

The Hamming distance $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^n$ is defined as the number of coordinates where the vectors differ. The Hamming weight $wt(\mathbf{x})$ of a vector $\mathbf{x}$ is the number of coordinates where the vector is nonzero.

Proposition

The Hamming distance function is a metric. That is, for all vectors $\mathbf{u}, \mathbf{v}$ and $\mathbf{w}$:

1. $d(\mathbf{u}, \mathbf{v}) \geqslant 0$.
2. $d(\mathbf{u}, \mathbf{v}) = 0$ if and only if $\mathbf{u} = \mathbf{v}$.

Hamming distance as a metric

Definition

The Hamming distance $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^n$ is defined as the number of coordinates where the vectors differ. The Hamming weight $wt(\mathbf{x})$ of a vector $\mathbf{x}$ is the number of coordinates where the vector is nonzero.

Proposition

The Hamming distance function is a metric. That is, for all vectors $\mathbf{u}, \mathbf{v}$ and $\mathbf{w}$:

1. $d(\mathbf{u}, \mathbf{v}) \geqslant 0$.
2. $d(\mathbf{u}, \mathbf{v}) = 0$ if and only if $\mathbf{u} = \mathbf{v}$.
3. $d(\mathbf{u}, \mathbf{v}) = d(\mathbf{v}, \mathbf{u})$.

Hamming distance as a metric

Definition

The Hamming distance $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^n$ is defined as the number of coordinates where the vectors differ. The Hamming weight $wt(\mathbf{x})$ of a vector $\mathbf{x}$ is the number of coordinates where the vector is nonzero.

Proposition

The Hamming distance function is a metric. That is, for all vectors $\mathbf{u}, \mathbf{v}$ and $\mathbf{w}$:

1. $d(\mathbf{u}, \mathbf{v}) \geqslant 0$.
2. $d(\mathbf{u}, \mathbf{v}) = 0$ if and only if $\mathbf{u} = \mathbf{v}$.
3. $d(\mathbf{u}, \mathbf{v}) = d(\mathbf{v}, \mathbf{u})$.
4. $d(\mathbf{u}, \mathbf{w}) \leqslant d(\mathbf{u}, \mathbf{v}) + d(\mathbf{v}, \mathbf{w})$.

Definition

If C is a linear code, then the minimum distance d_C of C is defined as

$$d_C = \min(d(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}) = \min(wt(\mathbf{x}) | \mathbf{x} \in C, \mathbf{x} \neq 0)$$

Definition

If C is a linear code, then the minimum distance d_C of C is defined as

$$d_C = \min(d(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}) = \min(wt(\mathbf{x}) | \mathbf{x} \in C, \mathbf{x} \neq 0)$$

Definition

A code C is said to be t-error correcting if for every vector $\mathbf{x} \in \mathbb{F}_q^n$, there is at most one codeword $c \in C$ within distance t of $\mathbf{x}$, that is, with $d(\mathbf{x}, \mathbf{c}) \leqslant t$.

Definition

If C is a linear code, then the minimum distance d_C of C is defined as

$$d_C = \min(d(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}) = \min(wt(\mathbf{x}) | \mathbf{x} \in C, \mathbf{x} \neq 0)$$

Definition

A code C is said to be t-error correcting if for every vector $\mathbf{x} \in \mathbb{F}_q^n$, there is at most one codeword $c \in C$ within distance t of $\mathbf{x}$, that is, with $d(\mathbf{x}, \mathbf{c}) \leqslant t$.

Theorem 6

Let C be a code.

1. C can correct t errors iff $d_C \geqslant 2t + 1$.

Definition

If C is a linear code, then the minimum distance d_C of C is defined as

$$d_C = \min(d(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}) = \min(wt(\mathbf{x}) | \mathbf{x} \in C, \mathbf{x} \neq 0)$$

Definition

A code C is said to be t-error correcting if for every vector $\mathbf{x} \in \mathbb{F}_q^n$, there is at most one codeword $c \in C$ within distance t of $\mathbf{x}$, that is, with $d(\mathbf{x}, \mathbf{c}) \leqslant t$.

Theorem 6

Let C be a code.

1. C can correct t errors iff $d_C \geqslant 2t + 1$.
2. C can detect s errors iff $d_C \geqslant s + 1$.