Information and Coding Theory

MA41024/ MA60020/ MA60262

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

Lecture 15
March 13, 2023

Codes

In general, a code of block length n over an alphabet Σ is a subset of Σ^n. Set $q = |\Sigma|$. Then codewords are elements of Σ^n

$\rightarrow$ a codeword $\mathbf{v} = (v_1, \ldots, v_n)$ can also be described as a function $f : [n] \rightarrow \Sigma$ with $f(i) = v_i$, $1 \leq i \leq n$ and $[n] = \{1, \ldots, n\}$

Codes

In general, a code of block length n over an alphabet Σ is a subset of Σ^n. Set $q = |\Sigma|$. Then codewords are elements of Σ^n

- $\rightarrow$ a codeword $\mathbf{v} = (v_1, \ldots, v_n)$ can also be described as a function $f : [n] \rightarrow \Sigma$ with $f(i) = v_i$, $1 \leq i \leq n$ and $[n] = \{1, \ldots, n\}$
- $\rightarrow$ A code C can also be defined as $C : [M] \rightarrow \Sigma^n$, where $|C| = M$

Codes

In general, a code of block length n over an alphabet Σ is a subset of Σ^n. Set $q = |\Sigma|$. Then codewords are elements of Σ^n

- $\rightarrow$ a codeword $\mathbf{v} = (v_1, \ldots, v_n)$ can also be described as a function $f : [n] \rightarrow \Sigma$ with $f(i) = v_i$, $1 \leq i \leq n$ and $[n] = \{1, \ldots, n\}$
- $\rightarrow$ A code C can also be defined as $C : [M] \rightarrow \Sigma^n$, where $|C| = M$
- $\rightarrow$ The dimension of a code C is defined as

$$k = \log_q |C|$$

Codes

In general, a code of block length n over an alphabet Σ is a subset of Σ^n. Set $q = |\Sigma|$. Then codewords are elements of Σ^n

→ a codeword $\mathbf{v} = (v_1, \ldots, v_n)$ can also be described as a function $f : [n] \to \Sigma$ with $f(i) = v_i$, $1 \leq i \leq n$ and $[n] = \{1, \ldots, n\}$

→ A code C can also be defined as $C : [M] \to \Sigma^n$, where $|C| = M$

→ The dimension of a code C is defined as

$$k = \log_q |C|$$

Hamming distance Given two vectors $\mathbf{u}, \mathbf{v} \in \Sigma^n$, the Hamming distance between $\mathbf{u}, \mathbf{v}$ is the number of positions in which $\mathbf{u}$ and $\mathbf{v}$ differ

Codes

In general, a code of block length n over an alphabet Σ is a subset of Σ^n. Set $q = |\Sigma|$. Then codewords are elements of Σ^n

- $\rightarrow$ a codeword $\mathbf{v} = (v_1, \ldots, v_n)$ can also be described as a function $f : [n] \rightarrow \Sigma$ with $f(i) = v_i$, $1 \leq i \leq n$ and $[n] = \{1, \ldots, n\}$
- $\rightarrow$ A code C can also be defined as $C : [M] \rightarrow \Sigma^n$, where $|C| = M$
- $\rightarrow$ The dimension of a code C is defined as

$$k = \log_q |C|$$

Hamming distance Given two vectors $\mathbf{u}, \mathbf{v} \in \Sigma^n$, the Hamming distance between $\mathbf{u}, \mathbf{v}$ is the number of positions in which $\mathbf{u}$ and $\mathbf{v}$ differ

An n-symbol t-Error Channel over the alphabet Σ is a function $Ch : \Sigma^n \rightarrow \Sigma^n$ which satisfies $d(\mathbf{v}, Ch(\mathbf{v})) \leq t$ for every $\mathbf{v} \in \Sigma^n$.

Codes

A code C is said to be a *t-error-correcting code* if there exists a decoding scheme/function D such that for every message $\mathbf{m} \in [|C|]$ every t-error channel Ch we have $D(Ch(C(\mathbf{m}))) = \mathbf{m}$

Codes

A code C is said to be a t-error-correcting code if there exists a decoding scheme/function D such that for every message $\mathbf{m} \in [|C|]$ every t-error channel Ch we have $D(Ch(C(\mathbf{m}))) = \mathbf{m}$

t-error detection code Let $C \subseteq \Sigma^n$ and $t \geqq 1$ be an integer. Then C is said to be t-error-detecting code if there exists a detecting procedure D such that for every message $\mathbf{m}$ and every received vector $\mathbf{r} \in \Sigma^n$ satisfying $d(C(\mathbf{m}), \mathbf{r}) \leq t$, it holds that D outputs 1 if $\mathbf{r} = C(\mathbf{m})$ and 0 otherwise

Codes

A code C is said to be a t-error-correcting code if there exists a decoding scheme/function D such that for every message $\mathbf{m} \in [|C|]$ every t-error channel Ch we have $D(Ch(C(\mathbf{m}))) = \mathbf{m}$

t-error detection code Let $C \subseteq \Sigma^n$ and $t \geqq 1$ be an integer. Then C is said to be t-error-detecting code if there exists a detecting procedure D such that for every message $\mathbf{m}$ and every received vector $\mathbf{r} \in \Sigma^n$ satisfying $d(C(\mathbf{m}), \mathbf{r}) \leq t$, it holds that D outputs 1 if $\mathbf{r} = C(\mathbf{m})$ and 0 otherwise

Hamming ball For any vector $\mathbf{x} \in [q]^n$, and a nonnegative integer ϵ,

$$B(\mathbf{x}, \epsilon) = \{\mathbf{y} \in [q]^n : d(\mathbf{x}, \mathbf{y}) \leq \epsilon\}$$

Codes

A code C is said to be a t-error-correcting code if there exists a decoding scheme/function D such that for every message $\mathbf{m} \in [|C|]$ every t-error channel Ch we have $D(Ch(C(\mathbf{m}))) = \mathbf{m}$

t-error detection code Let $C \subseteq \Sigma^n$ and $t \geqq 1$ be an integer. Then C is said to be t-error-detecting code if there exists a detecting procedure D such that for every message $\mathbf{m}$ and every received vector $\mathbf{r} \in \Sigma^n$ satisfying $d(C(\mathbf{m}), \mathbf{r}) \leq t$, it holds that D outputs 1 if $\mathbf{r} = C(\mathbf{m})$ and 0 otherwise

Hamming ball For any vector $\mathbf{x} \in [q]^n$, and a nonnegative integer ϵ,

$$B(\mathbf{x}, \epsilon) = \{\mathbf{y} \in [q]^n : d(\mathbf{x}, \mathbf{y}) \leq \epsilon\}$$

Notation: A code $C \subseteq \Sigma^n$ with dimension k, minimum distance $d_{\min}$ will be called a $(n, k, d_{\min})_\Sigma$ code

Codes

Hamming bound a trade off between redundancy and error-correction capability

Codes

Hamming bound a trade off between redundancy and error-correction capability

Theorem (Hamming bound for $d_{\min} = 3$) For any $(n, k, 3)_{\{0,1\}}$ code:

$$k \leq n - \log_2(n+1)$$

Codes

Hamming bound a trade off between redundancy and error-correction capability
Theorem (Hamming bound for $d_{\text{min}} = 3$) For any $(n, k, 3)_{\{0,1\}}$ code:

$$k \leq n - \log_2(n+1)$$

Question What happens to binary Hamming code?

Codes

Hamming bound a trade off between redundancy and error-correction capability

Theorem (Hamming bound for $d_{\min} = 3$) For any $(n, k, 3)_{\{0,1\}}$ code:

$$k \leq n - \log_2(n+1)$$

Question What happens to binary Hamming code?

Theorem For any $(n, k, d_{\min})_{\Sigma}$ code:

$$k \leq n - \log_q \left(\sum_{i=0}^{\lfloor \frac{(d_{\min}-1)}{2} \rfloor} \binom{n}{i} (q-1)^i \right),$$

where $q = |\Sigma|$

Codes

Perfect code Codes that meet Hamming bound are called perfect codes

Codes

Perfect code Codes that meet Hamming bound are called perfect codes

Interpretation: If we construct Hamming balls of radius $\lfloor \frac{d-1}{2} \rfloor$ around all the codewords then we would cover the entire ambient space i.e. every possible vector will lie in one of these Hamming balls

Codes

Perfect code Codes that meet Hamming bound are called perfect codes

Interpretation: If we construct Hamming balls of radius $\lfloor \frac{d-1}{2} \rfloor$ around all the codewords then we would cover the entire ambient space i.e. every possible vector will lie in one of these Hamming balls

Question Can you relate this definition of perfect code with that one we discussed for linear block codes!