Códigos detectores e corretores de erros:
uma introdução

Prof. Victor Martins - DMPA/CCENS/ UFES

Programa de Verão do IME-UFBA 2024
Semana Temática de Álgebra e Topologia Algébrica
29 a 31 de janeiro de 2024

Resumo

- Proposta do minicurso;
- Introdução;
- Teoria básica de códigos;
- Códigos com estrutura algébrica;
- Temas para aprofundamento.

Proposta

- Códigos sobre álgebras de grupo e códigos sobre anéis de polinômios skew;
- Códigos sobre anéis e módulos;
- Códigos e reticulados;
- Códigos algébricos geométricos.
- Códigos quânticos topológicos

Proposta

- Códigos sobre álgebras de grupo e códigos sobre anéis de polinômios skew;
- Códigos sobre anéis e módulos;
- Códigos e reticulados;
- Códigos algébricos geométricos.
- Códigos quânticos topológicos

Objetivo: Apresentar a base da teoria de códigos para prosseguimento em qualquer um dos tópicos acima.

Introdução à teoria de códigos

Os códigos corretores de erros estão presentes nos sistemas de envio de informações que conhecemos: assistir um vídeo no Youtube, mandar mensagem pelo Whatsapp ou fazer uma ligação.

Introdução à teoria de códigos

Os códigos corretores de erros estão presentes nos sistemas de envio de informações que conhecemos: assistir um vídeo no Youtube, mandar mensagem pelo Whatsapp ou fazer uma ligação.

Trata-se de uma maneira organizada de transmitir uma mensagem, isto é, nos permite ao receber uma informação, que seja possível detectar e corrigir erros, garantindo segurança ao usuário.

Introdução à teoria de códigos

Os códigos corretores de erros estão presentes nos sistemas de envio de informações que conhecemos: assistir um vídeo no Youtube, mandar mensagem pelo Whatsapp ou fazer uma ligação.

Trata-se de uma maneira organizada de transmitir uma mensagem, isto é, nos permite ao receber uma informação, que seja possível detectar e corrigir erros, garantindo segurança ao usuário.

O embrião dos códigos corretores de erros pode ser rastreado até as comunicações militares durante a Segunda Guerra Mundial.

A teoria surgiu no final dos anos 40, quando o matemático americano C. E. Shanon, do Laboratório Bell, se questionou sobre o porque as máquinas não eram capazes de encontrar a posição de um determinado erro e corrigí-lo, uma vez que elas podiam detectá-lo.

A teoria surgiu no final dos anos 40, quando o matemático americano C. E. Shanon, do Laboratório Bell, se questionou sobre o porque as máquinas não eram capazes de encontrar a posição de um determinado erro e corrigí-lo, uma vez que elas podiam detectá-lo.

Durante as missões espaciais, como as do programa Apollo nas décadas de 1960 e 1970, a NASA adotou esses códigos para garantir a transmissão confiável de dados entre a Terra e as espaçonaves.

Exemplo

Seja $\mathcal{A}$ o alfabeto brasileiro. Vamos denotar por $\mathcal{P}$ o conjunto das palavras da língua portuguesa. Uma palavra da língua portuguesa pode ser considerada um elemento de $\mathcal{A}^{46}$, onde 46 é a quantidade de letras da maior palavra de $\mathcal{P}$.

Exemplo

Seja $\mathcal{A}$ o alfabeto brasileiro. Vamos denotar por $\mathcal{P}$ o conjunto das palavras da língua portuguesa. Uma palavra da língua portuguesa pode ser considerada um elemento de $\mathcal{A}^{46}$, onde 46 é a quantidade de letras da maior palavra de $\mathcal{P}$.

pneumoultramicroscopicossilicovulcanoconiótico

Note que $\mathcal{P}$ é um subconjunto próprio de $\mathcal{A}^{46}$, o que faz com que esse código seja detector e corretor de erros.

Suponha que ao enviar a mensagem “saudade” ocorresse alguma interferência de modo que a palavra recebida foi, na verdade, “sautade”. Como essa palavra não pertence a $\mathcal{P}$, percebe-se imediatamente que houve erro, e corrigí-lo é muito simples, já que a palavra em $\mathcal{P}$ que mais se aproxima de “sautade” é “saudade”.

Suponha que ao enviar a mensagem “saudade” ocorresse alguma interferência de modo que a palavra recebida foi, na verdade, “sautade”. Como essa palavra não pertence a $\mathcal{P}$, percebe-se imediatamente que houve erro, e corrigí-lo é muito simples, já que a palavra em $\mathcal{P}$ que mais se aproxima de “sautade” é “saudade”.

Agora suponha que ao enviar a mensagem “gato” ocorra erro em que a mensagem recebida seja “rato”. Neste caso, a detecção desse erro será muito dificil.

Suponha que ao enviar a mensagem “saudade” ocorresse alguma interferência de modo que a palavra recebida foi, na verdade, “sautade”. Como essa palavra não pertence a $\mathcal{P}$, percebe-se imediatamente que houve erro, e corrigí-lo é muito simples, já que a palavra em $\mathcal{P}$ que mais se aproxima de “sautade” é “saudade”.

Agora suponha que ao enviar a mensagem “gato” ocorra erro em que a mensagem recebida seja “rato”. Neste caso, a detecção desse erro será muito dificil.

Suponha que ainda sim foi possível detectar a existência de um erro. Um pensamento natural seria pensar em como corrigí-lo, o que também não seria fácil.

Conceito

Um código corretor de erros é um mecanismo utilizado em comunicações digitais para detectar e corrigir erros que possam ocorrer durante a transmissão de dados. A ideia fundamental por trás dos códigos corretores de erros é a introdução de redundância nos dados transmitidos.

Na transmissão de informações, primeiro é preciso converter as informações em sinal digital, ou melhor, codificá-las. Na transmissão a mensagem pode ser adulterada pela interferência de ruídos (ou erros), que se dão por causa do meio físico (computadores, celulares, etc), os chamados **canais**. Para resolver este problema, foram traçadas algumas estratégias, a mais comum é a técnica de repetição.

Na transmissão de informações, primeiro é preciso converter as informações em sinal digital, ou melhor, codificá-las. Na transmissão a mensagem pode ser adulterada pela interferência de ruídos (ou erros), que se dão por causa do meio físico (computadores, celulares, etc), os chamados **canais**. Para resolver este problema, foram traçadas algumas estratégias, a mais comum é a técnica de repetição.

Essas repetições geram custo. Então é preciso encontrar um balanço entre custo e confiabilidade na transmissão, sabendo que quanto maior for a quantidade de repetições, maior será a confiança de que a mensagem será entregue corretamente, ao mesmo passo que quanto maior for a quantidade de repetições, maior será o custo.

Exemplo

Considere um helicóptero de controle remoto, onde suas únicas direções possíveis de vôo são norte, sul, leste, oeste, sudeste, nordeste, sudoeste e noroeste. Tomando $A = \{0, 1\}$, os oito movimentos podem ser codificados em elementos de $\{0, 1\} \times \{0, 1\} \times \{0, 1\}$, como:

Exemplo

Considere um helicóptero de controle remoto, onde suas únicas direções possíveis de vôo são norte, sul, leste, oeste, sudeste, nordeste, sudoeste e noroeste. Tomando $A = \{0, 1\}$, os oito movimentos podem ser codificados em elementos de $\{0, 1\} \times \{0, 1\} \times \{0, 1\}$, como:

Leste $\mapsto 000$	Nordeste $\mapsto 110$
Oeste $\mapsto 001$	Sudeste $\mapsto 101$
Norte $\mapsto 011$	Noroeste $\mapsto 010$
Sul $\mapsto 100$	Sudoeste $\mapsto 111$

Exemplo

Considere um helicóptero de controle remoto, onde suas únicas direções possíveis de vôo são norte, sul, leste, oeste, sudeste, nordeste, sudoeste e noroeste. Tomando $A = \{0, 1\}$, os oito movimentos podem ser codificados em elementos de $\{0, 1\} \times \{0, 1\} \times \{0, 1\}$, como:

Leste $\mapsto 000$	Nordeste $\mapsto 110$
Oeste $\mapsto 001$	Sudeste $\mapsto 101$
Norte $\mapsto 011$	Noroeste $\mapsto 010$
Sul $\mapsto 100$	Sudoeste $\mapsto 111$

O código numérico à direita é chamado de **código da fonte**.

Para melhorar a capacidade de correção de erros, o que se faz é recodificar as palavras, introduzindo uma série de redundâncias. Agora em $\{0,1\}^6$.

Para melhorar a capacidade de correção de erros, o que se faz é recodificar as palavras, introduzindo uma série de redundâncias. Agora em $\{0,1\}^6$.

Leste $\mapsto 000000$	Nordeste $\mapsto 110010$
Oeste $\mapsto 001011$	Sudeste $\mapsto 101110$
Norte $\mapsto 011100$	Noroeste $\mapsto 010111$
Sul $\mapsto 100101$	Sudoeste $\mapsto 111001$

Para melhorar a capacidade de correção de erros, o que se faz é recodificar as palavras, introduzindo uma série de redundâncias. Agora em $\{0,1\}^6$.

Leste $\mapsto 000000$	Nordeste $\mapsto 110010$
Oeste $\mapsto 001011$	Sudeste $\mapsto 101110$
Norte $\mapsto 011100$	Noroeste $\mapsto 010111$
Sul $\mapsto 100101$	Sudoeste $\mapsto 111001$

O novo código introduzido é chamado de **código de canal**.

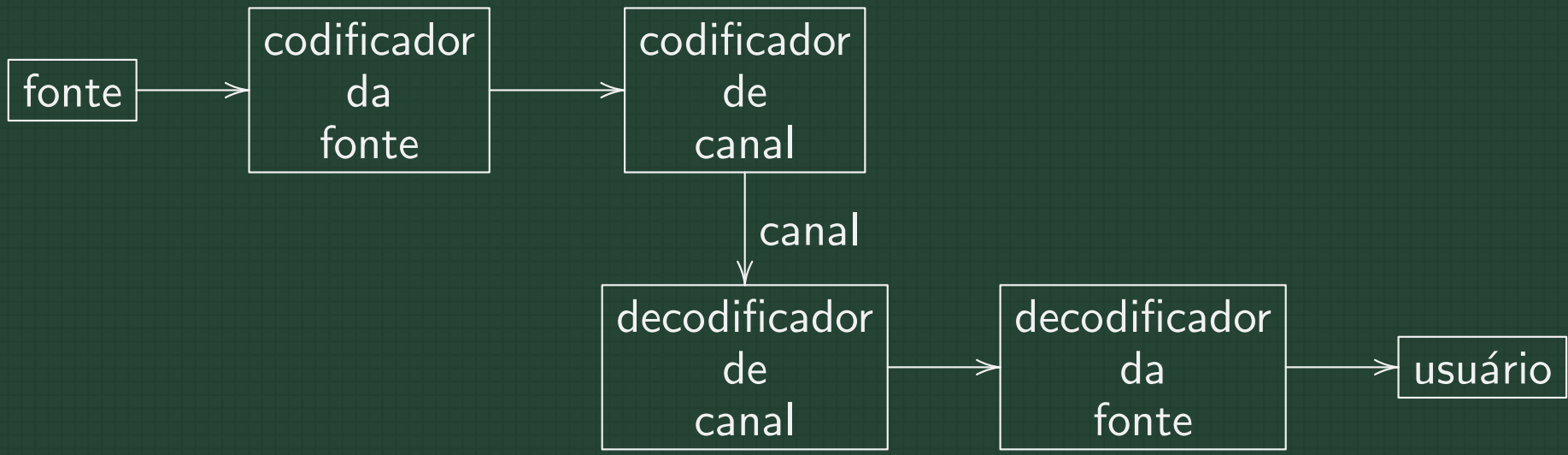
Suponhamos que ao se transmitir a mensagem 110010, tenha ocorrido um erro de modo que a palavra recebida foi 111010. Comparando essa mensagem com as do código, vemos que a que "mais se aproxima" de 111010 é 110010, que é precisamente a mensagem inicialmente transmitida.

Processos de codificação e decodificação

A teoria de códigos tem como objetivo transformar o código da fonte em código de canal, em detectar e corrigir erros e em decodificar o código de canal em código da fonte.

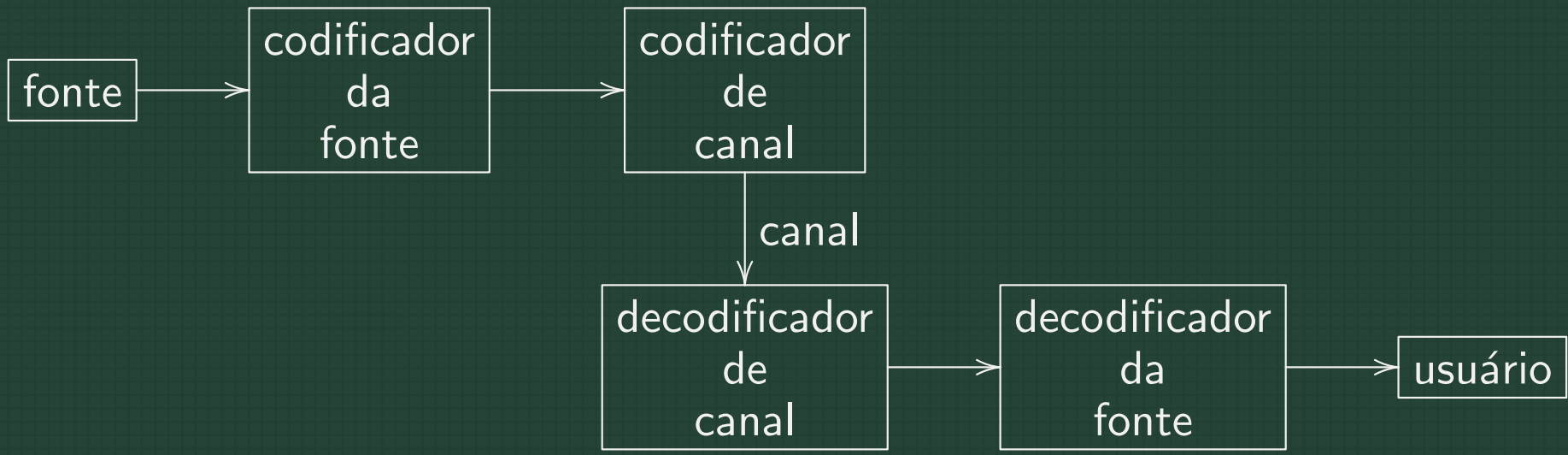
Processos de codificação e decodificação

A teoria de códigos tem como objetivo transformar o código da fonte em código de canal, em detectar e corrigir erros e em decodificar o código de canal em código da fonte.



Processos de codificação e decodificação

A teoria de códigos tem como objetivo transformar o código da fonte em código de canal, em detectar e corrigir erros e em decodificar o código de canal em código da fonte.



O estudo da teoria de códigos tem como um de seus principais pilares encontrar algoritmos de codificação e decodificação cada vez melhores.

Objetos básicos

- **Alfabeto:** um conjunto finito $\mathcal{A}$ com q elementos;
- **Letras** ou **dígitos:** os elementos de $\mathcal{A}$;
- **Palavra:** uma sequência de letras e o **comprimento** dessa palavra é o número de letras que a compõe;
- $\mathcal{A}^n = \{(c_0, \ldots, c_{n-1}) : c_i \in \mathcal{A}, 0 \leq i \leq n-1\}$ é o conjunto de todas as palavras de comprimento n sobre $\mathcal{A}$.

Objetos básicos

- **Alfabeto:** um conjunto finito $\mathcal{A}$ com q elementos;
- **Letras** ou **dígitos:** os elementos de $\mathcal{A}$;
- **Palavra:** uma sequência de letras e o **comprimento** dessa palavra é o número de letras que a compõe;
- $\mathcal{A}^n = \{(c_0, \ldots, c_{n-1}) : c_i \in \mathcal{A}, 0 \leq i \leq n-1\}$ é o conjunto de todas as palavras de comprimento n sobre $\mathcal{A}$.

Um **código** é um subconjunto próprio de $\mathcal{A}^n$.

Distância de Hamming

Dados dois elementos $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ em $\mathcal{A}^n$, a **distância de Hamming** entre u e v é dada por

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|.$$

Distância de Hamming

Dados dois elementos $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ em $\mathcal{A}^n$, a **distância de Hamming** entre u e v é dada por

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|.$$

Se $\mathcal{C}$ é um código então chamamos de **distância mínima** de $\mathcal{C}$ o número

$$d = min\{d(u, v) : u, v \in \mathcal{C} \text{ e } u \neq v\}.$$

Exemplo

Seja $\mathcal{A} = \{0, 1\}$. Considere o código $\mathcal{C} = \{0000, 0101, 1011, 1111\} \subset \mathcal{A}^4$.
Vamos calcular as distâncias entre os elementos de $\mathcal{C}$.

Exemplo

Seja $\mathcal{A} = \{0, 1\}$. Considere o código $\mathcal{C} = \{0000, 0101, 1011, 1111\} \subset \mathcal{A}^4$.
Vamos calcular as distâncias entre os elementos de $\mathcal{C}$.

$$d(0000, 0101) = 2, \quad d(0000, 1011) = 3, \quad d(0000, 1111) = 4,$$

$$d(0101, 1011) = 3, \quad d(0101, 1111) = 2, \quad d(1011, 1111) = 1.$$

Exemplo

Seja $\mathcal{A} = \{0, 1\}$. Considere o código $\mathcal{C} = \{0000, 0101, 1011, 1111\} \subset \mathcal{A}^4$.
Vamos calcular as distâncias entre os elementos de $\mathcal{C}$.

$$d(0000, 0101) = 2, \quad d(0000, 1011) = 3, \quad d(0000, 1111) = 4,$$

$$d(0101, 1011) = 3, \quad d(0101, 1111) = 2, \quad d(1011, 1111) = 1.$$

Logo a distância mínima de $\mathcal{C}$ é $d = 1$.

Proposição

A distância de Hamming determina uma métrica em $\mathcal{A}^n$, ou seja, dados u, v e $w \in \mathcal{A}^n$, valem as seguintes propriedades:

- *Positividade: $d(u,v) \geq 0$, valendo a igualdade se, e somente se, $u = v$.*
- *Simetria: $d(u,v) = d(v,u)$.*
- *Desigualdade Triangular: $d(u,v) \leq d(u,w) + d(w,v)$.*

Disco

Dados $c \in \mathcal{A}^n$ e $t > 0$ um inteiro, define-se o **disco** de centro c e raio t, por:

$$D(c;t) = \{u \in \mathcal{A}^n : d(u,c) \leq t\}.$$

Disco

Dados $c \in \mathcal{A}^n$ e $t > 0$ um inteiro, define-se o **disco** de centro c e raio t, por:

$$D(c;t) = \{u \in \mathcal{A}^n : d(u,c) \leq t\}.$$

É possível mostrar que

$$|D(c;t)| = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

Lema

Seja $\mathcal{C}$ um código com distância mínima d. Se c e c' são palavras distintas de $\mathcal{C}$, então

$$D(c;\kappa) \bigcap D(c';\kappa) = \emptyset$$

onde $\kappa = [\frac{d-1}{2}]$ e $[t]$ representa a parte inteira de um número real t.

Lema

Seja $\mathcal{C}$ um código com distância mínima d. Se c e c' são palavras distintas de $\mathcal{C}$, então

$$D(c;\kappa) \bigcap D(c';\kappa) = \emptyset$$

onde $\kappa = [\frac{d-1}{2}]$ e $[t]$ representa a parte inteira de um número real t.

Seja $\mathcal{C} \subset \mathcal{A}^n$ um código com distância mínima d . O código $\mathcal{C}$ será dito **perfeito** se

$$\bigcup D(c;\kappa) = \mathcal{A}^n.$$

Capacidade de correção

Teorema

Seja $\mathcal{C}$ um código com distância mínima d. Então $\mathcal{C}$ pode corrigir até $\kappa = [\frac{d-1}{2}]$ erros e detectar até $d-1$ erros.

Os **três parâmetros fundamentais** de um código $\mathcal{C} \subset \mathcal{A}^n$ são $[n; M; d]$, onde n é o comprimento do código, M o número de elementos e d a distância mínima de $\mathcal{C}$.

Os **três parâmetros fundamentais** de um código $\mathcal{C} \subset \mathcal{A}^n$ são $[n; M; d]$, onde n é o comprimento do código, M o número de elementos e d a distância mínima de $\mathcal{C}$.

Dados três inteiros positivos arbitrários n, M e d, nem sempre existe um código com esses parâmetros.

Códigos com estrutura algébrica

A inserção de estruturas algébricas surge como uma abordagem fundamental para aprimorar e otimizar o desempenho dos códigos corretores de erros. Ao incorporar estruturas algébricas na teoria de códigos corretores de erros, ampliamos significativamente nosso entendimento sobre os processos subjacentes à detecção e correção de erros em transmissões de dados.

Códigos lineares

- O alfabeto do código será sempre um corpo finito $\mathbb{K}$;
- Para cada n natural temos um $\mathbb{K}$-espaço vetorial $\mathbb{K}^n$ de dimensão n;

Códigos lineares

- O alfabeto do código será sempre um corpo finito $\mathbb{K}$;
- Para cada n natural temos um $\mathbb{K}$-espaço vetorial $\mathbb{K}^n$ de dimensão n;

Dizemos que $\mathcal{C} \subset \mathbb{K}^n$ é um **código linear** se $\mathcal{C}$ é um subespaço vetorial próprio de $\mathbb{K}^n$.

Um código linear possui 3 parâmetros principais n, k e d, que são a dimensão do espaço vetorial, a dimensão do código como subespaço vetorial e a distância mínima.

Um código linear possui 3 parâmetros principais n, k e d, que são a dimensão do espaço vetorial, a dimensão do código como subespaço vetorial e a distância mínima.

Seja $k = \dim \mathcal{C}$ e $\{\mathbf{v_1}, ..., \mathbf{v}_k\}$ uma de suas bases, então todo elemento de $\mathcal{C}$ se escreve como

$$\lambda_1 \mathbf{v_1} + \lambda_2 \mathbf{v_2} + ... + \lambda_k \mathbf{v}_k,$$

onde $\lambda_i \in \mathbb{K}$.

Um código linear possui 3 parâmetros principais n, k e d, que são a dimensão do espaço vetorial, a dimensão do código como subespaço vetorial e a distância mínima.

Seja $k = \dim \mathcal{C}$ e $\{\mathbf{v_1}, ..., \mathbf{v}_k\}$ uma de suas bases, então todo elemento de $\mathcal{C}$ se escreve como

$$\lambda_1 \mathbf{v_1} + \lambda_2 \mathbf{v_2} + ... + \lambda_k \mathbf{v}_k,$$

onde $\lambda_i \in \mathbb{K}$.

Daí

$$M = |\mathcal{C}| = q^k.$$

Peso

Definição

Dado $x = (x_1, x_2, \ldots, x_n) \in \mathbb{K}^n$, define-se o **peso** *de x como sendo o número inteiro*

$$\omega(x) := |\{i : x_i \neq 0\}|.$$

Em outras palavras, $\omega(x) = d(x, 0)$, onde d é a distância de Hamming.

Peso

Definição

Dado $x = (x_1, x_2, \ldots, x_n) \in \mathbb{K}^n$, define-se o **peso** *de x como sendo o número inteiro*

$$\omega(x) := |\{i : x_i \neq 0\}|.$$

Em outras palavras, $\omega(x) = d(x, 0)$, onde d é a distância de Hamming.

O **peso** de um código linear $\mathcal{C}$ é o inteiro

$$\omega(\mathcal{C}) := min\{\omega(x) : x \in \mathcal{C} \backslash \{0\}\}.$$

Em um código linear $\mathcal{C}$ com distância mínima d, temos que $d(\mathbf{u}, \mathbf{v}) = \omega(\mathbf{u} - \mathbf{v})$, para quaisquer $\mathbf{u}, \mathbf{v} \in \mathbb{K}^n$ e, ainda, $d = \omega(\mathcal{C})$.

Exemplo

O código do helicóptero é linear. O alfabeto é o corpo finito $\mathbb{F}_2 = \{0, 1\}$.

Leste $\mapsto 000000$	Nordeste $\mapsto 110010$
Oeste $\mapsto 001011$	Sudeste $\mapsto 101110$
Norte $\mapsto 011100$	Noroeste $\mapsto 010111$
Sul $\mapsto 100101$	Sudoeste $\mapsto 111001$

Este código pode ser realizado como imagem da transformação linear

$$\begin{array}{cccc} T & : {\mathbb{F}_2}^3 & \longrightarrow & {\mathbb{F}_2}^6 \\ & (x_1, x_2, x_3) & \mapsto & (x_1, x_2, x_3, x_1 + x_2, x_2 + x_3, x_1 + x_2 + x_3) \end{array},$$

que é um subespaço de ${\mathbb{F}_2}^6$.

Este código pode ser realizado como imagem da transformação linear

$$\begin{array}{rccc} T & : {\mathbb{F}_2}^3 & \longrightarrow & {\mathbb{F}_2}^6 \\ & (x_1, x_2, x_3) & \mapsto & (x_1, x_2, x_3, x_1 + x_2, x_2 + x_3, x_1 + x_2 + x_3) \end{array},$$

que é um subespaço de ${\mathbb{F}_2}^6$.

As palavras 110010 e 111001 têm respectivamente pesos 3 e 4 e calculando os demais pesos das palavras deste código verificamos que este possui peso 3.

Descrição de um código linear como imagem de T

- $\{e_1, \ldots, e_n\}$ a base canônica de $\mathbb{K}^n$, para algum n natural.
- $\{v_1, ..., v_k\}$ uma base de um código $\mathcal{C} \subset \mathbb{K}^n$. Então $\mathcal{C}$ é isomorfo a $\mathbb{K}^k$.

Descrição de um código linear como imagem de T

- $\{e_1, \ldots, e_n\}$ a base canônica de $\mathbb{K}^n$, para algum n natural.
- $\{v_1, ..., v_k\}$ uma base de um código $\mathcal{C} \subset \mathbb{K}^n$. Então $\mathcal{C}$ é isomorfo a $\mathbb{K}^k$.

Podemos definir uma aplicação linear injetora $T : \mathbb{K}^k \longrightarrow \mathbb{K}^n$ por $T(e_i) = v_i$, para $0 \leq i \leq k$.

Descrição de um código linear como imagem de T

- $\{e_1, \ldots, e_n\}$ a base canônica de $\mathbb{K}^n$, para algum n natural.
- $\{v_1, ..., v_k\}$ uma base de um código $\mathcal{C} \subset \mathbb{K}^n$. Então $\mathcal{C}$ é isomorfo a $\mathbb{K}^k$.

Podemos definir uma aplicação linear injetora $T : \mathbb{K}^k \longrightarrow \mathbb{K}^n$ por $T(e_i) = v_i$, para $0 \leq i \leq k$.

Por construção de T vemos que $Im(T) = \mathcal{C}$.

Descrição de um código linear como núcleo de T'

Dada uma base $\{v_1, ..., v_k\}$ de $\mathcal{C}$ podemos ampliá-la a uma base $\{v_1, ..., v_k, c_1, ..., c_{n-k}\}$ de $\mathbb{K}^n$.

Descrição de um código linear como núcleo de T'

Dada uma base $\{v_1, ..., v_k\}$ de $\mathcal{C}$ podemos ampliá-la a uma base $\{v_1, ..., v_k, c_1, ..., c_{n-k}\}$ de $\mathbb{K}^n$.

Logo $v \in \mathbb{K}^n$ pode ser escrito como

$$v = \lambda_1 v_1 + \ldots + \lambda_k v_k + \lambda_{k+1} c_1 + \ldots + \lambda_n c_{n-k}.$$

Descrição de um código linear como núcleo de T'

Dada uma base $\{v_1, ..., v_k\}$ de $\mathcal{C}$ podemos ampliá-la a uma base $\{v_1, ..., v_k, c_1, ..., c_{n-k}\}$ de $\mathbb{K}^n$.

Logo $v \in \mathbb{K}^n$ pode ser escrito como

$$v = \lambda_1 v_1 + \ldots + \lambda_k v_k + \lambda_{k+1} c_1 + \ldots + \lambda_n c_{n-k}.$$

Defina a transformação linear sobrejetora $T' : \mathbb{K}^n \longrightarrow \mathbb{K}^{n-k}$ por

$$v \longmapsto v' = \lambda_{k+1} c_1 + \ldots + \lambda_n c_{n-k}.$$

Descrição de um código linear como núcleo de T'

Dada uma base $\{v_1, ..., v_k\}$ de $\mathcal{C}$ podemos ampliá-la a uma base $\{v_1, ..., v_k, c_1, ..., c_{n-k}\}$ de $\mathbb{K}^n$.

Logo $v \in \mathbb{K}^n$ pode ser escrito como

$$v = \lambda_1 v_1 + \ldots + \lambda_k v_k + \lambda_{k+1} c_1 + \ldots + \lambda_n c_{n-k}.$$

Defina a transformação linear sobrejetora $T' : \mathbb{K}^n \longrightarrow \mathbb{K}^{n-k}$ por

$$v \longmapsto v' = \lambda_{k+1} c_1 + \ldots + \lambda_n c_{n-k}.$$

Portanto, $Ker(T') = \mathcal{C}$.

Equivalência de códigos

Definição

Dizemos que uma aplicação linear $T : \mathbb{K}^n \to \mathbb{K}^n$ *é uma* **isometria** *de* $\mathbb{K}^n$ *se*

$$d(T(\mathbf{u}), T(\mathbf{v})) = d(\mathbf{u}, \mathbf{v}), \forall\ \mathbf{u}, \mathbf{v} \in \mathbb{K}^n.$$

Equivalência de códigos

Definição

Dizemos que uma aplicação linear $T : \mathbb{K}^n \to \mathbb{K}^n$ é uma **isometria** *de $\mathbb{K}^n$ se*

$$d(T(\mathbf{u}), T(\mathbf{v})) = d(\mathbf{u}, \mathbf{v}), \forall\ \mathbf{u}, \mathbf{v} \in \mathbb{K}^n.$$

Dizemos que $\mathcal{C}'$ é **linearmente equivalente** a $\mathcal{C}$ se existir uma isometria T de $\mathbb{K}^n$ tal que $T(\mathcal{C}) = \mathcal{C}'$.

Equivalência de códigos

Definição

Dizemos que uma aplicação linear $T : \mathbb{K}^n \to \mathbb{K}^n$ *é uma* **isometria** *de* $\mathbb{K}^n$ *se*

$$d(T(\mathbf{u}), T(\mathbf{v})) = d(\mathbf{u}, \mathbf{v}), \forall\ \mathbf{u}, \mathbf{v} \in \mathbb{K}^n.$$

Dizemos que $\mathcal{C}'$ é **linearmente equivalente** a $\mathcal{C}$ se existir uma isometria T de $\mathbb{K}^n$ tal que $T(\mathcal{C}) = \mathcal{C}'$.

A equivalência de códigos é uma relação de equivalência. Códigos equivalentes têm os mesmos parâmetros.

Teorema

Dois códigos lineares $\mathcal{C}$ e $\mathcal{C}'$ são equivalentes se, e somente se, existem uma permutação π de $\{1, \ldots, n\}$ e elementos $c_1, \ldots, c_n$ em $\mathbb{K}$ tais que

$$\mathcal{C}' = \{(c_1(x_{\pi(1)}), \ldots, c_n(x_{\pi(n)})) : (x_1, \ldots, x_n) \in \mathcal{C}\}.$$

Teorema

Dois códigos lineares $\mathcal{C}$ e $\mathcal{C}'$ são equivalentes se, e somente se, existem uma permutação π de $\{1, \ldots, n\}$ e elementos $c_1, \ldots, c_n$ em $\mathbb{K}$ tais que

$$\mathcal{C}' = \{(c_1(x_{\pi(1)}), \ldots, c_n(x_{\pi(n)})) : (x_1, \ldots, x_n) \in \mathcal{C}\}.$$

Isto é, dois códigos lineares são equivalentes se, e só se, cada um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

- Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras.
- Permutação das posições de todas as palavras do código, mediante uma permutação fixa de $\{1, \ldots, n\}$.

Matriz geradora de um código

Seja $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ uma base de um código linear $\mathcal{C}$. A matriz G a seguir é chamada de **matriz geradora** de $\mathcal{C}$ associada à base $\mathcal{B}$

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

Considere a transformação linear definida por

$$\begin{aligned} T : \mathbb{K}^k &\to \mathbb{K}^n \\ \mathbf{c} &\mapsto \mathbf{c}G. \end{aligned}$$

Considere a transformação linear definida por

$$\begin{aligned} T : \mathbb{K}^k &\to \mathbb{K}^n \\ \mathbf{c} &\mapsto \mathbf{c}G. \end{aligned}$$

Se $\mathbf{c} = (c_1, \ldots, c_k)$, temos que

$$T(\mathbf{c}) = \mathbf{c}G = c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k.$$

Considere a transformação linear definida por

$$\begin{aligned} T : \mathbb{K}^k &\to \mathbb{K}^n \\ \mathbf{c} &\mapsto \mathbf{c}G. \end{aligned}$$

Se $\mathbf{c} = (c_1, \ldots, c_k)$, temos que

$$T(\mathbf{c}) = \mathbf{c}G = c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k.$$

Logo $T(\mathbb{K}^k) = \mathcal{C}$. Daí, podemos considerar $\mathbb{K}^k$ como o **código da fonte**, $\mathcal{C}$ o **código do canal** e T uma **codificação**.

Duas matrizes geradoras de um mesmo código podem ser obtidas uma da outra por sequências de operações do tipo:

- Permutação de duas linhas;
- Multiplicação de uma linha por um escalar não nulo;
- Adição de um múltiplo escalar de uma linha a outra.

Exemplo

Seja $\mathbb{F}_2$ o alfabeto de um código linear $\mathcal{C}$, e considere a seguinte transformação linear

$$\begin{aligned} T : \mathbb{F}_2^3 &\to \mathbb{F}_2^5 \\ \mathbf{c} &\mapsto \mathbf{c}G. \end{aligned}$$

Seja $\mathcal{B} = \{(1,0,1,0,1),(1,1,0,1,0),(1,1,1,1,1)\} \subset \mathbb{F}_2^5$ uma base de $\mathcal{C}$. Desta forma,

Exemplo

Seja $\mathbb{F}_2$ o alfabeto de um código linear $\mathcal{C}$, e considere a seguinte transformação linear

$$\begin{aligned} T : \mathbb{F}_2^3 &\to \mathbb{F}_2^5 \\ \mathbf{c} &\mapsto \mathbf{c}G. \end{aligned}$$

Seja $\mathcal{B} = \{(1,0,1,0,1), (1,1,0,1,0), (1,1,1,1,1)\} \subset \mathbb{F}_2^5$ uma base de $\mathcal{C}$. Desta forma,

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

é uma matriz geradora de um código $\mathcal{C}$ em $\mathbb{F}_2^5$. Fazendo $T((1,1,0))$, obtemos $(0,1,1,1,1)$ como codificação.

Agora, suponha que se queira decodificar a palavra $(1,0,0,0,0)$ do código de canal. Basta resolver o sistema linear

$$(c_1, c_2, c_3)G = (1,0,0,0,0),$$

ou seja,

$$\begin{cases} c_1 + c_2 + c_3 = 1 \\ c_2 + c_3 = 0 \\ c_1 + c_3 = 0 \\ c_2 + c_3 = 0 \\ c_1 + c_3 = 0 \end{cases}$$

cuja solução é $c_1 = 1, c_2 = 1$ e $c_3 = 1$.

Forma padrão

Definição

Seja G uma matriz geradora de um código linear $\mathcal{C}$. Dizemos que G está na **forma padrão** *se*

$$G = (Id_k \mid A),$$

onde Id_k é a matriz identidade $k \times k$ e A uma matriz $k \times (n-k)$.

Forma padrão

Definição

Seja G uma matriz geradora de um código linear $\mathcal{C}$. Dizemos que G está na **forma padrão** *se*

$$G = (Id_k \mid A),$$

onde Id_k é a matriz identidade $k \times k$ e A uma matriz $k \times (n-k)$.

Nem sempre conseguimos encontrar uma matriz geradora de $\mathcal{C}$ na forma padrão. Contudo, se G é uma matriz geradora de $\mathcal{C}$, podemos permutar colunas de G, obtendo uma matriz G' que é a matriz geradora na forma padrão de um código $\mathcal{C}'$ equivalente a $\mathcal{C}$.

Forma padrão

Definição

Seja G uma matriz geradora de um código linear $\mathcal{C}$. Dizemos que G está na **forma padrão** *se*

$$G = (Id_k \mid A),$$

onde Id_k é a matriz identidade $k \times k$ e A uma matriz $k \times (n-k)$.

Nem sempre conseguimos encontrar uma matriz geradora de $\mathcal{C}$ na forma padrão. Contudo, se G é uma matriz geradora de $\mathcal{C}$, podemos permutar colunas de G, obtendo uma matriz G' que é a matriz geradora na forma padrão de um código $\mathcal{C}'$ equivalente a $\mathcal{C}$.

Teorema

Dado um código linear $\mathcal{C}$, existe um código $\mathcal{C}'$ equivalente a $\mathcal{C}$ que possui matriz geradora na forma padrão.

Códigos duais

Dados $\mathbf{u} = (u_1, \ldots, u_n)$ e $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{K}^n$, define-se o produto interno de $\mathbf{u}$ e $\mathbf{v}$ por

$$\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n.$$

Códigos duais

Dados $\mathbf{u} = (u_1, \ldots, u_n)$ e $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{K}^n$, define-se o produto interno de $\mathbf{u}$ e $\mathbf{v}$ por

$$\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n.$$

Define-se **código dual** de $\mathcal{C}$ em $\mathbb{K}^n$ por

$$\mathcal{C}^{\perp} = \{\mathbf{v} \in \mathbb{K}^n : \mathbf{u} \cdot \mathbf{v} = 0, \forall \mathbf{u} \in \mathcal{C}\} = \{\mathbf{v} \in \mathbb{K}^n : G\mathbf{v}^t = \mathbf{0}\}.$$

Proposição

Seja $\mathcal{C} \subset \mathbb{K}^n$ um código de dimensão k com matriz geradora $G = (Id_k \mid A)$ na forma padrão. Então

(i) $\dim \mathcal{C}^\perp = n - k$;

(ii) $H = (-A^t | Id_{n-k})$ *é uma matriz geradora de* $\mathcal{C}^\perp$;

(iii) $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Condição de anulamento

Proposição

Sejam $\mathcal{C} \subset \mathbb{K}^n$ um código linear tal que $\mathcal{C}^\perp$ tem matriz geradora H e $\mathbf{v} \in \mathbb{K}^n$. Então

$$\mathbf{v} \in \mathcal{C} \iff H\mathbf{v}^t = \mathbf{0}.$$

Condição de anulamento

Proposição

Sejam $\mathcal{C} \subset \mathbb{K}^n$ um código linear tal que $\mathcal{C}^\perp$ tem matriz geradora H e $\mathbf{v} \in \mathbb{K}^n$. Então

$$\mathbf{v} \in \mathcal{C} \iff H\mathbf{v}^t = \mathbf{0}.$$

A matriz geradora H de $\mathcal{C}^\perp$ é chamada de **matriz teste de paridade** de $\mathcal{C}$. Com isso, os elementos de $\mathcal{C}$ ficam determinados por uma condição de anulamento, tendo um custo computacional baixo, pois basta determinar se $H\mathbf{v}^t$ é o vetor nulo de $\mathbb{K}^n$ para que $\mathbf{v}$ pertença a $\mathcal{C}$.

Dados três inteiros positivos arbitrários n, M e d, nem sempre existe um código com esses parâmetros.

Dados três inteiros positivos arbitrários n, M e d, nem sempre existe um código com esses parâmetros.

Teorema (Cota de Singleton)

Os parâmetros $[n; k; d]$ de um código linear satisfazem à desigualdade

$$d \leq n - k + 1.$$

Dados três inteiros positivos arbitrários n, M e d, nem sempre existe um código com esses parâmetros.

Teorema (Cota de Singleton)

Os parâmetros $[n; k; d]$ de um código linear satisfazem à desigualdade

$$d \leq n - k + 1.$$

Quando tivermos um código em que $d = n - k + 1$, chamaremos esse código de MDS (*Maximum Distance Separable*).

Exemplo

Um **código de Hamming** de ordem m sobre $\mathbb{F}_2$ é um código com matriz teste de paridade H_m de ordem $m \times n$, cujas colunas são os elementos de $\mathbb{F}_2^m \setminus \{0\}$ numa ordem qualquer.

Sendo $\mathcal{C} \subset \mathbb{F}_2^n$ o código determinado pela matriz H_m, temos $n = 2^m - 1$. Com isso, sua dimensão é $k = n - m = 2^m - m - 1$.

A distância mínima em um código de Hamming é $d = 3$.

Para $m = 3$, a matriz teste de paridade será

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

Para $m = 3$, a matriz teste de paridade será

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

temos $n = 2^3 - 1 = 7$ e $k = 7 - 3 = 4$.

Para $m = 3$, a matriz teste de paridade será

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

temos $n = 2^3 - 1 = 7$ e $k = 7 - 3 = 4$.

Todo código de Hamming é perfeito.

Para $m = 3$, a matriz teste de paridade será

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

temos $n = 2^3 - 1 = 7$ e $k = 7 - 3 = 4$.

Todo código de Hamming é perfeito.

Um código de Hamming de ordem m é MDS se, e somente se, $m = 2$.

Códigos cíclicos

Um código linear $\mathcal{C} \subset \mathbb{K}^n$ é um **código cíclico** se $c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$ sempre que $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$.

Códigos cíclicos

Um código linear $\mathcal{C} \subset \mathbb{K}^n$ é um **código cíclico** se
$c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$ sempre que $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$.

Exemplo

O código $\mathcal{C} = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$ *é cíclico.*

Códigos cíclicos

Um código linear $\mathcal{C} \subset \mathbb{K}^n$ é um **código cíclico** se $c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$ sempre que $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$.

Exemplo

O código $\mathcal{C} = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$ *é cíclico.*

Note que $\mathcal{C}$ *é um subespaço vetorial de* $\mathbb{F}_2^4$ *e tem os seguintes parâmetros: comprimento* 4*, dimensão* 2 *e distância mínima* 2*.*

Anel de polinômios

Defina R_n como o anel quociente dado por

$$R_n = \frac{\mathbb{K}[x]}{\langle x^n - 1 \rangle}.$$

Anel de polinômios

Defina R_n como o anel quociente dado por

$$R_n = \frac{\mathbb{K}[x]}{\langle x^n - 1 \rangle}.$$

Assim, se $\overline{f(x)} \in R_n$, então

$$\overline{f(x)} = \{f(x) + g(x)(x^n - 1) : g(x) \in \mathbb{K}[x]\}.$$

Anel de polinômios

Defina R_n como o anel quociente dado por

$$R_n = \frac{\mathbb{K}[x]}{\langle x^n - 1 \rangle}.$$

Assim, se $\overline{f(x)} \in R_n$, então

$$\overline{f(x)} = \{f(x) + g(x)(x^n - 1) : g(x) \in \mathbb{K}[x]\}.$$

R_n munido da multiplicação por escalar $\lambda \in \mathbb{K}$, dada por

$$\lambda\overline{f(x)} = \overline{\lambda f(x)}, \quad \forall \ \overline{f(x)} \in R_n$$

é um $\mathbb{K}$-espaço vetorial de dimensão n com base $\mathcal{B} = \left\{1, \overline{x}, \ldots, \overline{x^{n-1}}\right\}$.

Temos o seguinte isomorfismo:

$$\begin{array}{rcl} \nu : \mathbb{K}^n & \to & R_n \\ (c_0, c_1, \ldots, c_{n-1}) & \mapsto & \overline{c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}}. \end{array}$$

Temos o seguinte isomorfismo:

$$\begin{array}{rcl} \nu : \mathbb{K}^n & \to & R_n \\ (c_0, c_1, \ldots, c_{n-1}) & \mapsto & \overline{c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}}. \end{array}$$

R_n possui as estruturas de anel e espaço vetorial e é isomorfo a $\mathbb{K}^n$, o que significa que todo código linear $\mathcal{C} \subset \mathbb{K}^n$ pode ser visto em R_n através do isomorfismo ν, o que nos permite usar ferramentas de anéis na busca de melhores algoritmos de codificação e decodificação.

Teorema

Um subespaço $\mathcal{C}$ de $\mathbb{K}^n$ é um código cíclico se, e somente se, $\nu(\mathcal{C})$ é um ideal de R_n.

Teorema

Um subespaço $\mathcal{C}$ de $\mathbb{K}^n$ é um código cíclico se, e somente se, $\nu(\mathcal{C})$ é um ideal de R_n.

Observe que para verificar se um subespaço vetorial $\mathcal{C}$ de $\mathbb{K}^n$ é um código cíclico sem a utilização do teorema, seria preciso verificar se todas as trocas cíclicas pertencem a $\mathcal{C}$, o que poderia ser muito trabalhoso.

Um ideal no anel quociente R_n é da forma $\langle \overline{p(x)} \rangle$, onde $p(x)$ é divisor de $x^n - 1$.

Um ideal no anel quociente R_n é da forma $\langle\overline{p(x)}\rangle$, onde $p(x)$ é divisor de $x^n - 1$.

Teorema

Seja $g(x)$ um polinômio divisor de $x^n - 1$ de grau s. Se $I = \left\langle\overline{g(x)}\right\rangle$ é um ideal de R_n, então

$$\dim_{\mathbb{K}} I = n - s,$$

e o código $\mathcal{C} = \nu^{-1}(I)$ tem matriz geradora dada por

$$G = \begin{pmatrix} \nu^{-1}\left(\overline{g(x)}\right) \\ \nu^{-1}\left(\overline{xg(x)}\right) \\ \vdots \\ \nu^{-1}\left(\overline{x^{n-s-1}g(x)}\right) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \dots & g_s & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_s & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & g_0 & \dots & g_s \end{pmatrix}$$

Seja $h(x) = h_0 + h_1 x + \cdots + h_t x^t$ um polinômio que divide $x^n - 1$.
Chamaremos de **polinômio recíproco** de $h(x)$, o polinômio

$$h^*(x) = x^t h(x^{-1}) = h_t + h_{t-1} x + \cdots + h_0 x^t.$$

Este polinômio também divide $x^n - 1$ e, portanto, é gerador de algum código cíclico.

Seja $h(x) = h_0 + h_1 x + \cdots + h_t x^t$ um polinômio que divide $x^n - 1$. Chamaremos de **polinômio recíproco** de $h(x)$, o polinômio

$$h^*(x) = x^t h(x^{-1}) = h_t + h_{t-1} x + \cdots + h_0 x^t.$$

Este polinômio também divide $x^n - 1$ e, portanto, é gerador de algum código cíclico.

Teorema

Seja $\mathcal{C} = \nu^{-1}(I)$ um código cíclico, onde $I = \left\langle \overline{g(x)} \right\rangle$ é um ideal de R_n e $h(x) = \frac{x^n - 1}{g(x)}$. Daí, $\mathcal{C}^\perp$ é cíclico e $\mathcal{C}^\perp = \nu^{-1}(J)$, onde J é o ideal de R_n gerado por $\overline{h^*(x)}$. Isto é, $J = \left\langle \overline{h^*(x)} \right\rangle$.

Além disso, o código $\mathcal{C}^{\perp}$ tem matriz geradora dada por

$$H = \begin{pmatrix} \nu^{-1}\left(\overline{h^*(x)}\right) \\ \nu^{-1}\left(\overline{xh^*(x)}\right) \\ \vdots \\ \nu^{-1}\left(\overline{x^{s-1}h^*(x)}\right) \end{pmatrix}$$

e, portanto, H é uma matriz teste de paridade para $\mathcal{C}$.

Temas para aprofundamento

- Códigos de grupo
- Códigos algébricos geométricos
- Códigos e reticulados

Sejam G um grupo e R um anel com unidade e considere RG o conjunto de todas as combinações lineares da forma

$$\alpha = \sum_{g \in G} a_g g,$$

em que $a_g \in R$ e $a_g = 0$, para quase todo $g \in G$.

Sejam G um grupo e R um anel com unidade e considere RG o conjunto de todas as combinações lineares da forma

$$\alpha = \sum_{g \in G} a_g g,$$

em que $a_g \in R$ e $a_g = 0$, para quase todo $g \in G$.

Pode-se munir RG com a estrutura de anel e de R-módulo.

Sejam G um grupo e R um anel com unidade e considere RG o conjunto de todas as combinações lineares da forma

$$\alpha = \sum_{g \in G} a_g g,$$

em que $a_g \in R$ e $a_g = 0$, para quase todo $g \in G$.

Pode-se munir RG com a estrutura de anel e de R-módulo.

Definição

O conjunto RG com as estruturas de anel e R-módulo é chamado de **anel de grupo** *de G sobre R. No caso em que R é comutativo, RG é chamado de* **álgebra de grupo** *de G sobre R.*

Álgebra de grupo cíclico

Seja $G = \langle a : a^n = 1 \rangle$ e $\mathbb{K}$ um corpo tal que $car(\mathbb{K}) \nmid |G|$. Considere o epimorfismo de anéis $\theta : \mathbb{K}[x] \mapsto \mathbb{K}G$ dado por

$$f(x) \in \mathbb{K}[x] \mapsto f(a) \in \mathbb{K}G.$$

Álgebra de grupo cíclico

Seja $G = \langle a : a^n = 1 \rangle$ e $\mathbb{K}$ um corpo tal que $car(\mathbb{K}) \nmid |G|$. Considere o epimorfismo de anéis $\theta : \mathbb{K}[x] \mapsto \mathbb{K}G$ dado por

$$f(x) \in \mathbb{K}[x] \mapsto f(a) \in \mathbb{K}G.$$

Pelo teorema do homomorfismo,

$$\mathbb{K}G \simeq \frac{\mathbb{K}[x]}{ker(\theta)}.$$

Álgebra de grupo cíclico

Seja $G = \langle a : a^n = 1 \rangle$ e $\mathbb{K}$ um corpo tal que $car(\mathbb{K}) \nmid |G|$. Considere o epimorfismo de anéis $\theta : \mathbb{K}[x] \mapsto \mathbb{K}G$ dado por

$$f(x) \in \mathbb{K}[x] \mapsto f(a) \in \mathbb{K}G.$$

Pelo teorema do homomorfismo,

$$\mathbb{K}G \simeq \frac{\mathbb{K}[x]}{ker(\theta)}.$$

É possível mostrar que $ker(\theta) = \langle x^n - 1 \rangle$ e, portanto,

$$\mathbb{K}G \simeq \frac{\mathbb{K}[x]}{\langle x^n - 1 \rangle}.$$

Código de grupo

Um **código de grupo** (à esquerda) de comprimento n é um código linear que é imagem de um ideal (à esquerda) de uma álgebra de grupo via um isomorfismo

$$\mathbb{K}G \to \mathbb{K}^n$$

que aplica G na base canônica de $\mathbb{K}^n$.

Código de grupo

Um **código de grupo** (à esquerda) de comprimento n é um código linear que é imagem de um ideal (à esquerda) de uma álgebra de grupo via um isomorfismo

$$\mathbb{K}G \to \mathbb{K}^n$$

que aplica G na base canônica de $\mathbb{K}^n$.

Definição

*Se G é um grupo de ordem n e $\mathcal{C} \subset \mathbb{K}^n$ é um código linear então $\mathcal{C}$ é um G-**código** (à esquerda) se existe uma bijeção entre a base canônica de $\mathbb{K}^n$ e G que se estende a um isomorfismo $\mathbb{K}^n \to \mathbb{K}G$ que aplica $\mathcal{C}$ em um ideal (à esquerda) de $\mathbb{K}G$.*

(BERNAL; RÍO; SIMÓN, 2009) trabalham com código de grupo para grupos que possuem uma certa decomposição em dois subgrupos abelianos. Em sua tese de doutorado, (ALDERETE, 2018) generaliza alguns dos resultados de Bernal, del Río e Símon para o caso de grupos que se decompõem em mais subgrupos abelianos.

(BERNAL; RÍO; SIMÓN, 2009) trabalham com código de grupo para grupos que possuem uma certa decomposição em dois subgrupos abelianos. Em sua tese de doutorado, (ALDERETE, 2018) generaliza alguns dos resultados de Bernal, del Río e Símon para o caso de grupos que se decompõem em mais subgrupos abelianos.

Outro tópico interessante a se explorar neste contexto é a ponte entre a matemática pura e aplicada envolvida no assunto. Obter bons parâmetros para os códigos estudados é algo que parece promissor, especialmente para aqueles que aplicam a teoria matemática desenvolvida.

(BERNAL; RÍO; SIMÓN, 2009) trabalham com código de grupo para grupos que possuem uma certa decomposição em dois subgrupos abelianos. Em sua tese de doutorado, (ALDERETE, 2018) generaliza alguns dos resultados de Bernal, del Río e Símon para o caso de grupos que se decompõem em mais subgrupos abelianos.

Outro tópico interessante a se explorar neste contexto é a ponte entre a matemática pura e aplicada envolvida no assunto. Obter bons parâmetros para os códigos estudados é algo que parece promissor, especialmente para aqueles que aplicam a teoria matemática desenvolvida.

Alguns pesquisadores brasileiros: Francisco César Polcino Milies, Thierry Petit Lobão, Raul Antônio Ferraz, Gladys Chalom, Marinês Guerreiro e Samir Assuena.

Códigos algébricos geométricos

Na área de estudo dos códigos algébricos geométricos conceitos abstratos de álgebra se entrelaçam com a geometria a fim de criar ferramentas para a transmissão segura e armazenamento confiável de informações digitais.

Códigos algébricos geométricos

Na área de estudo dos códigos algébricos geométricos conceitos abstratos de álgebra se entrelaçam com a geometria a fim de criar ferramentas para a transmissão segura e armazenamento confiável de informações digitais.

Os códigos algébricos geométricos combinam princípios da álgebra com a geometria algébrica para criar estruturas matemáticas que podem ser utilizadas na correção de erros. Álgebra, com suas operações sobre estruturas matemáticas, como corpos finitos, e geometria algébrica, que estuda as soluções de equações polinomiais.

Os códigos algébricos geométricos operam em espaços mais abstratos, utilizando polinômios e curvas algébricas para representar informações.

Os códigos algébricos geométricos operam em espaços mais abstratos, utilizando polinômios e curvas algébricas para representar informações.

Alguns pesquisadores brasileiros: Fernando Torres (in memoriam), Gilberto Brito de Almeida Filho, Saeed Tafazolian, Cícero Carvalho, Wanderson Tenório e Guilherme Tizziotti.

Códigos e reticulados

É uma área onde o estudo dos códigos explora as propriedades das estruturas envolvidas numa abordagem, sempre que possível, geométrica.

Códigos e reticulados

É uma área onde o estudo dos códigos explora as propriedades das estruturas envolvidas numa abordagem, sempre que possível, geométrica.

Em 1900 o problema de determinar qual é o empacotamento esférico que cobre a maior parte do espaço foi categorizado como um dos problemas de Hilbert e isso veio a obter destaque na teoria da informação.

Códigos e reticulados

É uma área onde o estudo dos códigos explora as propriedades das estruturas envolvidas numa abordagem, sempre que possível, geométrica.

Em 1900 o problema de determinar qual é o empacotamento esférico que cobre a maior parte do espaço foi categorizado como um dos problemas de Hilbert e isso veio a obter destaque na teoria da informação.

O problema do empacotamento de esferas foi conectado à area dos códigos em um artigo de Claude E. Shannon em 1948, onde foi exibida a relação entre códigos corretores de erros e reticulados com alta densidade de empacotamento.

Definição

Dado $\{v_1, \ldots, v_m\}$ um conjunto de vetores L.I. em $\mathbb{R}^n$, definimos por reticulado o conjunto

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i v_i, \quad \lambda_i \in \mathbb{Z}, \quad \forall\, i = 1, 2, \ldots m \right\}.$$

Um empacotamento esférico no $\mathbb{R}^n$ é uma reunião de esferas de mesmo raio no $\mathbb{R}^n$ de modo que quaisquer duas esferas ou não se interceptam ou se interceptam apenas no bordo, enquanto um empacotamento reticulado no $\mathbb{R}^n$ é um empacotamento esférico cujo o conjunto dos centros das esferas forma um reticulado.

Definição

Dado $\{v_1, \ldots, v_m\}$ um conjunto de vetores L.I. em $\mathbb{R}^n$, definimos por reticulado o conjunto

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i v_i, \quad \lambda_i \in \mathbb{Z}, \quad \forall\, i = 1, 2, \ldots m \right\}.$$

Um empacotamento esférico no $\mathbb{R}^n$ é uma reunião de esferas de mesmo raio no $\mathbb{R}^n$ de modo que quaisquer duas esferas ou não se interceptam ou se interceptam apenas no bordo, enquanto um empacotamento reticulado no $\mathbb{R}^n$ é um empacotamento esférico cujo o conjunto dos centros das esferas forma um reticulado.

Alguns pesquisadores brasileiros: Sueli Irene Rodrigues Costa, Marcelo Firer, Reginaldo Palazzo Junior, Marcelo Muniz Silva Alves, Antonio Aparecido de Andrade e Grasiele Cristiane Jorge.

Referências bibliográficas

ALDERETE, S. A. *Códigos corretores de erros sobre grupos com decomposição m - abeliana*. Tese (Doutorado) — UFBA/UFAL, Bahia, 2018.

BERNAL, J. J.; RÍO, Á. del; SIMÓN, J. J. textitAn intrinsical description of group codes. Designs, Codes and Cryptography, Springer, v. 51, n. 3, p. 289–300, 2009.

COELHO, F. U.; LOURENCO, M. L. *Um Curso de Álgebra Linear*. 2. ed. São Paulo: EdUSP, 2005.

COSTA, R. B. *Código de grupo cíclico*. Trabalho de conclusão de curso (Graduação em Licenciatura em Matemática),Departamento de Matemática Pura e Aplicada - CCENS, Universidade Federal do Espírito Santo, 2022.

FILHO, G. B. de A.; TAFAZOLIAN, S. *Códigos Geométricos*. Rio de Janeiro: 33º Colóquio Brasileiro de Matemática, IMPA, 2021.

GONÇALVES, A. *Introdução à álgebra*. 6. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2017.

HEFEZ, A.; FERNANDEZ, C. d. S. *Introdução à Álgebra Linear*. 2. ed. Rio de Janeiro: Coleção PROFMAT, SBM, 2016.

HEFEZ, A.; VILLELA, M. L. T. *Códigos corretores de erros*. Rio de Janeiro: Instituto de Matematica Pura e Aplicada, 2008.

JORGE, G. C. *Reticulados q-ários e algébricos*. Tese (Doutorado) — IMECC - UNICAMP, Campinas, 2012.

LAVOR, C. C.; ALVEZ, M. M.; ALL. et. *Uma introdução à teoria de códigos*. São Carlos: Notas em Matemática Aplicada, SBMAC, 2012.

LUCHETTA, V. O. J. *Códigos cíclicos como ideais em álgebras de grupo*. Dissertação (Mestrado) — IME - USP, São Paulo, 2005.

MILIES, C. P.; SEHGAL, S. K. *An introduction to group rings*. Dordrecht: Kluwer Academic Publishers, 2002.

MUITO OBRIGADO!!!

victormartins.net
victor.n.martins@ufes.br