congresso de pesquisa, ensino e extensão

11° conpeex

ANAIS DO XI CONPEEX

Congresso de Pesquisa, Ensino e Extensão
Universidade Federal de Goiás

Conhecimento, Inclusão Social e Desenvolvimento

3 a 5 de novembro de 2014

PICME

Apoio: FUNAPE Fundação de Apoio à Pesquisa - UFG; FAPEG Fundação de Amparo à Pesquisa do Estado de Goiás; CAIXA; Banco do Brasil; Coordenação de Aperfeiçoamento de Pessoal de Nível Superior; Conselho Nacional de Desenvolvimento Científico e Tecnológico

Realização: UFG Universidade Federal de Goiás

ÍNDICE DE ALUNOS

Aluno	Trabalho
ANGELO GUIMARAES	PRODUTO TENSORIAL DE ESPAÇOS VETORIAIS
BRUNO RAGONETE CARVALHO	RSA: UM ALGORITMO DE CRIPTOGRAFIA
ISRAEL RODRIGUES SOARES	FRACTAIS: O QUE SÃO?
JOAO VICTOR COSTA BARROS	CÓDIGOS CORRETORES DE ERROS
MARCOS LUCAS VELOSO JUNQUEIRA	INDUÇÃO MATEMÁTICA E A TORRE DE HANOI
TULIO MARCIO GENTIL DOS SANTOS	POLINÔMIOS EM UMA VARIÁVEL

Produto Tensorial de Espaços Vetoriais Reais.

Guimarães, Angelo[1] , IME/UFG - jilugyn@gmail.com
Oliveira, Ricardo N., IME/UFG - ricardo@ufg.br

Resumo

Sejam U, V espaços vetoriais de dimensão finita, sobre o corpo dos números reais $\mathbb{R}$. O produto tensorial dos espaços U e V é um par (W, ϕ), onde W é um espaço vetorial real, e $g : U \times V \to W$ é uma aplicação bilinear que satisfaz a seguinte propriedade universal

Para todo espaço vetorial W', sobre o corpo dos números reais $\mathbb{R}$, e para toda aplicação bilinear $\psi : U \times V \to W$, existe uma única aplicação linear

$$T : W \to W'$$

tal que

$$\psi(u, v) = T(\phi(u, v)),\ \forall u \in U\ e\ \forall v \in V.$$

O espaço vetorial W sobre o corpo dos reais, resultante do produto tensorial de U por V é denotado por $W = U \otimes_{\mathbb{R}} V$. Também definimos o conceito de produto tensorial por duas vias alternativas, onde usamos os conceitos de espaço dual e o espaço bidual, alguns isomorfismos canônicos, e os conceitos de soma direta e produto cartesiano entre espaços vetoriais. Vale lembrar que, o espaço dual de um espaço vetorial real é o conjunto dos funcionais lineares reais, isto é, aplicações lineares entre o espaço e o corpo base $\mathbb{R}$, veja [Hoffman and Kunze, 1971]. Estas três maneiras levam a construções equivalentes, conforme [Lima, 2010]. Além disso, dependendo do tipo de propriedade que queremos demonstrar, podemos escolher a definição que mais favorece a resolução do problema.

Em seguida, apresentamos várias propriedades, dentre as quais se destacam, a propriedade universal para produtos tensoriais, a unicidade de tal produto a menos de isomorfismos. Também definimos o conceito de produto tensorial de aplicações lineares, o produto de Kronecker e como se dão as mudanças de coordenadas de um tensor quando mudamos as bases dos respectivos espaços vetoriais. E finalmente estudamos o produto tensorial de vários espaços vetoriais, que é uma extensão natural do conceito de produto tensorial para dois espaços. Provamos várias propriedades deste produtos, por exemplo:

$$\begin{aligned} U \otimes V &\cong V \otimes U; \\ (U \otimes V) \otimes W &\cong U \otimes (V \otimes W); \\ (U \oplus V) \otimes W &\cong (U \otimes W) \oplus (V \otimes W) \end{aligned}$$

Referências

[Lima, 2010] Lima, Elon Lages, *Cáculo Tensorial,* Impa, 3 ed., 2010.

[Hoffman and Kunze, 1971] Hoffman, Kenneth; Kunze, Ray, *Linear Algebra,* Prentice Hall, 2 ed., 1971.

[Hungerford] Hungerford, Thomas W., *Algebra,* Springer, 1 ed., 2003.

[1]O autor agradece ao CNPQ/PICME pelo suporte finaceiro. Revisado pelo orientador.

Universidade Federal de Goiás
Instituto de Matemática e Estatística
XXII Seminário de Iniciação Científica da UFG/ XI CONPEEX
Tema do trabalho: Criptografia
Autor do projeto: Bruno Ragonete Carvalho – Bolsista PICME – IME/UFG
Orientador: Professor Doutor Romildo da Silva Pina – IME/UFG

RSA: Um algoritmo de criptografia

RSA é um sistema de criptografia com chave pública, que deve seu nome a três professores do MIT, Ronald Rivest, Adi Shamir e Leonard Adleman. É muito usado nas comunicações eletrônicas como cartões de crédito e tipos de comunicação em que é necessário usar assinatura eletrônica.

A matemática usada no RSA é elementar e se baseia nos conceitos básicos da teoria dos números. Para a implementação do RSA é necessário a escolha de dois números inteiros que são produtos de dois primos, mas que não podem ser fatorados facilmente, ou seja, cada um desses inteiros devem ser produtos de dois primos muito grandes (da ordem de 10^{100}).

Para entender o algoritmo, é necessário primeiramente conhecer o famoso "Pequeno Teorema de Fermat". Pequeno Teorema de Fermat: Seja p um número primo. Se a é um inteiro tal que $mdc(p,a) = 1$, então $a^{p-1} \equiv 1(mod\ p)$.

Também devemos conhecer a função $phi\ (\varphi)$ definida da seguinte forma:

$$\varphi(x) = \#\{n \in \mathbb{N} | n \leq x \wedge mdc(n,x) = 1\}$$

No RSA as chaves (pública e privada) são geradas da seguinte forma: Escolha dois números primos grandes p e q, da ordem de 10^{100} no mínimo. Seja $n = p \cdot q$, calcule $\varphi(n) = (p-1) \cdot (q-1)$. Escolha $e \in \mathbb{Z}$ tal que $1 < e < \varphi(n)$ e $mdc\big(e, \varphi(n)\big) = 1$. Seja d, de tal forma que $d \cdot e \equiv 1(mod\ \varphi(n))$. Então teremos uma chave pública (o par n e e) e uma chave privada (o par n e d).

Para transformar uma mensagem m, sendo $0 < m < n$, em uma mensagem c cifrada usando a chave pública, basta fazer: $c = m^e\ (mod\ n)$.

Para recuperar a mensagem m da mensagem cifrada c usando a chave privada, basta fazer: $m = c^d\ (mod\ n)$.

Em ambos cálculos teremos que usar o Pequeno Teorema de Fermat para resolve-los.

"revisado pelo orientador"

Fractais: O que são?

Aluno PICME: **Israel Rodrigues Soares** , Orientadora: **Shirlei Serconek**
Instituto de Matemática e Estatística
Universidade Federal de Goiás
isr321@hotmail.com, shirlei@ufg.br

1 Definição

Definição 1. *Fractal é um conjunto K em que a dimensão de Hausdorff Besicovitch é estritamente maior que a dimensão topológica, ou seja, K pertence ao conjunto dos fractais se e somente se:*

$$DimH(\ K\ ) > Dim(\ K\ )$$

Para entendermos melhor o que é um fractal precisamos ter uma ideia do que seria a dimensão de Hausdorff e a dimensão topológica de um conjunto. Vejamos a próxima seção:

2 Conceito intuitivo da Dimensão de Hausdorff e da Dimensão Topológica de um conjunto

A noção de dimensão é uma questão fundamental em sistemas dinâmicos. Ela está intimamente ligada ao número de informações necessárias para se localizar um ponto no espaço (no caso, dadas pelas coordenadas) e à noção de medida de comprimento. O conceito de dimensão topológica está relacionado com a seguinte ideia: um conjunto tem n dimensões quando podemos dividi-lo por meio de cortes que sejam eles próprios conjuntos de $n-1$ dimensões. Por essa definição, a reta terá dimensão 1 (porque pode ser separada por um ponto); o plano terá dimensão 2 (porque pode ser separado por uma reta); o espaço usual terá dimensão 3 (porque pode ser separado por um plano), e assim, sucessivamente, podemos imaginar conjuntos contínuos com um número crescente de dimensões. Exemplo: O triângulo tem dimensão topológica $1+1=2$, pois uma reta (dimensão 1) pode dividi-lo. Já o conceito de dimensão de Hausdorff está ligado ao efeito que as homotetias (dilatações) produzem na proporcionalidade dos objetos. Uma homotetia de razão três multiplica os comprimentos por 3, as superfícies por $3^2=9$, e os volumes por $3^3=27$ (o que, generalizando, permite calcular o 'volume' de um objeto de dimensão d por 3^d).

3 A curva de Koch

Definição 2. *A curva de Koch é definida a partir de um segmento de reta e de um processo de iteração. O processo de iteração consiste em acrescentar um 'chápeu de bruxa' em cada segmento de reta da iteração anterior (veja o que acontece entre as iterações 0 e 1 na figura abaixo para entender melhor). A curva de Koch é obtida quando iteramos um número infinito de vezes o segmento de reta:*

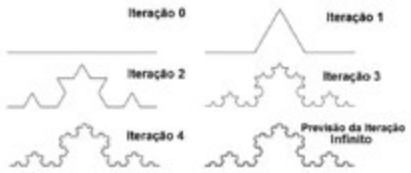

Figura 1: O processo iterativo para se chegar a curva de Koch

A cada nova iteração o tamanho da curva aumenta em $\frac{4}{3}$ vezes o tamanho da anterior; portanto, o tamanho da curva de Koch é infinito.

Agora, vamos descobrir a dimensão de Hausdorff e a dimensão topológica da curva de Koch. A dimensão topológica da curva de Koch é $0+1=1$, pois um ponto (dimensão 0) consegue dividi-la já que ela é proveniente de um segmento de reta (dimensão 1).

Seja K o conjunto de pontos da curva de Koch. Para descobrirmos a sua dimensão de Hausdorff vamos aplicar uma homotetia de razão 3 no seu segmento de reta gerador. Note que aumentamos em 4 vezes o seu tamanho:

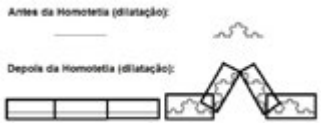

Figura 2: O efeito que a homotetia de razão 3 produz na curva de Koch

Portanto, a dimensão de Hausdorff da curva de Koch é:

$$3^{DimH(\ K\ )} = 4 \Rightarrow DimH(\ K\ ) = \frac{\ln 4}{\ln 3} \approx 1.2618$$

Logo, a curva de Koch é um fractal, pois $1.2618 > 1$, ou seja:

$$DimH(\ K\ ) > Dim(\ K\ )$$

4 O Triângulo de Sierpinski

Definição 3. *O triângulo de Sierpinski é definido a partir de um triângulo equilátero e de um processo de iteração que aplicamos sobre o triângulo um número infinito de vezes. O processo de iteração consiste em remover um triângulo equilátero do centro de cada triângulo da etapa anterior.*

A imagem a seguir ilustra o processo:

Figura 3: As 5 primeiras etapas da construção do Triângulo de Sierpinski

Este conjunto tem algumas propriedades bastante curiosas:

- Tem área zero, pois a cada passo a área reduz-se para $\frac{3}{4}$ da área do passo anterior. Por exemplo se a área inicial for 1, ao fim do primeiro passo é $\frac{3}{4}$, ao fim do segundo é $\frac{3}{4}*\frac{3}{4}$, ao fim do terceiro é $\frac{3}{4}*\frac{3}{4}*\frac{3}{4}$, pelo que a área limite é $\frac{3}{4}*\frac{3}{4}*\frac{3}{4}... \to 0$;
- É infinito, pois em particular o conjunto de pontos que não são retirados da base do triângulo inicial é infinito.
- É auto-semelhante, i.e. cada parte é uma cópia de si própria.
- Sua dimensão topológica é 1.
- Seja T o conjunto de pontos do triângulo de Sierpinski. Sua dimensão de Hausdorff é:

$$2^{DimH(\ T\ )} = 3 \Rightarrow DimH(\ T\ ) = \frac{\ln 3}{\ln 2} \approx 1.585 > 1$$

5 O conjunto de Mandelbrot

Os fractais foram popularizados por Mandelbrot em 1975 em seu livro Les Objets Fractals: Forme, Hasard et Dimension. Neste livro, Mandelbrot usou o termo fractal para descrever um número de fenômenos matemáticos que pareciam exibir comportamento caótico ou surpreendente. Todos estes fenômenos envolviam a definição de alguma curva ou algum conjunto através do uso de algumas funções ou algoritmos recursivos. O conjunto de Mandelbrot é um desses fenômenos e leva o nome de seu descobridor.

Definição 4. *O conjunto de Mandelbrot é definido como o conjunto de pontos c no plano complexo para o qual a sequência definida recursivamente:*

$$z_0 = 0$$

$$z_{n+1} = z_n^2 + c$$

não tende ao infinito.

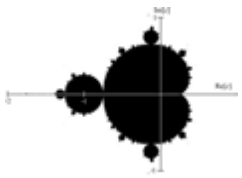

Figura 4: O conjunto de Mandelbrot no plano Complexo

O conjunto de Mandelbrot foi definido pela primeira vez em 1905 por Pierre Fatou, um matemático francês que trabalhou no campo da dinâmica analítica complexa. Fatou estudou processos recursivos como $z \to z^2 + c$. Começando com um ponto qualquer z_0 no plano complexo, podem-se gerar pontos sucessivos aplicando-se repetidamente esta fórmula. A sequência de pontos obtida é chamada órbita de z_0 sob a transformação $z \to z^2 + c$.

Fatou percebeu que a órbita de $z_0 = 0$ sob esta transformação forneceria alguma introspecção sobre o comportamento de tais sistemas. Existe um número infinito de tais funções - uma para cada valor de c. Fatou não teve acesso a um computador capaz de plotar as órbitas de todas essas funções, mas ele tentou fazer isso a mão. Ele provou que uma vez que um ponto atinge uma distância da origem maior que 2, a órbita explode para o infinito.

Fatou nunca viu uma imagem, como estamos acostumados a ver, do que hoje chamamos de conjunto de Mandelbrot pois a quantidade de cálculos necessária para se gerarem tais imagens está além da capacidade de um ser humano executar a mão. O Professor Benoît Mandelbrot foi a primeira pessoa a utilizar um computador para plotar o conjunto.

O conjunto de Mandelbrot assim como outros fractais possui uma estrutura fina em qualquer escala. A estrutura fina consiste em detalhamento infinito. Sucessivas ampliações de um fractal levam a mais e mais detalhes, indefinidamente. Isso não ocorre com as figuras geométricas convencionais, como a circunferência: se ampliarmos suficientemente um pequeno arco da mesma e dele retirarmos um pequeno arco que também ampliaremos, e repetindo sucessivamente o processo, obteremos um arco virtualmente retilíneo. Uma reta se caracteriza por não possuir detalhes. Nos fractais, isso não ocorre. A cada ampliação surgem mais detalhes, mesmo que se repita o processo indefinidamente. Se o fractal for construído na tela gráfica de um computador, os detalhes aparecerão nas ampliações sucessivas, até onde o computador suportar a realização dessas ampliações.

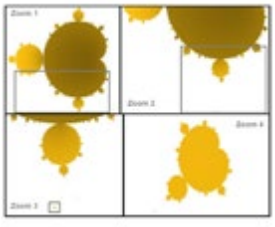

Figura 5: Sucessivas ampliações no conjunto de Mandelbrot o levam a ele mesmo

6 O conjunto de Julia

Definição 5. *O conjunto de Julia é definido como o conjunto de pontos c no plano complexo a partir de um dado número complexo z para qual a sequência definida recursivamente:*

$$z_0 = z$$

$$z_{n+1} = z_n^2 + z$$

não tende ao infinito.

Figura 6: Arte feita a partir de um conjunto de Julia

Sua definição é bem parecida com a do conjunto de Mandelbrot. Na verdade há uma relaçao bem forte entre esses conjuntos. Por exemplo, se o número complexo z usado para definir um conjunto de Julia pertencer o conjunto de Mandelbrot, esse conjunto de Julia será conexo, caso o contrário ele será desconexo. Note:

Figura 7: Relação entre o conjunto de Julia e o de Mandelbrot

Referências

[Man82] Benoit B Mandelbrot. *The fractal geometry of nature*. Freeman, San Francisco, CA, 1982.

CÓDIGOS CORRETORES DE ERROS

UNIVERSIDADE FEDERAL DE GOIÁS

Orientando : João Victor Costa Barros (j.victorbarros@hotmail.com)

Orientador: Mário José de Souza (mario_jose_souza@ufg.br)

RESUMO:

O presente trabalho busca desenvolver e apresentar os conceitos necessários para o entendimento da teoria de códigos corretores de erros, assim como tópicos importantes de álgebra linear e álgebra abstrata.

Foi proposta uma metodologia que consiste no estudo individual sob a supervisão do orientador, com encontros a cada duas semanas para a apresentação do desenvolvimento e esclarecimento das dúvidas que surgiram .

Este trabalho iniciou-se em setembro de 2013 com o estudo da álgebra linear e, assim sendo, foram estudados todos os conceitos desta disciplina: resolução de matrizes e sistemas lineares, espaço vetorial com produto interno, transformações lineares, autovalores e autovetores, diagonalização de operadores e as formas quadráticas, lineares e bilineares.

Após esses conceitos iniciais, foram trabalhados tópicos de álgebra abstrata , tais como a relação de equivalência, produto cartesiano e teoria de Galois elementar.

Por fim ,teoria de códigos foi trabalhada em todos os seus conceitos fundamentais, tais como a métrica de Hamming , equivalência de códigos, códigos lineares e cíclicos e decodificação.

PALAVRAS-CHAVE**:** Corpo finito, código de Hamming, código de Golay, decodificação.

Revisado pelo orientador.

CÓDIGOS CORRETORES DE ERROS

Orientando: **João Victor Costa Barros**
(j.victorbarros@hotmail.com)
Orientador: **Mário José de Souza**
(mario_jose_souza@ufg.br)

UNIVERSIDADE FEDERAL DE GOIÁS
(www.ufg.br)
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

INTRODUÇÃO

Com o advento da tecnologia em nosso dia a dia, tornou-se necessário a preocupação com a veracidade e a segurança com que as informações são passadas. Nesse sentido, a teoria de códigos corretores de erros é a base fundamental para que seja feita a transmissão de dados de maneira segura e eficaz, permitindo a detecção de possíveis erros que possam ocorrer e a sua correção. A teoria moderna de códigos originou-se com o trabalho de Claude Elwood Shannon, que teve um papel importante na criação da teoria da informação. Os códigos corretores de erros tem como elementos seqüência de símbolos pertencentes a um alfabeto, como por exemplo, os dígitos binários. Esses elementos são chamados de palavras, que juntamente com suas estruturas algébricas formam a base de muitos códigos importantes e conhecidos e, além disso, o estabelecimento de um conceito adequado de distância e o processo de avaliação dessa distância entre palavras são fundamentais no processo de decodificação.

DEFINIÇÕES

Seja F_q o corpo finito com q elementos.

$(F_q)^n = \{x = (x_1, x_{2,\dots}, x_n): x_i \in (F_q)^n\}$

A **distância do Hamming** entre x,y $\in (F_q)^n$ é dada por:
$d(x,y) = |\{i \mid x_i \neq y_i, 1 \leq i \leq n\}|$

Sendo a distância de Hamming uma métrica:

- $d(x,y) = 0 \rightarrow x = y$
- $d(x,y) = d(y,x), \forall x,y \in (F_q)^n$
- $d(x,y) \leq d(x,z) + d(y,z), \ \forall x,y,z \in (F_q)^n$;

Dado um elemento $x \in (F_q)^n$ e um inteiro positivo r chama-se **bola** de centro em a e raio r, ao conjunto.

$B_r(a) = \{x \in (F_q)^n : d(x,a) \leq r\}$ e **esfera** de centro em a *e raio* r**,** ao conjunto

$$S_r(a) = \{x \in (Fq)^n : d(x,a) = r\}.$$

Um código q–ário de comprimento n, com m palavras e distância mínima d , diz-se um (n, m, d) código.

Uma função $\varphi: (F_q)^n \rightarrow (F_q)^n$ é uma **isometria de Hamming** se:

$d(\varphi(x), \varphi(y)) = d(x,y), \forall x,y \in (F_q)^n$

Por ser injetora e sobrejetora , a função φ é bijetora.

Dado um elemento x num código linear C chama-se **peso** de x o número:

$$W(x) = d(x,0)$$

E o **peso** do código C o número:

$$W(c) = \min\{w(x) \mid x \in C, x \neq 0\}$$

TEOREMA: Dados $x = (x_1, x_2, \dots, x_n)$, y = ($y_1$, y_2,..., y_n) $\in C$ temos:

$d(x,y) = |\{i \mid x_i \neq y_i, 1 \leq i \leq n\}| = |\{i \mid x_i - y_i \neq 0, \ 1 \leq i \leq n\}|$

$$d(x,y) = d(x-y,0) = w(x-y)$$

$$d(C) = w(C)$$

Uma **Matriz de codificação** é uma matriz $G \in M_{nxk}(F)$cujas linhas formam uma base para o código C.

Seja $C \subset (F_q)^n$ num código linear então,

$C^{\perp} = \{v \in (F_q)^n : < u, v > = 0, \forall u \in C\}$ é o **código dual** de C.

Se G é a Matriz geradora de $C \subset (F_q)^n$:

- $C^{\perp}$ é um subespaço vetorial de $(F_q)^n$:
- $x \in C^{\perp} \Leftrightarrow G x^t = 0$.

Se $C \subset (\mathrm{Fq})^n$ é um código linear de dimensão K, com matriz geradora $G = [I_k|A]$, então:

- $dim\, C^{\perp} = n - k$
- $H = [-A^t \mid I_{n-k}]$é uma matriz geradora de C .

DECODIFICAÇÃO

Decodificação é o procedimento de detecção e correção de erros num determinado código.Inicialmente define-se o vetor **e** como sendo a diferença entre o vetor recebido **r** e o vetor transmitido **v**.

e = r-v

Se H é a matriz de verificação de paridade do código, temos que:

$He^t = H(r-v)^t = Hr^t - Hv^t = Hr^t, pois\ Hv^t = 0$

Portanto, a palavra recebida r tem a mesma síndrome do vetor erro e.

EXEMPLO: O CÓDIGO DE HAMMING

O código de Hamming é uma classe de códigos lineares binários que permite não apenas encontrar o erro, mas também a localização do bit errado. Por exemplo: seja uma palavra de oito bits numerados de

$$m_1 m_2 m_3 m_4 m_5 m_6 m_7 m_8$$

Agora, acrescentando mais quatro bits a essa palavra, temos:

$$x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9 x_{10} x_{11} x_{12}$$

Seja

$m_1 = x_3, m_2 = x_5, m_3 = x_6, m_4 = x_7, m_5 = x_9, m_6 = x_{10}, m_7 = x_{11}, m_8 = x_{12}$

Os quatro bits adicionados são calculados utilizando- se o operador $\oplus$ *ou exclusivo* que calcula os a paridade dos bits dados:

$$x_1 = x_3 \oplus x_5 \oplus x_7 \oplus x_9 \oplus x_{11}$$

$$x_2 = x_3 \oplus x_6 \oplus x_7 \oplus x_{10} \oplus x_{11}$$

$$x_4 = x_5 \oplus x_6 \oplus x_7 \oplus x_{12}$$

$$x_8 = x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12}$$

Agora suponha que esses doze bits são lidos como sendo:

$$y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12}$$

Se não houver erro, teremos $x_i = y_i$.

Se houver erro de um bit é possível detectá-lo e corrigi-lo.

P Para isso fazemos o cálculo com quatro bits $k_1, k_2, k_3\ e\ k_4$:

$$k_1 = y_1 \oplus y_3 \oplus y_5 \oplus y_7 \oplus y_9 \oplus y_{11}$$

$$k_2 = y_2 \oplus y_3 \oplus y_6 \oplus y_7 \oplus y_{10} \oplus y_{11}$$

$$k_3 = y_4 \oplus y_5 \oplus y_6 \oplus y_7 \oplus y_{12}$$

$$k_4 = y_8 \oplus y_9 \oplus y_{10} \oplus y_{11} \oplus y_{12}$$

Se $k_1 = k_2 = k_3 = k_4 = 0$, então não há erros.Senão o número binário codificado pelos quatro bits, $k_4 k_3 k_2 k_1$ determina a posição do bit errado.Por exemplo, se $k_4 k_3 k_2 k_1 = 0111,$ então o bit errado é o y_7.

Com esses conceitos de álgebra, é possível detectar e corrigir erros que possam aparecer na transmissão de dados, possibilitando o uso das tecnologias que estão cada vez mais presentes em nosso dia-a-dia!

BIBLIOGRAFIA

-HEFEZ, A. e VILELA,M.L.T, Códigos de Corretores deErros, IMPA, Rio de Janeiro, 2002.

*-VANSTONE, S. A. e OORSCHOT, P.*C.van.*An Introduction to Error Correcting Codes with Applications.*Kluwer Academic Publishers, 1989.

-Vera Pless. Introduction to the theory of error-correcting codes. New York :
Wiley, 1982, ISBN 04710868432

-BOLDRINI, José L.;Costa, SuelilR.;FIGUEIREDO, Vera L.; WETZLER, Henry G.Álgebra Linear.São Paulo: Ed.Harbra.3ª Edição, 1984.

-GONÇALVES, Adilson.Introdução à Álgebra.Projeto Euclides.Rio de Janeiro: IMPA.1979.

-Jacobs, K. "Discrete Stochastics". Birkhäuser Verlag Basel.1992

Indução matemática e a Torre de Hanoi [1]

Aluno: Marcos Lucas Veloso Junqueira
Orientadora: Profa. Dra. Kélem Gomes Lourenço

Resumo

O princípio de indução matemática é um mecanismo simples utilizado para demonstrar alguns resultados importantes na matemática, veja [2], e neste trabalho utilizamos este princípio para mostrar uma de suas aplicações. A Torre de Hanói, criado pelo matemático Edouard Lucas, é um jogo em que o objetivo é mover n discos de uma haste inicial para uma final, utilizando-se de 3 hastes. Sendo que um disco menor não pode estar sob um maior e só é permitido mover um disco (acima de todos) por vez, veja [1, 3]. O objetivo é apresentar a definição matemática do princípio de indução, as propriedades da Torre de Hanoi e um algoritmo baseado em operações binárias para a solução da mesma.

Referências Bibliográficas

[1] Formin, D.; Genkin, S.; Itenberg I.. *Círculos Matemáticos: A Experiência Russa.* Editora do IMPA, 2010.

[2] Shokranian, S.; Soares, M.; Godinho, H., *Teoria dos Números.* Editora UNB, 2 edição.

[3] Hefez, A. *Indução Matemática.* Programa de Iniciação Científica OBMEP.

[1] Revisado pela orientadora

Polinômios em uma variável*

Maurílio Márcio Melo - Orientador
Instituto de Matemática e Estatística, UFG, CEP 74001970, Campus Samambaia, Goiânia, GO, Brasil
E-mail: m3melo@ufg.br
Tulio Marcio Gentil dos Santos - Orientando
Instituto de Matemática e Estatísitca, UFG, CEP 74001970, Campus Samambaia, Goiânia, GO, Brasil
E-mail: tuliomathufg@hotmail.com

27 de setembro de 2014

Resumo

Os polinômios em $K[x]$, polinômios na variável x com coeficientes no corpo K, nos remetem a certos resultados, um dos mais importantes é o *algorítimo de Euclides*. Ele afirma que se f, $g \in K[x]$, g não identicamente nulo, então existem únicos $q, r \in K[x]$ que satisfazem a seguinte relação:

$$f(x) = g(x)q(x) + r(x), \text{ onde } r \equiv 0 \text{ ou } \partial r < \partial g.$$

Decorre deste, o seguinte resultado: se $f \in K[x]$ tal que $\partial f = n$, então o número de raízes de f em K é no máximo n, mais ainda, o número de raízes de f em uma extensão L de K é também no máximo n.

A verificação da irredutibilidade de um polinômio em um corpo K não é, em geral, um problema simples. O *lema de Gauss* afirma que se $f \in \mathbb{Z}[x]$ (polinômio na variável x com coeficientes inteiros) é irredutível em $\mathbb{Z}$, então f é irredutível sobre o corpo $\mathbb{Q}$. Através desse lema mostramos a validade do *critério de Eisenstein*: se $f(x) = a_0 + a_1x + ... + a_nx^n$ é um polinômio em $\mathbb{Z}[x]$ e existe p um inteiro primo, tal que $p \nmid a_n$, $p \mid a_0, a_1, ..., a_{n-1}$ e $p^2 \nmid a_0$, então f é irredutível em $\mathbb{Q}$.

Por fim, através do *lema de Gauss*, verificamos que se $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$, existe um inteiro primo p tal que $p \nmid a_n$ e $\bar{f}$ é irredutível em $\mathbb{Z}_p$, então f é irredutível em $\mathbb{Q}$.

Referências Bibliográficas

GONÇALVES, Adilson. *Introdução à Álgebra*, Rio de Janeiro: IMPA, 2013.

GARCIA, Arnaldo. *Elementos de Álgebra*, Rio de Janeiro: IMPA, 2003.

LIMA, Elon Lages. *A matemática do ensino médio* - volume 1 / LIMA, et al., Rio de Janeiro: SBM, 2006.

*Revisado pelo orientador.