Journal homepage http://revistas.unitru.edu.pe/index.php/SSMM

SELECCIONES MATEMÁTICAS
Universidad Nacional de Trujillo
ISSN: 2411-1783 (Online)
Vol. 02(01): 25 - 31 (2015)

Compactificação de Informação via métrica de Lee.

Compactification information via metric Lee.

Jaime Apaza Rodriguez * and Edson Donizete de Carvalho †

Received, Mar. 15, 2015 *Accepted, Jul. 15, 2015.*

DOI: http://dx.doi.org/10.17268/sel.mat.2015.01.03

Resumen

En este artículo formalizamos matemáticamente un juego de cartas, usando el concepto de métrica y un poco de algebra, y luego extendemos al caso general. Así ilustramos el proceso de compactificación de información.

Palabras clave. métrica, información, codificación.

Abstract

In this work, by using basics concepts about metrics and algebra, we show the formalization of a play of the pack of cards and we extend for general case. So we show that the compactification of information is posible.

Keywords. metric, information, codification.

1. Introducción. A teoria de conjuntos e teoria combinatória são ferramentas matemáticas que se complementam e nos auxiliam na solução de problemas envolvendo coleção ou agrupamento de objetos (de diversa natureza) e na contagem de seus respectivos elementos.

Por outro lado, o estudo das estruturas algébricas nos permite analisar, formalizar e classificar conjuntos, quando munidos de uma ou mais operaçãoes binárias, satisfazendo certas propriedades. Assim temos as estruturas de grupo, anel, corpo, espaço vetorial, módulo, etc., cada qual com suas propriedades inerentes, tendo aplicações na matemática pura e aplicada e em diversas áreas tecnológicas.

Além dos aspectos combinatórios e algébricos, um dado conjunto $\mathcal{A}$, não vazio, também pode ter uma estrutura geometrica-topológica, dada por meio de uma medida. Para isso é introduzida uma função $d : \mathcal{A} \times \mathcal{A} \to \mathbb{R}$, satisfazendo certas propriedades que determinam uma métrica em $\mathcal{A}$. Assim temos o conceito de espaço métrico, útil na matemática e, de um modo geral, em áreas do conhecimento onde há necessidade de avaliar o desempenho de determinados sistemas.

Na Teoria de Códigos o problema geral é lidar com transmissão e armazenamento de informação, de maneira confiável. Essa teoria é utilizada nas comunicações via computador, via satélite, na compactificação de dados em um CD, etc.

Um código, $\mathcal{C}$, é um conjunto de palavras-códigos, elementos de um espaço vetorial $\mathcal{A}^n$ ($\mathcal{A} \neq \emptyset$ é o alfabeto), na qual k dígitos de informação são transmitidos e os $n-k$ restantes são os digítos de redundância que desempenham importante papel na detecção de erros. Na prática, os conjuntos $\mathcal{A}$ de interesse são aqueles que possuim uma estrutura algébrica (corpo, grupo). Em geral, o fechamento de uma operação nestes conjuntos e a existência de elemento inverso reduz a complexidade computacional que aparece no processo de decodificação. Geometricamente, um código $\mathcal{C}$ possui uma estrutura de espaço métrico, ao

* Universidade Estadual Paulista, UNESP, Ilha Solteira, Brasil(jaime@mat.feis.unesp.br).
† Universidade Estadual Paulista, UNESP, Ilha Solteira, Brasil (edson@mat.feis.unesp.br).

considerar o mínimo das distâncias entre todas as palavras códigos do código, obtendo assim a distância mínima, que fornece uma forma de quantificar a capacidade de detecção e correção de erros.

Em [2] foi proposta uma formulação matemática para um jogo de entretenimento (jogo de baralho). O jogo consiste em extrair, aleatóriamente, 5 cartas de um baralho de 52, exibir 4 delas e adivinhar a última. Tal formulação foi baseada na forma de codificar conjuntos usando a noção de distância (distância de Lee) definida em um corpo finito.

Neste trabalho apresentamos a formalização e solução algébrica do problema do jogo de baralho apresentado em [2] e o extendemos para o caso geral. Mostramos que certos parâmetros que aparecem nessa generalização, satisfazem determinadas relações de congruência. Mais ainda, tal formalização fornece um procedimento de codificação da informação, via a métrica de Lee definida sobre corpos finitos, o que conduz à compactificação de informação. São exibidos alguns exemplos e observamos que, a medida que a cardinalidade do corpo aumenta, a relação custo-benefício de compactificação precisa ser estudada com mais cuidado, uma vez que se consegue uma compactificação através de um número alto de iterações computacionais.

Este trabalho está organizado como segue. Na seção 2 apresentamos a noção de métrica. Na seção 3 é apresentado o jogo do baralho e na seção 4 algebrizamos esse problema. Finalmente, na seção 5 estendemos o problema para o caso geral, mostramos algumas relações fundamentais entre os parâmetros que aparecen nessa generalização e suas conexões com a compactificação de informação.

2. Métricas e Aplicações em Codificação. Um conjunto não-vazio, $\mathbb{E}$, é denominado espaço métrico se existir uma função $d : \mathbb{E} \times \mathbb{E} \longrightarrow \mathbb{R}$, chamada métrica, satisfazendo as seguintes condições:

(1) $d(x, y) \geq 0$ e $d(x, y) = 0$ se, e somente se, $x = y, \forall x, y \in \mathbb{E}$.

(2) $d(x, y) = d(y, x), \forall x, y \in \mathbb{E}$.

(3) $d(x, z) \leq d(x, y) + d(y, z), \forall x, y, z \in \mathbb{E}$.

$(\mathbb{E}, d)$ denota o espaço métrico $\mathbb{E}$, munido da métrica d.

Por exemplo, se para todo $x, y \in \mathbf{R}$ definimos $d(x, y) = |x - y|$, temos que d satisfaz as condições (1), (2) e (3) acima, ou seja, $(\mathbb{R}, |\cdot|)$ é um espaço métrico. Esta métrica é a métrica usual da reta real.

Dizemos que um espaço métrico $(\mathbb{E}, d)$ é discreto se todo elemento $x \in \mathbb{E}$ é isolado, ou seja, quando existe uma bola aberta em torno do ponto x contendo unicamente o próprio ponto x. Se d é uma métrica discreta, então o espaço métrico $(\mathbb{E}, d)$ é dito discreto. Por exemplo, o conjunto dos inteiros $\mathbb{Z}$, com a métrica induzida da reta real, é um espaço discreto.

Dado $\mathbb{E}$ um conjunto qualquer, sempre é possível definir uma métrica d, chamada métrica discreta, na forma:

$$d(x, y) = \begin{cases} 0, & se \ \ x = y \\ 1, & se \ \ x \neq y. \end{cases}$$

No espaço n-dimensional $\mathbb{E}^n$, para $x, y \in \mathbb{E}^n$, definimos

$$d_H(x, y) = card\{i : x_i \neq y_i, 1 \leq i \leq n\}.$$

Verifica-se então que d_H é uma métrica em $\mathbb{E}^n$ (métrica de Hamming).

Por exemplo, em $\mathbb{Z}_2^3 = \{0, 1\}^3$, temos $d(000, 111) = 3,\ d(001, 111) = 2,\ d(100, 110) = 1$.

No caso do corpo finito $\mathbb{E} = \mathbb{Z}_q$, para $x \in \mathbb{Z}_q^n$, definimos o peso de Lee por $\omega_L(x) = \sum_{i=1}^{n} |x_i|$, onde

$$|x_i| = \begin{cases} x_i, & se \ \ 0 \leq x_i \leq q/2 \\ \\ q - x_i, & se \ \ q/2 < x_i \leq q - 1. \end{cases}$$

A distância de Lee entre $x, y \in \mathbb{Z}_q^n$ é dada por $d_L(x, y) = \omega_L(x - y)$. Verifica-se também que d_L é uma métrica.

Observação: A métrica de Hamming é utilizada em códigos binários. Por outro lado, a métrica de Lee é utizada em códigos provenientes de constelação de sinais $MPSK$, ou seja, quando os sinais estão igualmente espaçados sobre um círculo. Caso a constelação esteja sobre $\mathbb{R}^2$, o circulo em questão é uma circunferência. Em ambos casos, o uso destas métricas auxíliam a detecção e correção de possíveis erros que possam ocorrer em uma transmissão de informação.

3. O Jogo do Baralho. Uum dos truques mais criativos de adivinhação de cartas de um baralho, criado em 1920 por*William Fitch Cheney Jr.*, pode ser desvendado através do uso da codificação de conjuntos y usando a métrica de Lee.

Sabemos que um baralho de 52 cartas, sem repetição, possui 4 naipes e cada naipe com 13 cartas.

Podemos considerar a seguinte relação de ordem nas cartas:

$$A \leftrightarrow x_1,\ 2 \leftrightarrow x_2,\ 3 \leftrightarrow x_3, 4 \leftrightarrow x_4,\ 5 \leftrightarrow x_5,$$

$$6 \leftrightarrow x_6,\ 7 \leftrightarrow x_7,\ 8 \leftrightarrow x_8,\ 9 \leftrightarrow x_9,\ 10 \leftrightarrow x_{10},$$

$$J \leftrightarrow x_{11},\ Q \leftrightarrow x_{12},\ K \leftrightarrow x_{13}.$$

Embora dependa de cada jogo de baralho, adotaremos a seguinte relação de ordem entre os naipes como consta na figura 1.

Figura 3.1: copa, espada, ouro, paus

Imagine que um mágico peça a seu assistente retirar aleatóriamente 5 cartas do baralho, mostrar 4 delas, de modo que possa adivinhar a última carta.

O resto da divisão por 4 garante que entre as 5 cartas escolhidas, pelo menos duas são do mesmo naipe. Para obter o resultado desejado, as 4 primeiras cartas devem ser mostradas em uma determinada ordem, de modo a fornecer ao mágico uma pista para descobrir a úlitma.

Assim, a primeira pista é apresentar a menor carta do naipe repetido. Desta forma, o mágico saberá que a quinta carta é do mesmo naipe. Com isto restarão ainda 6 possibilidades. O segredo está na forma em que as 3 cartas do meio são apresentadas. Para isto é necessário definir uma distância entre as cartas, da seguinte forma. Colocamos os 13 pontos x_i em uma circunferência, igualmente espaçados, e definimos a distância $d(x_1, x_j)$ como sendo o mínimo do número de espaços comprendidos entre x_i *e* x_j. Assim $d(x_i, x_j) \in \{1, 2, 3, 4, 5, 6\}$.

Observar também que existe uma relação de ordem entre as cartas. Podemos assim definir sequências do tipo PMG (pequeno, meio, grande).

Temos assim 6 possibilidades e seus correspondentes códigos:

$$PMG \leftrightarrow 1,\ PGM \leftrightarrow 2,\ MPG \leftrightarrow 3,$$

$$MGP \leftrightarrow 4,\ GPM \leftrightarrow 5,\ GMP \leftrightarrow 6.$$

Suponha que o assistente tenha em mãos as cartas

$$A \text{ de paus } (x_1),\ 4 \text{ de paus } (x_4),\ 3 \text{ de ouro } (x_3),$$

$$\text{rei de copas } (x_{13}),\ 7 \text{ de espadas } (x_7).$$

Quando o assistente apresenta a primeira carta (A de paus), o mágico já sabe que a quinta carta será do naipe paus. Sobraram o 3 de ouro (P), rei de copas (G) e 7 de espada (M). Assim, o assistente sabe que $d(x_1, x_4) = 3$. Logo é preciso saber qual é o conjunto que apresenta o código 3. Nesta situação temos o subconjunto MPG e assim o assistente apresenta a sequência:

Segunda carta - 3 de ouro

Terceira carta - 7 de espada

Quarta carta - rei de copas

Finalmente, o mágico conta 3 posições e descobre que a quinta carta é 4 de paus.

Notemos que existe um paralelo entre a idéia básica do truque e a compactação da informação (que faz uso da Teoria de Códigos e de Informação), usada em programas de computador, como o popular Winzip. Usando apenas 4 cartas, o assistente consegue passar informação sobre as 5. Essa compactação de informação faz com as cartas o mesmo que um software faz com os bits.

4. Formalizando o problema. Considere o conjunto $G = \{1, 2, \cdots, 52\}$, com $card(G) = 52$ e, o corpo finito $\mathbb{Z}_{13}$.

Para $k \in \mathbf{Z}_{13}$, considere os seguintes subconjuntos de G:

$$H_0 = \{x \in G : x = 0 \cdot 13 + 1 + k\},$$

$$H_1 = \{x \in G : x = 1 \cdot 13 + 1 + k\},$$

$$H_2 = \{x \in G : x = 2 \cdot 13 + 1 + k\},$$

$$H_3 = \{x \in G : x = 3 \cdot 13 + 1 + k\}.$$

Em geral podemos escrever:

$$H_t = \{x \in G : x = t \cdot 13 + 1 + k\},$$

onde $k \in \mathbb{Z}_{13}$ e $t = 0, 1, 2, 3$.

Para $x, y \in G$, definimos a relação:

$$\text{Para algum } t: \ x, y \in H_t, \iff x - y \in \mathbb{Z}_{13}.$$

Verifica-se então o seguinte resultado.

Lema: *A relação acima definida é uma relação de equivalência em G.*

Observar que os subconjuntos H_t formam uma partição do conjunto G e como a relação definida é de equivalência, obtemos conjunto quociente, G_t, de G.

Agora, sejam x_1, x_2, x_3, x_4, x_5 as cinco cartas escolhidas aleatoriamente. Como $5 \equiv 1(mod\ 4)$, existem pelo menos dois elementos $x_i, x_j \in G$ que pertencem a um mesmo subconjunto H_t, ou seja, para algum t, tem-se que $x_i, x_j \in H_t$. Sem perda de generalidade, suponha que $x_1, x_2 \in H_t$.

Estratégica do jogo do baralho:

1) A primeira carta mostrada deve ser o mínimo entre x_1 e x_2. Isto sugere uma primeira pista para adivinhar a quinta carta.

2) As cartas x_3, x_4, x_5 devem ser mostradas em uma determinada ordem, o que fornece uma outra pista. Para exibir as cartas x_3, x_4, x_5 temos $6 = 3!$ possibilidades.

Lembremos que em $\mathbb{Z}_{13}$ temos definida a distância de Lee, dada por:

$$d(x_i, x_j) = \text{min}\{\text{espaços entre } x_i \ e \ x_j\}.$$

Assim temos que

$$d_{Lee}(\mathbb{Z}_{13}) \in \{1, 2, 3, 4, 5, 6\}.$$

3) São definidas sequências do tipo PMG (pequeno, medio, grande) com as cartas x_3, x_4, x_5. Assim obtemos as 6 possibilidades (código):

$$PMG(x_3x_4x_5) \longleftrightarrow 1 \qquad MPG(x_4x_3x_5) \longleftrightarrow 3$$

$$PGM(x_3x_5x_4) \longleftrightarrow 2 \qquad MGP(x_4x_5x_3) \longleftrightarrow 4$$

$$GPM(x_5x_3x_4) \longleftrightarrow 5 \qquad GMP(x_5x_4x_3) \longleftrightarrow 6$$

4) Calcular $d(x_1, x_2)$ para adivinhar a quinta carta x_2. O número $d(x_1, x_2)$ está associado a um dos rótulos acima considerados.

Exemplo: Suponha que foram escolhidas as cartas:

$$x_1 \longrightarrow A\ de\ paus,\ x_4 \longrightarrow 4\ de\ paus,$$

$$x_3 \longrightarrow 3\ de\ ouro,\ \ x_{13} \longrightarrow rei\ de\ copas,$$

$$x_7 \longrightarrow 7\ de\ espadas.$$

A primeira carta apresentada será $x_1 \longrightarrow A\ de\ paus$; logo a quinta carta deve ser do naipe paus.

As cartas intermediárias são 3 de ouro (P), 7 de espadas (M), e rei de copas (G).

A ordem de apresentação dessas cartas intermediarias será:

$$M \qquad P \qquad G$$

$$x_7 \qquad x_3 \qquad x_{13}$$

Como o assistente sabe que $d(x_1, x_4) = 3$, então a quinta carta será $x_4 = 4$ de paus.

5. O caso Geral. Em [1] foi estudado o caso de um baralho com 52 cartas, das quais extraídas 5, são exibidas 4, restando a última para adivinhar. Isso significa que houve um processo de compactação de informação onde, de cada 5 entradas guarda-se uma, ou seja, de 50 entradas compactificam-se 10 delas. Assim, a razão de compactificação é de 10/52.

Agora, vamos analisar esta situação no caso geral de n cartas (dados ou entradas), de modo que possa-se obter uma razão de compactificação razoável, similar ao caso do baralho ou, no mínimo, proporcionalmente equivalente. Para isso faremos alguns testes e serão obtidas algumas conclusões.

Suponha um conjunto G com n elementos. Podemos construir a seguinte tabela:

A_1	A_2	A_3	$\cdots$	A_k
x_{11}	x_{12}	x_{13}	$\cdots$	x_{1k}
x_{21}	x_{22}	x_{23}	$\cdots$	x_{2k}
x_{31}	x_{32}	x_{33}	$\cdots$	x_{3k}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_{q1}	x_{q2}	x_{q3}	$\cdots$	x_{qk}

Observamos que $n = kq$, onde q primo (ou potência de primo) é o número de elementos de cada conjunto A_i da partição de G e k é o número de conjuntos A_i nessa partição.

Na linguagem do jogo do baralho, denotamos por $m = k + 1$ o número de cartas a serem retiradas aleatoriamente (número de escolhas aleatórias dentre dos n elementos de G). Então $m - 2$ é o número de cartas restantes, logo após de ter mostrado a primeira carta e escondido a última.

Temos assim que $(m-2)!$ é o número de possibilidades (constituindo o código ou rotulamento) obtido com as $m - 2$ cartas. Isto fornece o número de elementos do código usado para adivinhar a última carta.

Como a **distância de Lee** entre $x, y \in \mathbb{Z}_q^n$ é dada por $d_L(x, y) = \omega_L(x - y)$, temos que

$$d_{Lee}(\mathbb{Z}_q) \in \{1, 2, \cdots, \frac{q-1}{2}\}.$$

Cada possibilidade (elemento do código) acima mencionada estará associada a um número do conjunto $\{1, \cdots, \frac{q-1}{2}\}$.

Surge assim a seguinte questão: Quando será válida a igualdade

$$(m-2)! = \frac{q-1}{2},$$

ou equivalentemente,

$$q = 2(m-2)! + 1?$$

Para responder esta pergunta, vamos realizar alguns cálculos.

Alguns Testes:

a) Seja $m = 3$. Então temos $q = 3$. Logo estamos em $\mathbb{Z}_3$. Neste caso, $k = 2$ e $n = kq = 6$. Assim, retirando 3 cartas, 2 delas estãrão na mesma classe. Temos também que $d_{Lee}(\mathbb{Z}_3) = \{1\}$. Portanto obtemos o código trivial.

b) Seja $m = 4$. Então temos $q = 5$. Logo estamos em $\mathbb{Z}_5$. Neste caso, $k = 3$ e $n = kq = 15$. Retirando 4 cartas, 2 delas estão na mesma classe. Temos que $d_{Lee}(\mathbb{Z}_5) = \{1, 2\}$.

Consideremos a seguinte tabela:

A_1	A_2	A_3
x_{11}	x_{12}	x_{13}
x_{21}	x_{22}	x_{23}
x_{31}	x_{32}	x_{33}
x_{41}	x_{42}	x_{43}
x_{51}	x_{52}	x_{53}

Suponha que as cartas retiradas aleatoriamente sejam $x_{11}, x_{51}, x_{32}, x_{43}$. Observamos que x_{11} e x_{51} estão na mesma classe A_1. Mostrando a primeira x_{11}, saberemos que a última é x_{51}. Logo x_{32} e x_{43} podem ser exibidas de duas formas. Independentemente da forma em que essas cartas sejam mostradas, como $d(x_{11}, x_{51}) = 3$, temos que a última carta é x_{51}.

c) Seja $m = 5$. Então temos $q = 13$, que é o caso do jogo do baralho.

d) Seja $m = 6$. Então temos $q = 49 = 7^2$, onde sabemos que $\mathbb{Z}_7$ é um corpo. Neste caso temos $k = 5$ e $n = 5 \cdot 49 = 245$ cartas.

Consideremos a seguinte tabela:

A_1	A_2	A_3	A_4	A_5
x_{11}	x_{12}	x_{13}	x_{14}	x_{15}
x_{21}	x_{22}	x_{23}	x_{24}	x_{25}
x_{31}	x_{32}	x_{33}	x_{34}	x_{35}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$x_{49,1}$	$x_{49,2}$	$x_{49,3}$	$x_{49,4}$	$x_{49,5}$

Dado que $m = 6$, temos $(m-2)! = 4! = 24$ possibilidades (elementos do código). Também temos que

$$d_{Lee}(\mathbb{Z}_{49}) = \{1, 2, \cdots, 24\}.$$

Assim podemos definir sequências do tipo $PMIG$ (pequeno, medio, intermediario, grande) e combinando todas elas obtemos o código:

$$PMIG \leftrightarrow 0,\ PMGI \leftrightarrow 1,\ PIMG \leftrightarrow 2,$$

$$PIGM \leftrightarrow 3,\ PGIM \leftrightarrow 4,\ PGMI \leftrightarrow 5,$$

$$MPIG \leftrightarrow 6,\ MPGI \leftrightarrow 7,\ MIPG \leftrightarrow 8,$$

$$MIGP \leftrightarrow 9,\ MGIP \leftrightarrow 10,\ MGPI \leftrightarrow 11,$$

$$IPMG \leftrightarrow 12,\ IPGM \leftrightarrow 13,\ IMPG \leftrightarrow 14,$$

$$IMGP \leftrightarrow 15,\ IGMP \leftrightarrow 16,\ IGPM \leftrightarrow 17,$$

$$GPMI \leftrightarrow 18,\ GPIM \leftrightarrow 19,\ GMPI \leftrightarrow 20,$$

$$GMIP \leftrightarrow 21,\ GIPM \leftrightarrow 22,\ GIMP \leftrightarrow 23.$$

Observar que neste caso explicitamos o código correspondente ao rotulamento proposto.

Dos casos analisados acima obtemos:

Se $m = 3$, então $q = 3$. Assim $n = 6$.

Se $m = 4$, então $q = 5$. Assim $n = 15$.

Se $m = 5$, então $q = 13$. Assim $n = 52$.

Se $m = 6$, então $q = 49 = 7^2$. Assim $n = 245$.

Se $m = 7$, então $q = 241$. Assim $n = 1446$.

Se $m = 8$, então $q = 1441$. Assim $n = 10087$.

Se $m = 9$, então $q = 10081$. Assim $n = 80648$.

Assim, para diferentes valores de m, obtemos valores para q e, portanto, valores para n.
Obtemos assim as seguintes conclusões:

1) $n \equiv q \ (mod \ (k-1))$.

De fato, basta observar que $n = kq$ e substituindo obtemos $n - q = kq - q = q(k-1)$.

Por outro lado, observando a sequência de primos (ou potências de primos) obtidos nos testes acima, temos

2) $q \equiv 3 \ (mod \ 2)$.

De fato, sendo $q = 2(m-2)! + 1$, temos que $q - 1$ é par e portanto $q - 3$ é também par. Logo $q - 3$ é divisível por 2.

As conclusões acima descritas respondem à questão anteriormente colocada. Observamos que $n - k$ será sempre divisível por $k - 1 = m - 2$, sendo que $m - 2$ é o número de cartas (valores) intermediarias e $q - 3$ deverá ser sempre um número par.

Também podemos estimar a razão de compactificação de informação. Se de cada $m = k + 1$ cartas guardamos uma, então teremos uma razão de compactificação da ordem mq/n.

Em função dos testes feitos acima, podemos considerar a seguinte tabela, com os parámetros m, q, n, para alguns valores:

m	q	n
3	3	6
4	5	15
5	13	52
6	49	245
7	241	1446
8	1441	10087
9	10081	80648

Referencias

[1] A. HEFEZ E M. L. T. VILELA, *Códigos Corretores de Erros*, Instituto Nacional de Matemática Pura e Aplicada - IMPA, Série de Computação e Matemática, Rio de Janeiro, 2002.

[2] J. E. A. RODRIGUEZ E E. D. DE CARVALHO, *Codificando Conjuntos e Aplicações*, submetido à Revista Universitária, Sociedade Brasileira de Matemática (SBM), 2008.

[3] J. E. A. RODRIGUEZ E E. D. DE CARVALHO, *Tópicos de Matemática Discreta*, Mini-curso ERMAC, I Encontro Regional de Matemática Aplicada e Computacional, Bauru, São Paulo, 2008.

[4] L. LOVÁSZ, J. PELIKÁN AND K. VESZTERGOMBI, *Discrete Mathematics*, Springer - Verlag - New York Inc., 2003.

[5] E. LIMA, *Espaços Métricos*, Projeto Euclides, IMPA, Rio de Janeiro, 2003.

[6] J. FRALEIGH AND V. J. KATZ, *A First Course in Abstract Algebra*, Addison-Wesley, 2002.