MATEMÁTICA DISCRETA

primeiras aulas, a partir de 05/08/2013

Prof. Maurício Fabbri

APRESENTAÇÃO DO CURSO

descrição: técnicas matemáticas de representação e de resolução de problemas relevantes para a computação, tanto em software como em hardware

computação: implementação de algoritmos em máquinas digitais

algoritmo: sequência de passos realizáveis em uma máquina de Turing que deve atingir um estado final especificado a partir de um dado estado inicial e de informações digitalizadas conhecidas.

objetivo: familiarizar e treinar o aluno nos tópicos mais importantes da matemática discreta, com ênfase nas aplicações

EMENTA E BIBLIOGRAFIA: Ver plano de ensino

DINÂMICA DAS AULAS: exposição e discussão com a classe dos tópicos, seguida de resolução de exercícios em grupo pelos alunos, sob orientação

AVALIAÇÕES: 70% prova individual, 30% exercícios entregues semanalmente (às vezes em grupos, às vezes individuais). Serão considerados as 75% melhores notas dos exercícios solicitados. (75% = índice mínimo de frequência às aulas para aprovação)

Data das provas: ver plano de ensino

SIGNIFICADO do nome "matemática discreta"

computação: máquina de Turing : número finito de estados (portanto, *contáveis*)

conjuntos que são contáveis são ditos "discretos", e os que não o são, "contínuos".

Ocorre que essa questão *contínuo* $\times$ *discreto* não é nada intuitiva.

CONTAR ou ENUMERAR um conjunto significa obter uma relação biunívoca entre os elementos desse conjunto e os números naturais $\mathbb{N}$ = {0, 1, 2, 3, ...} (ou, se preferirmos, os naturais positivos $\mathbb{N}_+$ = {1, 2, 3, ...}).

Em computação, isso é equivalente a atribuir um índice a cada elemento do conjunto.

Exemplo: seja um conjunto com os elementos: a, banana, vaca, Pedro, sapo, Belo Horizonte, azul, 123

	↕	↕	↕	↕	↕	↕	↕	↕
uma maneira de atribuir índices é:	1	2	3	4	5	6	7	8

Enumerar conjuntos finitos é tarefa fácil na maioria dos casos - se bem que às vezes precisamos fazer uma enumeração mais elaborada (como no caso de endereçamento de memória para uma matriz multidimensional).

Quando conseguimos enumerar um conjunto, dizemos que ele é isomorfo (em linguagem corriqueira, "equivalente") aos números inteiros. Isso porque qualquer elemento do conjunto pode ser referenciado apenas pelo seu índice. (rigorosamente, o conceito de isomorfismo é um tanto mais complicado e exigente - não basta apenas uma correspondência biunívoca, é necessário que haja uma equivalência entre as operações definidas entre os elementos dos dois conjuntos)

Em se tratando de conjuntos infinitos as coisas se complicam.

Só para início de conversa, note que se voce retira uma parte de um conjunto infinito, isso pode não fazer nenhuma diferença importante. Por exemplo, $\mathbb{N}$ é equivalente a $\mathbb{N} - \{0,1,2,3\}$:

4 5 6 7 8 9 .....
⇕ ⇕ ⇕ ⇕ ⇕ ⇕
1 2 3 4 5 6 .....

Ou seja, do ponto de vista de enumeração, os conjuntos $\mathbb{N}$ e $\mathbb{N} - \{0,1,2,3\}$ tem "o mesmo número de elementos". Claro que dizer isso é um tanto impreciso, uma vez que os dois tem infinitos elementos. Dizemos que eles tem a mesma **cardinalidade**.

Outro exemplo: é fácil mostrar que o conjunto dos números pares tem a mesma cardinalidade de $\mathbb{N}$.

ENUMERAÇÃO E CARDINALIDADE

NOTAÇÃO: se $\mathbb{A}$ é um conjunto contável, então seus elementos podem ser indexados: $\mathbb{A} = \{a_1, a_2, a_3, ...\}$.

Definimos a função índice $I(x)$ como sendo o valor do índice do elemento x. Assim, $I(a_1) = 1$.

Definimos a função elemento $E(n)$ como sendo o elemento do conjunto que tem índice n. Assim, $E(3) = a_3$.

Note que a função I é a inversa da função E: $I = E^{-1}$ $I(E(n)) = n$ $E(I(x)) = x$

EXERCÍCIO 1: Seja $\mathbb{Z}$ o conjunto dos números inteiros { ...., –3, –2, –1, 0, 1, 2, 3, ... }.

(a) Mostre que Z tem a mesma cardinalidade de N, e defina uma função índice e uma função elemento.
(b) No seu esquema, qual inteiro terá índice 59? Qual o índice do inteiro –1348?

Observe que pode ser muito difícil, senão impossível, encontrar a forma explícita das funções I e E.

Para que um conjunto seja enumerável, "basta" provarmos que existe uma correspondência biunívoca entre seus elementos e os números naturais. Isto não exige que se conheça a expressão analítica (fórmula) dessas funções.

Um exemplo famoso é o conjunto dos números primos, $\mathbb{P} = \{2, 3, 5, 7, 11, 13, ...\}$.

$\mathbb{P}$ é claramente enumerável, pois podemos sempre encontrar qual é o primeiro, o segundo, o terceiro, ou o quinquagésimo número primo (embora seja muito trabalhoso e computacionalmente proibitivo encontrar primos consecutivos muito grandes). Não se conhece nenhuma fórmula para as funções I e E no caso dos primos, ou seja, não se conhece uma maneira de calcular rapidamente qual será o n-ésimo número primo.

É de interesse computacional a prova de Euclides de que existem infinitos números primos. Ele provou isso tomando os N primeiro números primos $p_1, p_2, p_3, ..., p_N$ e construindo o número seguinte:

$$p = p_1 \times p_2 \times p_3 \times .... \times p_N + 1$$

Lembremos agora que, quando dividimos um número n por um número m (naturais positivos), se o quociente é q e o resto é r, escrevemos

$$n = q \times m + r$$

Lembremos também que todo número pode ser escrito como um produto de fatores primos (teorema fundamental da aritmética). Portanto não precisamos considerar aqui nenhum numero que não seja primo.

É fácil ver que o número p acima não é divisível por nenhum dos p_i, pois dá sempre resto 1. Então, ou ele é primo, ou ele é divisível por um primo maior do que p_N. Em qualquer desses dois casos, teremos um número primo maior do que p_N. Portanto, p_N não pode ser o maior primo que existe. Logo, existem infinitos números primos.

Cuidado: NOTE que o número p não é o p_{N+1} !!!! Na verdade, p nem sempre é primo. Por exemplo,

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$$

(mais sobre isso, ver http://www.educ.fc.ul.pt/icm/icm98/icm12/infinitos.htm)

Os números primos são os componentes básicos da criptografia moderna, e são úteis na geração de números aleatórios por computador. Aparecem quando menos se espera. Alguns dos problemas mais famosos e difíceis da matemática dizem respeito a eles. Até hoje não foram domados por ninguém (no dia em que forem, todos os sistemas de segurança digitais vão entrar em colapso).

EXEMPLOS E EXERCÍCIOS A SEREM TRABALHADOS EM SALA DE AULA

EXEMPLO 2: Mostre que o conjunto $\mathbb{Q}$ dos números racionais é enumerável.

EXEMPLO 3: (diagonalização de Cantor) Mostre que o conjunto $\mathbb{R}$ dos números reais não é enumerável, ou seja, tem uma cardinalidade maior que $\mathbb{N}$ ou $\mathbb{Q}$.

Os números reais se dividem em duas grandes classes: o dos números algébricos e a dos transcendentes. Um número é algébrico quando é raiz de um polinômio com coeficientes racionais. Por exemplo, $\sqrt{2}$ é algébrico. Em 1882, Lindemann provou que π é transcendente (veja a prova em http://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/Transcendencia.pdf). Pode-se provar que o conjunto dos números algébricos é enumerável. Portanto, em um certo sentido, podemos dizer que os números reais são dominados pelos transcendentes.

É aqui que aparece pela primeira vez a diferença entre "contínuo" e "discreto". Uma grandeza discreta é enumerável, ao passo que o contínuo não é. Observe que isso tem pouco a ver com o fato de termos valores próximos ou não (entre duas frações, sempre existe uma terceira). O que conta é o fato de podermos enumerar os elementos, usar um índice para ordená-los. Graças aos trabalhos de Cantor (1845-1918), hoje compreendemos melhor a natureza dos conjuntos infinitos.

Na prática, todas as grandezas numéricas que medimos ou computamos são racionais. Os números irracionais são utilizados por necessidade matemática e simplificação dos conceitos e fórmulas (seria um trabalho infernal trabalhar

só com frações). Além disso, acreditamos que vivemos em um Universo contínuo - nenhum experimento até hoje contradisse isso. Portanto, acreditamos que a natureza de números como π e e seja real.

Mas para que diabos servem essas coisas no trabalho de um Engenheiro? Ocorre que as técnicas utilizadas nesse tipo de matemática encontram utilidade quando se desenvolve um algoritmo, um sistema especialista, uma matriz de portas lógicas, um sistema de endereçamento, uma estruturação eficiente de dados, etc. E respondem a questões importantes, tais como saber se todas as tarefas são passíveis de computação, ou analisar a eficiência de certo tipos de procedimentos. É como ocorre na indústria aeroespacial: pouca gente está interessada em ir a Marte ou saber o que existe em Andrômeda, mas todas se beneficiam com a tecnologia e o conhecimento produzidos por essas atividades.

EXERCÍCIO 2: Enumerar um conjunto finito de pares ordenados (i, j), $1 \le i \le N$, $1 \le j \le M$, por linhas. Encontre as funções I e E.

EXERCÍCIO 3: Enumerar um conjunto finito de pares ordenados (i, j), $1 \le i \le N$, $1 \le j \le M$, por diagonais. *(nesse caso, as funções I e E são um tanto complicadas. Fica como sugestão que voce implemente essas funções na forma de um algoritmo)*

EXERCÍCIO 4: Enumerar um conjunto infinito de pares ordenados (i, j), $i \ge 1$, $j \ge 1$.

Note que o método de linhas não funciona nesse caso. Use um sistema de numeração por diagonais. Em sala de aula, vamos encontrar as funções I e E.

EXERCÍCIO 5: *(Recursividade)* Enumerar um conjunto infinito de triplas ordenadas (i, j, k), $i \ge 1$, $j \ge 1$, $k \ge 1$.

EXERCÍCIOS EM GRUPO, EM SALA DE AULA

Os exercícios abaixo são referentes ao sistema de enumeração em diagonal de conjuntos infinitos de *n-uplas*, como trabalhado nos Exercícios 4 e 5.

EXERCÍCIO 6: No sistema de enumeração de duplas ordenadas em diagonal,

(a) qual será o índice da dupla (314, 893)?
(b) qual será a dupla com índice 1340?

EXERCÍCIO 7: No sistema de enumeração de triplas ordenadas em diagonal,

(a) qual será o índice da tripla (3,2,4)?
(b) qual será a tripla de número 128?

EXERCÍCIO 8: Enumerando quadras (i, j, k, l) pelo mesmo sistema anterior,

(a) qual será o índice da quadra (5,3,8,2)?
(b) qual será a quadra que terá índice 367821?