Notas de aula de Matemática Discreta*

As notas de aula são apenas uma parte do conteúdo necessário para o entendimento dos assuntos abordados em aula, aqui se apresenta um resumo do conteúdo do livro Fundamentos matemáticos para Ciência da Computação com comentários e informações de entendimento do professor. Para informações mais precisas e elaboradas, sugiro utilizarem os livros base da disciplina como fonte de informação.

1. Conjuntos

Definições são importantes em qualquer ciência porque contribuem para a comunicação precisa. No entanto, se procurarmos uma palavra em um dicionário, a definição é expressa usando-se outras palavras, que são definidas usando-se ainda outras palavras, e assim por diante. Desse modo, temos que ter um ponto de partida para as definições onde o significado fique claro; nosso ponto de partida nessa discussão é a noção de conjunto, um termo que não definiremos formalmente. Ao invés disso, usaremos simplesmente a ideia intuitiva de que um conjunto é uma coleção de objetos. Em alguns casos, podemos dizer que elementos dos conjuntos possuem alguma propriedade em comum, além de pertencerem ao mesmo conjunto; assim qualquer objeto que possua esta propriedade pertence ao conjunto específico e todo objeto que não possui a mesma propriedade não pertence a tal conjunto.

1.1. Notação

Usaremos letras maiúsculas para denotar conjuntos e o símbolo $\in$ para denotar pertinência em um conjunto. Assim, $a \in A$ significa que o objeto a **pertence** ao conjunto A, ou também que a é um elemento de A; e $b \notin A$ significa que o objeto b **não pertence** ao conjunto A (ou simplesmente que b não é um elemento de A).

Se $A = \{$violeta, verde, castanho$\}$, então verde $\in A$ e magenta $\notin A$.

Os elementos em um conjunto não têm nenhuma ordem, de modo que $\{$violeta, verde, castanho$\}$ é o mesmo que $\{$violeta, castanho, verde$\}$. Além disso, cada elemento do conjunto é listado apenas uma vez. Dois conjuntos são **iguais** se contêm os mesmos elementos.

$$A = B \text{ significa } (\forall x)[(x \in A \to x \in B) \wedge (x \in B \to x \in A)]$$

Um conjunto que não possui elementos é chamado de **conjunto vazio**, e é representado por $\emptyset$ ou simplesmente por $\{\ \}$.

Os conjuntos podem ser representados de diversas maneiras analíticas e gráficas. Em geral a representação de um conjunto é suficiente para identificar quais elementos pertencem ou não pertencem ao conjunto em questão.

1.1.1. Representação por Descrição

A representação por descrição é uma representação baseada em linguagem natural, por exemplo: "O conjunto A possui todos os números pares maiores que 5 e menores que 10", assim sabemos que o conjunto A possui os elementos 6 e 8.

1.1.2. Representação por Lista

A representação por listagem consiste em elencar todos os elementos, por exemplo: $A = \{6,\ 8\}$.

* "Never. I'll never turn to the dark side.", Luke Skywalker

1.1.3. Representação por Predicados

A representação por predicados consiste em descrever através de propriedades predicativas, por exemplo: $P(x)$ é um predicado verdadeiro sempre que x é um número ímpar positivo, então $B = \{x \mid P(x)\}$ é o conjunto que contém os números ímpares, $B = \{1,\ 3,\ 5,\ 7, \ldots\}$.

Podemos entender que o a formulação por predicados é uma forma de representação por uma fórmula lógica, sempre que o predicado for verdadeiro para algum elemento, então aquele elemento pertence ao conjunto.

Exemplo:

a) $P(x)$: x é um número ímpar;
b) $Q(x)$: x é um número par;
c) $R(x)$: x é um número positivo;
d) $S(x)$: x é um número negativo.

$C = \{x \mid P(x) \wedge R(x)\}$, também pode ser representado por $C = \{1,\ 3,\ 5,\ 7, \ldots\}$.
$D = \{x \mid P(x) \wedge Q(x)\}$, também pode ser representado por $D = \{\ \} = \emptyset$.

1.1.4. Representação por Recorrência

A representação por recorrência consiste em estabelecer regras de formação para o conjunto. Essas regras são divididas em dois grupos: 1) Regras base, que estabelecem quais os elementos que pertencem diretamente ao conjunto; e 2) Regras de formação, estabelece iterações sobre os elementos do conjunto para encontrar novos elementos.

Exemplo:

1) $2 \in E$;
2) Se $n \in E$, então $(n + 2) \in E$.

Portanto: $E = \{2,\ 4,\ 6,\ \ldots\}$.

1.1.5. Diagramas Gráficos

Prontamente ignorados.

1.2. Cardinalidade

Dado um conjunto S a **cardinalidade**, representada por $|S|$, de um conjunto refere-se a quantidade de elementos que o conjunto possui, nesse contexto dizemos que o conjunto pode ser finito ou infinito. O conjunto será finito quando a sua cardinalidade for um número natural, ou seja se $|S| \in \mathbb{N}$, por outro lado, dizemos que S é um conjunto infinito quando ele for tão grande quanto se queira (o conjunto E é um exemplo de conjunto infinito). O conjunto vazio possui cardinalidade zero: $|\emptyset| = 0$.

1.3. Subconjuntos

Sejam $F = \{2,\ 3,\ 5,\ 12\}$ e $G = \{2,\ 3,\ 4,\ 5,\ 9,\ 12\}$ dois conjuntos, podemos perceber que todo elemento que está em F também está em G, portanto dizemos que F é um **subconjunto** de G. Uma definição mais formal seria: dados dois conjuntos S e T, dizemos que S é subconjunto de T se:

$$(\forall x)(x \in S \rightarrow x \in T)$$

Se um conjunto S for subconjunto de um conjunto T, escreveremos $S \subseteq T$, mas se existe pelo menos um elemento de T que não está em S dizemos que S é um **subconjunto próprio** de T e podemos escrever como $S \subset T$.

Observe que com a definição de subconjuntos, podemos entender que dois conjuntos S e T são iguais se, e somente se, $S \subseteq T$ e $T \subseteq S$.

1.4. Conjunto das Partes

Observe que inicialmente utilizamos os objetos como elementos básicos dentro do universo que estamos trabalhando. Porém esta ideia inicial é equivocada, pois podemos ter conjuntos como elementos de outros conjuntos e é onde costumamos encontrar alguns problemas de interpretação. Por exemplo, sejam $H = \{1, 2, \{3\}\}$ e $I = \{\{1, 2\}, 3\}$, temos:

$$1 \in H, 1 \notin I$$

$$3 \notin H, 3 \in I$$

$$\{3\} \in H, \{3\} \subseteq I$$

$$\{1, 2\} \subset H, \{1, 2\} \in I$$

$$|H| = 3, |I| = 2$$

Dito isso, dado um conjunto S, o **conjunto das partes** de S ($\mathcal{P}(S)$) é um conjunto formado por todos os subconjuntos de S.

Exemplo: seja $J = \{1, 2, 3\}$, então $\mathcal{P}(J) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Uma maneira intuitiva de pensarmos o conjunto das partes é lembrar que ele contém todos os subconjuntos de cardinalidade zero (0), contém também os de cardinalidade 2, 3, assim por diante até o conjunto inteiro (que é subconjunto dele mesmo).

É importante perceber que para qualquer conjunto S, a cardinalidade do conjunto das partes de S é sempre maior que a cardinalidade do conjunto inicial.

$$|\mathcal{P}(S)| > |S|$$

1.5. Operações em Conjuntos

Dado um conjunto $\mathcal{U}$ que possui todos objetos em que podemos trabalhar, chamaremos este conjunto de **Universo** .

1.5.1. União

Sejam dois conjuntos S e T, o conjunto resultante V da **união** dos conjuntos S e T, denotada por $V = S \cup T$, contém todos os elementos de S e T.

$$V = S \cup T = \{x \mid x \in S \lor x \in T\}$$

1.5.2. Interseção

Sejam dois conjuntos S e T, o conjunto resultante V da **interseção** dos conjuntos S e T, denotada por $V = S \cap T$, contém os elementos que estão em S e T ao mesmo tempo.

$$V = S \cap T = \{x \mid x \in S \land x \in T\}$$

1.5.3. Diferença

Sejam dois conjuntos S e T, o conjunto resultante V da **diferença** dos conjuntos S e T, denotada por $V = S - T$, contém os elementos que estão em S e não estão T.

$$V = S - T = \{x \mid x \in S \wedge x \notin T\}$$

1.5.4. Complemento

Seja um conjunto S o complemento de S, denotado por $\overline{S}$, contém todos os elementos de $\mathcal{U}$ que não estão em S.

$$\overline{S} = \mathcal{U} - S = \{x \mid x \in \mathcal{U} \wedge x \notin S\}$$

1.5.5. Produto Cartesiano

Sejam a e b objetos do nosso universo, podemos formar um novo objeto (a, b), denominado **par ordenado**. Diferentemente dos conjuntos, a ordem dos elementos nos pares ordenados é importante e faz com que, a for diferente de b, então $(a, b) \neq (b, a)$.

Sejam dois conjuntos S e T, o **produto cartesiano** $V = S \times T$ consiste em todos os pares ordenados (x, y) tais que $x \in S$ e $y \in T$.

$$V = S \times T = \{(x, y) \mid x \in S \wedge y \in T\}$$

2. Relações

Dado um conjunto S uma **relação binária** (ou simplesmente relação) em S é um subconjunto de $S \times S$ (um conjunto de pares ordenados de elementos de S).

Da mesma maneira, uma relação entre dois conjuntos diferentes S e T, uma relação de S para T, é um subconjunto do produto cartesiano $S \times T$.

Analogamente, podemos pensar em relações envolvendo muitos conjuntos $(S_1, S_2, \ldots, S_n)$, uma relação n-ária é um subconjunto do produto cartesiano $S_1 \times S_2 \times \ldots \times S_n$.

Assim, normalmente uma relação ρ de S em T ($\rho : S \to T$) consiste em escolher pares ordenados que satisfazem alguma regra que irá relacionar elementos de S aos elementos de T.

Por exemplo, sejam $A = \{1, 2, 3, 4, 5\}$ e $B = \{6, 7, 8, 9, 10\}$.

Uma relação $R : A \to B$ que relacione um número com o seu dobro, assim $R = \{(3, 6), (4, 8), (5, 10)\}$.

Uma relação $S : A \to B$ que relacione um número com todos os valores maiores que o seu triplo, assim $R = \{(1, 6), (1, 7), (1, 8), (1, 9), (1, 10), (2, 7), (2, 8), (2, 9), (2, 10), (3, 10)\}$.

As relações podem ser definidas como regras arbitrárias que relacionam os elementos dos dois conjuntos,

2.1. Propriedades

Dado um conjunto S e uma relação binária ρ de S em S, de acordo com os elementos que estão em ρ dizemos que esta relação possui ou não possui alguma propriedade, abaixo relaciona-se algumas propriedades que as relações podem possuir.

2.1.1. Reflexiva

A propriedade reflexiva estabelece que se o elemento x pertence ao conjunto S, então o par ordenado (x, x) está na relação ρ.

$$(\forall x)(x \in S \rightarrow (x, x) \in \rho)$$

2.1.2. Simétrica

A propriedade simétrica estabelece que se o par ordenado (x, y) está na relação ρ, então o par ordenado (y, x) também deve estar.

$$(\forall x)(\forall y)((x, y) \in \rho \rightarrow (y, x) \in \rho)$$

2.1.3. Transitiva

A propriedade transitiva estabelece que se os pares ordenados (x, y) e (y, z) pertencem a relação ρ, então o par ordenado (x, z) também deve estar.

$$(\forall x)(\forall y)(\forall z)((x, y) \in \rho \wedge (y, z) \in \rho \rightarrow (x, z) \in \rho)$$

2.1.4. Anti-Simétrica

A propriedade anti-simétrica estabelece que se os pares ordenados (x, y) e (y, x) pertencem a relação ρ, então x deve ser igual a y.

$$(\forall x)(\forall y)((x, y) \in \rho \wedge (y, x) \in \rho \rightarrow x = y)$$

2.2. Fecho de Relação

Dado uma relação ρ em um conjunto S, o fecho de uma relação (ρ^*) em relação a uma propriedade P é o conjunto minimal[1] tal que $rho \subset \rho^*$ e ρ^* possui a propriedade P.

2.3. Relação Inversa

Dado uma relação $\rho : S \rightarrow T$, uma relação inversa ($\rho^{-1} : T \rightarrow S$) é tal que se (x, y) está em ρ, então (y, x) está em ρ^{-1}.

$$(\forall x)(\forall y)((x, y) \in \rho \ \rightarrow (y, x) \in \rho^{-1}$$

2.4. Domínio e Contradomínio

3. Funções

Uma função é uma regra de correspondência que associa a cada elemento x de um certo conjunto (*domínio*) a um, e apenas um, elemento y de um outro conjunto (*contra domínio*).

Sejam X e Y conjuntos. Uma função de X em Y é um terno (f, X, Y), sendo f uma relação de X para Y satisfazendo:

[1] observe a diferença entre mínimo e minimal

a) $Dominio(f) = X$;
b) Se $(x, y) \in f$ e $(x, z) \in f$, então $y = z$.

A *imagem* de uma função são os elementos $y \in Y$, tais que existe pelo menos um $x \in X$ e $f(x) = y$.

$$im(f) = \{y|f(x) = y\}$$

3.1. Injetora

Uma função é dita *injetora*, se não existem dois valores x_1 e x_2 relacionados com o mesmo valor de y.

$$x_1, x_2 \in f \wedge f(x_1) = f(x_2) \leftrightarrow x_1 = x_2$$

3.2. Sobrejetora

Uma função é dita *sobrejetora*, se existe pelo menos um valor x do domínio relacionado a cada valor y do contra domínio.

$$Im(f) = CD(f)$$

3.3. Bijetora

Uma função é dita *bijetora*, se é ao mesmo tempo injetora e bijetora.

3.4. Função Inversa

Dada uma função $f : S \to T$, dizemos que a relação inversa $f^{-1} : T \to S$ é uma função inversa de f se satisfaz as propriedades de função.

Uma função f admite função inversa se, e somente se, for uma função bijetora.

3.5. Conjuntos Contáveis

Pesquisar - Trabalho.

4. Indução Matemática

A indução matemática é uma técnica muito importante para provar resultados que envolvem números naturais e estruturas recursivas. Por exemplo, provar que:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

A ideia intuitiva da indução matemática deriva da dependência da ocorrência de um fato a ocorrência de um fato anterior. Por exemplo, uma fila de dominós alinhados. Se o primeiro dominó cair, ele vai derrubar o segundo, o segundo vai derrubar o terceiro e assim por diante, então o k-ésimo dominó vai derrubar o $(k+1)$-ésimo dominó.

Matematicamente, devemos provar que dada uma afirmação $P(k)$, para uma função $P(n), n \in \mathbb{N}$, essa afirmação implica em $P(k+1)$. Assim, quando mostramos que $P(1)$ vale, logo $P(2)$ também vale, pois $P(k) \to P(k+1)$. Portanto $P(j)$ vale para todo $j \in \mathbb{N}$.

Formalização:

Seja $P(n)$ uma função, para $n \in \mathbb{N}$.

- Se $P(1)$ é uma afirmação verdadeira; e
- $P(k) \to P(k+1), \forall k \in \mathbb{N}$.

Exemplo:

Seja $P(n) = 1 + 2 + 3 + \ldots + n$. Vamos provar que $P(n) = \frac{n(n+1)}{2}$;

Primeiro passo, provar para o primeiro valor que n é válido, $n = 1$.

$P(1) = 1$;

$n = 1 : \frac{n(n+1)}{2} = \frac{1*(1+1)}{2} = 1$

Logo, $P(1) = \frac{1*(1+1)}{2}$.

Segundo passo, assumir que $P(n)$ é válido para algum k (**Hipótese de Indução - HI**):

HI: $P(k) = 1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$

Terceiro passo, mostrar que $P(k)$ implica em $P(k+1)$ (ou seja, devemos mostrar que dado $P(k)$, temos $P(k+1) = \frac{[(k+1)+1](k+1)}{2}$):

$$P(k+1) = \mathbf{1} + \mathbf{2} + \mathbf{3} + \ldots + \mathbf{k} + (k+1)$$

$$P(k+1) = HI + (k+1)$$

$$P(k+1) = \frac{k(k+1)}{2} + (k+1)$$

$$P(k+1) = \frac{k(k+1) + 2(k+1)}{2}$$

$$P(k+1) = \frac{(k+2)(k+1)}{2}$$

$$P(k+1) = \frac{[(k+1)+1](k+1)}{2}$$

Logo, $P(k) \to P(k+1), \forall k, k \in \mathbb{N}$. Portanto $P(n) = \frac{n(n+1)}{2}$.

Exemplo 2:

Seja $P(n) = 1 + 3 + 5 + \ldots + (2n-1)$. Vamos provar que $P(n) = n^2$;

Primeiro passo, provar para o primeiro valor que n é válido, $n = 1$.

$P(1) = 1$;

$n = 1 : n^2 = 1^2 = 1$

Logo, $P(1) = 1^2$.

Segundo passo, assumir que $P(n)$ é válido para algum k (**Hipótese de Indução - HI**):

HI: $P(k) = 1 + 3 + 5 + \ldots + (2k - 1) = k^2$

Terceiro passo, mostrar que $P(k)$ implica em $P(k + 1)$ (ou seja, devemos mostrar que dado $P(k)$, temos $P(k + 1) = (k + 1)^2$):

$$P(k+1) = \mathbf{1} + \mathbf{2} + \mathbf{3} + \ldots + (\mathbf{2k} - \mathbf{1}) + (2k - 1 + 2)$$
$$P(k+1) = HI + (2k+1)$$
$$P(k+1) = k^2 + 2k + 1$$
$$P(k+1) = (k+1)(k+1)$$
$$P(k+1) = (k+1)^2$$

Logo, $P(k) \rightarrow P(k + 1), \forall k, k \in \mathbb{N}$. Portanto, $P(n) = n^2$.

Outro Exemplo:

Prove que $\forall n, n \geq 2$, n é um número primo ou um produto de números primos.

Nota: Todo inteiro n pode ser decomposto por fatores menores ou n é um número primo.

Tentativa 1: Utilizar suposição que vale para $p(k)$.

Passo 1: Mostrar para base: 2 é primo. Portanto vale que e número primo ou produto de números primos.

Passo 2: Hipótese de indução:

Suponha que para o inteiro $k > 2$, k é primo ou pode ser decomposto por fatores primos.

- k é primo; ou
- $k = a.b$, onde a e b são primos ou produtos de primos.

Passo 3: Prova para $k + 1$.

- Se $k + 1$ for primo, é trivial;
- Se $k + 1$ não for primo, então sabemos que ele pode ser reescrito como fator de dois números menores: $k + 1 = a'.b'$.

Porém, não temos afirmação nenhuma sobre os valores a' e b' e não temos como prosseguir. Neste caso, nossa hipótese de indução deve ser mais ”forte”.

Passo 2: Passo de Indução Forte:

Suponha que para todo valor inteiro y, no intervalo $2 \leq y \leq k$, então y é primo ou é um produto de primos: $y = a.b$.

Passo 3: Prova para $k + 1$:

- Se $k + 1$ for primo, é trivial;
- Se $k + 1$ não for primo, então sabemos que ele pode ser reescrito como fator de dois números menores: $k+1 = a'.b'$, tal que $2 \leq a' < k+1$ e $2 \leq b' < k+1$. Logo, $2 \leq a' \leq k$ e $2 \leq b' \leq k$ e são primos ou fatores de primos. Portanto, pela hipótese de indução, $k + 1 = a'.b'$ é produto de números primos.

5. Relação de Recorrência

5.1. Objetivo

Apresentar técnica recursiva que permite reduzir um problema envolvendo n objetos a outro problema semelhante com n' ($n' < n$) objetos, que por sua vez pode ser reduzido para um problema com n''

($n'' < n'$) objetos e assim por diante até que o problema seja suficientemente pequeno e fácil de resolver.

Uma **relação de recorrência** é uma fórmula que relaciona a_n aos seus predecessores: $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$.

Exemplo:

Seja S_n a soma dos primeiros n númeores naturais. Determine a relação de recorrência em termos de S_{n-1}.

$$S_n = 1 + 2 + \ldots + (n-1) + n$$
$$S_n = S_{n-1} + n$$

Porém, é necessário que se estabeleça uma condição de parada para a recursão, neste caso: $S_1 = 1$.

Exemplo - Problema dos coelhos

O problema dos coelhos foi proposto em 1202 por Leonardo de Pisa e consiste em determinar o numero de pares de coelhos ao final de 12 meses sob as seguintes condições:

a) Inicialmente tem-se um único par de coelhos recém nascidos;

b) Todo mês, cada par de coelhos com pelo menos 2 meses produz um novo casal de coelhos; e

c) Nenhum coelho morre durante o processo.

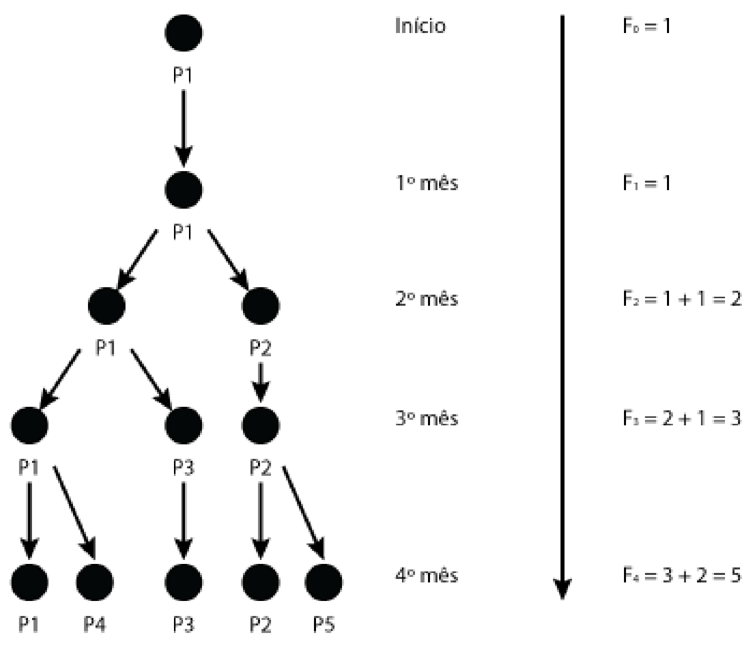

Figura 1. Evolução dos pares de coelhos.

A figura 1 ilustra a evolução da quantidade de pares de coelhos em função do tempo. Que pode ser representada na fórmula a seguir:

$$F_n = F_{n-1} + F_{n-2}$$
$$F_1 = 1$$
$$F_0 = 1$$

Outro Exemplo - Torre de Hanoi

Determine o menor número de movimentos para passar n discos de uma torre para outra.

a) Todos os discos se encontram inicialmente na primeira torre;

b) Só é permitido mover um disco por movimento;

c) Discos maiores não devem ser colocados sobre discos menores.

6. Autômatos Finitos

6.1. Autômatos Finitos Determinísticos

6.2. Autômatos Finitos Não Determinísticos