Tópico 05

Matemática para Computação

Relações de ordem e equivalência

1. Introdução

As relações entre conjuntos são a base para o entendimento das funções na matemática e, por isso, são de suma importância. Iremos estudar esse tema com um pouco mais de profundidade neste tópico. As quatro principais propriedades das relações as classificam e nos permitem a compreender o comportamento da relação de interesse e traçar estratégias para a soluções dos problemas.

De maneira intuitiva, no nosso dia a dia, podemos observar relações em diversos aspectos, principalmente as relações binárias. Na família, a relação entre dois parentes (pai e filho, sobrinho e tio etc.), na vida profissional, na escola etc. Na matemática, os números e elementos se conectam por meio de conjuntos definidos, que podem ou não definir funções que modelam determinado comportamento ou fenômeno.

Estendendo os conceitos, veremos casos especiais das relações de ordem e equivalência, fecho de uma relação e diagrama de Hasse para visualização da topologia de uma relação.

2. Representações de relações

Quando pensamos em relações, o caso que mais aparece na matemática são as relações binárias entre dois conjuntos finitos. Pela definição, temos que uma relação binária de A e B é um subconjunto do produto cartesiano A x B e escrevemos xRy sendo (x, y) um par ordenado em A x B. Vamos observar diferentes formas de visualizar uma relação, sem explicitar a propriedade ou listar seus elementos. Veja o exemplo a seguir:

Exemplo: Considere os conjuntos A = {1, 2, 3} e B= {1, 3, 6} e o subconjunto de relação R = {(1, 1), (1, 3), (2, 1), (3, 6)}

A lista de elementos que pertencem a R:

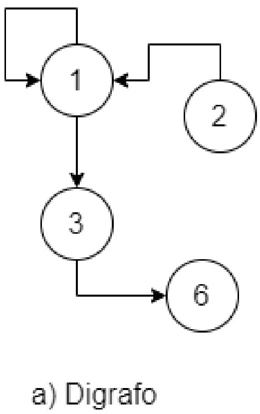
- 1R1, 1R3, 2R1, 3R6

A figura abaixo mostra duas configurações possíveis. A primeira é conhecida como digrafo ou grafo orientado, os elementos dos conjuntos são representados por "nós" ou "vértices" e a relação pelos arcos que ligam os elementos dos pares ordenados. Ao lado, temos uma matriz que representa as conexões entre os elementos, que é obtida da seguinte maneira:

Seja r_{ij} o elemento contido na linha i e coluna j, temos:

- $r_{ij} = 1$ se (a_i, b_j) pertence a R, isto é, $a_i R b_j$.
- $r_{ij} = 0$ se (a_i, b_j) não pertence a R.

A figura seguinte mostra a representação de R do exemplo acima:



$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

b) Matriz de relação

Visualizações de relações.

Agora, vamos relembrar as cinco principais propriedades da relação. Seja A um conjunto, (x, y) um par ordenado de elementos de A e R uma relação, podemos escrever:

Podemos caracterizar as propriedades utilizando os dígrafos ou as matrizes de relação. Para uma relação reflexiva, temos que para um elemento de a A, o par ordenado (x, x) deve pertencer a relação R, dessa forma, no dígrafo nos vértices de elementos, existe uma aresta que liga a ele mesmo e, na matriz, isso significa elementos da diagonal principal ser igual a 1. Veja a imagem seguinte.

Relação reflexiva.

Nas relações simétricas, se o par ordenado (x,y) pertencer à relação R, (y, x) também deve pertencer. No dígrafo, isso significa que dois elementos compartilham aresta nos dois sentidos, já na matriz da relação, M_R deve ser simétrica em relação à diagonal principal, isto é, $M_R = M_R^T$.

Relação simétrica.

Em relações antissimétricas, temos que na matriz $M_{R,}$ pode ter a diagonal igual a zero e $r_{ij} \neq r_{ji.}$ Na representação por dígrafos, se de algum vértice do dígrafo partir uma aresta para um outro vértice, não pode existir uma aresta no sentido contrário. Veja a Figura abaixo.

Relação antimétrica.

Para demonstrar assimetria, na representação por dígrafos, se algum vértice partir de uma aresta para um outro vértice, não deve existir uma aresta no sentido contrário, caso oposto da relação simétrica. E, para a matriz M_R, a diagonal principal deve ser igual a zero, além disso, $r_{ij} \neq r_{ji}$.

Relação assimétrica.

Leia mais sobre dígrafos em:

Clique aqui

Vale a pena assistir!

3. Fecho de uma relação

Se uma relação binária R em um conjunto arbitrário A não possuir uma determinada propriedade *p*, podemos estender R e obter uma nova relação R* também no conjunto A, que contém os elementos de R e os elementos adicionais necessários para que a propriedade p seja válida. Chamamos essa estratégia de fecho de uma relação. Olhe atentamente para a definição:

DEFINIÇÃO: Seja A um conjunto, R uma relação binária em A e uma propriedade *p*. O fecho de R é a relação binária R* em A que possui a propriedade *p* e satisfaz as três condições seguintes:

Podemos encontrar três tipos de fechos de relações: reflexivo, simétrico e transitivo. Caso uma relação binária R em um conjunto A tenha a propriedade *p* de interesse, ela já é seu próprio fecho uma vez que satisfaz a propriedade *p*.

O fecho transitivo (em inglês, *transitive closure*) de uma relação binária R é a relação binária R^t em um conjunto A que satisfaz as três condições abaixo:

Exemplo:

Seja o conjunto A = {0,1,2,3}, considere a relação R definida em A como:

R = {(0,1), (1,2),(2,3)}

Vamos determinar a relação de fecho transitivo de R. Relembrando o conceito de relação transitiva, para todo (x,y) ∈ R, se (y,z)∈ R também, então (x,z) deve pertencer a R. Olhamos para os elementos de R:

Os elementos ((0,2) e (1,3) não pertencem a R e são elementos que precisam estar na relação para ela ser transitiva. Logo:

Mas R1 ainda não é o fecho transitivo pois temos agora

E daí completam o fecho transitivo

Grafo de R e R^t.

Assim como no fecho transitivo, o conceito pode ser estendido para fecho reflexivo, fecho simétrico, fecho assimétrico. A ideia central continua como sendo encontrar uma relação complementar à propriedade desejada.

4. Relação de ordem

No nosso dia a dia, em muitos momentos, a ordem da disposição de pessoas ou elementos é importante. Imagine uma fila em um cinema, ou a ordem de prioridades de realizações de atividades, a ordenação léxica de nomes em uma lista de presença. Vamos ver mais um pouco a respeito do conceito de relações de ordem.

Podemos pensar em relação de ordem como uma generalização do conceito de menor ou igual ($\leq$) ou de maior ou igual ($\geq$). A relação de ordem é interna do conjunto, isto é, só existe para comparar elementos de um mesmo conjunto. A principal característica de relações de ordem é assegurar as três propriedades: reflexiva, antissimétrica e transitiva.

Exemplo: considere a relação binária R = {(1,1), (2, 2), (3, 3), (1, 2), (2, 3), (1, 3)} no conjunto A = {1, 2, 3}, temos um exemplo de relação:

- Reflexiva: (1,1), (2, 2), (3,3) pertence a R.
- Assimétrica: (1, 2) e (2, 3) pertencem a R e (2, 1) e (3, 2) não pertencem.
- Transitiva: (1, 2) e (2, 3) pertencem a R logo (1, 3) também pertence.

Temos dois tipos de relações de ordem: total e parcial. Para uma relação de ordem total em um conjunto não vazio A, todos os elementos de A são comparáveis 2 a 2 pela relação R, isto é, todos os elementos podem ser comparáveis entre si.

Exemplo: Seja a relação R no conjunto A = {2, 4, 8, 16, …, 2n, … } definida por "x é múltiplo de y" é uma relação de ordem total em A.

Na relação de ordem parcial, nem todos os elementos são comparáveis entre si. Ainda assegura as três propriedades, reflexiva, antissimétrica e transitiva, mas não é universal.

Exemplo: a relação no conjunto dos números naturas “x divide y” é uma relação de ordem parcial, uma vez que dois números naturais nem sempre são comparáveis por esta ordem, como, por exemplo, 5 e 7 – 5 não divide 7, e 7 não divide 5.

Se um conjunto A é finito, e uma relação R em A é de ordem parcial, podemos representar graficamente a relação por meio do diagrama de Hasse. Cada elemento é representado por pontos ou vértices, e os elementos distintos que estão em relação são ligados por um segmento de reta. O segmento de reta liga x a y, de modo que xRy pertença à relação e x esteja por baixo, ao ponto que representa y, semelhante ao dígrafo visto anteriormente, mas de forma simplificada. Algumas arestas não precisam estar presentes em virtude das propriedades reflexiva – *loops* entre elementos – e transitiva da relação. Veja o exemplo seguinte:

Considere o dígrafo da relação de ordem R “menor ou igual” sobre o conjunto A = {1, 2, 3, 4}. A listagem dos pares ordenados da relação é:

R = {(1, 1), (1, 2), (1, 3), (1, 4) (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)}

Observe, na figura seguinte, a construção do diagrama de Hasse.

Conversão da representação de dígrafo para diagrama de Hasse.

Exemplo: considere o conjunto de partes de p({1,2}) e uma relação de inclusão ⊆. Este é um conjunto parcialmente ordenado, também conhecido como **poset** (do inglês, *partially ordered set*). Os elementos do conjunto de partes são:

A relação consiste nos pares ordenados:

O diagrama de Hasse pode ser representado como mostrado na figura seguinte.

Diagrama de Hasse
relação de inclusão.

Vale a pena assistir!

Ordem parcial e elementos notáveis de um conjunto parcialmente ordenado

Vale a pena assistir!

5. Relação de Equivalência

Vamos supor que a matrícula de estudantes em uma determinada escola segue um esquema de ordem alfabética. A divisão forma três grupos com horários de atendimento diferentes. Observe a tabela seguinte:

Considere A como sendo o conjunto de todos os alunos que vão se matricular na escola e R a relação que contém (x, y) para todo x e y estudantes de um mesmo horário de atendimento, isto é, estudantes com nomes começando com letras de um mesmo bloco. Em outras palavras, se (x, y) pertencem à relação R, logo, tais alunos podem se encontrar na hora de fazer a matrícula na escola. Esse é um exemplo de relação equivalente: ela é reflexiva, simétrica e transitiva. Observe também que R divide os estudantes em três classes equivalentes.

Definição: uma relação R em um conjunto A é uma relação de equivalência se R for: reflexiva, simétrica e transitiva.

Exemplo: seja o conjunto A = {1, 2, 3, 4} e a relação R = {(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)}

- R é reflexiva pois {(1, 1), (2, 2), (3, 3), (4, 4)} está contido em R.
- R é simétrica uma vez que para xRy e yRx: {(1, 2), (2, 1), (3, 4), (4, 3)} está contido em R
- R é transitiva pois xRy e yRz então xRz

Vamos, agora, conhecer um outro exemplo de relação de equivalência, aplicando no conceito de congruência na matemática. Mas, antes, vamos relembrar alguns conceitos importantes.

Em uma divisão de números inteiros, temos os seguintes elementos:

Na qual A é o dividendo, B é o divisor, Q é o quociente e R é o resto. Por exemplo, se dividimos 26 por 3, temos:

$$A = 26$$

$$B = 3$$

$$Q = 8$$

$$R = 2$$

Em alguns casos, estamos interessados em observar o valor do resto da divisão (em inglês, *mod*) e utilizamos a seguinte notação, considerando os mesmos conceitos apresentados anteriormente: A (mod B) = R. Ou, no exemplo:

$$26 \ (\text{mod } 3) = 2$$

Agora, considere um número m pertencente ao conjunto dos números naturais e os números a, b ao conjunto dos números inteiros. Dizemos que a e b são **congruentes** módulo m se os restos de sua divisão por m são iguais. A notação é a seguinte:

Exemplo: temos que **-6 ≡ 15 (mod 7)**, uma vez que o resto da divisão de -6 e 7 é 1 e o resto da divisão de 15 por 7 também é 1.

Um teorema importante da congruência diz que a e b são congruentes módulo m, se, e somente se, a subtração (b – a) for divisível por m, um jeito bem mais simples de verificar se o resto da divisão é igual. Vamos verificar utilizando os mesmos números do exemplo acima.

Assim, como -21 é divisível por 7, temos que -6 e 15 são congruentes módulo 7. De forma matemática, escrevemos o teorema como:

Tendo dito isso, considere uma relação R de congruência, que pode ser descrita como:

Vamos provar que R é uma relação de equivalência sobre o conjunto dos números inteiros. Tendo em mente o teorema mostrado anteriormente da subtração dos números pelo módulo.

Exemplo:

A criptografia é o estudo de métodos para enviar e receber mensagens secretas. A aritmética módulo m vista anteriormente é uma das técnicas utilizadas na criptografia. O exemplo mais tradicional é conhecido como código de César, no qual cada letra do alfabeto é associada a um número, como na tabela seguinte, e depois transladava três casas mais à frente e tomava o módulo $m = 26$.

É definido assim, uma função $f(n) = (n+3)mod26$ para encriptar uma mensagem, chamada de função encriptadora. Para decodificar a mensagem, isto é, recuperar a mensagem original, utiliza-se a sua inversa $f-1(n) = (n-3)mod26$, chamada de função desencriptadora.

Exemplo:

Uma outra situação em que encontramos aplicação de congruência é no número do Cadastro de Pessoas Físicas, ou CPF, no Brasil. O número do CPF é composto por 11 dígitos, dividido em dois blocos: 9 alegorismos iniciais e 2 dígitos de controle. Para determinarmos os dígitos de controle, utilizamos a congruência módulo m.

Obtemos um dígito de controle por vez, utilizando o mesmo procedimento. Para o primeiro dígito, determinamos a somatória ponderada dos 9 dígitos do primeiro bloco. Os pesos atribuídos são {1,2,3,4,5,6,7,8,9}. Assim, vamos supor o CPF 235 343 104, teremos:

$$S = 2\times1 + 3\times2 + 5\times3 + 3\times4 + 4\times5 + 3\times6 + 1\times7 + 0\text{x}8 + 4\times9 = 116$$

Em seguida, o décimo dígito (a10) é obtido de forma tal que diferença S – a10 seja um número múltiplo de 11, em outros termos, $S - a10 \equiv 0 \pmod{11}$. Assim, temos que o dígito é o próprio resto da divisão de S por 11.

Fazendo a divisão, obtemos o número 6, isto é, $116 = 11\times10 + 6$. Esse seria nosso primeiro dígito de validação. O segundo dígito é obtido da mesma maneira, e a soma ponderada agora é feita utilizando o décimo dígito que determinamos e os pesos, com os números de 0 a 9.

Tente a obter o segundo dígito de validação do exemplo acima! Utilize o mesmo procedimento explicado para o primeiro dígito.

Para mais detalhes sobre a descrição matemática do número completo do CPF, confira, na apresentação abaixo:

Vale a pena assistir!

Uma aplicação de congruência – Autenticação e validação de um CPF

6. Partição

Vamos agora ilustrar um aspecto importante das relações de equivalência em um conjunto. Considere, por exemplo, um conjunto S = { x | x é um aluno de sua classe} e a relação R = “ x senta na mesma coluna de cadeiras que y”, sendo (x, y) um par ordenado de alunos do conjunto S. Podemos indicar todos os alunos de S que se relacionam uns com os outros. Podemos dividir o conjunto S em vários subconjuntos referentes a relação R, observe a figura abaixo.

Particionamento de S.

Cada grupo representado na divisão acima é um subconjunto de alunos da classe que compartilham a mesma coluna. Chamamos essa característica das relações de equivalência de partição de um conjunto. Vamos a definição formal:

DEFINIÇÃO: uma partição de um conjunto S é uma coleção de subconjuntos distintos e não vazios de S cuja união resulta no próprio S.

- Cada elemento de S pertence a um dos subconjuntos de R.
- Se A_1 e A_2 são elementos distintos de R, então a intersecção de A_1 e A_2 é vazia, isto é, são subconjuntos disjuntos.

As relações de equivalência podem ser particionadas em subconjuntos. Esses subconjuntos são chamados de blocos da partição e são formados pelo grupamento dos elementos que se relacionam.

Exemplo: Considere um conjunto A = {1, 2, 3, 5, 7, 9, 11, 13}. Observe o particionamento na figura abaixo:

Particionamento de A.

Temos que a relação R define uma partição P do conjunto A em quatro blocos:

$$P = \{A_1, A_2, A_3, A_4\}$$

Uma partição P pode ser utilizada para construir uma relação de equivalência sobre um conjunto A.

Teorema: seja P uma partição sobre um conjunto A, defina uma relação R sobre o conjunto A, como:

R = aRb se, e somente se, a e b são membros do mesmo bloco.

Dessa forma, R é uma relação de equivalência sobre o conjunto A. Podemos provar matematicamente que assegura as três propriedades que definem:

- Reflexiva: se a pertence a A, então a está no mesmo bloco que ele mesmo, isto é, aRa.
- Simétrica: se aRb, significa que a e b estão no mesmo bloco, logo, b e a também estão no mesmo bloco, isto é, bRa.
- Transitiva: se aRb e bRc compartilham o mesmo bloco, logo, aRc também estão. aRb e bRc à aRc

Exemplo: seja A = {1, 2, 3, 4} e considere a partição P = {{1,2,3}, {4}}. Ache a relação de equivalência por P.

Tente apresentar a prova de que R é uma relação de equivalência mostrando que assegura as três propriedades: reflexiva, simétrica e transitiva.

Os dois blocos pertencentes a P são {1, 2, 3} e {4}. Para construir a relação R que define, cada elemento do bloco deve estar relacionado com todos os outros elementos no mesmo bloco e somente esses elementos.

$$R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 4)\}$$

Vale a pena assistir!

7. Conclusões

Neste tópico, continuamos nossos estudos das relações binárias e suas propriedades. Vimos as diferentes maneiras de representações, utilizando os dígrafos e as matrizes da relação. Em seguida, definimos fecho de uma relação, que mostra que podemos determinar elementos que completem determinada propriedade que não está contida em uma relação.

Olhamos com mais detalhes os conceitos de relação de ordem e relação de equivalência, apresentando uma nova forma de representar as relações de ordem por meio dos diagramas de Hasse. Além de apresentar provas matemáticas de relações de equivalência como na congruência entre números.

Por fim, definimos o conceito de partição de uma relação de equivalência com um exemplo intuitivo de uma classe em uma turma, na qual o conjunto de alunos foi dividido em subconjuntos que chamamos de blocos, e a união de blocos representa o próprio conjunto original.

8. Referências

FEOFILOFF, Paulo. Grafos. IME-USP. 2017. Disponível em: < https://www.ime.usp.br/~pf/algoritmos_para_grafos/aulas/graphs.html >

ROISENBERG, Mauro. Fundamentos de matemática discreta para computação: Relações. UFSC – Santa Catarina: 06 jun. 2009, 01 dec. 2009. Notas de Aula.

ANDRADE, D. Algumas Aplicações da aritmética à criptografia, Jornal Eletrônico de Ensino e Pesquisa de Matemática (1s). v. 2 2 (2018). 16-24. ISSN-2594-6323;

GERSTING, Judith L.. Mathematical Structures for Computer Science. 5a edição. Hawai: Michelle Russel Julet, 2003..

GRAHAM, Ronald L.; KNUTH, Donald E.; PATASHNIK, Oren. Matemática concreta: fundamentos para a ciência da computação. 2. ed. Rio de Janeiro: LTC, 1995.

DOLCE, Osvaldo; POMPEO, José Nicolau. Fundamentos de matemática elementar 10: geometria espacial, posição e métrica. 5. ed. São Paulo, SP: Atual, 1999. 440 p. ISBN 85-7056-411-2.

GIOVANNI, J. R.; BONJORNO, J. R. Matemática Completa. São Paulo: FTD, 2005. 3v.

YouTube. (2017). Enori Carelli. Ordem parcial e elementos notáveis de um conjunto parcialmente ordenado. Disponível em: <https://www.youtube.com/watch?v=1LxYP6qY-is>.

YouTube. (2020). Anderson Martins Rocha do Prado. Uma aplicação de congruência – Autenticação e validação de um CPF. Disponível em: < https://www.youtube.com/watch?v=aExyYOVyTus >.

Parabéns, esta aula foi concluída!

O que achou do conteúdo estudado?

Péssimo Ruim Normal Bom Excelente

Deixe aqui seu comentário

Mínimo de caracteres: 0/150

Enviar