Aspectos Formais da Computação

Aparecida Francisco da Silva
Clotilzio Moreira dos Santos

unesp
CULTURA ACADÊMICA Editora
PRÓ REITORIA DE GRADUAÇÃO

Programa de Apoio à Produção de Material Didático

Aparecida Francisco da Silva
Clotilzio Moreira dos Santos

ASPECTOS FORMAIS DA COMPUTAÇÃO

unesp

CULTURA ACADÊMICA Editora

PRÓ REITORIA DE GRADUAÇÃO

São Paulo
2009

Silva, Aparecida Francisco da
S586a Aspectos formais da computação / Aparecida Francisco da Silva [e] Clotilzio Moreira dos Santos . – São Paulo : Cultura Acadêmica : Universidade Estadual Paulista, Pró-Reitoria de Graduação, 2009
395 p.

ISBN 978-85-98605-88-3

1. Computabilidade. 2. Matemática de computador. 3. Relações binárias. I. Santos, Clotilzio Moreira dos. II. Título.

CDD 004.0151

Ficha catalográfica elaborada pela Coordenadoria Geral de Bibliotecas da Unesp

Cultura Acadêmica Editora
Praça da Sé, 108 - Centro
CEP: 01001-900 - São Paulo-SP
Telefone: (11) 3242-7171

APOIO

FUNDAÇÃO EDITORA DA UNESP
CGB - COORDENADORIA GERAL DE BIBLIOTECAS

APOIO TÉCNICO

Ivonette de Mattos
José Welington Gonçalves Vieira

PROJETO GRÁFICO

DESIGNJR.
Empresa Júnior de Design
designjunior@gmail.com

PROGRAMA DE APOIO
À PRODUÇÃO DE MATERIAL DIDÁTICO

Considerando a importância da produção de material didático-pedagógico dedicado ao ensino de graduação e de pós-graduação, a Reitoria da UNESP, por meio da Pró–Reitoria de Graduação (PROGRAD) e em parceria com a Fundação Editora UNESP (FEU), mantém o Programa de Apoio à Produção de Material Didático de Docentes da UNESP, que contempla textos de apoio às aulas, material audiovisual, *homepages, softwares*, material artístico e outras mídias, sob o selo CULTURA ACADÊMICA da Editora da UNESP, disponibilizando aos alunos material didático de qualidade com baixo custo e editado sob demanda.

Assim, é com satisfação que colocamos à disposição da comunidade acadêmica mais esta obra, "***Aspectos Formais da Computação***", de autoria dos **Professores Dra. Aparecida Francisco da Silva e Dr. Clotilzio Moreira dos Santos**, do Instituto de Biociências, Letras e Ciências Exatas do Câmpus de São José do Rio Preto, esperando que ela traga contribuição não apenas para estudantes da UNESP, mas para todos aqueles interessados no assunto abordado.

Dedicatória

Ao Felipe (AFS)
À Rita e Isabela (CMS),
dedicamos.

Prefácio

Este livro nasceu de notas de aulas para o curso de Bacharelado em Ciências da Computação do IBILCE-UNESP-SÃO JOSÉ DO RIO PRETO. O que motivou sua escrita foi que os livros em língua portuguesa que se encontram no mercado sobre o assunto são escassos e com uma linguagem pouca voltada às ciências da computação.

Especificamente, o seu conteúdo é o programa da disciplina Aspectos Formais de Computação, ministrada hoje com 60 h semestrais para os alunos ingressantes. Destacamos que muitos exercícios e alguns aspectos apresentados são devidos ao complemento da disciplina no seu formato original que abordava computabilidade de funções.

No livro são apresentados temas introdutórios de lógica clássica, aritmética dos números inteiros e um pouco de estruturas algébricas: relações e álgebra booleana, necessárias e voltadas às ciências da computação. Os temas foram desenvolvidos como fundamentação inicial, de modo mais auto-suficiente e acessível possível, de forma que qualquer aluno ingressante no ensino superior possa ler o livro e entendê-lo sem dificuldades.

O capítulo um trata da lógica clássica, basicamente das leis do cálculo proposicional e os métodos de prova, muito útil às ciências da computação. O capítulo dois, sobre aritmética dos números inteiros, é assunto clássico e não poderíamos deixar de escrever alguma coisa sobre ele, pois trata de fundamentação. Aproveitamos para fazer aplicações simples em Criptografia e representações de números em diferentes bases, especialmente as bases 2, 4, 8, 16 bastante úteis nas ciências da computação. A fundamentação

da linguagem matemática voltada para a computação continua no capítulo três, onde desenvolvemos a linguagem inicial da teoria dos conjuntos. Segue um capítulo sobre relações, onde começamos a estruturação de conjuntos. Neste ponto desenvolvemos as importantes relações de equivalência, de ordem e funções. No caso de funções, exibimos aquelas que são importantes dentro da teoria, devido a sua forte ocorrência, em vez de seguir um caminho mais tradicional voltado aos cursos de matemática. No capítulo cinco, sobre operações, apresentamos o anel de inteiro módulo m, especialmente quando m é uma potência de dois, para explorarmos a aritmética binária truncada módulo m. A seguir, desenvolvemos a teoria inicial de anéis e álgebras de Boole, e exploramos a relação que estas estruturas têm com o conjunto das proposições e aritmética binária. Terminamos o capítulo cinco associando as álgebras de Boole com circuitos, como tem sido nossa preocupação deste o início. Concluímos o livro com um capítulo sobre computabilidade de funções, onde exploramos o conceito de enumerabilidade aplicado nas máquinas de Turing e a tese de Church. Seguem-se as noções iniciais de funções recursivas primitivas, onde são exibidos vários exemplos.

Os capítulos um, dois e três são auto-suficientes e as noções de lógica vistas no capítulo um sub-jaz a todos eles. Os capítulos um e três são fortemente usados no capítulo quatro. A menos de noções de funções e divisibilidade, o capítulo seis é auto-suficiente. Segundo gostaríamos que o livro fosse, faltou um pouco de teoria de grupos, grafos e contagem, assim como monóides, semi-grupos e reticulados, o que, talvez, será incluído nas próximas edições. No entanto, achamos que é material suficiente para um curso de 60 h como se apresenta hoje.

Esperamos que o livro seja útil em dois aspectos: o primeiro, que atenda completamente os alunos ingressantes em ciências da computação, pois foi para eles que o livro foi inicialmente escrito; o segundo, que o aluno "quebre"uma estrutura mental criada nos cursos pré-vestibulares, ou cursinhos, caracterizada por perguntas e respostas imediatas. Para isto procuramos escrever o livro em uma linguagem suave, desenvolvemos a teoria com bastante exemplos e muitos exercícios com diferentes níveis de dificuldades no

final de cada tópico. Em geral, quando não se trata de verificação, são dadas a maioria das respostas dos exercícios, até o capítulo quatro. As respostas dos exercícios dos outros capítulos ficam para uma próxima edição. Outro ponto com que nos preocupamos foi escrever o livro em uma dificuldade crescente do primeiro para o último capítulo. Finalmente, esperamos que o leitor aprecie a proposta apresentada e agradecemos ao Prof. Dr. Claudio Aguinaldo Buzzi pela prestimosa colaboração na utilização dos comandos do latex. Também estamos abertos a críticas e sugestões do leitor, e a possíveis correções de erros que podem ser encontrados.

IBILCE/UNESP, São José do Rio Preto, dezembro de 2009.

Os Autores.

Sumário

Capítulo 1

LÓGICA

1.1 Introdução

Segundo Pierce, mais de uma centena de definições já foram propostas para responder a questão, "o que é lógica?". Mas, para ele, a principal função da lógica é a classificação das argumentações, de modo que se possa separar as "boas"das "más". Lógica seria (ou é), então, o estudo e a análise de métodos e princípios empregados para distinguir boas (corretas) e más (incorretas) argumentações. Lembramos que os argumentos são, via de regra, elaborados com o fito de convencer, e esta é, realmente, uma de suas mais importantes e legítimas funções. Indivíduos diferentes formulam cada enunciado com métodos diferentes, como adivinhar ou sonhar, e então vêm com o problema de convencer os demais (por vezes eles próprios) da veracidade do palpite.

Além dos métodos inspiracionais e pessoais, como usam os artistas e os místicos, três outros métodos são conhecidos.

O primeiro, embora seja bárbaro, é muito empregado pela humanidade. Consiste em dizer "O enunciado tal é verdadeiro porque o chefe (ou o uso, ou o governo, etc.) diz que é", e os descrentes são "convencidos"por algum tipo de força. Este método tem uma desvantagem a longo prazo, porque pode bem acontecer que um grande projeto baseado em princípios impostos por um chefe saia errado, com grande desperdício de tempo e dinheiro. A história está repleta de exemplos.

Dois outros métodos são conhecidos: um deles é o método indutivo das ciências naturais. Aplicando esse método ao famoso Teorema de Pitágoras "para um triângulo ABC com ângulo reto em B, temos $\overline{AC}^2 = \overline{AB}^2 + \overline{BC}^2$", poderíamos argumentar assim: o enunciado foi verificado dentro dos limites de erro experimental, pelo exame de uma grande amostra de triângulos. Portanto, acreditamos que o mesmo seja verdadeiro, até encontrarmos um contra-exemplo, quando então modificaremos nossas crenças, de acordo com esse fato. Mas, neste caso, não podemos ter certeza de que o enunciado não deva ser

$$\overline{AC}^2 = \overline{AB}^2 + \overline{BC}^2 + (t - t_1)(t - t_2)\ldots(t - t_n)$$

onde t é o tempo agora e t_i são os tempos de verificações anteriores, ou ainda, $\overline{AC}^2 = \overline{AB}^2 + \overline{BC}^2 + d$ com $d \neq 0$, uma constante pequena demais para ser detectado experimentalmente.

Poderíamos argumentar que a primeira afirmação é válida porque é mais simples, baseando-se em que "A NATUREZA É SIMPLES". Mas, isto introduz uma hipótese não provada (embora útil, e a história da humanidade apresenta muitos exemplos em que o que é "complexo"para uma geração é "simples" para a seguinte).

A descoberta do terceiro método, aparentemente, foi um feito peculiar da civilização grega. Recordando o problema: *achar um modo pelo qual o indivíduo A pode fazer uma afirmação k e tê-la aceita por um outro indivíduo B, que talvez no início esteja descrente.*

O método encontrado pelos gregos, e usado com bastante sucesso no estudo da geometria, consiste em formular um conjunto imparcial de regras, pelo qual B ouve o argumento de A em apoio a k e concorda em deixar A continuar em cada estágio do argumento, se certas condições estiverem satisfeitas. Se A satisfaz a essas condições em cada estágio do argumento, até que o argumento esteja completo, então B concorda em se convencer.

Segundo este método, são apresentados certos axiomas e definições cujo objetivo é limitar a argumentação de modo que, para se estabelecer qualquer proposição, pode-se partir dos axiomas (que são pensados como expressando verdades que nenhuma pessoa sã

de espírito pode negar). Assim, um argumento em prol de uma afirmação k é verdadeiro se o argumento usa apenas as regras lógicas admitidas e apela apenas para os axiomas ou para as proposições previamente estabelecidas pelo mesmo método.

Como já afirmamos, os argumentos são, via de regra, elaborados com o intuito de convencer, e esta é uma de suas mais importantes tarefas, mas a lógica não se interessa pelo poder de persuasão que os argumentos possam ter. Há argumentos logicamente incorretos que convencem e argumentos logicamente impecáveis que não têm nenhum poder de persuasão. O que a lógica procura é estudar os tipos de relações que possam existir entre a evidência e a conclusão, ou seja, responder às seguintes questões:
(a) supondo verdadeiras as premissas, a conclusão deve ser verdadeira?
(b) as premissas constituem evidência para a conclusão?
(c) as premissas são, realmente, evidência para esta conclusão?

Considerando-se que a legitimidade independe do conteúdo das asserções que compõem os argumentos, é muito mais fácil analisá-los escrevendo-os em uma notação simbólica apropriada, de modo que questões de "conteúdo"sejam afastadas de consideração. É por isso que a lógica usa o simbolismo (da matemática, em particular), criando uma linguagem própria e adequada. Letras substituem sentenças comuns e símbolos especiais são introduzidos com o objetivo de formular os argumentos em toda a sua nudez.

Observe as expressões a seguir:

Bom dia!	(1)
Que horas são?	(2)
Está chovendo.	(3)
Não vou correr.	(4)
Se João ler a carta, ele se sentirá infeliz.	(5)
Às segundas vou à escola e às sextas ao cinema.	(6)
Vou a Miami ou ao Caribe.	(7)
Puxa vida!	(8)
Leia isso.	(9)

Há algumas sentenças para as quais não faz sentido dizer se

são falsas ou não, e há outras para as quais (em determinadas circunstâncias) isto é possível.

Vejamos, sobre (1), (2), (8) e (9) nada podemos afirmar sobre verdade ou falsidade. As demais, se soubermos o suficiente sobre as circunstâncias, podem ser classificadas em falsas ou verdadeiras. Essas são as sentenças que vão nos interessar daqui para a frente, as quais chamaremos de proposição. Mais precisamente:

Definição 1.1 Uma *Proposição* ou *sentença* é qualquer oração declarativa (falada ou escrita) que pode ser classificada como verdadeira (V) ou falsa (F), mas não ambas.

Observe que, ao atribuirmos valor-verdade a uma sentença ou proposição, estamos adotando os seguintes princípios:

(*I*) *Princípio da não contradição*: uma proposição não pode ser verdadeira e falsa ao mesmo tempo.

(*II*) *Princípio do terceiro excluído*: toda proposição, ou é verdadeira, ou é falsa, isto é, verifica-se sempre um destes casos e nunca um terceiro.

Estes são os princípios da lógica clássica que nos nortearam na apresentação a seguir:

1.2 Cálculo Proposicional

Definição 1.2 Uma proposição é dita *simples* ou *atômica* se ela não contém outra proposição como parte integrante de si mesma. Caso contrário, a proposição é dita *composta.*

Segundo as definições anteriores, as orações "*A Terra é esférica*"e "*A caneta não está sobre a mesa*"são proposições simples e "*Hoje está chovendo e eu estou estudando*"é uma composta, pois contém as proposições "*Hoje está chovendo*"e "*Eu estou estudando*".

Para obtermos proposições compostas, em geral, fazemos uso dos *conectivos.* A seguir apresentamos os conectivos, os símbolos usados para representá-los e a negação:

	Símbolo Utilizado
e	$\wedge$ ou &
ou	$\vee$ ou +
ou (exclusivo)	$\underline{\vee}$
se então	$\longrightarrow$
se, e somente se	$\longleftrightarrow$
não	$\neg$ ou $\sim$

Estudaremos os valores-verdade da negação de uma proposição e de proposições compostas obtidas usando-se cada um dos conectivos.

1. Negação (não)

Negamos a verdade de uma proposição afirmando sua negação. Por exemplo, a negação da proposição "*Está chovendo*"é "*Não está chovendo*". Em geral, a negação de uma proposição simples é fácil. No entanto, a negação de uma proposição composta nem sempre é fácil. Vejamos:

Considere a proposição "*se chover, não sairei de casa*". Podemos negá-la da seguinte maneira:

> "*Não é verdade que, se chover, não sairei de casa*"
> ou
> "*É falso que, se chover, não sairei de casa*".

Não importando qual a forma utilizada para a negação de uma proposição (seja ela simples ou composta), temos sempre o mesmo significado:

"*A negação de uma proposição verdadeira é falsa, e a negação de uma proposição falsa é verdadeira*".

Usando p para a proposição em questão, $\sim p$ sua negação, V para verdadeiro e F para falso, podemos resumir a informação anterior na seguinte tabela:

p	$\sim p$
V	F
F	V

Exercício (a): Negar as seguintes proposições:

(a) $2 + 3 = 5$
(b) $7 < 3$
(c) Roma é capital da França.
(d) Todos os homens são bons.
(e) Algumas mulheres são inteligentes.

2. Conjunção

Observe a sentença: "*Estou cansado e com sono*". Podemos decompô-la em duas:

$$p: \text{ "}estou\ cansado\text{"} \qquad q: \text{ "}estou\ com\ sono\text{"}$$

e representá-la por $p \wedge q$ ou $p\&q$ ou $p.q$.

O valor-verdade de $p \wedge q$ é o mesmo do linguajar corrente, ou seja, "$p \wedge q$ *é verdadeira se, e somente se, ambas,* p *e* q, *forem verdadeiras*".

O valor-verdade de $p \wedge q$ depende, então, dos valores-verdade da proposições p e q. Esses valores-verdade podem ser combinados de quatro formas diferentes. Essas combinações, bem como o resultado, podem ser resumidos numa tabela, chamada *tabela-verdade,* onde são apresentadas todas as possíveis combinações de valores-verdade de p e q, distribuídos da seguinte forma: na primeira coluna indicamos os valores-verdade para p, na segunda os valores-verdade para q e na terceira os valores-verdade de $p \wedge q$ em função dos valores-verdade de p e q.

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Exercício (b): Dê os valores-verdade das seguintes proposições:
(a) A neve é branca, e $2 < 5$.
(b) O sal é verde, e 7 é um número primo.

(c) $\pi > 4$, e $\sin(\pi/2) = 0$.
(d) Paris é capital da França, e $9 - 4 = 5$.

3. Disjunção

Na linguagem coloquial, a palavra "**ou**"tem dois sentidos. Veja os exemplos:

(1) Carlos é médico ou professor.
(2) Mário é alagoano ou gaúcho.

Na proposição (1) estamos indicando que pelo menos uma das afirmações ("*Carlos é médico*", "*Carlos é professor*") é verdadeira, podendo serem ambas verdadeiras: "*Carlos é médico e professor*". Mas a proposição (2) está indicando que apenas uma das afirmações ("*Mário é alagoano*", "*Mário é gaúcho*) é verdadeira, não podendo ocorrer ambas simultaneamente.

No primeiro caso dizemos que "ou" é **inclusivo**, enquanto que, no segundo, "ou" é **exclusivo**.

Usamos o símbolo "$\vee$"para "ou inclusivo" e "$\underline{\vee}$"para "ou exclusivo".

Os valores-verdade das disjunções são dados por:

"*A disjunção inclusiva de duas orações é verdadeira desde que uma delas o seja, e a disjunção exclusiva de duas proposições é verdadeira desde que uma, e apenas uma, o seja*".

Resumindo, em tabelas-verdade, temos:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

p	q	$p \underline{\vee} q$
V	V	F
V	F	V
F	V	V
F	F	F

Para destacar o ou exclusivo podemos escrever "ou ... ou...", por exemplo "ou Carlos é médico ou Carlos é professor" "ou Mário é alogoano ou Mario é gaucho".

4. Condicional ($\rightarrow$)

Usamos os termos "se $\cdots$ então" para obter uma proposição composta chamada condicional. No sentido da linguagem comum, é difícil precisar em quais circunstâncias a maior parte das pessoas aceita como verdadeira uma proposição condicional. Considere o exemplo:

"*Se João andou rápido*, *então João chegou cedo em casa*"
(1) (2)

Se a afirmação (1) é verdadeira e a segunda é falsa, quase todos concordam que a condicional é falsa. Da mesma forma que, se ambas as afirmações forem verdadeiras, quase todos concordam que a sentença composta é verdadeira. As duas possibilidades discutidas são as únicas que, em geral, são levantadas no dia-a-dia. No entanto, existem mais duas possibilidades. Suponha que a proposição "*Se João andou rápido*" seja falsa. O que podemos afirmar da proposição composta se a proposição "*João chegou cedo em casa*" for falsa? E se for verdadeira? A linguagem comum não tem uma "solução" para esta indagação, mas, para efeito de análise do valor-verdade, assumiremos que, se p for falsa, então "se p então q" é verdadeira.

Os valores-verdade da proposição condicional $p \rightarrow q$, em função dos valores-verdade de p e q podem, então, ser resumidos da seguinte forma:

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Nota (1) A construção "se $\cdots$ então $\cdots$", muito usada em linguagem de programação, é diferente da construção "se $\cdots$ então $\cdots$" usada em lógica. De fato, muitos casos de programação contêm

proposições "se p então S", onde p é uma proposição e S é um programa (uma ou mais proposições) a ser executado. Quando se executa o programa todo e se encontra uma tal proposição $p \rightarrow S$, então S é executado se p for verdadeiro, e S não é executado se p for falso.

Outras maneiras de ler $p \rightarrow q$ são:

p é condição suficiente para q
q é condição necessária para p
p somente se q
q se p
q sempre que p.

Assim "*Se João é Paulista, então João é Brasileiro*". Podemos escrever, também: "*Uma condição necessária para que João seja Paulista é que ele seja Brasileiro*", ou ainda, "*Uma condição suficiente para João ser Brasileiro é João ser Paulista*".

5. Bicondicional

Usamos a expressão "se, e somente se"para formar a proposição bicondicional. A proposição composta $p \leftrightarrow q$ é verdadeira desde que p e q tenham o mesmo valor-verdade. Resumindo em tabela-verdade temos:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Os conectivos lógicos são muito usados em pesquisas ou busca de termos em grande coleção de informações, como é o caso das páginas da Web. Como estas buscas empregam técnica da lógica de proposição, elas são chamadas de *pesquisa* (ou *busca*) *booleana*. Na busca booleana, o conectivo *e* é usado para juntar dois termos que se quer na pesquisa, e o conectivo *ou* é usado para trazer um dos termos ou ambos quando eles são encontrados. O conectivo

não (ou *e não*) serve para excluir, na busca, o termo em questão quando ele é encontrado.

Por exemplo, suponhamos que queremos buscar páginas da Web que contenha o termo "Universidade de Mato Grosso". No espaço próprio, entramos com: "Universidade + Mato + Grosso". Com o comando "enter", serão exibidos todas as páginas que se encontram na Web que contenham o termo "Universidade de Mato Grosso", inclusive "Universidade de Mato Grosso do Sul". Caso não interessa as universidades de Mato Grosso do Sul, basta entrar com o termo: "(Universidade + Mato + Grosso) + ¬ Sul", onde + é o conectivo *e*, e ¬ é o conectivo *não*.

Definição 1.3 *Tautologia* é uma proposição composta T sempre verdadeira, quaisquer que sejam os valores-verdade das proposições atômicas que a compõem. Em outras palavras, a coluna de T em sua tabela-verdade contém apenas v´s.

Exemplo 1.4 $p \vee \sim p$ é sempre verdadeira, independentemente do valor-verdade de p.

p	$\sim p$	$p \vee \sim p$
V	F	V
F	V	V

Definição 1.5 *Contradição* é uma proposição composta C, cujo valor-verdade é falso, quaisquer que sejam os valores-verdade das proposições atômicas que a compõem.

p	$\sim p$	$p \wedge \sim p$
V	F	F
F	V	F

Claro que $\sim T$ é uma contradição e $\sim C$ é uma tautologia.

Definição 1.6 Toda proposição, que não seja uma tautologia nem contradição, é dita *indeterminada* ou *contingência.* Assim, a tabela-verdade de uma contingência admite, em sua coluna final, valores falsos e também verdadeiros.

Observação 1.7 Se uma proposição é composta de outras n proposições simples, então sua tabela-verdade tem 2^n linhas.

Assim, precisaremos da ajuda de um computador para verificar se uma proposição composta constituída de 20 (vinte) proposições atômicas é uma tautologia. De fato, tal proposição possui $2^{20} = 1.048.576$ linhas. Um computador atual leva pelo menos um trilhão de anos para fazer a tabela-verdade de uma proposição composta constituída de mil proposições atômicas. Esta tabela-verdade terá 2^{1000} (um número com 300 decimais) combinações possíveis de valores-verdade. Pelo que conhecemos até hoje, não se conhece um método efetivo de cálculo. Este tipo de problema está inserido na teoria de complexidade de algoritmos.

A Questão do Parênteses

Proposições compostas que envolvem vários símbolos lógicos podem ter significados ambíguos. Por exemplo, as proposições $(\sim p) \wedge q$ e $\sim (p \wedge q)$ não têm *sempre* o mesmo valor-verdade e, portanto, não podem, de alguma forma, ser equivalentes. Por isto é necessário o uso de parênteses na expressão $\sim p \wedge q$, a menos que se defina qual das duas expressões acima é representada pela expressão $\sim p \wedge q$. Neste caso, e em qualquer outro, será considerado que a negação tem preferência sobre todos os outros símbolos. Por exemplo, $\sim p \wedge q$ significará a conjunção $(\sim p) \wedge q$ e não a negação $\sim (p \wedge q)$. Por $\sim p \rightarrow q$ entende-se o condicional $(\sim p) \rightarrow q$ e não a negação $\sim (p \rightarrow q)$, etc.

Em outras palavras, de agora em diante a negação terá preferência sobre os símbolos lógicos $\wedge$, $\vee$, $\veebar$, $\longrightarrow$, $\longleftrightarrow$ e nenhum destes símbolos lógicos terá preferência sobre os demais. Portanto, usaremos parênteses, colchetes ou chaves em expressões do tipo $p \wedge q \vee r$, $\quad p \wedge q \longrightarrow r$, que tem significados ambíguos. Assim, ou escreveremos $(p \wedge q) \vee r$, ou $p \wedge (q \vee r)$, nunca $p \wedge q \vee r$. Do mesmo modo, escreveremos, ou bem a conjunção $p \wedge (q \longrightarrow r)$, ou bem a condicional $(p \wedge q) \longrightarrow r$, nunca a expressão ambígua $p \wedge q \longrightarrow r$.

Como exemplo, vamos escrever a seguinte proposição, usando símbolos lógicos: "*Você não pode acessar a internet no pólo computacional se você não for estudante, a menos que você*

trabalhe no pólo computacional".

Sejam p a proposição: "*Você pode acessar a internet no pólo computacional*", q: "*Você é estudante*" e r a sentença: "*Você trabalha no pólo computacional*". Em símbolos fica:

$$(\sim q \wedge \sim r) \rightarrow \sim p.$$

Apresentamos a seguir dois exemplos dos chamados jogos lógicos:

Exemplo (1) Depois de uma chuva, os filhos de Pedro, João e Maria, pedem ao pai para brincar na lama. O pai deixa com a condição de que não voltem sujos para dentro da casa. Quando as crianças terminam de brincar e voltam para dentro da casa, o pai nota que pelo menos uma das crianças tem a testa suja e faz a seguinte colocação: "*Pelo menos um de vocês tem a testa suja*". Sem olhar no espelho e olhando apenas para a testa do irmão, vocês devem responder ao mesmo tempo se a sua testa está suja ou não. As respostas, nesta fase da brincadeira podem ser: "*Minha testa está suja*", "*Minha testa está limpa*"ou "*Não sei*". Conhecidas estas resposta, o pai pergunta novamente para as crianças: "*Quem de vocês tem a testa suja*?"Agora, ambas as crianças dão a resposta exata.

De fato, sendo p e q, respectivamente, as proposições: "*A testa de João está suja*" e "*a testa de Maria está suja*", a informação dada pelo pai de que pelo menos uma das crianças tem a testa suja significa que "$p \vee q$ é verdadeira". Assim, se João olha para Maria e vê que esta tem a testa limpa, ele sabe que a sua está suja e vai responder com certeza: "*Minha testa está suja*"para a primeira pergunta do pai. Caso a testa da Maria estiver suja ele vai responder "*Não sei*"à primeira pergunta do pai, pois sua testa pode estar suja ou não. O mesmo vale para a resposta da Maria. Cada criança, tendo a resposta dada pelo irmão (irmã) à primeira questão, faz a seguinte análise: A resposta da minha irmã (do meu irmão) é "*Não sei*"se minha testa está suja e se a resposta dada foi: "*Minha testa está suja*"é porque a minha testa está limpa. Com isto ambas as crianças acertam na segunda tentativa.

Exemplo (2) Vamos analisar os valores-verdade de cada proposição, no conjunto das seguintes proposições: João diz o seguinte

sobre o caráter de Pedro, p: "*Pedro não mente*" e Pedro afirma o seguinte, q: "*Exatamente um de nós mente*".

Se p é verdadeiro então a sentença q: "*Exatamente um de nós mente*"é verdadeira, ou seja, ambas as proposições são verdadeiras. Mas a proposição q afirma que p ou q é falsa. Uma contradição, pois ambas são verdadeiras. Logo a proposição p : "*Pedro não mente*"tem que ser falsa. Portanto, Pedro mente e por isso é falsa a proposição q : "*Exatamente um de nós mente*". Como p já é falsa, então ambas as proposições p e q são falsas.

Exercícios (c)

(1) Quais das seguintes frases representam proposições:

(a) O pasto está amarelo.
(b) Formosas rosas brancas!
(c) O número 5 é primo?
(d) Todas as áreas da matemática são fáceis e algumas são mais ainda.
(e) Dê-me o livro.

(2) Sejam p: "*as ciências matemáticas são fáceis*"e q: "2 *é menor que* 3". Escreva em português as proposições representadas por:

(a) $p \wedge q$
(b) $\sim (p \vee q)$
(c) $p \vee q$
(d) $\sim p \vee \sim q$

(3) Sejam p a proposição "x *é número par*"e q, "x *é o produto de dois inteiros*". Traduza para a linguagem simbólica as seguintes proposições:

(a) ou x é um número par ou é o produto de dois inteiros.
(b) x é um número ímpar e o produto de dois inteiros.
(c) ou x é par e um produto de dois números inteiros ou x é ímpar e não é o produto de dois números inteiros.
(d) x não é um número par nem o produto de dois números inteiros.

(4) Escreva em português a negação de cada uma das seguintes

proposições:

(a) O tempo está frio e estou cansado.
(b) Ou é desejável a boa saúde, ou fui mal informado.
(c) As laranjas não são adequadas para usá-las em saladas de frutas.
(d) Existe um número real que somado a 6 dá como resultado 13.

(5) Decida o valores-verdade das proposições compostas a seguir, sabendo que p é verdadeira e q e r são falsas.

(a)	$\sim p$	(e)	$p \vee q$
(b)	$(p \vee q) \vee r$	(f)	$\sim p \vee (q \vee r)$
(c)	$(p \wedge q) \vee (q \wedge r)$	(g)	$\sim p \vee \sim (q \vee r)$
(d)	$p \wedge q$	(h)	$(p \wedge q) \vee (\sim p \wedge \sim q)$

(i) $[(p \vee q) \vee (\sim p \wedge \sim q)] \vee [(\sim p \wedge q) \vee (p \wedge \sim q)]$.

(6) Determine quais das expressões a seguir são tautologias, construindo a tabela-verdade correspondente:

(a) $(p \wedge q) \vee (\sim p \vee \sim q)$
(b) $(p \vee q) \vee (\sim p)$
(c) $(p \wedge \sim q) \vee (\sim p \wedge q)$
(d) $(p \wedge \sim q) \vee [\sim p \wedge [(q \wedge r) \vee \sim (\sim q \wedge r)]]$
(e) $(p \wedge q) \wedge (\sim p \vee q) \wedge (p \wedge \sim q)$
(f) $[(p \to q) \wedge (q \to r)] \longrightarrow [p \to r]$
(g) $[p \wedge (p \to q)] \longrightarrow q$
(h) $(\sim p) \longrightarrow (p \to q)$

(7) Usando a convenção 1 para tautologia e 0 para contradição, . para conectivo **e**, + para o conectivo **ou**, e $'$ para a negação, demonstre que são tautologias as seguintes proposições:

(a) $(p + p) \longleftrightarrow p$ e $(p.p) \longleftrightarrow p$.
(b) $[(p + q) + r] \longleftrightarrow [p + (q + r)]$ e $[(p.q).r] \longleftrightarrow [p.(q.r)]$.
(c) $(p + q) \longleftrightarrow (q + p)$ e $(p.q) \longleftrightarrow (q.p)$.
(d) $[p + (q.r)] \longleftrightarrow [(p + q).(p + r)]$ e
$[p.(q + r)] \longleftrightarrow [(p.q) + (p.r)]$.
(e) $(p + 0) \longleftrightarrow p$ e $(p.0) \longleftrightarrow 0$.
(f) $(p.1) \longleftrightarrow p$ e $(p + 1) \longleftrightarrow 1$.
(g) $(p + p') \longleftrightarrow 1$ e $(p.p') \longleftrightarrow 0$.
(h) $(p')' \longleftrightarrow p$ e $0' \longleftrightarrow 1$.

(i) $1' \longleftrightarrow 0$ e $(p+q)' \longleftrightarrow (p'.q')$.
(j) $(p.q)' \longleftrightarrow (p'+q')$ e $[p \leftrightarrow (p.q)] \longleftrightarrow [p \leftrightarrow q]$.
(k) $[(p \to q).(p \to r)] \longleftrightarrow [p \to (q.r)]$ e
$[(p \to q)+(p \to r)] \longleftrightarrow [p \to (q+r)]$.
(l) $[p.(q+p)] \longleftrightarrow p$ e $[p+(q.p)] \longleftrightarrow p$.
(m) $[(p+q)+p] \longleftrightarrow [p+q]$ e $[(p.q).p] \longleftrightarrow (p.q)$.

1.3 Equivalência e Implicação Lógica

Se as proposições P e Q ocorrem em um mesmo contexto denotemos por $p_1, \ldots, p_n$ todas as proposições atômicas que ocorrem em P ou (inclusivo) em Q. Escreveremos $P = P(p_1, \ldots, p_n)$ e $Q = Q(p_1, \ldots, p_n)$. Por exemplo, se P é a proposição $p \to p$ e $Q: \ q \vee \sim r$, também escrevemos $P(p,q,r): \ p \to p$ e $Q(p,q,r): \ q \vee \sim r$.

Definição 1.8 Duas proposições $P = P(p_1, \ldots, p_n)$ e $Q = Q(p_1, \ldots, p_n)$, $n \geq 1$, são *logicamente equivalentes* se P e Q sempre assumem valores-verdade iguais (ou V ou F), quaisquer que sejam os valores-verdade atribuídos às proposições $p_1, \ldots, p_n$. Em outras palavras, P e Q são logicamente equivalentes se, e somente se, $P \longleftrightarrow Q$ for uma tautologia, ao ainda, as colunas das tabelas-verdade de P e Q são iguais.

Notação: $P \Longleftrightarrow Q$ ou $P \equiv Q$.

Exemplo 1.9 $(p \to q) \Longleftrightarrow (\sim q \to \sim p)$. De fato, denotando na tabela abaixo $p \to q$ por A e $\sim q \to \sim p$ por B para simplificar, então a tautologia $(p \to q) \longleftrightarrow (\sim q \to \sim p)$ pode ser vista por meio da tabela-verdade a seguir:

p	q	$p \to q$	$\sim q$	$\sim p$	$\sim q \to (\sim p)$	$A \longleftrightarrow B$
V	V	V	F	F	V	V
V	F	F	V	F	F	V
F	V	V	F	V	V	V
F	F	V	V	V	V	V

Exemplo 1.10 $\sim (p \rightarrow q) \equiv (p \wedge \sim q)$, como pode ser observado na tabela a seguir, onde D é $\sim (p \rightarrow q)$ e E é $p \wedge \sim q$.

p	q	$p \rightarrow q$	$\sim (p \rightarrow q)$	$\sim q$	$p \wedge \sim q$	$D \longleftrightarrow E$
V	V	V	F	F	F	V
V	F	F	V	V	V	V
F	V	V	F	F	F	V
F	F	V	F	V	F	V

Observação 1.11 Desde que $\sim (p \rightarrow q)$ e $p \wedge \sim q$ são logicamente equivalentes, temos uma forma para a negação de $p \rightarrow q$. Por exemplo, ao invés de dizer "*não é verdade que, se o aluno tirar média maior ou igual a cinco, ele passa de ano*", podemos dizer "*o aluno tira média maior ou igual a cinco e não passa de ano*".

Teorema 1.12 *Para quaisquer proposições p e q tem-se:*
$p \veebar q \equiv (p \vee q) \wedge \sim (p \wedge q) \equiv (p \wedge \sim q) \vee (\sim p \wedge q)$.

Demonstração: Provemos apenas que $p \veebar q$ e $(p \wedge \sim q) \vee (\sim p \wedge q)$ têm a mesma tabela-verdade. Para simplificar denotaremos $p \wedge \sim q$ por A, $\sim p \wedge q$ por B, $p \vee q$ por C e $\sim (p \wedge q)$ por D e apresentaremos em uma mesma tabela-verdade os valores-verdade de $p \veebar q$, $A \vee B$, e de $C \wedge D$.

p	q	$\neg p$	$\neg q$	$\boldsymbol{p \veebar q}$	$\boldsymbol{C \wedge D}$	$\boldsymbol{A \vee B}$	A	B
V	V	F	F	F	F	F	F	F
V	F	F	V	V	V	V	V	F
F	V	V	F	V	V	V	F	V
F	F	V	V	F	F	F	F	F

Logo, $p \veebar q$, $A \vee B$ e $(p \vee q) \wedge \neg (p \wedge q)$ são logicamente equivalentes. □

Outras propriedades são dadas no seguinte teorema.

Teorema 1.13 *Para quaisquer proposições p, q e r, se T é uma tautologia e C uma contradição, tem-se:*

(a) $p \vee (q \vee r) \equiv (p \vee q) \vee r$ *e* $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$.

(b) $p \vee q \equiv q \vee p$ *e* $p \wedge q \equiv q \wedge p$.

(c) $p \to q \equiv (\sim p) \vee q$ *e* $p \longleftrightarrow q \equiv (p \to q) \wedge (q \to p)$.

(d) $\sim (p \vee q) \equiv \sim p \wedge \sim q$ *e* $\sim (p \wedge q) \equiv \sim p \vee \sim q$.

(e) $\sim (p \to q) \equiv p \wedge \sim q$.

(f) $\sim (p \longleftrightarrow q) \equiv \sim p \longleftrightarrow q \equiv p \longleftrightarrow \sim q$.

(g) $p \vee \sim p \equiv T$, *e* $p \wedge \sim p \equiv C$.

(h) $\sim \sim p \equiv p$, $\sim T \equiv C$ *e* $\sim C \equiv T$.

(i) $p \vee p \equiv p \wedge p \equiv p$.

(j) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ *e* $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.

(k) $p \vee C \equiv p$, $p \wedge C \equiv C$, $p \vee T \equiv T$ *e* $p \wedge T \equiv p$.

O ítem (a) é a lei associativa, (b) comutativa, (d) é conhecido como leis de DeMorgan, (g) e (h) leis complementares, (i) idempotentes, (j) são as propriedades distributivas e, (k) são as identidades.

As proposições p, q e r podem ser substituídas por proposições compostas P, Q e R.

Demonstração: Demonstremos apenas $p \to q \equiv \sim p \vee q$ e $\sim (p \wedge q) \equiv \sim p \vee \sim q$, construindo suas tabelas-verdade, como na demonstração do Teorema1.12. Os outros ítens ficam como exercício.

$p \longrightarrow q \equiv \sim p \vee q$

$$\overbrace{\text{mesma} \quad \text{tabela}}$$
$$\downarrow \qquad \downarrow$$

p	q	$p \longrightarrow q$	$\neg p \vee q$	$\neg p$	q
V	V	V	V	F	V
V	F	F	F	F	F
F	V	V	V	V	V
F	F	V	V	V	F

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

$$\overbrace{\text{mesma} \quad \text{tabela}}$$
$$\downarrow \qquad \downarrow$$

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$	$\neg p$	$\neg q$
V	V	V	F	F	F	F
V	F	F	V	V	F	V
F	V	F	V	V	V	F
F	F	F	V	V	V	V

□

A primeira observação que fazemos dos Teoremas 1.12 e 1.13 é que estas propriedades iniciais de equivalência lógica podem ser usadas para construir ou verificar outras equivalências lógicas. A razão disto é que podemos trocar uma proposição composta por outra que é logicamente equivalente a ela sem mudar o valor-verdade da proposição composta. Vamos exemplificar esta técnica que, muitas vezes, serve para obter uma proposição mais simples logicamente equivalente à proposição composta original. Este processo é dito *simplificação.*

Exemplo Mostre que $(p \wedge q) \rightarrow (p \vee q)$ é uma tautologia, sem usar tabela-verdade.

Solução:

$$\begin{aligned}
&(p \wedge q) \rightarrow (p \vee q) \\
\equiv &\sim (p \wedge q) \vee (p \vee q) && \text{(Prop. do condicional)} \\
\equiv &(\sim p \vee \sim q) \vee (p \vee q) && \text{(Leis de DeMorgan)} \\
\equiv &(\sim p \vee p) \vee (\sim q \vee q) && \text{(Leis assoc. e comut.)} \\
\equiv &T \vee T && \text{(Leis complementares)} \\
\equiv &T && \text{(idempotentes).}
\end{aligned}$$

A segunda observação é que, em geral, usamos sentenças logicamente equivalentes para negar determinados tipos de proposições compostas. Mais precisamente, usando os ítens (c), (d), (h) e (e), temos formas para a negação de sentenças compostas. Por exemplo, a negação da proposição: "*João é Paulista ou Paulo é Carioca*" é "*João não é Paulista e Paulo não é Carioca*", (ítem (d)

do Teorema 1.13). A negação da proposição: "*Se João é Paulista então João é Brasileiro*" é "*João é Paulista e João não é Brasileiro*", (item (e) do Teorema 1.13).

Finalmente, a última observação a fazer sobre as conseqüências dos Teoremas 1.12 e 1.13 é que cada fórmula proposicional ou proposição composta é logicamente equivalente a uma proposição composta constituída usando apenas os símbolos lógicos $\neg$ (negação), $\wedge$ (conjunção) e $\vee$ (disjunção). Isto será tratado em detalhes na seção sobre formas canônicas de funções booleanas. Por exemplo, vamos obter uma proposição equivalente a $(p \to q) \veebar r$ usando apenas os símbolos $\neg$, $\wedge$ e $\vee$.

$$
\begin{array}{ll}
\quad (p \to q) \veebar r & \\
\equiv (\neg p \ \vee q) \veebar r & (\text{ Teo. 1.13(e)}) \\
\equiv [(\neg p \vee q) \wedge \neg r] \vee [\neg(\neg p \vee q) \wedge r] & (\text{Teo. 1.12}) \\
\equiv [(\neg p \vee q) \wedge \neg r] \vee [(\neg\neg p \wedge \neg q) \wedge r] & (\text{Leis de DeMorgan}) \\
\equiv [(\neg p \vee q) \wedge \neg r] \vee [(p \wedge \neg q) \wedge r] & (\text{Teo. 1.13(h)})
\end{array}
$$

Esta última expressão é uma das formas canônicas da proposição composta $(p \to q) \veebar r$. Veja seção 5 do capítulo 5.

Definição 1.14 Dizemos que $P = P(p_1, \ldots, p_n)$ *implica logicamente* $Q = Q(p_1, \ldots, p_n)$ e denotamos por $P \Longrightarrow Q$ se, toda atribuição de valores-verdade à $p_1, \ldots, p_n$ que tornam P verdadeiro, também tornam Q verdadeiro. Em outras palavras, se a proposição composta $P \to Q$ for uma tautologia.

Exemplo 1.15 $p \Longrightarrow (p \vee q)$, pois, como pode ser visto na tabela a seguir, $p \to (p \vee q)$ é uma tautologia:

p	q	$p \vee q$	$p \to (p \vee q)$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	V

Note que nem é preciso fazer a tabela para verificar esta implicação lógica, desde que $p \vee q$ é verdadeira sempre que p o for.

Também são muito simples as verificações de que $p \Longrightarrow p$, $p \wedge q \Longrightarrow q$.

Como consequência dos ítens (c) e (d) do Teorema 1.13, temos a seguinte caracterização da implicação lógica.

Teorema 1.16 *Dadas proposições P e Q, são equivalentes*
(i) $P \Longrightarrow Q$.
(ii) $\neg P \vee Q$ *é uma tautologia,*
(iii) $P \wedge \neg Q$ *é uma contradição.*

Exercícios

(1) Demonstre que: **(i)** $p \longrightarrow q \equiv \neg q \longrightarrow \neg p \equiv \neg p \vee q$,
(ii) $p \longleftrightarrow q \equiv (\sim p \vee q) \wedge (p \vee \sim q)$.
(2) Prove que o símbolo *condicional* não é associativo, ou seja, prove que $[(p \to q) \to r] \not\equiv [p \to (q \to r)]$.
(3) Para proposições p e q demonstre que:
(i) $(p \vee q) \vee p \equiv p \vee q$, **(ii)** $(p \wedge q) \wedge p \equiv p \wedge q$,
(iii) $p \vee (\sim p \wedge q) \equiv p \vee q$ e $p \wedge (\sim p \vee q) \equiv p \wedge q$.
(4) Verifique se: $[(p \to \sim q) \wedge (r \to q) \wedge r] \Longrightarrow \sim p$.
(5) Construa as tabelas-verdade e simplifique cada uma das seguintes proposições compostas:
(i) $\sim [(\sim p \wedge q) \to (p \to r)] \vee [(r \to p) \vee r]$,
(ii) $[p \to (\neg q \vee r)] \wedge \neg [q \vee (p \leftrightarrow \neg r)]$,
(iii) $\neg\{p \vee [q \to (q \to (p \wedge \neg p)]\} \longrightarrow \{q \wedge (r \leftrightarrow r)\}$.
(6) Verifique se: **(a)** $p \Longrightarrow (p \vee q)$, **(b)** $p \Longrightarrow (p \wedge q)$,
(c) $(p \wedge q) \Longrightarrow (p \leftrightarrow q)$.
(7) Demonstre as seguintes leis:
(a) $(p \to q) \wedge p \Longrightarrow q$, **(b)** $p \wedge q \Longrightarrow p$,
(c) $(p \to q) \wedge \sim q \Longrightarrow \sim p$,
(d) **(i)** $p \to (p \wedge q) \Longleftrightarrow p \to q$, **(ii)** $(p \vee q) \to q \Longleftrightarrow p \to q$,
(iii) $p \wedge (p \vee q) \equiv p$ e $p \vee (p \wedge q) \equiv p$, (prop. Absorção).
(8) Demonstre a propriedade distributiva à esquerda de "$\to$"em relação a "$\wedge$", isto é: $[p \to (q \wedge r)] \equiv [(p \to q) \wedge (p \to r)]$.
(9) Duas operações bastante usadas em circuitos lógicos são o *NAND* (do inglês, *não e*) que pode ser denotado e definido por

$p|q := \neg(p \wedge q)$ e *NOR* (do inglês, *não ou*), que pode ser denotado e definido por $p \downarrow q := \neg(p \vee q)$.

(i) Use as propriedades já vistas e faça a tabela para as operações *NAND* e *NOR*.

(ii) Com base na tabela construída, reescreva as definições.

(10) Complete as demonstrações dos Teoremas 1.12 e 1.13.

1.4 Predicados, Sentenças Abertas e Quantificadores

De agora em diante denotaremos por $\mathbb{N}$ o conjunto dos números naturais, por $\mathbb{Z}$ o dos números inteiros, por $\mathbb{Q}$ o conjunto dos números racionais e por $\mathbb{R}$ o conjunto dos números reais. Estes conjuntos serão considerados de conhecimento do leitor bem como intervalos de números reais e as relações de ordem "menor ou igual"($\leq$) e "maior ou igual"($\geq$) definidas sobre estes conjuntos. Maiores detalhes sobre estes conceitos podem ser vistos em [5].

Funções Proposicionais ou *Sentenças Abertas* são sentenças que envolvem pelo menos uma variável. Por exemplo, "$x > 0$", "$x = y + 3$"são sentenças abertas. Este tipo de sentença ocorre frequentemente em matemática e em programas de computação. A princípio, estas proposições não possuem valores lógicos, a menos que as variáveis assumam valores. A variável x na primeira sentença (x e y na segunda sentença) é dito *sujeito* da sentença aberta, e a propriedade "*maior que zero*"na primeira sentença é dito *predicado* da sentença aberta. Denotemos por $P(x)$: "$x > 0$" e denotemos por $Q(x, y)$ a sentença: "$x = y + 3$".

Em qualquer caso é preciso estabelecer *a priori* o conjunto U dos possíveis valores que o sujeito (variável) pode assumir. Para um elemento a do universo U, por $P(a)$ entende-se o predicado P aplicado em a, enquanto que $P(x)$ é o predicado em um elemento genérico x do universo U. Assim, $P(x)$ é o próprio predicado.

Nota: Em programas de computadores, ocorrem muitas funções proposicionais. Por exemplo, considere a sentença:

"*se* $x \geq 0$ *então* $x := x + 1$"

Quando esta proposição é encontrada ao executar o programa, o valor x neste estágio da execução do programa é colocado em $P(x)$: "$x \geq 0$". Se $P(x)$ é verdadeiro para este valor de x, a proposição $Q(x)$: "$x := x + 1$" é executada, e o valor x é substituído por $x + 1$. Se $P(x)$ é falso (ou seja: $x < 0$), a proposição $Q(x)$ não é executada e o valor x permanece para o que se segue.

Definição 1.17 Uma *sentença aberta* ou *função proposicional* sobre um conjunto não vazio U, é uma sentença que contém variáveis e que se torna uma proposição quando substituímos as variáveis por elementos do conjunto U.
Em símbolos temos:

$\boldsymbol{P(x)}$**: sentença aberta em** $\boldsymbol{U} \iff \boldsymbol{P(a)}$**: proposição para todo** $\boldsymbol{a \in U}$.

Seja $P(x)$ uma sentença aberta sobre um conjunto não vazio U. O *Conjunto Verdade* ou *Conjunto Solução* é o subconjunto de U constituído pelos elementos $a \in U$ que tornam $P(x)$ verdadeira.

Notação: $V(P(x))$ ou V_P.

Assim podemos escrever: $V_P = \{a \in U \mid P(a)\}$ e neste caso se lê: "V_P é o conjunto dos elementos $a \in U$ tal que $P(a)$ é verdadeira". Podemos também escrever: $V_P = \{x \in U \mid P(x)\}$ que se lê: V_P é o conjunto dos elementos $x \in U$ que satisfazem $P(x)$.

Exemplo (i) $A = \mathbb{R}$ e $P(x)$: "$x^2 + 2 < 0$". Então $V(P(x)) = \emptyset$ pois não existe número real x que satisfaça a desigualdade $x^2 + 2 < 0$.

(ii) $A = \mathbb{N} \times \mathbb{R}$ e $X = (x, y) \in \mathbb{N} \times \mathbb{R}$, $P(X) = P(x, y)$: "$x^2 + y^2 = 4$". Então $V_P = \{(0, -2),\ (0, 2),\ (1, -\sqrt[2]{3}),\ (1, \sqrt[2]{3}),\ (2, 0)\}$

Como vimos, atribuindo valores às variáveis que figuram em uma sentença aberta, esta se torna uma proposição. No entanto, essa não é a única forma de transformar uma sentença aberta em proposição. Há uma outra: fazendo uso dos quantificadores universal e existencial.

A *Quantificação Universal* de $P(x)$ é a proposição:

"*Para todos os valores de x no universo de discurso, $P(x)$ é verdadeira*".

Notação: $\forall x, P(x)$ ou $\forall x \in U, P(x)$.

Note que a proposição: "$\forall x,\ P(x)$" é verdadeira apenas quando $V_P = U$.

Exemplo (1) Seja $P(x)$: "$x^2 \geq x$" e o universo de discurso o conjunto $\mathbb{N}$ dos números naturais. A proposição "$\forall x, P(x)$"é verdadeira, pois, para todo número natural x, é verdadeira a desigualdade: $x^2 \geq x$.

No entanto, se o universo de discurso é o conjunto $\mathbb{R}$ dos números reais, então "$\forall x, P(x)$" é falso, pois não é verdade que $(\frac{1}{2})^2 \geq \frac{1}{2}$. Isto mostra que o valor-verdade da proposição "$\forall x, P(x)$" pode depender do universo de discurso.

Exemplo (2) Seja $U = \{1, 2, 3\}$ e $P(x)$: "$x^2 < 10$".

Então "$\forall x, P(x)$" significa: "$P(1) \wedge P(2) \wedge P(3)$".

Exemplo (3) Considere a sentença: "*Todo homem é mortal*".

O predicado de *ser mortal* está definido sobre o conjunto universo U constituído por todos os homens. Sendo assim, podemos traduzir: "$\forall x \in U,\ P(x)$" ou "$\forall x,\ P(x)$".

Definição 1.18 A *Quantificação Existencial* de $P(x)$ é a proposição

"*Existe x no universo de discurso tal que $P(x)$ é verdadeira*".

Notação: $\exists x, P(x)$ ou $\exists x \in U, P(x)$.

Note que a proposição "$\exists x,\ P(x)$" é verdadeira apenas quando V_P não é vazio.

Exemplo (1) Seja $P(x)$: "$x^2 \geq x$", definida sobre $\mathbb{R}$. Então:

"$\exists x,\ P(x)$"

significa:

"*Existe $x \in \mathbb{R}$ tal que $x^2 \geq x$*"

que é uma sentença verdadeira, pois $P(2)$ é verdadeira.

Exemplo (2) Considere a sentença aberta $Q(x)$: "$x+1 = 7$" sobre o conjunto dos números inteiros. Por "$\exists x \in \mathbb{Z} : \ Q(x)$"estamos indicando a proposição

"*Existe um inteiro* x *tal que* $x + 1 = 7$",

que é verdadeira, pois $Q(6)$ é verdadeira.

Dupla Quantificação

Muitas vezes, em matemática e em outras ciências, ocorrem sentenças abertas ou proposições com duas ou mais variáveis. Por exemplo, considere a proposição: "*Todos os alunos do Ibilce têm um computador ou têm um colega (aluno do Ibilce) que tem um computador*". Esta proposição pode ser posta em linguagem matemáti ca como segue. Seja $C(x)$: "x *tem um computador*" e "$F(x, y) : \ x$ *e* y *são colegas*", onde $x, \ y$ pertencem ao universo de discurso U constituídos pelos alunos do Ibilce. A sentença pode ser traduzida na forma:

"$\forall x \in U, \ [C(x) \ \vee \ (\exists y \in U : \ C(y) \ \wedge \ F(x, y))]$".

Exemplo (1) A proposição: "$\forall x \in \mathbb{Z}, \forall y \in \mathbb{R} : x + y = 4$" é lida do seguinte modo: "*Para todo* x *em* $\mathbb{Z}$, *para todo* y *em* $\mathbb{R}$, $x + y = 4$", ou então "*Para todo número inteiro* x *e todo número real* y, $x + y = 4$". Note que esta proposição é falsa, pois, por exemplo $P(0, 0)$ é falsa, onde $P(x, y) :$ "$x + y = 4$".

Outro modo de escrever esta proposição pode ser: "$\forall (x, y) \in \mathbb{Z} \times \mathbb{R} : x+y = 4$," que pode ser lida do seguinte modo: "*Para todo par* (x, y) *em* $\mathbb{Z} \times \mathbb{R} : x$ *mais* y *é igual a* 4".

Exemplo (2) A leitura da proposição: "$\forall x \in \mathbb{Z}, \exists y \in \mathbb{R} : x + y = 4$" é: "*Para todo* x *em* $\mathbb{Z}$ *(ou para todo inteiro* x*) existe* y *em* $\mathbb{R}$ *(ou existe um número real* y*), tal que* $x + y = 4$".

Esta proposição é verdadeira pois, para cada $x \in \mathbb{Z}$, basta tomar $y = 4 - x \in \mathbb{R}$ que temos $P(x, 4 - x)$ verdadeira, pois $P(x, 4 - x)$ é "$x + (4 - x) = 4$".

Note que na quantificação "$\forall x, \exists y : \ P(x, y)$", em geral, y fica dependendo de x e, às vezes, fica melhor ler assim: "Para *cada* $x, \ \exists y, \ P(x, y)$".

Quando invertemos os quantificadores, o sentido é outro bem

diferente, veja:

Exemplo (3) A proposição: "$\exists x \in \mathbb{Z}, \forall y \in \mathbb{R} : x + y = 4$" deve ser lida do seguinte modo:

"*Existe um inteiro* x, *para todo número real* y, $x + y = 4$".

Nesta proposição, depois da variável x deve ser entendido que existe o termo *tal que*. Assim a leitura fica:

"*Existe um inteiro* x, **tal que** *para todo número real* y : $x+y = 4$".

Assim, esta proposição é falsa, pois não existe um número inteiro x que satisfaça "$x + y = 4$" para todo número real y. Aqui o sentido é a existência de um número inteiro x fixado, tal que "$x + y = 4$" é satisfeita para todo y real. Às vezes podem existir outros elementos x que satisfazem $P(x, y)$, $\forall y$; por exemplo, a proposição: "$\exists x$, $\forall y$: $x + y^2 \geq 0$" sobre o conjunto universo dos números reais é tal que qualquer número real positivo $x = a$ fixado torna a expressão: "$a + y^2 \geq 0$ *para todo* $y \in \mathbb{R}$" verdadeira.

Finalmente a proposição:

Exemplo (4) "$\exists x \in \mathbb{Z}$, $\exists y \in \mathbb{R}$: $x + y = 4$" é verdadeira e se lê: "*Existe* $x \in \mathbb{Z}$, *existe* $y \in \mathbb{R}$ *tal que* $x + y = 4$", $P(0, 4)$ é verdadeira.

Resumindo, temos os seguintes tipos de quantificações para funções proposicionais com duas variáveis: $\forall x, \forall y, P(x, y)$; $\forall x, \exists y, P(x, y)$; $\exists x, \forall y, P(x, y)$; $\exists x, \exists y, P(x, y)$.

A quantificação de proposições pode ser estendida para sentenças abertas com mais de duas variáveis com os devidos cuidados.

Negações de Proposições Quantificadas

Para negar uma proposição quantificada, trocam-se os quantificadores e nega-se a sentença aberta $P(x)$. Em outras palavras:

$\sim [\forall x : P(x)]$ é a proposição "$\exists x : \sim P(x)$".

A negação da sentença: $\exists x : P(x)$ é a sentença "$\forall x : \neg P(x)$". Em símbolos:

$$\neg[\exists x : \ P(x)] \equiv [\forall x : \neg P(x)].$$

Exemplo (a) (i) $\sim [\exists x : \ x+1=7] \ \equiv \ (\forall x : x+1 \neq 7)$.
(ii) $\sim [\forall x : x+1=7] \ \equiv \ [\exists x : x+1 \neq 7]$.
(iii) $\sim [(\forall x \in \mathbb{Z})(\forall y \in \mathbb{R}) : x+y=4] \ \equiv \ (\exists x \in \mathbb{Z})(\exists y \in \mathbb{R}) : x+y \neq 4$.
(iv) $\sim [(\forall x \in \mathbb{Z})(\exists y \in \mathbb{R}) : x+y=4] \ = \ (\exists x \in \mathbb{Z})(\forall y \in \mathbb{R}) : x+y \neq 4$, etc..

Exemplo (b) Seja H o conjunto de todos os humanos e $P(x)$ o predicado "*x é mortal*". Então a proposição"*Todo homem é mortal*"pode ser traduzida para "$\forall x \in H : P(x)$". A negação desta sentença é: "$\exists x \in H : \ \neg P(x)$", que se lê: "*Existe um homem que não é mortal*".

Exemplo (c) Sejam $P(x)$ e $Q(x)$ respectivamente os predicados: $P(x)$: "$x \geq 0$" e $Q(x)$: "*x é um quadrado*". Então traduzimos a sentença "*todo número real positivo é um quadrado*"por

$$\text{"}\forall x \in \mathbb{R} : \ P(x) \longrightarrow Q(x)\text{"}$$

ou seja, para todo número real x, se x é positivo então x é um quadrado. Logo a negação de "*Todo número real positivo é um quadrado*"pode ser escrita do seguinte modo:

$$\begin{aligned} \sim [\forall x \in \mathbb{R} : P(x) \rightarrow Q(x)] \ &\equiv \ [\exists x \in \mathbb{R} \mid \sim (P(x) \rightarrow Q(x))] \\ &\equiv \ [\exists x \in \mathbb{R} : P(x) \wedge \sim Q(x)], \end{aligned}$$

ou seja "*Existe um número real x que é positivo e não é quadrado*"

Exemplo (d) Vamos traduzir em linguagem matemática a proposição:

"*Todo homem tem exatamente um grande amigo*"

Esta sentença pode ser reescrita como: "*Qualquer que seja o homem x, x tem exatamente um grande amigo*".

O universo de discurso é o conjunto U de todos os homens. Precisamos caracterizar o predicado "*y é o grande amigo de x*". Seja $B(x,y)$ o predicado "*y é o grande amigo de x*". Então $B(x,y)$ é caracterizado da seguinte forma: Se z é uma pessoa qualquer que não é y, então z não é o grande amigo de x.

Em símbolos:

$$\text{“}\forall z \in U,\ (z \neq y \longrightarrow \neg B(x,z))\text{”}.$$

Agora a proposição: “*Todo homem tem exatamente um grande amigo*” traduz-se por:

$$\text{“}\forall x \in U, \exists y \in U : [B(x,y)\ \wedge\ (\forall z \in U,\ z \neq y \longrightarrow \neg B(x,z))]\text{”}.$$

O símbolo $\exists!$ se lê: “*Existe um único*”. Ele é razoavelmente usado em textos matemáticos e serve, muitas vezes, para simplificar expressões. Usando-o na sentença acima podemos escrever:

$$\text{“}\forall x \in U, \exists! y \in U \mid B(x,y)\text{”},$$

que se lê: “*Para todo x pertencente a U existe um único y pertencente a U tal que* $B(x,y)$”.

1.5 Métodos de Prova

Os métodos de provas são bastante usados em ciências da computação em geral. Por eles verifica-se se um programa está correto, dando segurança ao sistema operacional, faz-se deduções na área de inteligência artificial e assim por diante. Portanto, entender as técnicas de provas é essencial tanto para a matemática como para as ciências de computação.

1.5.1 Argumentos e Regras de Inferência

Já foi mencionado que a lógica também trata das formas de argumentação e das maneiras de encadear nosso raciocínio para justificar, a partir de fatos básicos, nossas conclusões. A argumentação pode ser vista como um jogo de raciocínio, que consiste em “*combinar*”uma ou mais proposições para com elas chegar a uma conclusão. As regras desse “*jogo*”são chamadas regras de inferência. E o jogo tem a seguinte forma:

Começam com um conjunto de proposições que chamaremos *premissas*. O objetivo do jogo é aplicar as regras de modo que se obtenha alguma outra proposição dada (conclusão desejada).

O conjunto de premissas corresponde à posição inicial de um jogador no jogo. Por uma sucessão de jogadas, sancionadas por

regras, chegamos à posição de triunfo: a conclusão buscada. Como em todo jogo, as regras permitem jogadas soltas. O problema consiste, então, em aprender a executar jogadas pertinentes.

O jogo não terá validade quando a conclusão apresentada não for uma conseqüência lógica das premissas, isto é, quando as premissas não implicarem logicamente a conclusão. Quando isto acontece? Quando há falta de premissas ou quando não há falta de premissas, mas existe entre as mesmas uma ou mais que não sejam compatíveis com as demais.

Um *argumento* ou *forma de argumentação* é dito *válido* (*válida*) se quando todas as hipóteses (*premissas*) são verdadeiras, a conclusão também é verdadeira. Conseqüentemente, demonstrar que Q segue logicamente das premissas $p_1,\ p_2, \ldots, p_n$ é o mesmo que demonstrar a implicação

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Longrightarrow Q.$$

Quando todas as proposições usadas em um argumento válido são verdadeiras, isto nos leva a uma conclusão verdadeira, e é este tipo de argumentação que nos interessa dentro de qualquer teoria. Entretanto um argumento, ou forma de argumentação válida pode nos levar a uma conclusão incorreta se uma ou mais proposições falsas forem usadas no argumento.

Observação 1.19 *:* No caso de uma argumentação podem ocorrer premissas supérfluas que impeçam a nossa conclusão. São premissas para outros argumentos ou premissas que seriam conclusões para outras premissas dadas.

Vejamos alguns exemplos de argumentação:

Alguém diz: "— *Maria foi para a Universidade*".
O interlocutor (solicitando justificativa) indaga: "– *Como sabe*?"
"– *Ora, porque se fosse ao cinema telefonaria.*"
Podemos "*condensar*"esse diálogo da seguinte forma:
– *Maria vai ao cinema ou à Universidade.*
– *Se for ao cinema, telefonará.*

– *Maria não telefonou.*
Conclusão: – *Maria foi à Universidade.*

As três primeiras linhas são as premissas e a última é a conclusão. Isto é um argumento.

Mais um exemplo:
— *Se eu fosse presidente, seria famoso*
— *Eu não sou presidente.*
Conclusão: — *Eu não sou famoso.*

Observe que o primeiro argumento apresentado é válido, enquanto o segundo não.

Assim como no estudo dos valores-verdades de proposições compostas, para verificar as argumentações fica mais fácil se trabalharmos com símbolos, desde que a única coisa que importar para a validade do argumento sejam os valores-verdade das proposições.

Deste modo, numa argumentação indicamos as premissas por $\boldsymbol{p_1, \ldots, p_n}$ e a conclusão por $\boldsymbol{c}$. O argumento feito $\boldsymbol{a}$, para obter $\boldsymbol{c}$ a partir das premissas $\boldsymbol{p_1, \ldots, p_n}$ é indicado por

$$\boldsymbol{p_1, p_2, \ldots, p_n \vdash c.}$$

Assim, o primeiro argumento pode ser representado por

p: *Maria vai à Universidade.*
q: *Maria vai ao cinema.*
r: *Maria telefona.*

$$\begin{array}{l} p_1 : p \vee q \\ p_2 : q \rightarrow r \\ \hline p_3 : \sim r \\ \hline c : p \end{array}$$

e então $p_1, p_2, p_3 \vdash c$ ou ainda $(p \vee q),\ (q \rightarrow r),\ (\sim r) \vdash p$.

Podemos testar a validade de um argumento. Para fazê-lo levamos em conta a seguinte definição.

Definição 1.20 *Um argumento $p_1, \ldots, p_n \vdash q$ é válido se q for verdadeiro sempre que $p_1, \ldots, p_n$ forem verdadeiros. Em outras*

palavras, se $(p_1 \wedge \ldots \wedge p_n) \rightarrow q$ *for uma tautologia, ou equivalentemente* $(p_1 \wedge \ldots \wedge p_n) \Rightarrow q$.

Exercício: (1) Teste a validade do primeiro argumento apresentado.
(2) Represente por símbolos o segundo argumento e verifique a sua validade.

Observe que, quanto maior for o número de premissas envolvidas, maior será o seu trabalho. Se você tiver n premissas dadas, quantas linhas aparecerão em sua tabela?

Para cada argumento apresentado você pode começar por testar sua validade. Há, no entanto, certos tipos de argumentação bastante comuns que são conhecidos como **Regras de Inferência**, que passaremos a apresentar a seguir:

Regra 1: ***Adjunção* (*Adj*)**

Dada duas proposições como premissas p e q, podemos concluir a proposição composta $p \wedge q$. Por exemplo, dada:

p: *Jorge é adulto*
q: *Maria é criança,*

podemos juntá-las e obter c: *Jorge é adulto e Maria é criança.* Em símbolos escrevemos

$$\begin{array}{l} p \\ q \\ \hline p \wedge q \end{array}$$

As demais regras serão apresentadas de forma simbólica, e sugerimos ao leitor que enriqueça cada situação com um exemplo.

Regra 2: ***Simplificação* (*S*)** são as implicações do tipo $(p \wedge q) \Longrightarrow p$. Elas são descritas como argumentos por

$$\frac{p \wedge q}{p} \quad \text{ou} \quad \frac{p \wedge q}{q}$$

Regra 3: ***Adição* (*A*)** são as implicações do tipo $p \Rightarrow (p \vee q)$. Elas são representadas na forma de argumento por:

$$\frac{p}{p \vee q}$$

Regra 4: ***Modus Ponens* (*MP*)** São as implicações do tipo $[(p \rightarrow q) \wedge p] \Longrightarrow q$. Elas são representadas na forma de argumento por:

$$\begin{array}{l} p \rightarrow q \\ \underline{p \qquad} \\ q \end{array}$$

Regra 5: ***Modus Tollens* (*MT*)** são as implicações do seguinte tipo $[(p \rightarrow q) \wedge (\sim q)] \Longrightarrow \sim p$. Elas são representadas na forma de argumento por:

$$\begin{array}{l} p \rightarrow q \\ \sim q \\ \hline \sim p \end{array}$$

Regra 6: ***Dupla negação* (*DN*)** são as implicações do tipo $[\sim (\sim p) \Longrightarrow p]$ (ou $[p \Longrightarrow \sim (\sim p)]$). Na forma de argumento, podemos representá-las por:

$$\frac{\sim (\sim p)}{p} \quad \text{ou} \quad \frac{p}{\sim (\sim p)}$$

Regra 7: ***Regra de Absorção* (*RA*)** são as implicações do tipo $[p \rightarrow (p \wedge q)] \Longrightarrow [p \rightarrow q]$. Elas são representadas na forma de argumento por:

$$\frac{p \rightarrow (p \wedge q)}{p \rightarrow q}$$

Regra 8: ***Silogismo Hipotético* (*SH*)** são as implicações do tipo $[(p \rightarrow q) \wedge (q \rightarrow r)] \Longrightarrow p \rightarrow r$. Elas são representadas na forma de argumento por:

$$\frac{\begin{array}{c} p \to q \\ q \to r \end{array}}{p \to r}$$

Regra 9: **Silogismo Disjuntivo (*SD*)** são as implicações do tipo $[(p \vee q) \wedge \neg p] \Longrightarrow q$. Elas são representadas na forma de argumento por:

$$\frac{\begin{array}{c} p \vee q \\ \sim p \end{array}}{q}$$

Regra 10: ***Regras do Bicondicional* (*RBC*)**

$$(a) \quad \frac{\begin{array}{c} p \to q \\ q \to p \end{array}}{p \leftrightarrow q} \qquad (b) \quad \frac{p \leftrightarrow q}{(p \to q) \wedge (q \to p)}$$

são as implicações:
(a) $[(p \to q) \wedge (q \to p)] \Longrightarrow (p \leftrightarrow q)$
(b) $[(p \leftrightarrow q) \Longrightarrow [(p \to q) \wedge (q \to p)]$.

Regra 11: ***Dilema Construtivo* (*DC*)** é dada por implicações do tipo $[(p \to q) \wedge (r \to s) \wedge (p \wedge r)] \Longrightarrow (q \wedge s)$, cuja representação na forma de argumento é:

$$\frac{\begin{array}{c} p \to q \\ r \to s \\ p \wedge r \end{array}}{q \wedge s}$$

Regra 12: ***Dilema Destrutivo* (*DD*)** são implicações do tipo $[(p \to q) \wedge (r \to s) \wedge (\sim q \wedge \sim s)] \Longrightarrow \sim p \wedge \sim r$. Elas são representadas na forma de argumento por:

$$\frac{\begin{array}{c} p \to q \\ r \to s \\ \sim q \wedge \sim s \end{array}}{\sim p \wedge \sim r}$$

Exemplo (1). "*Se* $2 > 3$ *então* $2^2 > 3^2$"
é um argumento válido, baseado no Modus Ponens. No entanto, a conclusão do argumento $4 > 9$ é falso, pois $4 < 9$. Isto segue do fato que a proposição falsa "$2 > 3$" foi usada no argumento e daí a conclusão do argumento pode ser (e neste caso é) falsa. Claro que premissas falsas não serão aceitas em nenhum argumento, para que nossa teoria fique consistente.

Exemplo (2). Considere as premissas: "*Não está ensolarada esta tarde e ontem fez frio*". "*Iremos à praia somente se esta tarde estiver ensolarada*". "*Se não formos à praia, iremos passear de barco*"e "*se formos passear de barco, estaremos de volta em casa ao por do sol*". Conclua que "*estaremos de volta em casa ao por do sol*".

Solução:

Sejam p a proposição: "*está ensolarado esta tarde*", q: "*ontem fez frio*", r: "*Iremos à praia*", s: "*iremos passear de barco*"e finalmente t: "*estaremos de volta em casa ao por do sol*". O que se quer é construir um argumento para mostrar que estas hipóteses nos garante que a proposição t é verdadeira. Temos as premissas: $p_1 : \neg p \wedge q$, $p_2 : r \to p$, $p_3 : \neg r \to s$, e $p_4 : s \to t$ e queremos verificar que $(p_1 \wedge p_2 \wedge p_3 \wedge p_4) \longrightarrow t$ é verdadeira. Veja a tabela.

Passos	Justificativa
1. $\neg p \wedge q$	(hipótese)
2. $\neg p$	(simplificação)
3. $r \to p$	(hipótese)
4. $\neg r$	(modus tollens de 2 e 3)
5. $\neg r \to s$	(hipótese)
6. s	(modus ponens de 4 e 5)
7. $s \to t$	(hipótese)
8. t	(modus ponens de 6 e 7).

Logo a proposição t: "*estaremos de volta em casa ao por do sol*"é verdadeira.

Exemplo (3). Mostre que as hipóteses: "*Se você me enviar os da-*

dos por uma mensagem de e-mail, então eu terminarei de escrever o trabalho". "*Se você não me enviar os dados em uma mensagem de e-mail, então irei dormir mais cedo*". E "*se eu for dormir mais cedo, amanhã acordarei disposto para concluir o trabalho*", nos leva à conclusão de que "*Se eu não terminar o trabalho então amanhã acordarei disposto para concluí-lo*".

Solução: De fato, considere as proposições p: "*Você me envia os dados por e-mail*", q: "*Eu termino de escrever o trabalho*", r: "*Vou dormir mais cedo*", s: "*Acordarei disposto para concluir o trabalho*". Temos os passos:

Passos	Justificativa
1. $p \to q$	(hipótese)
2. $\neg q \to \neg p$	(contra recíproca de 1)
3. $\neg p \to r$	(hipótese)
4. $\neg q \to r$	(silogismo hipotético de 2 e 3)
5. $r \to s$	(hipótese)
6. $\neg q \to s$	(silogismo hipotético de 4 e 5)

Logo temos $\neg q \to s$, que é a conclusão desejada.

Regra 13: ***Resolução***

Muitos programas de computador usam a implicação lógica

$$[(p \vee q) \wedge (\neg p \vee r)] \Longrightarrow (q \vee r)$$

que é representada na forma de argumento por

$$\begin{array}{l} p \vee q \\ \sim p \vee r \\ \hline q \vee r \end{array}$$

e é conhecida como *resolução*.
A conclusão "$q \vee r$" é chamada de *resolvente*. No caso em que r é a própria q, ou r é uma contradição, a resolvente é q, pois $q \vee q \equiv q$ e $q \vee C \equiv q$. Em resumo:

$$[(p \vee q) \wedge (\neg p \vee q)] \rightarrow q \qquad \text{e} \qquad [(p \vee q) \wedge \neg p] \rightarrow q$$

Exemplo. "*John está esquiando ou não está nevando*" e "*está nevando ou Smith está jogando hóquei*". Isto implica que "*John está esquiando ou Smith está jogando hóquei*".

Esta regra tem papel importante em linguagens de programação baseadas em regras lógicas, tais como o Prolog (onde são aplicadas a resolução para proposições quantificadas).

Falácias

Muitas argumentações são baseadas em argumentos errados. A princípio parecem regras de inferência, mas estão baseadas em contingências em vez de tautologias. A proposição

$$[(p \rightarrow q) \wedge q] \longrightarrow p$$

não é uma tautologia, pois é falsa quando p é falsa e q é verdadeira. No entanto, existem muitos argumentos errados que a tratam como se fosse uma tautologia.

Este tipo de raciocínio (ou argumentação) incorreto é chamado de

Falácia da afirmação da conclusão.

Exemplo (a) "*Se chover, então faz frio*". Caso esteja frio, não podemos concluir que choveu, como as vezes o fazemos!!
(b) Falácia Política: "*Se aplicarmos recursos na educação, o ensino melhorará*". Como neste ano o ensino está bom, então o governo, que discursa, diz que isto prova que tem investido pesados recursos na educação!!!
(c) "*Se você faz todos os exercícios das listas de AFC, então você passa em AFC*" e "*você passou em AFC*". Isto não implica que "*Você fez todos os exercícios da lista de AFC*"!!!

Do mesmo modo a proposição

$$Q : \text{“}[(p \rightarrow q) \wedge \neg p] \longrightarrow \neg q\text{”}$$

não é tautologia, desde que Q é falsa quando p é falsa e q é verdadeira. Portanto muitas argumentações são incorretas quando a usam como uma regra de inferência. Este tipo de falácia é chamada de

Falácia por negação da hipótese.

(d). "*Se você fez todos os exercícios das listas de AFC, então você aprendeu AFC*", e "*você não fez todos os exercícios da lista de AFC*". Destas premissas não podemos concluir que "*Você não aprendeu AFC*"!!!

A seguir resumimos numa tabela as regras de inferência:

Tabela 1 | **Regras de Inferência**

Regras de Inferência	Tautologia	Nome
p q $\therefore\ p \wedge q$	$((p) \wedge (q)) \rightarrow p \wedge q$	Conjunção ou Adjunção
$p \wedge q$ $\therefore\ p$	$(p \wedge q) \rightarrow p$	Simplificação
p $\therefore\ p \vee q$	$p \rightarrow (p \vee q)$	Adição
$p \rightarrow q$ p $\therefore\ q$	$[(p \rightarrow q) \wedge p] \rightarrow q$	Modus Ponens
$p \rightarrow q$ $\sim q$ $\therefore\ \sim p$	$[(p \rightarrow q) \wedge \sim q] \rightarrow \sim p$	Modus Tollens
$\sim (\sim p)$ $\therefore\ p$	$\neg(\neg p) \rightarrow p$	Dupla Negação
$p \rightarrow (p \wedge q)$ $\therefore\ p \rightarrow q$	$[p \rightarrow (p \wedge q)] \rightarrow [p \rightarrow q]$	Absorção
$p \rightarrow q$ $q \rightarrow r$ $\therefore\ p \rightarrow r$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Silogismo Hipotético
$p \vee q$ $\sim p$ $\therefore\ q$	$[(p \vee q) \wedge \sim p] \rightarrow q$	Silogismo Disjuntivo
$p \rightarrow q$ $q \rightarrow p$ $\therefore\ p \longleftrightarrow q$	$[(p \rightarrow q) \wedge (q \rightarrow p)] \rightarrow [p \longleftrightarrow q]$	Bicondicional
$p \longleftrightarrow q$ $\therefore\ (p \rightarrow q) \wedge (q \rightarrow p)$	$[p \longleftrightarrow q] \rightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$	Bicondicional

Tabela 1 | **Regras de Inferência**

Regras de Inferência	Tautologia	Nome
$p \to q$ $r \to s$ $\underline{p \wedge r}$ $\therefore \quad q \wedge s$	$[(p \to q) \wedge (r \to s) \wedge (p \wedge r)] \to [q \wedge s]$	Dilema Construtivo
$p \to q$ $r \to s$ $\underline{\neg q \wedge \neg s}$ $\therefore \quad \neg p \wedge \neg r$	$[(p \to q) \wedge (r \to s) \wedge (\neg q \wedge \neg s)] \longrightarrow [\neg p \wedge \neg r]$	Dilema Destrutivo
$p \vee q$ $\underline{\sim p \vee r}$ $\therefore \quad q \vee r$	$[(p \vee q) \wedge (\sim p \vee r)] \to (q \vee r)$	Resolução

Parte do teorema que segue já foi feito, em alguns exemplos, usando tabelas-verdade. Vamos demonstrá-lo como aplicação das regras de inferência.

Teorema 1.21 *As seguintes proposições são logicamente equivalentes.*

(a) $P \longrightarrow Q$ *é uma tautologia.*

(b) $\neg Q \longrightarrow \neg P$, *é uma tautologia (Contra-Recíproca).*

(c) $\neg P \vee Q$ *é uma tautologia.*

(d) $P \wedge \neg Q$ *é uma contradição (Redução ao Absurdo).*

Demonstração: Temos que demonstrar que **(a)**, **(b)**, **(c)** e **(d)** são logicamente equivalentes, e para isto basta demonstrar que **(a)**$\Rightarrow$ **(b)**$\Rightarrow$**(c)**$\Rightarrow$**(a)** e **(c)** $\Leftrightarrow$ **(d)**.

Façamos **(a)**$\Rightarrow$**(b)**.

Temos que demonstrar que, se $\neg Q$ é verdadeiro então $\neg P$ é verdadeiro, tendo como hipótese que $P \to Q$ é uma tautologia. Suponhamos que $\neg Q$ é verdadeiro. Como, por hipótese, $P \to Q$ é tautologia, segue que $\sim P$ é verdadeiro pela regra de inferência Modus Tollens. Logo $\sim Q \to \sim P$ é uma tautologia. Em outras palavras, **(a)**$\Longrightarrow$ **(b)**.

Agora façamos **(b)**$\Rightarrow$**(c)**. A hipótese é que $\neg Q \to \neg P$ é uma tautologia e devemos demonstrar que $\sim P \vee Q$ é uma tautologia. Façamos por casos. (1). Se Q é verdadeira, pela regra da adição $\neg P \vee Q$ é verdadeira.

(2) Se Q é falsa, então $\neg Q$ é verdadeira, e como por hipótese $\neg Q \rightarrow \neg P$ é verdadeira, por modus ponens $\neg P$ é verdadeira. Novamente por adição $\neg P \vee Q$ é verdadeira. De (1) e (2) temos $\neg P \vee Q$ é uma tautologia.

Outro modo de provar que **(b)** implica **(c)** é usar que $\sim P \vee Q \equiv \sim Q \rightarrow \sim P$. Como $\sim Q \rightarrow \sim P$ é tautologia, $\sim P \vee Q$ também é.

(c)⇔(d). Segue das Leis de De Morgan e do fato que P é uma tautologia se e somente se $\sim P$ é uma contradição.

(c)⇒(a). Queremos provar que Q é verdadeira quando P é verdadeira, tendo que $\neg P \vee Q$ é verdadeira. Suponhamos que P é verdadeira. Por silogismo disjuntivo concluimos que Q é verdadeira. Isto concluir a prova do Teorema. □

Nota: Note que se uma das ocorrências **(a)**, **(b)**, **(c)** ou **(d)** for verdadeira, então todas as ocorrências serão verdadeiras. De fato, construindo uma tabela-verdade eliminando a ocorrência P verdadeiro e Q falso temos:

P	Q	$\neg Q$	$\neg P$	$P \rightarrow Q$	$\neg Q \rightarrow \neg P$	$\neg P \vee Q$	$P \wedge \neg Q$
V	V	F	F	V	V	F	V
F	V	F	V	V	V	F	V
F	F	V	V	V	V	F	V

Segue-se que, quando as equivalências lógica $P \rightarrow Q \equiv \sim Q \rightarrow \sim P \equiv \sim P \vee Q$ são tautologias, "sua negação" $P \wedge \sim Q$ é uma contradição. A ocorrência P verdadeiro e Q falso nos dá que todas as proposições em (a), (b), (c) e (d) são falsas. Logo (a), (b), (c) e (d) continuam logicamente equivalentes, o que já era esperado. Com isto, o Teorema também fica demonstrado.

Observação 1.22 - Devido às condições equivalentes do teorema, se quisermos demonstrar um teorema da forma $P \Longrightarrow Q$, podemos usar **(a)** e demonstrar diretamente, deduzindo Q tendo P como proposição verdadeira. Se for viável, podemos usar a contra-recíproca (caso **(b)**), deduzindo $\neg P$ tendo $\neg Q$ como proposição verdadeira. Podemos ainda fazer a demonstração do teorema "$P \Longrightarrow Q$" por redução ao absurdo, também chamado por contradição,

supondo que P e $\neg Q$ são proposições verdadeiras na teoria e, a partir daí, deduzir uma contradição na teoria. Note que neste caso P e $\neg Q$ não podem ser proposições verdadeiras ao mesmo tempo na teoria e, tendo P como uma proposição verdadeira, somos obrigados a aceitar Q como uma proposição verdadeira, chegando ao que foi afirmado. Mais ainda, esta demonstração é aceita aqui porque estamos admitindo o princípio do terceiro excluído: se $\neg Q$ é falsa então Q é verdadeira. Se não estivéssemos admitindo este princípio, o fato de $\neg Q$ nos dar uma contradição não significaria que Q é verdadeira, pois há outras ocorrências como valores-verdade para Q.

Estes tipos de demonstrações, exceto o caso direto, embora muitas vezes útil para resolver o problema imediatamente, levam consigo o péssimo defeito de não ser uma demonstração dita construtiva, que não dá um método de construir passo a passo a veracidade da Tese a partir da Hipótese dada. Existem áreas da matemática e/ou escolas de filosofia da matemática que não aceitam estes tipos de demonstrações; ou por filosofia, ou porque usam lógicas não clássicas, nas quais não cabe tal argumento.

Exemplo (a). Considere a sentença: "*Se* $a = 2$ *então* $a^2 = 4$".

Esta proposição é (logicamente) equivalente às seguintes proposições: "*Se* $a^2 \neq 4$ *então* $a \neq 2$" (Contra-recíproca); "*É falso que* $a = 2$ *e* $a^2 \neq 4$" (Contradição); "*É verdade que* $a \neq 2$ *ou* $a^2 = 4$".

Exemplo (b) APLICAÇÃO - Para números $a,\ b \in \mathbb{Z}$ dizemos que a divide b e denotamos por $a|b$ se existe $q \in \mathbb{Z}$ tal que $b = aq$. Caso contrário, denotamos por $a \nmid b$. Dizemos também que $b \in \mathbb{Z}$ é par se $2|b$, ou seja, se $b = 2q,\ q \in \mathbb{Z}$. Caso contrário, dizemos que b é ímpar. Neste caso, $b = 2q + 1,\ q \in \mathbb{Z}$. (Veja mais sobre a relação de divisibilidade no próximo capítulo). Agora tente demonstrar a seguinte proposição diretamente na forma que está no enunciado.

$\mathbf{P}_1$ - "*Se* $8 \nmid (a^2 - 1)$ *então* a *é par*". Prove e convença-se de que é bem mais simples a prova da seguinte proposição logicamente equivalente a esta

$\mathbf{P}_2$ - "*Se* a *é ímpar então* $8|(a^2 - 1)$".

1.5.2 Regras de Inferência para Proposições Quantificadas

As regras de inferência para proposições quantificadas também são extensivamente usadas em argumentos matemáticos, muitas vezes sem ser explicitamente mencionadas.

O *Universal Instantâneo* é a regra de inferência usada para concluir que $P(c)$ é verdadeiro (onde c é um elemento particular do universo de discurso), tendo "$\forall x\ P(x)$".

Por exemplo, por esta regra de inferência podemos concluir que "*João é mortal*" tendo que "*Todo homem é mortal*"; podemos concluir que $(-1)^2 \geq 0$ tendo que "*para todo* x *em* $\mathbb{R}$, $x^2 \geq 0$".

A *Generalização Universal* é a regra de inferência que nos garante que "$\forall x\ P(x)$" é verdadeira, dada a premissa (proposição inicial, hipótese) que $P(c)$ é verdadeira para cada elemento c no universo de discurso. Assim, ao selecionar um elemento arbitrário e não específico c no universo de discurso e provar que $P(c)$ é verdadeiro, pode-se concluir que "$\forall x\ P(x)$" é verdadeira, pois c é um elemento arbitrário.

Esta regra é usada implicitamente em muitas demonstrações em matemática e é raramente mencionada explicitamente.

O *Existencial Instantâneo* é a regra que nos permite concluir que existe um elemento particular c no universo de discurso para o qual $P(c)$ é verdadeiro. Em geral, não sabemos qual é o elemento c que satisfaz $P(x)$, sabemos apenas que ele existe. Desde que existe, damos um nome a ele: c e continuamos o nosso argumento.

A *Generalização Existencial* é a regra de inferência que é usada para concluir que "$\exists x\ P(x)$" quando é sabido que existe um elemento particular c no universo de discurso que satisfaz $P(x)$ (isto é: $P(c)$ é verdadeira). Em outras palavras, se sabemos que existe (ou conseguimos) um elemento c no universo de discurso, tal que $P(c)$ é verdadeira, então podemos concluir que "$\exists x\ P(x)$" é verdadeira. Em resumo, temos a tabela.

Tabela 2	**Regras de Inferência para Proposições Quantificadas**

Regras de Inferência	Nome
$\underline{\forall x\ P(x)}$ $\therefore\ P(c)$	Universal Instantâneo
$\underline{P(c)$ para c: arbitrário$}$ $\therefore\ \forall x\ P(x)$	Generalização Universal
$\underline{\exists x\ P(x)}$ $\therefore\ P(c)$, para algum c	Existencial Instantâneo
$\underline{P(c)$ para algum $c$$}$ $\therefore\ \exists x\ P(x)$	Generalização Existencial

Exemplo - Mostre que as premissas: "*Algum aluno desta classe não leu o livro-texto*"e "*Todos os alunos desta classe foram aprovados*". implicam que: "*Algum aluno desta classe foi aprovado sem ter lido o livro-texto*".

Solução: Sejam $C(x)$: "*x está nesta classe*", $L(x)$: "*x leu o livro texto*", e $P(x)$: "*x foi aprovado*". Temos os passos

(1) $\exists x,\ (C(x) \wedge \neg L(x))$

(2) $\forall x,\ (C(x) \rightarrow P(x))$ e queremos

(3) $\exists x,\ (P(x) \wedge \neg L(x))$.

(a) De (1) temos $C(a) \wedge \sim L(a)$ para algum a	Existencial Instantâneo
(b) De (2) temos $C(a) \rightarrow P(a)$	(Universal Instantâneo)
(c) $C(a)$	(simplificação de (a))
(d) $P(a)$	(modus ponens de (b) e (c))
(e) $P(a) \wedge \sim L(a)$	(conjunção de (d) e (a))
(f) $\exists x\ (P(x) \wedge \sim L(x))$	(generalização existencial)

O item (f) é exatamente o que queríamos.

Nota (1) Os argumentos matemáticos, muitas vezes, incluem passos que envolvem regras de inferência para proposições e para quantificadores ao mesmo tempo. Por exemplo, a regras universal instantâneo e modus ponens muitas vezes são usadas juntas. Quando

elas são combinadas, a hipótese "$\forall x\ P(x) \rightarrow Q(x)$" e $P(c)$, onde c é um elemento no universo de discurso, mostra que a conclusão $Q(c)$ é verdadeira.

Nota (2) Para os teoremas em matemática que afirmam que uma determinada propriedade vale para todos os elementos de um conjunto, o quantificador universal deveria aparecer em algum instante no corpo do enunciado. Mas, às vezes para se ter uma escrita mais limpa, ele é costumeiramente omitido desde que não dê à sentença um sentido diferente daquela que de fato se quer dizer com o uso do quantificador. Por exemplo, a proposição "*Se* $x > y$, *onde* x *e* y *são números naturais, então* $x^2 > y^2$", significa:

"*Para todos números naturais* x *e* y, *se* $x > y$, *então* $x^2 > y^2$".

Em símbolos:

$$\forall x \in \mathbb{N}, \forall y \in \mathbb{N},\ x > y \longrightarrow x^2 > y^2.$$

Além disso, quando um destes teoremas é provado, a regra de generalização universal é usada muitas vezes sem fazer menção explicita. O primeiro passo da prova usualmente envolve a seleção de um elemento genérico do universo de discurso. Então demonstra-se que este elemento tem a propriedade em questão. Como o elemento é genérico, a generalização universal implica que o teorema vale para todos os elementos do universo de discurso.

Nas seções subseqüentes, seguiremos a convenção usual e nem sempre faremos menção explícita ao uso da quantificação universal ou generalização universal. No entanto, ficará claro quando estas regras de inferência estão sendo implicitamente aplicadas.

1.5.3 Métodos de Demonstração de Teoremas

Uma importante questão em matemática é saber quando um argumento está correto. Outra é saber quais métodos podem ser usados na construção de argumentos matemáticos.

Um *teorema* é uma proposição que pode ser demonstrada que é verdadeira. Em outras palavras, é uma *Proposição Verdadeira*. As proposições verdadeiras que são importantes dentro de uma teoria matemática são destacadas como:

Teoremas: são Proposições verdadeiras, fortes e centrais na teoria.

As proposições mais simples são classificadas em *Proposições* (propriamente ditas), *Lemas* em geral, são proposições simples de uso restrito na teoria, normalmente servem de preparação para teoremas que seguem, e *Corolários* são consequências mais ou menos imediatas de teoremas ou Proposições anteriores.

Às vezes o Lema é auto-suficiente e forte por si só. Um exemplo é o *Lema de Zorn*. Um exemplo de teorema é o *Teorema Fundamental do Cálculo*. Quando estes elementos estão bem postos dentro de uma teoria, os teoremas resumem bem os resultados mais importantes da Teoria.

Em geral os enunciados que aparecem nos teoremas são do tipo $P \Longrightarrow Q$ (ou $P \Longleftrightarrow Q$), mas qualquer que seja o enunciado entende-se que ele é uma proposição verdadeira. Se o enunciado é do tipo $P \Longrightarrow Q$, então P é dito *hipótese* e Q é dito *tese* do teorema. Assim a *demonstração* do teorema consiste em deduzir logicamente que $P \longrightarrow Q$ é uma tautologia. Em outras palavras, concluir que Q é uma proposição verdadeira supondo que P é verdadeira.

Isto é feito através de uma seqüência lógica dedutiva, onde se passa de proposição verdadeira à proposição verdadeira até obter Q. Isto é chamado de *Prova* ou *Demonstração* do teorema, e a seqüência de proposições que foi usada na prova forma o argumento. Com isto temos provado o teorema: $P \Longrightarrow Q$.

Se o enunciado for da forma $P \Longleftrightarrow Q$, deve-se provar também $Q \Longrightarrow P$. Um exemplo de teorema da forma $P \Longrightarrow Q$ é:

"Se $f : [a, b] \to \mathbb{R}$ é uma função contínua, então f possui máximo e mínimo em $[a, b]$".

(**Nota**: Note que usamos "*se... então...*"em vez do símbolo $\Longrightarrow$. Em geral é este o procedimento feito no enunciado do teorema para não carregá-lo demais com o símbolo $\Longrightarrow$. No entanto, deve-se entender que o enunciado é uma implicação lógica e ela deve ser provada. O mesmo vale para o símbolo $\Longleftrightarrow$ que é trocado pela escrita "*se, e somente se*", no corpo do enunciado).

Para fazer uma demonstração, ou construir um método de demonstração, é necessário derivar novas proposições de outras proposições da teoria. As proposições usadas na demonstração incluem os *Axiomas* ou *Postulados* que são proposições inicialmente aceitas como verdadeiras na teoria, e a hipótese do teorema.

Pode ser muito difícil provar teoremas e, em geral, vários métodos são necessários para se chegar a uma conclusão desejada. Pelo fato de que muitos teoremas são implicações, as técnicas para provar implicações são importantes. Relembremos que $P \to Q$ é verdadeira, a menos que P é verdadeira e Q é falsa. Assim, para demonstrar que $P \Longrightarrow Q$ (ou que $P \to Q$ é uma tautologia) é necessário (e também suficiente) provar apenas que Q é verdadeira se P for verdadeira. Segue algumas técnicas comuns para demonstrar implicações.

(A) Demonstração Direta

A implicação $P \Longrightarrow Q$ pode ser provada supondo que P é verdadeira e deduzindo que Q é verdadeira, fazendo uso das regras de inferência e usando teoremas já demonstrados. Isto mostra que a combinação P verdadeira e Q falsa nunca ocorre. Portanto $P \Longrightarrow Q$. Uma demonstração deste tipo é chamada *Demonstração Direta.* Veja Teorema 1.21(a).

Exemplo (A) Demonstre diretamente que: "*Se n é um inteiro ímpar, então n^2 é ímpar*".

Solução: Por definição, um inteiro n é *par* se existe um inteiro k tal que $n = 2k$, e n é *ímpar* se existe um inteiro k tal que $n = 2k+1$. (Note que um inteiro ou é par ou é ímpar).

Suponhamos que a hipótese da implicação é verdadeira, ou seja, n é ímpar. Então $n = 2k + 1$, onde k é um inteiro. Segue-se que $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Portanto, n^2 é um inteiro ímpar (pois é duas vezes um inteiro mais um).

(B) Demonstração por Contra Recíproca

A implicação $P \Longrightarrow Q$ é logicamente equivalente a sua contra recíproca $\sim Q \Longrightarrow \sim P$. Veja Teorema 1.21(b). Assim, se provarmos diretamente que $\sim Q \Longrightarrow \sim P$, dizemos que provamos que $P \Longrightarrow Q$ por contra recíproca.

Exemplo (B) Prove: "*$3n + 2$ é ímpar, então n é ímpar*".

Solução: Suponhamos que a tese do teorema é falsa. Então $n = 2k$ para algum inteiro k. Segue-se que $3n+2 = 3.2k+2 = 2(3k+1)$. Logo $3n + 2$ é par. Conseqüentemente $3n + 2$ não é ímpar. Como a negação da tese implica que a hipótese é falsa, a implicação original

é verdadeira.

(C) Demonstração por Vacuidade

Suponhamos que a hipótese P da implicação $P \Longrightarrow Q$ a ser demonstrada é falsa. Como $f \rightarrow v$ ou $f \rightarrow f$ são verdadeiras, segue-se que $P \rightarrow Q$ é verdadeira, qualquer que seja o valor-verdade da proposição Q. Conseqüentemente, se P é falso, então a demonstração de $P \Longrightarrow Q$ é chamada de *Prova por Vacuidade*. Este tipo de prova é muitas vezes usado para estabelecer casos especiais de teoremas.

Exemplo (C) Considere a função proposicional definida sobre o conjunto dos números naturais: $P(n)$: "*Se* $n > 1$, *então* $n^2 > n$". Vamos demonstrar que $P(0)$ é verdadeira. $P(0)$: "*Se* $0 > 1$, *então* $0^2 > 0$". Como "$0 > 1$" é falso, segue-se por vacuidade que $P(0)$ é verdadeira. (Note que $0^2 > 0$ é falso, mas como $0 > 1$ também é falso, então $0 > 1 \Longrightarrow 0^2 > 0$").

(D) Demonstração Trivial

Quando a conclusão Q da implicação $P \Longrightarrow Q$ é verdadeira, então $P \rightarrow Q$ é verdadeira qualquer que seja o valor-verdade de P. Assim, se sabemos que Q é verdadeiro, independente de P, a demonstração de $P \Longrightarrow Q$ é dita *Demonstração Trivial*. Essas demonstrações muitas vezes aparecem em casos especiais ou particulares de um teorema, por exemplo, quando se faz demonstrações por indução matemática.

Exemplo (D) Seja $P(n)$ a função proposicional: "*Se* a *e* b *são inteiros positivos com* $a \geq b$, *então* $a^n \geq b^n$". Vamos demonstrar que $P(0)$ é verdadeira.

$P(0)$ é a seguinte proposição: "*Se* a *e* b *são inteiros positivos com* $a \geq b$, *então* $a^0 \geq b^0$".

Desde que $a^0 = b^0 = 1$, segue-se que $P(0)$ é verdadeira independente das restrições sobre a e b. Este é um exemplo de demonstração trivial.

(E) Demonstração por Contradição ou Redução ao Absurdo

Um outro método usado para provar teoremas é a *Demonstração por Contradição* ou por *Redução ao Absurdo*. Se o

teorema é do tipo $P \Longrightarrow Q$, o método consiste em supor que $P \wedge \neg Q$ é verdadeiro e daí derivar na teoria uma contradição, em geral do tipo $r \wedge \neg r$. Logo $P \wedge \neg Q$ tem que ser falso. Como $\neg(P \to Q) \equiv P \wedge \neg Q$ segue que $P \to Q$ é verdadeiro. Com isso temos provado que $P \Longrightarrow Q$, indiretamente. Veja Teorema 1.21(d).

Se o teorema é uma afirmação do tipo "$\forall x\ P(x)$"temos que verificar que "$\neg(\forall x, P(x))$"dá uma contradição e, finalmente, se o teorema for uma afirmação do tipo "$\exists x, P(x)$", então prove que "$\forall x,\ \neg P(x)$"é falso.

Exemplo (E) Provemos por contradição que $\sqrt{2}$ é irracional.

Solução: Seja P a proposição: "$\sqrt{2}$ *é irracional*". Suponhamos que $\neg P$ é verdadeira. Então $\sqrt{2}$ é racional. Vamos mostrar que isto nos leva a uma contradição.

Por hipótese existem inteiros a e b tais que $\sqrt{2} \overset{(1)}{=} \dfrac{a}{b}$, e podemos supor que a e b não têm fatores comuns (se tiverem, podemos cancelá-los sem afetar a fração). Seja r a proposição:

r: "*a e b não têm fatores comuns diferente de 1*".

Elevando a igualdade (1) ao quadrado, ficamos com $2 = a^2/b^2$ e portanto $a^2 = 2b^2$. Logo a^2 é par. Isto implica que a é par (se fosse ímpar a^2 seria ímpar; veja exemplo (A)). Logo existe um inteiro k tal que $a = 2k$. Portanto $a^2 = 4k^2$. Substituindo na expressão: $a^2 = 2b^2$ ficamos com $4k^2 = 2b^2$ e daí $b^2 = 2k^2$. Pelo mesmo raciocínio anterior b também é par, digamos $b = 2c$, c inteiro. Mas sendo a e b pares, 2 é fator comum de ambos. Logo $\neg r$ é verdadeira e temos r e $\neg r$ são ambas verdadeiras. Uma contradição!! Como que esta contradição pode ser construída caso $\sqrt{2}$ for racional, somos obrigados a aceitar que $\sqrt{2}$ é irracional.

Nota. As provas por contra recíproca e por contradição são também ditas *Demonstrações Indiretas*.

Observação: O método de demonstração a ser usado em um teorema pode ser qualquer um deles, a princípio. Em geral, o método direto é inicialmente tentado e, dependendo da natureza do teorema $P \Longrightarrow Q$, não é o mais adequado, e sim um outro método. Não existe uma regra para saber qual método aplicar no momento, e só

com a experiência, ou visão do método e, finalmente, por tentativa e erro, chegaremos ao método adequado.

Por exemplo, vamos demonstrar que, "*se n é um inteiro e n^2 é ímpar, então n ímpar*".

Supondo n^2 ímpar (onde n é um inteiro), por definição existe um inteiro k tal que $n^2 = 2k + 1$. Daí $n = \sqrt{2k+1}$ e assim fica muito difícil provar que n é ímpar. Então é melhor tentar provar por outro método. Suponha que n não é ímpar, ou seja, n é par. Então existe um inteiro c tal que $n = 2c$. Daí $n^2 = 2(2c^2)$. Logo n^2 também é par. Pela contra recíproca, segue-se que a proposição dada é verdadeira. Neste caso o método contra recíproca foi mais eficiente que o método direto.

(F) Demonstração por Casos

Se o teorema $P \Longrightarrow Q$ a ser provado é tal que $P = p_1 \vee p_2 \vee \cdots \vee p_n$, então podemos provar o teorema provando que $p_i \rightarrow Q$ é verdadeira para cada $i = 1, 2, \ldots, n$, individualmente. Com isto temos provado o teorema desde que
$[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow Q] \equiv [(p_1 \rightarrow Q) \wedge (p_2 \rightarrow Q) \wedge \cdots \wedge (p_n \rightarrow Q)]$.
Um tal argumento é chamado *Demonstração por Casos.*

Exemplo (F) Se queremos provar que $|x||y| = |xy|$, onde x e y são números reais, podemos dividir em quatro casos.

De fato, todo número real é positivo ou negativo. Sejam P : "*x e y são números reais*" e Q: "$|x||y| = |xy|$". Então $P = p_1 \vee p_2 \vee p_3 \vee p_4$, onde p_1 : "$x \geq 0$ e $y \geq 0$", p_2 : "$x \geq 0$ e $y < 0$", p_3 : "$x < 0$ e $y \geq 0$" e p_4 : "$x < 0$ e $y < 0$". Com isto temos que demonstrar que $p_1 \rightarrow Q$, $p_2 \rightarrow Q$, $p_3 \rightarrow Q$ e $p_4 \rightarrow Q$ são verdadeiras. Fica como exercício.

(G) Demonstração de Equivalência

Para demonstrar um teorema do tipo "$P \Longleftrightarrow Q$"devemos demonstrar que $P \rightarrow Q$ e $Q \rightarrow P$ são verdadeiras. Com isto o teorema está demonstrado, pois $P \Longleftrightarrow Q$ é logicamente equivalente à $(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$.

Exemplo (G) O teorema "*O inteiro n é ímpar se, e somente se, n^2 é ímpar*"é da forma $P \Longleftrightarrow Q$, onde P : "*n é ímpar*" e Q : "*n^2 é ímpar*". Para demonstrá-lo basta demonstrar que P é suficiente

para Q, $(P \Longrightarrow Q)$ e P é necessário para Q, $(Q \Longrightarrow P)$.

Algumas vezes um teorema afirma que várias proposições P_1, $P_2, \ldots, P_n$ são equivalentes. Isso pode ser escrito na forma: $P_1 \Leftrightarrow P_2 \Leftrightarrow \cdots \Leftrightarrow P_n$, o que afirma que todas proposições têm o mesmo valor-verdade, ou seja, P_i e P_j, $1 \leq i, j \leq n$ são equivalentes. Um meio de provar estas equivalências é usar a tautologia

$$[P_1 \longleftrightarrow P_2 \longleftrightarrow \cdots \longleftrightarrow P_n] \equiv$$
$$\equiv [(P_1 \rightarrow P_2) \wedge (P_2 \rightarrow P_3) \wedge \cdots \wedge (P_n \rightarrow P_1)].$$

Assim o teorema está demonstrado se demonstrarmos que
$P_1 \rightarrow P_2,\ P_2 \rightarrow P_3, \ldots, P_{n-1} \rightarrow P_n,\ P_n \rightarrow P_1$ são tautologias.

Às vezes a ordem da seqüência dos P_i's faz com que a demonstração fique muito longa e é melhor a demonstração de $P_i \rightarrow P_j$ $i \neq j$, é uma tautologia para i e j convenientes, e re-enumerar a seqüência de implicações.

Teoremas e Quantificadores

Muitos teoremas são proposições que envolvem quantificadores. Existem vários métodos usados para demonstrar teoremas que são quantificações. Alguns dos mais importantes são:

(a_1) Demonstração Existencial

Alguns teoremas afirmam que existe um objeto com determinada propriedade. Por exemplo: "$\exists x\ P(x)$", onde P é um predicado. A demonstração do teorema é dita *Demonstração de Existência.*

Existem vários caminhos para provar um teorema deste. Uma demonstração pode ser dada exibindo um elemento a do universo de discurso que satisfaça a propriedade $P(x)$ (ou seja, $P(a)$ é verdadeira). Esta prova de existência é dita *Prova Construtiva.*

Uma *Prova Não Construtiva* do teorema é feita provando o teorema "$\exists x,\ P(x)$", mas sem exibir qualquer elemento a que satisfaça $P(x)$. Um método de uma prova não construtiva pode ser feita por contradição, onde se nega a quantificação existencial e obtém-se uma contradição.

Exemplo (a_1)(1) Prova Construtiva

Mostre que "*Existe um inteiro positivo que pode ser escrito de dois modos, como soma de dois quadrados*".

Solução: Por tentativa e erro encontramos $50 = 1^2 + 7^2 = 5^2 + 5^2$, ou se exigir quadrados distintos: $65 = 1^2 + 8^2 = 4^2 + 7^2$.

Exemplo (a_1)(2) Prova Não Construtiva

Mostre que "*Existem números irracionais x e y tais que x^y é racional*".

Solução: Pelo exemplo (E) $\sqrt{2}$ é irracional. Logo, se $\sqrt{2}^{\sqrt{2}}$ é racional, basta considerar $x = \sqrt{2}$ e $y = \sqrt{2}$. Se $\sqrt{2}^{\sqrt{2}}$ é irracional, tome $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$. Daí $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}.\sqrt{2}} = \sqrt{2}^2 = 2$. Logo, x^y é racional neste caso.

Esta demonstração é não construtiva porque demonstramos a validade da afirmação sem exibir os elementos x e y que satisfazem a condição "*x^y é racional*". Neste caso, chegamos bem próximo ao exibirmos dois pares $(x, y) = (\sqrt{2}, \sqrt{2})$ ou $(x, y) = (\sqrt{2}^{\sqrt{2}}, \sqrt{2})$, tal que exatamente um deles tem a propriedade desejada, mas não sabemos qual dos dois pares tem a propriedade desejada.

(b_1) Demonstração de Unicidade

Alguns teoremas afirmam que existe exatamente um elemento com uma determinada propriedade. Para demonstrar um teorema deste tipo, é necessário demonstrar que existe um elemento com a propriedade desejada e, além disso, demonstrar de algum modo que qualquer outro elemento distinto deste não tem esta propriedade. Assim, a demonstração de um teorema deste tipo envolve dois passos:

(i) Existência - Provar que existe um elemento x com a propriedade desejada.

(ii) Unicidade - Provar que se $y \neq x$, então y não tem a propriedade desejada.

Portanto demonstrar que existe um único elemento a que satisfaz $P(x)$ é o mesmo que demonstrar a proposição:

$$\exists x \; P(x) \wedge \forall y (y \neq x \rightarrow \neg P(y)).$$

Note que $\exists x \; P(x)$: se refere à existência e "$\forall y, \; \big(y \neq x \rightarrow \neg P(y)\big)$" se refere à unicidade.

Desde que "$(y \neq x) \rightarrow (\neg P(y))$"é logicamente equivalente a "$P(y) \rightarrow (y = x)$"(pela contra recíproca), a unicidade pode ser demonstrada assim:

Supor que para algum y, $P(y)$ é verdadeiro e concluir que $y = x$. Este método é bastante usado, também.

(c) Contra-Exemplo

A proposição quantificada: "$\forall x\ P(x)$"é falsa se exibirmos um elemento particular a no conjunto universo tal que $P(a)$ é falsa. Quando se apresenta uma proposição da forma "$\forall x\ P(x)$" que, ou acreditamos ser falsa, ou que tenha "resistido" a toda tentativa de demonstração, em geral buscamos um contra-exemplo.

Exemplo. Mostre que é falsa, a proposição: "*Todo inteiro positivo é soma de quadrados de três inteiros*"(ou seja, "*soma de três quadrados*").

Solução - Para mostrar que esta proposição é falsa, precisamos achar um contra-exemplo: exibir um inteiro positivo a que não é soma de três quadrados. Ou seja, exibir um inteiro positivo a tal que para quaisquer inteiros x, y, z tem-se: $a \neq x^2 + y^2 + z^2$. Isto segue do fato que

$$\neg[\forall a, \exists b, \exists c, \exists d :\ a = b^2 + c^2 + d^2] \equiv$$
$$\equiv [\exists a, \forall b, \forall c, \forall d : a \neq b^2 + c^2 + d^2].$$

Vejamos: $1 = 0^2 + 0^2 + 1^2$, $2 = 0^2 + 1^2 + 1^2$, $3 = 1^2 + 1^2 + 1^2$, $4 = 0^2 + 0^2 + 2^2$, $5 = 0^2 + 1^2 + 2^2$, $6 = 1^2 + 1^2 + 2^2$. No entanto, se $7 = a^2 + b^2 + c^2$, então a^2, b^2 e c^2 devem pertencer ao conjunto $\{0, 1, 4\}$. Mas nenhuma soma de três elementos deste conjunto dá como resultado final 7, como pode ser verificado. Logo a proposição: "*Todo inteiro positivo é soma de três quadrados*"é falsa.

Nota. Um erro comum na demonstração de teoremas é, depois de fazer várias tentativas com resultados verdadeiros, concluir a veracidade do teorema. Por exemplo o teorema:

"*Todo inteiro positivo pode ser escrito como soma de dezoito potências quartas de inteiros*".

As potências quartas de inteiros são: 0, $1 = 1^4$, $16 = 2^4$, $81 = 3^4, \ldots$ Para cada inteiro $n \geq 0$ é possível selecionar dezoito destes

números cuja soma dá n, a menos que $n = 79$. Fica como exercício a verificação de que 79 não é soma de dezoito potências quartas de inteiros.

Erros em demonstrações

Existem muitos erros comuns em construções de provas matemáticas. Em geral, a maioria deles são erros de aritmética e álgebra básica. Até matemáticos profissionais cometem tais erros, especialmente quando trabalham com fórmulas complicadas. Cada passo da prova tem que ser feito e estar correto, pois a conclusão deve seguir logicamente dos passos que a precedem. Seguem alguns exemplos simples de erros em demonstrações que nos levam a conclusões erradas.

Exemplo (i) Vamos "provar"que $1 = 2$.

Passos	**Justificativas**
1. $a = b$	Dados
2. $a^2 = ab$	Mult. os membros de (1) por a
3. $a^2 - b^2 = ab - b^2$	Subtr. b^2 dos membros de (2)
4. $(a-b)(a+b)=(a-b)b$	Fator. dos membros de (3)
5. $a + b = b$	Div. de (4) por $a-b$
6. $2b = b$	Trocando a por b, pois $a = b$
7. $2 = 1$	Div. os membros de (6) por b

Determine os erros da "demonstração" dada.

Exemplo (ii) Determine o erro cometido na "demonstração"do teorema "*Se n^2 é positivo então, n é positivo*".

Demonstração: Suponha que n^2 seja positivo. Como a proposição "*Se n é positivo, então n^2 é positivo*"é verdadeira, podemos concluir que n é positivo.

Solução: Seja $P(n)$ a proposição: "*n^2 é positivo*"e $Q(n)$: "*n é positivo*". Agora a proposição "*Se n^2 é positivo, então n é positivo*"se escreve na forma:

$$\text{“}\forall n\ (P(n) \longrightarrow Q(n))\text{”}.$$

Assim, de $Q(n) \longrightarrow P(n)$ verdadeira e $P(n)$: verdadeira não podemos concluir que $Q(n)$ é verdadeira, pois nenhuma regra de inferência foi usada, ou outra justificativa foi dada. Aliás, esta prova é um exemplo de *falácia da afirmação da conclusão*. Note também

que a proposição é falsa e um contra-exemplo é dado para $n = -1$, para o qual n^2 é positivo, mas n é negativo.

Exemplo (iii) Consideremos a proposição: "*Se n não é positivo, então n^2 não é positivo*", que é a contra-recíproca do teorema do exemplo (ii). Verifique que a "prova" que segue está errada.

Prova: Suponhamos que n não é positivo. Desde que "*se n é positivo, então n^2 é positivo*"é uma proposição verdadeira, concluímos que n^2 não é positivo.

De fato a "prova"é uma *falácia por negação da hipótese.*

Finalmente, outro tipo de erro em demonstrações ocorrem quando se usa a falácia chamada *Raciocínio Circular*. Ela ocorre quando um ou mais passos da prova são baseados em verdades a serem provadas. Em outras palavras, esta falácia aparece quando a proposição é provada usando ela mesma como hipótese, ou uma proposição equivalente a ela.

Por exemplo, se queremos provar que

"*n é um inteiro par, quando n^2 é par*"

Segue a "prova":

Suponhamos n^2: par, ou seja, $n^2 = 2k$ para algum inteiro k. Seja $n = 2l$, para algum inteiro l. Isto mostra que n é par!!

Este argumento é incorreto, pois a proposição: "*seja $n = 2l$, para algum inteiro l*"ocorre na prova como hipótese, e isto é exatamente o que se pretende como tese. Esta é uma falácia por *raciocínio circular*, pois a proposição "*n é par*"é equivalente a proposição "*$n = 2l$, para algum inteiro l*".

Exercícios dos ítens 1.4 e 1.5.

(1) Quantificar a fim de obter proposições verdadeiras:
(a) $x^2 + y^2 = (x + y)^2 - 2xy, x, y \in \mathbb{R}$, **(b)** $x + y = 8, x, y \in \mathbb{N}$,
(c) $\sec^2 x = 1 + \tan^2 x,\ x \in A = \{x \in \mathbb{R} : 0 < x < \pi\}$.

(2) Negue as proposições:
(a) $\forall x :\ (P(x) \vee Q(x)) \to S(x)$. **(b)** $\forall x : P(x) \to S(x)$.
(c) $\exists x : A(x) \wedge B(x)$. **(d)** $\exists x : A(x) \leftrightarrow C(x)$.

(3) Negue cada uma das proposições abaixo e, depois, verifique

se as proposições obtidas são verdadeiras: **(a)** $mdc(2,3) = 3$ ou $mmc(2,3) \neq 6$, **(b)** $\frac{3}{5} \neq \frac{6}{10}$ ou $5.6 = 3.10$, **(c)** Se $\frac{1}{2} \leq \frac{2}{3}$ então $2.2 \geq 1.3$, **(d)** Nem todo número inteiro é um número primo.

(4) Sejam $M = \{$Joana, Sílvia, Maria$\}$ e $H = \{$João, André$\}$ e entende-se por "xRy": x é irmão de y. Dê a sentença verbal para:
(i) $\exists x \in M : \forall y \in H,\ xRy$, **(ii)** $\exists x \in M, \exists y \in H : xRy$,
(iii) $\forall x \in M \wedge \forall y \in H : xRy$.

(5) Seja $A = \{1,2,3\}$. Determine os valor-verdade de cada uma das proposições e, no caso de ser falso, negue-a e apresente o conjunto solução: **(a)** $\exists x,\ \exists y : x^2+y^2 < 12$, **(b)** $\exists x,\ \forall y,\ x^2 < y+1$, **(c)** $\forall x,\ \forall y : x^2+y^2 < 12$, **(d)** $\exists x,\ \exists y, \exists z : x^2 + y^2 < 2z^2$, **(e)** $\exists x, \exists y, \forall z : x^2 + y^2 < 2z^2$.

(6) Seja $A = \{1,2,3\}$.
(a) Negue a proposição $p(x,y,z)$ abaixo e verifique o valor-verdade da proposição obtida: $P(x,y,z) : \exists x \in A,\ \exists y \in A, \forall z \in A : x + 2y + 3z \geq 12$. **(b)** Dê uma sentença aberta sobre A.

(7) Traduza em linguagem matemática:
(i) Todas as pessoas possuem exatamente uma mãe. **(ii)** Todo número real não nulo é inversível. **(iii)** Para todo $\epsilon > 0$ existe $\delta > 0$, tal que para todo número real x diferente de a, se o módulo de $x - a$ é menor que δ, então o módulo de $f(x) - L$ é menor que ϵ.

(8) **(i)** Seja a um número inteiro. Prove que: "a^2 *é ímpar* $\Rightarrow$ a *é ímpar*".
(ii) Qual o tipo de demonstração que você usou?
(iii) Demonstre novamente usando um outro tipo de demonstração.

(9) Para P : "$a = 3$" e Q : "$a^2 = 4$", enuncie cada um dos ítens do Teorema 1.21 e verifique o valores-verdade de cada uma das proposições obtidas. Isto contradiz ou confirma o Teorema 1.21?

Exercícios do Capítulo 1.

(1) Quais das sentenças dadas são proposições? Quais são os valores-verdade das sentenças que são proposições?

(a) Senegal fica no continente europeu. (b) $2 + 3 = 5$. (c) Responde esta questão. (d) $2 + 7 = 10$. (e) $x+y = y+x$ para quaisquer $x, y \in \mathbb{R}$. (f) $x + 2 = 11$. (g) $x + 1 = 5$, se $x = 1$ ou $x = 4$. (h) Bem vindo a Rio Preto.

(2) Qual é a negação das proposições:
(i) "*Hoje é terça-feira*", (ii) "*Não existe poluição em São Paulo*", (iii) "*O verão no Rio de Janeiro é quente e ensolarado*".

(3) Sejam p e q as proposições: "*A eleição está decidida*"e "*Os votos foram contados*", respectivamente. Expresse cada uma das proposições compostas como uma sentença em língua portuguesa:
(a) $\neg p$ (b) $p \vee q$ (c) $\neg p \wedge q$ (d) $q \rightarrow p$ (e) $\neg q \rightarrow \neg p$
(f) $\neg p \rightarrow \neg q$ (g) $p \longleftrightarrow q$ (h) $\neg q \vee (\neg p \wedge q)$.

(4) Considere as proposições p:"*Você tirou dez no exame final*", q: "*Você fez todos os exercícios de AFC*"e r : "*Você é um aluno desta classe*". Escreva as proposições abaixo usando p, q e r e os símbolos lógicos.

(a) "*Você tirou dez no exame final, mas você não fez todos os exercícios de AFC*".

(b) "*Você fez todos os exercícios de AFC apesar de não ser aluno desta classe*".

(c) "*Você tirou dez no exame final, mas não fez todos os exercícios de AFC, no entanto, você é um aluno desta classe*".

(d) "*Uma condição necessária para você tirar dez no exame final é você fazer todos os exercícios de AFC e ser aluno desta classe*".

(e) "*Uma condição necessária, mas não suficiente, para você tirar dez no exame final é você fazer todos os exercícios de AFC e ser aluno desta classe*".

(f) "*Você fez todos os exercícios de AFC quando você tira dez no exame final*".

(5) Determine quando o condicional ou o bicondicional são verdadeiros ou falsos.
(a) "*Se* $1 + 1 = 2$, *então* $2 + 2 = 5$",
(b) "*Se* $1 + 1 = 3$, *então* $2 + 2 = 4$",
(c) "*Se* $1 + 1 = 3$, *então* $2 + 2 = 5$",
(d) "*Se elefante voa, então* $1 + 1 = 2$",

(e) "*Se* $1+1=3$, *então Deus existe*",
(f) "$1+1=3$ *se, e somente se, elefante voa*",
(g) "$1+1=3$ *se, e somente se,* $3=5$",
(h) "*Elefante não voa se, e somente se,* $1=0$".

(6) Escreva usando os símbolos lógicos "ou" ou "ou exclusivo".

(a) Com duzentos reais (R$200,00) você compra um par de sapatos de R$130,00 ou um tênis de R$160,00. (b) Domingo à tardinha vou assistir ao jogo ou vou assistir a um filme.

(7) Dê a negação e a contra-recíproca da proposição: "*Se chover hoje, então amanhã vai fazer frio*".

(8) Faça as tabelas-verdade das proposições compostas

(a) $(p \vee q) \rightarrow (p \underline{\vee} q)$ (b) $(p \underline{\vee} q) \rightarrow (p \wedge q)$
(c) $(\sim p \leftrightarrow \sim q) \longleftrightarrow (p \leftrightarrow q)$ (d) $(p \leftrightarrow q) \underline{\vee} (\sim p \leftrightarrow q)$
(e) $(p \vee q) \underline{\vee} (p \wedge q)$ (f) $(\sim p) \longrightarrow (q \rightarrow r)$.

(9) A teoria de jogos lógicos é usada em inteligência artificial. Nela uma proposição tem um valor-verdade que é um número entre 0 (zero) e 1 (um), inclusive. Uma proposição com o valor-verdade 0 (zero) é falsa e com o valor-verdade 1 (um) é verdadeira. Valores-verdade entre 0 e 1 indicam vários graus de verdade. O valor-verdade da proposição "*João é feliz*"é 0.8, desde que João seja feliz a maior parte do tempo (exatamente 0.8 do tempo), e a proposição "*Paulo é feliz*"tem valor-verdade 0.4.

Sabendo-se que o valor-verdade da negação de uma proposição p, na teoria de jogos lógicos, é 1 menos o valor-verdade de p, o valor-verdade da conjunção $p \wedge q$ é o mínimo dos valores-verdade de p e de q, e finalmente, o valor-verdade da disjunção de duas proposições p e q é o máximo dos valores-verdade de p e de q; dê os valores-verdade das proposições:
(i) "*João e Paulo são felizes*", (ii) "*João e Paulo não são felizes*", (iii) "*João é feliz ou Paulo é feliz*", (iv) "*João não é feliz ou Paulo não é feliz*".

(10) "*Esta proposição é falsa*" é uma proposição? Por quê?

(11) A n-ésima proposição em uma lista de 100 proposições é: "*Exatamente n proposições desta lista é falsa*".

(a) Que conclusão podemos tirar destas proposições?

(b) Responda o item (a) se a n-ésima proposição é: "*Pelo menos n proposições desta lista são falsas*".

(12) Verifique quais das proposições dadas são tautologias:

(a) $(\neg p) \rightarrow (p \rightarrow q)$ (b) $(p \wedge q) \rightarrow (p \rightarrow q)$
(c) $[\neg(p \rightarrow q)] \rightarrow p$ (d) $(\neg p) \rightarrow [q \rightarrow p]$
(e) $[\neg(p \rightarrow q)] \rightarrow (\neg q)$ (f) $[p \vee (p \wedge q)] \longleftrightarrow p$
(g) $[p \wedge (p \vee q)] \longleftrightarrow p$

13) (i) Apresente uma proposição composta P, envolvendo as proposições p, q e r, que é verdadeira quando p e q são verdadeiras e r falsa, e P é falsa nos outros casos.

(ii) Apresente uma proposição composta Q, envolvendo as proposições p, q e r, que é verdadeira exatamente quando duas das proposições p, q e r são verdadeiras (portanto, falsa nos outros casos).

(14) Seja $P(x)$ a proposição: "$x \leq 4$". Quais são os valores-verdade de (a) $P(0)$, (b) $P(4)$, (c) $P(6)$.

(15) Seja $Q(x)$ a sentença aberta "*a palavra x contém a letra a*". Quais são os valores-verdade de: (a) Q(limão), (b) Q(laranja), (c) Q(impressor).

(16) Seja $L(x, y)$ a sentença aberta: "*x é a capital de y*". Quais são os valores-verdade de: (a) L(São Paulo, São Paulo), (b) L(Brasília, Goiás), (c) L(New York, EUA), (d) L(Rio de Janeiro, Rio de Janeiro).

(17) Seja $P(x)$ a sentença aberta: "*x passa mais de 5 horas por semana em classe*", onde o universo de discurso consiste de todos os estudantes. Expresse cada uma das proposições em português: (i) "$\exists x\ P(x)$", (ii) "$\forall x\ P(x)$", (iii) "$\exists x\ \neg P(x)$", (iv) "$\forall x\ \neg P(x)$".

(18) Traduza as proposições seguintes para o português, onde $C(x)$ é: "*x é um motorista*"e $F(x)$ é: "*x é atencioso*", e o universo de discurso consiste de todas as pessoas. (a) $\forall x\ (C(x) \rightarrow F(x))$, (b) $\forall x\ (C(x) \wedge F(x))$, (c) $\exists x\ (C(x) \rightarrow F(x))$, (d) $\exists x(C(x) \wedge F(x))$.

(19) Considere as sentenças $C(x)$: "*x tem um carro*", $D(x)$: "*x tem um computador*"e $F(x)$: "*x tem um notebook*". Expresse cada uma das proposições em termos de $C(x)$, $D(x)$ e $F(x)$, quantificadores e símbolos lógicos, onde o universo de discurso é constituído por todos os alunos de sua classe.

(a) "*Um estudante de sua classe tem um carro, um computador e um notebook*". (b) "*Todos os estudantes de sua classe tem um carro, um computador, ou um notebook*". (c) "*Algum estudante de sua classe tem um carro, e um computador, mas não tem um notebook*". (d) "*Nenhum estudante de sua classe tem um carro, um computador, e um notebook*". (e) "*Para cada um dos objetos: carro, computador e notebook, existe um aluno de sua classe que o possui*".

(20) Traduza para a linguagem matemática cada uma das proposições, a seguir, usando predicados, quantificadores, símbolos, etc. (a) "*Ninguém é perfeito*", (b) "*Nem todos são perfeitos*", (c) "*Todos os seus amigos são perfeitos*", (d) "*Um dos seus amigos é perfeito*", (e) "*Todos são seus amigos e são perfeitos*", (f) "*Nem todos são seus amigos ou alguém é perfeito*".

(21) (i) Seja $P(x)$ a proposição: "$x = x^2$", onde o conjunto universo U consiste de todos os inteiros. Determine o valores-verdade de: (a) $P(0)$, (b) $P(1)$, (c) $P(2)$, (d) $P(-1)$, (e) $\exists x\ P(x)$, (f) $\forall x\ P(x)$.

(ii) Idem para $Q(x)$: "$x + 1 > 2x$"e (a) $Q(0)$, (b) $Q(-1)$, (c) $Q(1)$, (d) $\exists x\, Q(x)$, (e) $\forall x\, Q(x)$, (f) $\exists x \sim Q(x)$, (g) $\forall x \sim Q(x)$.

(22) Determine os valores-verdade das proposições abaixo onde o universo $U = \mathbb{Z}$.

(a) $\forall n\ (n + 1 > n)$, (b) $\exists n(2n = 3n)$, (c) $\exists n(n = -n)$,

(d) $\forall n(n^2 \geq n)$.

(23) Seja $P(x)$ uma sentença aberta definida sobre o conjunto $U =$ {–1,0,1,2}. Escreva cada uma das proposições seguintes usando apenas disjunções, conjunções e negações. (a) $\exists x P(x)$, (b) $\forall x P(x)$, (c) $\exists x \sim P(x)$, (d) $\forall x \sim P(x)$, (e) $\sim (\exists x P(x))$, (f) $\sim (\forall x\ P(x))$.

(24) Expresse cada uma das proposições de (a) a (d) usando símbolos lógicos, predicados e quantificadores. (a) "*Algumas proposições são tautologias*", (b) "*A negação de uma contradição é uma tautologia*", (c) "*A disjunção de duas contingências pode ser uma tautologia*", (d) "*A conjunção de duas tautologias é uma tautologia*".

(25) Traduza para a língua portuguesa as sentenças matemáticas seguintes, onde $D(p)$ é: "*a p-ésima impressora está com defeito*", $A(p)$: "*a p-ésima impressora está ativa*", $P(j)$: "*a j-ésima impressão foi perdida*"e $F(j)$: "*a j-ésima impressora tem uma longa fila*".

(a) $\exists p(D(p) \wedge A(p)) \longrightarrow \exists j P(j)$, (b) $\forall p A(p) \longrightarrow \exists j F(j)$,

(c) $\exists j, k(F(j) \wedge P(k)) \longrightarrow \exists p D(p)$, (d) $(\forall p A(p) \wedge \forall j F(j)) \longrightarrow \exists i P(i)$.

(26) Determine se $\forall x(P(x) \longrightarrow Q(x))$ e $\forall x P(x) \longrightarrow \forall x Q(x)$ têm o mesmo valor-verdade. Dê um exemplo que confirme a resposta.

(27) Mostre que "$\forall x(P(x) \wedge Q(x))$" e "$\forall x P(x) \wedge \forall x Q(x)$" têm o mesmo valor-verdade.

(28) Mostre que "$\exists x(P(x) \vee Q(x))$" e "$\exists x P(x) \vee \exists x Q(x)$" têm o mesmo valor-verdade.

(29) Para uma proposição fixada A sem envolver quantificadores, mostre que: (a) $(\forall x P(x)) \wedge A \equiv \forall x(P(x) \wedge A)$, (b) $(\exists x P(x)) \wedge A \equiv \exists x(P(x) \wedge A)$.

(30) Mostre que (i) "$\forall x P(x) \vee \forall x Q(x)$" e "$\forall x(P(x) \vee$"$Q(x))$"não são logicamente equivalentes e (ii) "$\exists x P(x) \wedge \exists x Q(x)$"e "$\exists x(P(x) \wedge Q(x))$" não são logicamente equivalentes.

(31) Traduzir para o português as proposições seguintes, onde o universo de discurso para cada variável é o conjunto de todos os números reais:

(a) $\forall x \exists y(x < y)$, **(b)** $\forall x \forall y \Big([(x \geq 0) \wedge (y \geq 0)] \longrightarrow [xy \geq 0] \Big)$,

(c) $\forall x \forall y \exists z(xy = z)$, **(d)** $\exists x \forall y(xy = y)$.

(32) Seja $Q(x, y)$ a proposição: "*x tem enviado uma mensagem por e-mail para y*", onde o universo de discurso consiste de todos os alunos da classe. Expresse em português as proposições:

(a) $\exists x \exists y Q(x, y)$, **(b)** $\exists x \forall y Q(x, y)$, **(c)** $\forall x \forall y Q(x, y)$,

(d) $\exists y \forall x Q(x, y)$, **(e)** $\forall y \exists x Q(x, y)$.

(33) Expresse as proposições em linguagem matemática, usando símbolos lógicos: **(a)** "*A soma de dois inteiros negativos é negativa*", **(b)** *A diferença de dois inteiros positivos não é necessariamente positiva*", **(c)** "*A soma de quadrados de dois inteiros (soma de dois quadrados) é maior ou igual ao quadrado de sua soma*", **(d)** "*Todo inteiro positivo é uma soma de quatro quadrados*".

(34) Para os conjuntos universo indicados, quais são os valores-verdade das proposições seguintes: **(I)** $U = \mathbb{Z}$.

(a) $\forall n \exists m(n^2 < m)$, **(b)** $\exists n \forall m(n < m^2)$, **(c)** $\forall n \exists m(m + n = 0)$, **(d)** $\exists n \forall m\ (n.m = m)$, **(e)** $\exists n \exists m(n^2 + m^2 = 5)$, **(f)** $\exists n \exists m(n^2 + m^2 = 6)$,

(g) $\exists n \exists m(n + m = 4 \wedge n - m = 1)$, **(h)** $\forall n \forall m \exists p\Big(p = \dfrac{(m + n)}{2}\Big)$.

(II) $U = \mathbb{R}$.

(a) $\forall x \exists y(x^2 = y)$, **(b)** $\exists x \forall y(x.y = 0)$, **(c)** $\exists x \forall y(y \neq 0 \longrightarrow x.y = 1)$, **(d)** $\forall x \forall y \exists z\Big(z = \dfrac{x + y}{2}\Big)$, **(e)** $\exists x \exists y(x + y \neq y + x)$.

(35) Um número real l é chamado de limite superior de um subconjunto não vazio S de números reais se l é maior ou igual a qualquer elemento de S. E s é chamado de supremo de S se s é um limite superior, e qualquer outro limite superior de S é maior ou igual a s. Use os símbolos lógicos e coloque as definições de limite superior e supremo de um subconjunto S em termos matemáticos.

(36) Use símbolos lógicos para definir $\lim_{n\to\infty} a_n = L$, onde $a_n \in \mathbb{R}$, $\forall n \in \mathbb{N}$.

(37) Mostre que $\log_2 3$ não é um número racional, ou seja, não pode ser escrito na forma a/b, com a e b inteiros.

(38) Determine quando cada um desses argumentos é válido. E se um argumento é válido, que regra de inferência foi usada? Se não é válido, que erro lógico ocorreu?

(a) "*Se* n *é um número real tal que* $n > 1$, *então* $n^2 > 1$",

(b) Afirmação: "*O número* $\log_2 3$ *é irracional, pois ele não é o quociente de dois inteiros. Portanto, desde que* $\log_2 3$ *não pode ser escrito na forma* $\frac{a}{b}$, *com* a, b *inteiros, conclui-se que ele é irracional*",

(c) "*Se* n *é um número real e* $n > 3$, *então* $n^2 > 9$. *Portanto se* $n^2 \leq 9$, *então* $n \leq 3$".

(d) "*Se* n *é um número real e* $n > 2$, *então* $n^2 > 4$. *Portanto, se* $n \leq 2$, *então* $n^2 \leq 4$".

(39) Determine quando os argumentos são válidos:

(a) "*Se* x^2 *é irracional, então* x *é irracional. Portanto, se* x *é irracional, segue-se que* x^2 *é irracional*".

(b) "*Se* x^2 *é irracional, então* x *é irracional. O número* $x^2 = \pi^2$ *é irracional. Portanto* $x = \pi$ *é irracional*".

(40) Prove que o quadrado de um número par é par, usando (i) Prova direta e (ii) Prova por contradição.

(41) Prove que: **(a)** A soma de dois inteiros ímpares é par,

(b) O produto de dois inteiros ímpares é ímpar,

(c) A soma de um número irracional com um número racional é irracional (Sugestão: Por contradição) e

(d) O produto de dois números racionais é racional.

(42) Prove ou dê um contra-exemplo: O produto de dois números irracionais é irracional.

(43) Prove por contradição que, de 64 dias escolhidos, pelo menos 10 caem em um mesmo dia da semana.

(44) Use prova por casos e prove que,

(i) $\max\{x, y\} + \min\{x, y\} = x + y$, para quaisquer $x, y, z \in \mathbb{R}$,

(ii) $\min\{x, \min\{y, z\}\} = \min\{\min\{x, y\}, z\}, \quad \forall x, y, z \in \mathbb{R}$.

(45) (i) Prove que o último dígito de um quadrado de um número inteiro é: 0, 1, 4, 5, 6, ou 9. (Sugestão: escreva $n = 10k + l$, l um inteiro entre 0 e 9 inclusive).

(ii) Prove que o último dígito de uma quarta potência de um número inteiro é: 0, 1, 5, ou 6.

(46) Prove que as seguintes proposições são equivalentes, onde n é um número inteiro.

(i) "$3n+2$ *é um inteiro par*", **(ii)** "$n+5$ *é um inteiro ímpar*", **(iii)** "n^2 *é um inteiro par*".

(47) **(i)** Prove que existe uma sequência de 100 números inteiros consecutivos que não são quadrados perfeitos, isto é: não é da forma n^2 para algum inteiro n. A prova dada é construtiva? **(ii)** Prove que $2.10^{500}+15$ ou $2.10^{500}+16$ não é um quadrado perfeito. A prova dada é construtiva ou não-construtiva?

(48) Considere as premissas:

(1) "*Lógica é difícil ou poucos estudantes gostam de lógica*".

(2) "*Se matemática é fácil, então lógica não é difícil*", e determine quando as seguintes conclusões são válidas baseadas nestas premissas:

(a) "*Matemática não é fácil se muitos estudantes gostam de lógica*".

(b) "*Poucos estudantes gostam de lógica se matemática não é fácil*".

(c) "*Matemática não é fácil ou lógica é difícil*".

(d) "*Lógica não é difícil ou matemática não é fácil*".

(e) "*Se poucos estudantes gostam de lógica, então, ou matemática não é fácil, ou lógica não é difícil*".

Capítulo 2

ARITMÉTICA DOS NÚMEROS INTEIROS

No §1.4 do capítulo **1** já citamos uma referência para a teoria dos números inteiros. Outras referências sobre os números inteiros e sua ordem usual "$\leq$," bem como sobre o princípio que segue são livros de álgebra para cursos de graduação, por exemplo, a referência [3].

Axioma 2.1 Princípio do Menor Inteiro ou Boa Ordem.
Seja L um subconjunto de $\mathbb{Z}$ não vazio e limitado inferiormente. Então L possui um mínimo (denotado por $\min L$).

É bom explicar o que diz o princípio já que nada foi dito até agora sobre os conceitos de *ordem, limite inferior* e *mínimo*. O princípio afirma que, se existe em $\mathbb{Z}$ um elemento m que é menor ou igual a qualquer elemento de L, então existe em L um elemento l, que é menor ou igual a qualquer elemento de L. Em símbolos: Se $\exists m \in \mathbb{Z} \mid m \leq l,\ \forall l \in L$ então $\exists l_0 \in L \mid l_0 \leq l,\ \forall l \in L$. Por exemplo, se $L = \{x \in \mathbb{Z} : |x| \leq 10\}$, então $\min L = -10$. O subconjunto $L_1 = \{x \in \mathbb{Z} : x^2 > 3\}$ não possui mínimo, pois não é limitado inferiormente. Esta é uma propriedade importante dos subconjuntos dos números inteiros que não é válida para os subconjuntos dos números racionais ou reais, como pode ser visto nos exemplos a seguir.

Por exemplo, o subconjunto de números racionais $\{\frac{1}{n+1},\ n \in \mathbb{N}\}$ é limitado inferiormente pelo número zero, mas não tem mínimo em $\mathbb{Q}$. O subconjunto de números reais $\{x \in \mathbb{R} : 0 < x < 1\}$ também não tem mínimo, apesar de ser limitado inferiormente pelo número zero. Tente demonstrar ou convencer-se disto.

2.1 Indução

Primeiro Princípio de Indução Finita (P.I.F.)
Dado $a \in \mathbb{Z}$ e $P(n)$ uma sentença aberta definida para todo $n \in \mathbb{Z},\ n \geq a$. Se

(i) *$P(a)$ é verdadeira,*

(ii) *$\forall r \geq a,\ P(r) \Longrightarrow P(r+1)$,*

então $P(n)$ é verdadeira para todo $n \geq a$.

O Princípio de Indução Finita é uma poderosa ferramenta matemática e pode ser expressa como regra de inferência da seguinte forma:

$$[P(a) \wedge (\forall r \geq a,\ P(r) \rightarrow P(r+1))] \Longrightarrow [\forall n \geq a, P(n)].$$

Uma boa visualização deste princípio é o chamado efeito dominó.

Quando trabalhamos com subconjuntos dos números inteiros, por vezes é interessante utilizarmos uma outra versão para este princípio, chamada Segundo Princípio de Indução Finita.

Segundo Princípio de Indução Finita (P.I.F.)
Dado $a \in \mathbb{Z}$ e $P(n)$ uma sentença aberta definida para todo $n \in \mathbb{Z},\ n \geq a$.
Se

(i) *$P(a)$ é verdadeira,*

(ii) *Dado $r > a$, se $P(k)$ é verdadeira para $a \leq k \leq r$, então $P(r+1)$ é verdadeira;*

então $P(n)$ é verdadeira para todo $n \geq a$.

Em outras palavras,

$$P(a) \wedge [(P(a+1) \wedge P(a+2) \wedge \cdots \wedge P(r)) \rightarrow P(r+1)] \Longrightarrow \forall n P(n).$$

Demonstração: (Do 1º e do 2º Princípio). Apresentaremos uma demonstração para estes princípios por redução ao absurdo, fazendo uso do princípio da boa ordem. Seja $L = \{x \geq a \mid P(x) : \text{falsa}\}$. Suponhamos $L \neq \emptyset$. Como L é limitado inferiormente por a pelo princípio do menor inteiro, L possui um mínimo. Seja $l_0 = min\ L$. Então $a \leq l_0$, pois $l_0 \in L$. Como por (i) $P(a)$ é verdadeiro e $P(l_0)$ é falso (pois $l_0 \in L$), segue que $a \neq l_0$. Assim, $a \leq l_0 - 1 < l_0$ e,

portanto, $l_0 - 1 \notin L$, (pois $l_0 = min\ L$). Isto implica que $P(l_0 - 1)$ é verdadeira. Por **(ii)** vem que $P(l_0)$ é verdadeira, absurdo. Logo $L = \emptyset$. □

Observação 2.2 Na prática verifica-se **(i)** e demonstra-se **(ii)** que o Princípio garante que $P(n)$ é verdadeira para todo $n \geq a$,

Exemplo.
(1). Toda postagem de 12 centavos ou mais, pode ser paga usando moedas de quatro e cinco centavos.

De fato, uma postagem de 12 centavos pode ser paga usando três moedas de quatro centavos.

Suponhamos que uma postagem de k centavos, $k \geq 12$, possa ser paga usando moedas de quatro e cinco centavos, e consideremos uma postagem de $k + 1$ centavos. Temos os casos:

(a) Se k foi paga usando pelo menos uma moeda de quatro centavos, troque uma moeda de quatro centavos por uma moeda de cinco centavos.

(b) Se k foi pago só com moedas de cinco centavos, foram necessárias pelo menos três moedas de cinco centavos, pois $k \geq 12$. Troque três moedas de cinco centavos por quatro moedas de quatro centavos.

(2). Prove que a soma dos n primeiros números naturais não-nulos é $\frac{n(n+1)}{2}$.

Solução Temos que provar que $P(n)$ é verdadeira para todo número natural $n \geq 1$, onde $P(n)$ é a igualdade: $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. $P(1)$ é verdadeira pois $1 = \frac{1(1+1)}{2}$. Suponhamos agora que $P(k) :\ 1 + 2 + \ldots + k = \frac{k(k+1)}{2}$ é verdadeira e provemos que $P(k+1) :\ 1+2+\ldots+k+(k+1) = \frac{(k+1)[(k+1)+1]}{2}$ é verdadeira. Partindo do lado esquerdo da igualdade, temos $1 + 2 + \ldots + k + (k + 1) = [1 + 2 + \ldots + k] + (k + 1)$ que, por hipótese de indução, é $\frac{k(k+1)}{2} + (k + 1)$. Reduzindo ao mesmo denominador, temos $1 + 2 + \ldots + k + (k + 1) = \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$,

que é o 2º membro. Pelo primeiro princípio de indução obtemos $1+2+\ldots+n=\dfrac{n(n+1)}{2}$ para todo número natural $n>0$.

(3). Prove que $P(n):\ 2+2.3+2.3^2+\cdots+2.3^n=3^{n+1}-1$ para todo número natural n.

Solução $P(0):\ 2=3^1-1$ é verdadeira. Suponhamos que, para $k\geq 0$, $P(k):\ 2+2.3+2.3^2+\ldots+2.3^k=3^{k+1}-1$ é verdadeira, e provemos que $P(k+1):\ 2+2.3+2.3^2+\ldots+2.3^k+2.3^{k+1}=3^{k+2}-1$ é verdadeira. Partindo do primeiro membro, temos $2+2.3+2.3^2+\ldots+2.3^k+2.3^{k+1}=[2+2.3+2.3^2+\ldots+2.3^k]+2.3^{k+1}\stackrel{\text{h.i.}}{=}[3^{k+1}-1]+2.3^{k+1}=3.3^{k+1}-1=3^{k+2}-1$. O primeiro princípio de indução garante que $2+2.3+2.3^2+\ldots+2.3^n=3^{n+1}-1$ para todo $n\in\mathbb{N}$.

(4). Prove que 7 divide $3^{2n+1}+2^{n+2},\ n\geq 0$.

Seja $x_n=3^{2n+1}+2^{n+2}$. Temos que provar que $x_n=7.q_n$, para algum $q_n\in\mathbb{N}$, dependendo de n. Como $x_0=7.1$, $q_0=1$. Vamos supor que exista $q_k\in\mathbb{N}$, tal que $x_k=7.q_k$. Daí $x_{k+1}=3^{2(k+1)+1}+2^{(k+1)+2}=3^{2k+3}+2^{k+3}=3^2.3^{2k+1}+2.2^{k+2}=(7+2)3^{2k+1}+2.2^{k+2}=7.3^{2k+1}+2x_k\stackrel{\text{hip.}}{=}7.3^{2k+1}+2.7.q_k=7(3^{2k+1}+2q_k)$. Logo 7 divide x_{k+1}. Pelo primeiro princípio de indução finita concluímos que "7 divide $3^{2n+1}+2^{n+2}$, para todo $n\geq 0$".

(5). Prove que $(1+a)^n\geq 1+n.a,\ \forall n\in\mathbb{N}^*,\ \forall a\in\mathbb{R}, a\geq -1$ fixo.

Para $n=1$ a afirmação $1+a\geq 1+a$ está correta. Para provar a condição (ii) do primeiro princípio de indução, suponhamos que $(1+a)^k\geq 1+ka$. Como $1+a$ é positivo, multiplicando por $1+a$ ambos os lados da desigualdade e desenvolvendo o membro da direita obtemos: $(1+a)^{k+1}\geq 1+ka+a+ka^2$. Então $(1+a)^{k+1}\geq 1+(k+1)a+ka^2$. Como $ka^2\geq 0$ segue-se que $(1+a)^{k+1}\geq 1+(k+1)a$. O primeiro princípio de indução garante que $P(n)$: "$(1+a)^n\geq 1+na,\ \forall n\in\mathbb{N}^*,\ \forall a\in\mathbb{R},\ a\geq -1$" é verdadeira.

Observação 2.3 Ao utilizarmos o P.I.F., assim como em toda argumentação, devemos ter muitos cuidados para não cairmos em "armadilhas".
(1) Considere o seguinte "teorema"e sua "prova"
Teorema Todos os cidadãos são tratados igualmente pela lei.

Prova (Por indução sobre o número i de cidadãos). Quando $i = 1$, existe apenas um cidadão e o teorema é trivialmente verdadeiro.

Suponha o teorema verdadeiro para quaisquer k cidadãos e considere um grupo de $k+1$ cidadãos, denotados por $c_1, c_2, \ldots, c_k, c_{k+1}$. Por hipótese de indução, $c_1, c_2, \ldots, c_k$ são tratados igualmente perante a lei, e o mesmo ocorre com $c_2, \ldots, c_k, c_{k+1}$. Portanto, os tratamentos pela lei de $c_1, c_2, \ldots, c_k, c_{k+1}$ são os mesmos que o de c_2, e devem ser iguais. Então, o teorema é verdadeiro para $i = k+1$.

Deixando de lado os argumentos políticos, há uma falácia nesta prova. Veja se descobre.

(2) Considere o seguinte "teorema"e sua "prova".
Teorema Para todo $i \geq 0$

$$\sqrt{1+i\sqrt{1+(i+1)\sqrt{1+(i+2)\sqrt{1+(i+3)\sqrt{\ldots}}}}} = i+1$$

Prova (Por indução sobre i). Para $i = 0$, o teorema se reduz a $\sqrt{1+0} = 0+1$, que é obviamente verdadeiro. A hipótese de indução é:

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

de onde obtemos (elevando-se ao quadrado, subtraindo 1 e dividindo-se por k):

$$\sqrt{1+(k+1)\sqrt{1+(k+2)\sqrt{1+(k+3)\sqrt{1+(k+4)\sqrt{\ldots}}}}} =$$

$$= \frac{(k+1)^2-1}{k} = \frac{k^2+2k}{k} = k+2 = (k+1)+1.$$

Novamente, há uma falácia nesta prova. Qual é ela?

Recursão por Curso de Valores

A idéia de *recursão por curso de valores* é usada para calcular o valor de uma função f (ou verificar se uma determinada propriedade é verdadeira) no $(n+1)$-ésimo número natural, não somente em termos do valor de f em n, mas usando também os demais valores de f em $0, 1, \ldots, n-1$, previamente obtidos. As definições que usam a recursão por curso de valores são ditas recursivas ou recorrentes. Para formalizar melhor temos:

Definição 2.4 *Definição Recursiva ou por Recorrência.*

São definições do tipo:

(i) Define-se em alguns valores iniciais e,

(ii) Os próximos valores são definidos em função dos valores previamente estabelecidos e dos valores já obtidos.

Exemplos

(1) A *seqüência de Fibonacci* é definida por

(i) $f(0) = f(1) = 1$ e

(ii) $f(n+1) = f(n) + f(n-1), \quad n \geq 1,$

de modo que seus termos iniciais são 1, 1, 2, 3, 5, 8, 13, ...

(Nota: Se n representar a quantidade de anos, $f(n-1)$ representa a quantidades de ramos de uma planta com a seguinte característica: Cada ramo que nasce, depois de dois anos de vida, faz brotar de si um ramo por ano. Com isto, no n-ésimo ano de vida da planta temos $f(n-1)$ ramos. Esta seqüência também serve para descrever a população de coelhos no n-ésimo ano, partindo de um casal e admitindo-se perfeitas condições para seu desenvolvimento.

(2) A **adição** de números naturais é definida por:

(i) $a + 0 = a$,

(ii) $a + (n+1) = (a+n) + 1, \ n \geq 0.$

Por exemplo, para calcular $3+2$ usamos (ii) $3+2 = (3+1)+1$ e precisamos de calcular $3+1$. Para calcular $3+1$ usamos (ii) para obter $3+1 = (3+0)+1$. Daí, sabendo-se que $3+0 = 3$, substitui-se na expressão anterior $(3+0)$ por 3 para obter $3+1$, daí obtém-se $3+2$. Então o processo é recorrente.

(3) A multiplicação de números naturais é definida por:

(i) $a.0 = 0$,

(ii) $a.(n+1) = a + (a.n),\ n \geq 0$.

Por exemplo, para calcular 3.2, o processo é o mesmo do exemplo anterior: precisamos de $3.0 = 0$. Daí $3.1 \overset{def.}{=} 3+3.0 = 3+0 = 3$ (pelo caso anterior). Agora $3.2 = 3 + 3.1 = 3 + 3$. Agora $3 + 3$ se calcula pela definição anterior para obter a quantidade denotada por 6.

(4) Para um número real $a > 0$, definimos potências naturais de a por:

(i) $a^0 = 1$,

(ii) $a^{n+1} = a.a^n,\ n \geq 0$.

Por exemplo, para calcular 3^2, precisaremos de 3^0 e 3^1. Temos $3^1 \overset{\text{def}}{=} 3.3^0 \overset{\text{def.}}{=} 3.1 = 3$ (caso anterior). Daí $3^2 = 3.3^1 = 3.3$, que se calcula pelo exemplo anterior, para obter uma quantidade que é denotada por 9.

Usando o P.I.F. pode-se provar as seguintes propriedades da potenciação:

Propriedades Para $a,\ b \in \mathbb{R},\ a > 0,\ b > 0$ e $n,\ m \in \mathbb{N}$, tem-se: **(a)** $a^n.a^m = a^{n+m}$, **(b)** $(a^n)^m = a^{n.m}$, **(c)** $(ab)^n = a^n.b^n$ e **(d)** $\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$.

Para ilustrar, vamos demonstrar a propriedade (a) por indução sobre n, e as demonstrações das outras propriedades ficam como exercícios de aplicação dos princípios de indução.

Temos $a^0.a^m \overset{\text{def.}}{=} 1.a^m = a^m = a^{0+m}$, e a condição (i) do primeiro princípio de indução está satisfeita. Para provar a condição (ii) suponha que $a^k.a^m = a^{k+m}$. Então $a^{k+1}.a^m \overset{\text{def.(ii)}}{=\!=} (a.a^k)a^m \overset{\text{assoc.}}{=\!=} a.(a^k.a^m) \overset{\text{hip.}}{=\!=} a.a^{k+m} \overset{\text{def.(ii)}}{=\!=} a^{1+(k+m)} = a^{(1+k)+m}$. Pelo primeiro princípio de indução finita, obtemos $a^n.a^m = a^{n+m}$ para todo $a > 0,\ a \in \mathbb{R}$ e $n,\ m \in \mathbb{N}$.

(5) $n!$ definido por $\begin{cases} \textbf{(i)}: & 0! = 1, \\ \textbf{(ii)}: & n! = n.(n-1)!, \quad n > 0 \end{cases}$

Por exemplo, $1! = 1,\ 2! = 2.1! = 2.1 = 2,\ 3! = 3.2! = 3.2 = 6$.

(6) A Função de Ackermann $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ é definida por:

$$\begin{cases} \textbf{(i)}: & A(0,n) = n+1, & n \geq 0; \\ \textbf{(ii)}: & A(m,0) = A(m-1,1), & m \geq 1; \\ \textbf{(iii)}: & A(m,n) = A(m-1, A(m,n-1)), & m > 0, n > 0. \end{cases}$$

Por exemplo, para calcular $A(2,0)$ temos:

$A(2,0) = A(1,1)$ por (ii). Daí por (iii) vem que $A(2,0) = A(0,A(1,0))$, e precisamos de $A(1,0)$ que por (ii) e (i) nos dá $A(1,0) = A(0,1) = 1+1 = 2$. Finalmente substituindo temos $A(2,0) = A(0,A(1,0)) = A(0,2) = 1+2 = 3$.

A função de Ackermann tem importante papel na teoria de funções recursivas e no estudo da complexidade de certos algoritmos envolvendo reuniões de conjuntos. Ela é usada para medir níveis de complexidade de funções recursivas.

2.2 Múltiplos e Divisores

Fixado um número inteiro m, $m\mathbb{Z}$ denotará o seguinte subconjunto de $\mathbb{Z}$,

$$m\mathbb{Z} := \{mq,\ q \in \mathbb{Z}\} = \{0, \pm m,\ \pm 2m,\ \pm 3m,\ \ldots,\ \pm qm,\ \ldots\}.$$

Definição 2.5 Seja $m \in \mathbb{Z}$. Dizemos que $x \in \mathbb{Z}$ *é múltiplo de* m ou que m *divide* x, ou ainda que x *é divisível por* m se $x \in m\mathbb{Z}$.

A notação para dizer que m divide (não divide) x é: $m|x$ (respectivamente $m \nmid x$).

Por exemplo, $20 \in 5\mathbb{Z}$, pois $20 = 5.4$; $-35 \in 5\mathbb{Z}$, pois $-35 = 5(-7)$. Logo, 20 e -35 são múltiplos de 5. Também podemos escrever $5|20$ e $5|(-35)$.

Note que $0|0$, pois $0 \in 0\mathbb{Z} = \{0\}$; aliás, $m|0$ qualquer que seja $m \in \mathbb{Z}$.

Propriedades Para todos $a,\ b,\ c \in \mathbb{Z}$, tem-se:

(i) $a|a$, **(ii)** $a|b$ e $b|c \Rightarrow a|c$, **(iii)** $a|b$ e $b|a \Rightarrow a = \pm b$,

(iv) $a|b$ e $a|c \Rightarrow a|(bx \pm cy)$, para quaisquer $x,\ y \in \mathbb{Z}$.

Demonstração: Demonstraremos apenas o item (iv), e os demais ficam como exercícios para o leitor interessado. Como $a|b$ e $a|c$, existem q_1 e $q_2 \in \mathbb{Z}$, tais que $b = aq_1$ e $c = aq_2$. Daí para

todos $x,\ y \in \mathbb{Z}$, $\quad bx \pm cy = (aq_1)x \pm (aq_2)y = a(q_1x \pm q_2y)$, com $q_1x \pm q_2y \in \mathbb{Z}$. Por definição, $a|(bx \pm cy)$. □

Exemplo. Como 3|6 e 3|9, então $3|(6x \pm 9y)$ quaisquer que sejam $x,\ y \in \mathbb{Z}$. Isto é claro pois $6x \pm 9y = 3(2x \pm 3y) \in 3\mathbb{Z}$.

2.2.1 Números Primos

Vamos denotar por $D(b)$ o subconjunto de $\mathbb{Z}$, formado pelos divisores do número inteiro b, e por $D^+(b)$ o subconjunto de $\mathbb{Z}$, formado pelos divisores positivos de b. Como b e $-b$ dividem b e um deles é positivo, nenhum desses subconjuntos é vazio.

Um número inteiro m não-nulo admite os divisores 1, -1, m e $-m$ ditos *divisores impróprios* de m. Outros divisores diferente destes, caso existam, são ditos *divisores próprios* de m.

Definição 2.6 Seja p um número inteiro distinto de 1, -1 e zero. Dizemos que p é um número *primo* se $D^+(p) = \{1, |p|\}$, ou seja, p não admite divisores próprios. Caso contrário, dizemos que p é um número *composto*.

Exemplo. Os números 2, 3, -11 são primos, enquanto 4, 6 são compostos.

Para determinar se um dado número $n > 1$ é primo, ou se queremos os números primos compreendidos entre 1 e n, podemos fazer uso do *Crivo de Eratóstenes* que consiste no seguinte:

Escrevemos numa linha ou tabela retangular os números de 1 a n. Cancelamos 1, deixemos 2 (este é primo) e cancelamos os outros múltiplos de 2 até n. O próximo número não cancelado é o 3. Deixemos o 3 (este é primo) e cancelamos os outros múltiplos de 3 até n. O próximo número não cancelado é o 5 (este é primo). Deixemos o 5 e cancelamos os outros múltiplos de 5 até n. Assim sucessivamente até chegar em $\sqrt{n} + 1$ (veja a proposição a seguir). Os números que restaram são os números primos compreendidos entre 1 e n. Por exemplo, vamos obter os números

primos p, $1 < p \leq 72$.

1	**2**	**3**	4	**5**	6	**7**	8	9	10	**11**	12
13	14	15	16	**17**	18	**19**	20	21	22	**23**	24
25	26	27	28	**29**	30	**31**	32	33	34	35	36
37	38	39	40	**41**	42	**43**	44	45	46	**47**	48
49	50	51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70	**71**	72

Proposição 2.7 *Seja $n \in \mathbb{Z}$, $n > 1$. Se n é composto, então n admite um divisor próprio $a \leq \sqrt{n}$.* Em particular n admite um divisor primo $p \leq \sqrt{n}$.

Demonstração: Será feita por redução ao absurdo.

Por hipótese existe $b \in \mathbb{Z}$, $1 < b < n$, tal que $n = a.b$. Então, se todos os divisores próprios de n são maiores que $\sqrt{n}$, temos $a > \sqrt{n}$ e $b > \sqrt{n}$. Fazendo o produto membro a membro temos: $a.b > \sqrt{n}.\sqrt{n} = n = a.b$, o que é absurdo. Assim, a primeira parte da proposição está concluída. Por que n admite um divisor primo $p \leq \sqrt{n}$? □

Exemplo. Mostre que 211 é um número primo.

Solução: Basta verificar que ele não possui divisores primos p menores que $\sqrt{211} < 15$. Por tentativa verifica-se que nenhum dos primos 2,3,5,7, 11,13 dividem 211. Logo 211 é um número primo.

Lema 2.8 Sejam $a \in \mathbb{Z}$, $a \neq \pm 1, a \neq 0$ e $S = D^+(a) - \{1\}$. Então $S \neq \emptyset$ e $\min S$ é um número primo.

Demonstração: Como a ou $-a \in D^+(a)$, então $S \neq \emptyset$. Pelo princípio do menor inteiro existe $p = \min S$. Se p fosse composto, existiria um divisor próprio r de p com $1 < r < p$. Mas isto implica que $r \in S$ e portanto p não seria o $\min S$; absurdo. Então p é primo como queríamos. □

Este Lema nos diz, em particular, que, se um número inteiro a é composto, ele admite um divisor primo.

Nota: Os números primos são importantes em criptografia, o estudo de mensagens secretas. No caso de senhas públicas e individuais, elas são feitas baseadas em um número composto n que é produto de dois primos grandes e não conhecidos do público em geral. Isto dificulta a descoberta de uma senha individual, porque é difícil decompor um número grande em produto de primos.

No entanto, se existisse um número finito de primos, esta técnica não funcionaria. Mas no seu famoso texto *The Elements*, o matemático Euclides apresenta (aproximadamente em 300 A.C.) uma bela prova por contradição para o seguinte resultado:

Teorema 2.9 Existem infinitos números primos.

Demonstração: Suponhamos que exista apenas um número finito de primos. Logo existe um número finito de primos positivos. Suponhamos que sejam: $p_1,\ p_2, \ldots,\ p_n$. Considere o número $m = p_1.p_2 \cdots p_n + 1$. Desde que $m > p_i$, então $m \neq p_i$ para todo $i = 1, 2, \ldots, n$. Logo m não é um número primo. Pela Proposição 2.7, existe $i \in \{1, \ldots, n\}$, tal que $p_i | m$. Como p_i também divide o produto $p_1.p_2 \cdots p_n$, pela propriedade (iv) de divisibilidade, concluímos que p_i divide $1 = m - p_1.p_2 \cdots p_n$. Absurdo. Portanto existem infinitos primos. □

Nota: Ao longo dos últimos 300 anos, muitos pesquisadores procuraram descobrir primos grandes. O maior primo conhecido é do tipo especial $2^p - 1$, onde p é primo. Os primos do tipo $2^p - 1$ são ditos *Primos de Mersenne*, (Marin Mersenne 1566-1648).

A razão de os maiores primos conhecidos serem primos de Mersenne é que existe um teste extremamente eficiente, conhecido como teste de Lucas-Lehmer, para determinar quando um número do tipo $2^p - 1$ é primo. Além disto, o teste não é bom para verificar rapidamente se outros tipos de números distintos de $2^p - 1$, p : primo são ou não são primos.

Exemplo. Os números $2^2 - 1 = 3$, $2^3 - 1 = 7$ e $2^5 - 1 = 31$ são primos de Mersenne. Mas $2^{11} - 1 = 2.047$, não é um primo (de Mersenne), pois $2.047 = (23).(89)$. Note que, se $n = ab$ (composto),

então $2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{(b-1)a} + 2^{(b-2)a} + \cdots + 2^a + 1)$ também é composto.

Com o advento do computador, muitos primos de Mersenne têm sido descobertos. Até meados do ano 2002 eram conhecidos trinta e nove primos de Mersenne, com oito deles descobertos de 1990 para cá. O maior primo de Mersenne conhecido até meados de 2002 é $2^{13466917} - 1$, um número com mais de quatro milhões de dígitos, que foi provado que é primo em 2001.

Até o momento não existe um método que dê o n-ésimo número primo, e existem muitas perguntas importantes sobre números primos sem respostas. Uma pergunta interessante é: Quantos números primos existem entre 1 e um número n positivo, dado? Esta questão até hoje é de interesse matemático e por longos anos tem sido objeto de pesquisa. Nos últimos dezoito séculos, os matemáticos têm feito longas tabelas de números primos para obter evidências sobre a distribuição de primos. A seguinte conjectura é devido aos grandes matemáticos Gauss e Legendre.

Conjectura: *A razão do número de primos positivos não excedendo* n *e* $\dfrac{n}{\ln n}$ *aproxima de 1 quando* n *cresce infinitamente.*

Seja $\phi(n)$ a quantidade de números primos positivos que não excede n. A conjectura de Gauss Legendre afirma que o quociente $\dfrac{\phi(n)}{n/\ln n}$ tende a 1 quando n vai para o infinito, ou ainda, $\lim\limits_{n\to\infty} \dfrac{\phi(n)\ln n}{n} = 1$.

2.2.2 Máximo Divisor Comum (mdc).

Sejam a e b inteiros não ambos nulos. O maior inteiro d, tal que $d|a$ e $d|b$, é dito *máximo divisor comum* de a e b. Denota-se d por $mdc(a, b)$.

Define-se como sendo zero o $mdc(0, 0)$; $0 = mdc(0, 0)$.

O $mdc(a, b)$ sempre existe, pois o conjunto dos divisores positivos de um número inteiro não-nulo é finito. Para determiná-lo, basta considerar o conjunto de divisores comuns a a e b e tomar o

maior deles. Como a e $-a$ dividem a, e um deles é positivo, basta procurar d no conjunto $D^+(a) \cap D^+(b)$.

Exemplo

(1) Calcule $mdc(-24, 36)$.

Solução: Os divisores de -24 são os mesmos de 24. Logo, basta considerar: $D^+(24) \cap D^+(36) = \{1, 2, 3, 4, 6, 8, 12, 24\} \cap \{1, 2, 3, 4, 6, 9, 12, 18, 36\} = \{1, 2, 3, 4, 6, 12\}$. Por definição $mdc(-24, 36) = 12$.

(2) $mdc(7, 10) = 1$, pois $D^+(7) = \{1, 7\}$, e 7 não divide 10.

O processo natural de calcular o mdc de dois números dados, como exemplificado acima, não é muito prático. Existe um processo para o cálculo de $mdc(a, b)$ que consiste no seguinte procedimento: (1) Verifique se um dado número d é positivo; (2) Verifique se d divide a e b; (3) Tome um divisor comum de a e b, digamos d' e verifique se d' divide d. Caso d satisfaça estas condições, então d é o $mdc(a, b)$.

De fato, desde que $a|c \Longrightarrow (a|c \text{ e } -a|c)$ e o maior deles é positivo, tem-se que o $mdc(a, b) \geq 0$. A condição (2) é trivialmente satisfeita pelo $mdc(a, b)$. Agora, se pudermos escrever o $mdc(a, b)$ na forma $mdc(a, b) = ra + sb$, para algum $r, s \in \mathbb{Z}$, então a propriedade (iv) de divisibilidade nos dá que d' divide o $mdc(a, b)$, qualquer que seja o divisor d' de a e b. A igualdade $mdc(a, b) = ra + sb$, para algum $r, s \in \mathbb{Z}$, é conhecida como *identidade de Bezout* e será demonstrada adiante. Portanto, a condição (3) é também satisfeita e podemos redefinir o máximo divisor comum de dois números inteiros a e b dados, da seguinte forma:

Definição 2.10 Sejam a e $b \in \mathbb{Z}$, com a ou b não nulo. Um número inteiro d é dito *o máximo divisor comum de a e b* e escrevemos $d = mdc(a, b)$ se,

(1) $d \geq 0$,

(2) $d|a$ e $d|b$,

(3) Se $d'|a$ e $d'|b$ então $d'|d$.

Por convenção $0 := mdc(0, 0)$.

Definição 2.11 (i) Dois inteiros a e b são ditos *relativamente primos* quando $mdc(a, b) = 1$.

(ii) Os inteiros $a_1, a_2, \ldots, a_n$ são ditos *relativamente primos* 2 a 2, ou *relativamente primos aos pares*, se $mdc(a_i, a_j) = 1,\ \forall i, j,\ 1 \leq i < j \leq n$.

Teorema 2.12 (Algoritmo da Divisão Euclidiana)
Seja $m \in \mathbb{Z},\ m > 0$ fixo. Dado $a \in \mathbb{Z}$, existem q e $r \in \mathbb{Z}$ únicos nas condições: $a = qm + r$ e $0 \leq r < m$.

Os números q e r são ditos respectivamente quociente e resto da divisão (euclidiana) de a por m.

Demonstração: O subconjunto $S = \{a - qm \geq 0,\ q \in \mathbb{Z}\}$ é não vazio (pois $m\mathbb{Z}$ é ilimitado). Seja $r = minS$. Então existe $q \in \mathbb{Z}$ tal que $a = qm + r, 0 \leq r$. Se r fosse maior ou igual a m, existiria $b \in \mathbb{Z},\ b \geq 0$, tal que $r = m + b$. Disto segue-se que $0 \leq b < r$ e $b = r - m = (a - qm) - m = a - (q + 1)m \in S$, absurdo pois $r = minS$. Assim $0 \leq r < m$ como queríamos.

Para demonstrar a unicidade, suponhamos que $a = q_1m + r_1 = qm + r$, com $0 \leq r_1 < m$ e $0 \leq r < m$. Então $r - r_1 = (q_1 - q)m$. Como $0 \leq r,\ r_1 < m$ temos $|(q_1 - q)m| = |r - r_1| < m$. Se $q_1 - q \neq 0$, então $|(q_1 - q)m| \geq m$, o que dá um absurdo. Portanto $q_1 = q$ e, consequentemente, $r = r_1$, como queríamos. □

Exemplo. Para $m = 3$ e $a = 19$, o par (q, r) é $(6, 1)$, pois: $18 = 6.3 + 1$. Se $a = -13$, então $q = -5$ e $r = 2$, pois: $-13 = (-5)3 + 2$.

Note que qm é o maior múltiplo de m à esquerda de a (na reta real) para que $0 \leq r < m$.

Um método bastante usado para o cálculo do *mdc* de dois números inteiros $a,\ b$ dados é o processo das divisões sucessivas que será descrito a seguir. Devido às observações já feitas anteriormente, de que $D^+(c) = D^+(-c)$, podemos considerar a e b estritamente positivos e também distintos. O processo baseia-se essencialmente no seguinte lema:

Lema 2.13 *Sejam a, b inteiros estritamente positivos com $a > b$. Então $mdc(a, b) = mdc(b, r)$, onde r é o resto da divisão euclidiana de a por b.*

Demonstração: De fato, seja $d = mdc(a, b)$, vamos demonstrar que $d = mdc(b, r)$. Pelo algoritmo da divisão $a = bq + r$ com $0 \leq r < b$. Então $r = a - bq$. Como $d|a$ e $d|b$, pela propriedade (iv) de divisibilidade então $d|r$. Assim (1) $d \geq 0$, (2) $d|b$, $d|r$ e resta demonstrar a condição (3) da definição de mdc.

Se $d'|b$ e $d'|r$, novamente pela propriedade (iv) de divisibilidade, temos $d'|a$. Assim $d'|a$ e $d'|b$. Como $d = mdc(a, b)$, por definição temos $d'|d$ (pois $d = mdc(a, b)$). Portanto $d = mdc(b, r)$. □

O processo prático para obter o $mdc(a, b)$ envolve uma sucessão de divisões: divide-se o maior deles pelo menor obtendo um resto r_1. Supondo r_1 não-nulo, divide-se o quociente (menor dos números dados) por r_1 obtendo um quociente q_2 e um resto r_2. O processo continua sucessivamente dividindo q_i por r_i obtendo q_{i+1} e r_{i+1}, enquanto o resto obtido for diferente de zero (isto é $r_{j+1} = 0$). Note que, de fato, o processo pára desde que, nestas divisões sucessivas temos $0 = r_{j+1} < \cdots < r_j < r_{j-1} < \cdots < r_2 < r_1 < b < a$, onde, para $i \geq 3$, r_i é o resto da divisão de r_{i-2} por r_{i-1}.

Usando o Lema repetidas vezes, conclui-se que o último resto não nulo r_j é o $mdc(a, b)$. De fato, $mdc(a, b) = mdc(b, r) = mdc(r_1, r_2) = \cdots = mdc(r_j, r_{j-1}) = r_j$.

Resumindo isto em uma tabela, temos:

$a = bq + r_1,$	$0 < r_1 < b$	$d\|r_1$	$r_j\|a$
$b = r_1q_1 + r_2,$	$0 < r_2 < r_1$	$d\|r_2$	$r_j\|b$
$r_1 = r_2q_2 + r_3,$	$0 < r_3 < r_2$	$d\|r_3$	$r_j\|r_1$
$r_2 = r_3q_3 + r_4,$	$0 < r_4 < r_3$	$d\|r_4$	$r_j\|r_2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r_{j-2} = r_{j-1}q_{j-1} + r_j,$	$0 < r_j < r_{j-1}$	$d\|r_j$	$r_j\|r_{j-2}$
$r_{j-1} = r_jq_j,$	$0 = r_{j+1}$		$r_j\|r_{j-1}$

Aplicando este resultado para 30 e 34 temos:

divisores	34	30	4	2
quocientes		1	7	2
restos	4	2	0	

ou seja, $34 = 30.1 + 4$ e $30 = 4.7 + 2$.

O último resto não-nulo é 2, e então $2 = mdc(30, 34)$.

A partir deste processo temos um algoritmo para escrever $d = mdc(a, b)$ como combinação linear de a e b, ou seja, escrever d na forma $d = ra + sb$, $r, s \in \mathbb{Z}$.

Exemplo (i) Pelo exemplo anterior já vimos que $2 = mdc(30, 34)$. Vamos determinar r e s tais que $2 = r30 + s34$. Considerando as divisões feitas acima, temos:

$$\begin{cases} 34 = 30.1 + 4 \\ 30 = 4.7 + 2. \end{cases}$$

Isolando os restos temos: $\begin{cases} 4 = 1.34 + (-1).30 \\ 2 = (1).30 + (-7).4. \end{cases}$

Substituindo 4 da primeira equação na segunda, obtemos: $2 = (1).30+(-7)4 = (1).30+(-7)[(1).34+(-1)30] = (1).30+(-7).34+(7).(30)$. Ou seja, $2 = (8)(30) + (-7)(34)$, $r = 8$, $s = -7$ são soluções. Não temos unicidade para o par (r, s), e fica como exercício o cálculo de outras soluções de $2 = r30 + s34$.

(ii) Escreva $d = mdc(30, -34)$ na forma $d = r30 + s(-34)$.

Solução: Como $mdc(30, -34) = mdc(30, 34)$ e $2 = (8)(30) + (-7)(34)$, tem-se $2 = (8)(30) + (7)(-34)$. Logo $r = 8$ e $s = 7$.

Teorema 2.14 (Identidade de Bezout) *Sejam a, b números inteiros e $d = mdc(a, b)$. Então existem r, $s \in \mathbb{Z}$, tais que $d = r.a + s.b$.*

Demonstração: O caso $a = b = 0$ é obvio, pois $d = 0$. Se $a \neq 0$ ou $b \neq 0$, considere $L = \{x.a + y.b > 0,\ x,\ y \in \mathbb{Z}\}$. Como $|a|$ ou $|b| \in L$ e L é um subconjunto de $\mathbb{Z}$ limitado inferiormente, ele possui um mínimo, digamos d. Como $d \in L$, existem $r, s \in \mathbb{Z}$, tais que $d = r.a + s.b$. Provemos que $d = mdc(a, b)$, o que concluirá a demonstração.

Pelo Algoritmo da Divisão, existem q e r_1, tais que $a = dq + r_1$ e $0 \leq r_1 < d$. Assim, $r_1 = a - dq = (1 - qr)a - (qs)b$ e, se $r_1 \neq 0$, viria que $r_1 \in L$ com $r_1 < d$, absurdo. Então $r_1 = 0$ e portanto $d|a$. Analogamente se demonstra que $d|b$. Agora, para todo $d' \in \mathbb{Z}$, tal que $d'|a$ e $d'|b$, pela propriedade (iv) de divisores segue que $d'|d$. Por definição, concluímos que $d = mdc(a, b)$. □

2.3 Teorema Fundamental da Aritmética

Uma propriedade característica dos números primos, e bastante útil, é apresentada na proposição a seguir:

Proposição 2.15 Seja $p \in \mathbb{Z}$, $p \neq \pm 1$ e $p \neq 0$. O número p é primo se, e somente se, sempre que p divide $a.b$ tem-se que p divide a ou p divide b.

Demonstração - Suponhamos que p seja um número primo e que $p|a.b$. Vamos provar que, se $p \nmid a$, então $p|b$.

De fato, se $p \nmid a$, então $1 = mdc(p, a)$, pois p é primo. Pelo Teorema 2.14 existem $r, s \in \mathbb{Z}$, tais que $1 = r.p + s.a$. Multiplicando ambos os membros desta igualdade por b, obtemos: $b = p(r.b) + s(a.b)$. Como $p|p$ e $p|a.b$ (por hipótese), pela propriedade (iv) de divisores segue que $p|b$.

Reciprocamente, para mostrar que p só admite divisores impróprios basta mostrar que $D^+(p) = \{1, |p|\}$. Como $D^+(p) = D^+(-p)$, podemos considerar $p > 0$. Seja $x \in \mathbb{Z}$ um divisor de p com $1 \leq x \leq p$. Então existe $y \in \mathbb{Z}$, $1 \leq y \leq p$, tal que $p = x.y$. Como p divide p, temos $p|x.y$. Por hipótese $p|x$ ou $p|y$. Daí $x = pu$ ou $y = pu$, para algum $u \in \mathbb{Z}$. Substituindo em $p = x.y$ ficamos com $p = puy$ ou $p = xpu$ e cancelando p temos $1 = uy$ ou $1 = xu$. Como u e x são números naturais, vem que $u = 1$. Logo $x = p$ ou $x = 1$ (quando $p = y$). Portanto $D^+(p) = \{1, p\}$. □

Corolário 2.16 Seja $p \in \mathbb{Z}$ um número primo. Se p divide um produto $a_1 a_2 \cdots a_n$ de números inteiros, então p divide ao menos um dos a_i, $i \in \{1, 2, \ldots, n\}$.

A demonstração pode ser feita por indução sobre n e fica como exercício. □

Teorema 2.17 (Fundamental da Aritmética) *Todo número inteiro $a \neq \pm 1$, $a \neq 0$ se decompõe de modo único (a menos da ordem dos fatores) na forma*

$$a = up_1p_2 \cdots p_n,$$

onde p_i é um número primo positivo para todo $i = 1, 2, \ldots, n$ e $u \in \{\pm 1\}$.

Demonstração: Basta demonstrar para $a > 1$ e faremos a prova por indução sobre a.

(i) Se $a = 2$ nada a fazer, pois $2 = 1.2$ é primo.

(ii) Suponhamos o teorema verdadeiro para todo $b \in \mathbb{Z}$, $1 < b \leq k$ com $k \in \mathbb{Z}$, $k > 1$. Se $k + 1$ é primo, o resultado é obvio; senão, pelo Lema 2.13 $p_1 = min\{x \in \mathbb{Z} \mid x > 1 \text{ e } x|(k+1)\}$ é primo. Assim $k+1 = p_1.q$ com $1 < q \leq k$. Por hipótese de indução $q = p_2p_3 \cdots p_r$. Daí $k + 1 = p_1p_2 \cdots p_r$, com $p_1, p_2, \ldots, p_r$ números primos. O resultado segue-se pelo 2^o princípio de indução finita.

Unicidade - Consideremos duas decomposições para um número $a \in \mathbb{Z}$, $a > 1$.

$$a = p_1p_2 \cdots p_n = q_1q_2 \cdots q_m, \qquad (*)$$

com p_i e q_j primos. Então p_1 divide $q_1q_2 \cdots q_m$. Pelo Corolário 2.16 segue que p_1 divide q_j para algum j. Reordenando, se for necessário, podemos supor que $j = 1$, ou seja, $p_1|q_1$. Como ambos são primos é fácil ver que $p_1 = \pm q_1$. Substituindo em $(*)$ e cancelando p_1, ficamos com

$$\pm p_2 \cdots p_n = q_2 \ldots q_m.$$

Repetindo o argumento algumas vezes, ficaremos com $\pm 1 = q_{n+1} \cdots q_m$ caso $n < m$, ou $p_{m+1} \ldots p_n = \pm 1$ caso $n > m$, o que é absurdo. Então só nos resta $n = m$ e $p_i = \pm q_i$ depois de uma possível reordenação dos índices, se necessário. □

Exemplo. $18 = 2.3.3 = 3.2.3 = 2(-3)(-3) = (-3)(-2)3 = \cdots$ e estas decomposições são iguais, a menos dos números associados 2,-2 e 3,-3 e de permutação dos fatores primos.

Observação: Na decomposição em fatores primos, podemos agrupar os primos que se repetem e escrever $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, onde $\alpha_i > 0$. Algumas vezes, como veremos a seguir, é importante fazer aparecer na decomposição de n em fatores primos um primo que efetivamente não faz parte dela. Neste caso incluímos o primo com potência nula.

Um método prático para se calcular o máximo divisor comum dos números não-nulos a e b é considerar suas decomposições em fatores primos. De fato, sejam $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, $p_i \neq p_j$, se $i \neq j$, $\alpha_i \geq 0$ e $\beta_j \geq 0$, onde todos os primos p_i que ocorrem nas decomposições de a e de b estão incluídos em ambas as fatorações, com expoentes zero se necessário. Assim o $mdc(a, b)$ é dado por

$$mdc(a, b) = p_1^{min\{\alpha_1,\beta_1\}} p_2^{min\{\alpha_2,\beta_2\}} \cdots p_n^{min\{\alpha_n,\beta_n\}}.$$

De fato, $d = p_1^{min\{\alpha_1,\beta_1\}} p_2^{min\{\alpha_2,\beta_2\}} \cdots p_n^{min\{\alpha_n,\beta_n\}}$ divide ambos os inteiros a e b, desde que cada potência dos primos, que ocorre na fatoração de d, não excede as potências deste mesmo primo que ocorre nas decomposições de a e de b. Além disso, não existe um inteiro c maior que d que divide a e b, senão existiria um fator de c da forma $p_i^{t_i}$ com $p_i^{t_i} > p_i^{min\{\alpha_i,\beta_i\}}$. Portanto, t_i seria maior que $min\{\alpha_i, \beta_i\} = \alpha_i$ ou β_i. Logo, c não dividiria a ou não dividiria b.

Exemplo. Como as fatorações de 120 e 252 são: $120 = 2^3.3.5$ e $252 = 2^2.3^2.7$, escrevemos: $120 = 2^3.3.5.7^0$ e $252 = 2^2.3^2.5^0.7$. Daí $mdc(120, 252) =$

$$= 2^{min\{3,2\}} 3^{min\{1,2\}} 5^{min\{1,0\}} 7^{min\{0,1\}} = 2^2.3^1.5^0.7^0 = 12.$$

A fatoração de um número também pode ser usada para calcular o *mínimo múltiplo comum* de dois inteiros.

Definição 2.18 O *mínimo múltiplo comum* de dois inteiros a e b, denotados por $mmc(a, b)$, é o menor inteiro positivo divisível por ambos os inteiros a e b.

Como este conjunto é limitado inferiormente por zero, o Princípio do menor inteiro garante a existência de $mmc(a,b)$, quaisquer que sejam os inteiros a e b.

Consideremos novamente as decomposições de a e b em fatores primos: $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, com $\alpha_i \geq 0$, $\beta_i \geq 0$. Então é fácil provar que

$$mmc(a,b) = p_1^{max\{\alpha_1,\beta_1\}} p_2^{max\{\alpha_2,\beta_2\}} \cdots p_n^{max\{\alpha_n,\beta_n\}}.$$

De fato, um múltiplo comum de a e b deve conter pelo menos $max\{\alpha_i, \beta_i\}$ potências do primo p_i em sua fatoração.

Exemplo. Como as fatorações de 120 e 252 são: $120 = 2^3.3^1.5^1.7^0$ e $252 = 2^2.3^2.5^0.7^1$, então $mmc(120, 252) =$
$= 2^{max\{3,2\}}.3^{max\{1,2\}}.5^{max\{1,0\}}.7^{max\{0,1\}} = 2^3.3^2.5^1.7^1 = 2520.$

O seguinte teorema relaciona o máximo divisor comum e o mínimo múltiplo comum de dois inteiros e pode ser provado usando os resultados anteriores.

Teorema 2.19 Sejam a e b inteiros. Então

$$|a.b| = mdc(a,b).mmc(a,b).$$

□

Propriedades (do MDC e do MMC). Quaisquer que sejam $a, b, c \in \mathbb{Z}$, tem-se:

(i) $mdc(a,b) = mdc(b,a)$ e $mmc(a,b) = mmc(b,a)$.

(ii) $mdc(0,b) = |b|$ e $mmc(0,b) = 0$.

(iii) $mdc(a,b) = mdc(\pm a, \pm b)$ e $mmc(a,b) = mmc(\pm a, \pm b)$.

(iv) $mdc(mdc(a,b),c) = mdc(a, mdc(b,c))$ e
$mmc(mmc(a,b),c) = mmc(a, mmc(b,c))$. □

2.4 Congruência

Definição 2.20 Dado $m \in \mathbb{Z}$, $m > 1$ e b, $c \in \mathbb{Z}$, dizemos que b é *congruente* (ou *côngruo*) a c módulo m, se m divide $b - c$.
Notação $b \equiv c(mod\ m)$.

Exemplo $5 \equiv 5(mod\ 3)$ pois $3|(5-5)$, $5 \not\equiv 1(mod\ 3)$ pois $3 \nmid (5-1)$, $7 \equiv -11(mod\ 6)$ pois 6 divide $18 = 7-(-11)$.

Propriedades: Dado $m \in \mathbb{Z}$, $m > 1$, para todos $a, b, c, d \in \mathbb{Z}$, tem-se:

(i) $a \equiv a(mod\ m)$,
(ii) Se $a \equiv b(mod\ m)$, então $b \equiv a(mod\ m)$,
(iii) Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$, então $a \equiv c(mod\ m)$,
(iv) Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $a \pm c \equiv b \pm d(mod\ m)$ e $ac \equiv bd(mod\ m)$,
(v) Se $a \equiv b(mod\ m)$, então $ac \equiv bc(mod\ m)$,
(vi) Se $a \equiv b(mod\ m)$, então $a^n \equiv b^n(mod\ m)$, $\forall n \geq 0$.
(vii) $a \equiv r(mod\ m)$, onde r é o resto da divisão euclidiana de a por m.

Demonstração: **(i)** segue-se do fato que m divide $0 = a - a$.
(ii) Se m divide $a-b$, então $a-b = qm$, $q \in \mathbb{Z}$. Daí $b-a = (-q)m$. Logo m divide $b-a$, ou seja, $b \equiv a(mod\ m)$.
(iii) Por hipótese existem q_1, $q_2 \in \mathbb{Z}$, tais que $a - b = q_1 m$ e $b - c = q_2 m$. Somando as igualdades, membro a membro, obtém-se $a - c = (q_1 + q_2)m$. Daí $a \equiv c(mod\ m)$.
(iv) Por hipótese existem q_3, $q_4 \in \mathbb{Z}$, tais que

$$a - b = q_3 m \quad \text{e} \quad c - d = q_4 m. \qquad (*)$$

Somando (e subtraindo) membro a membro, obtemos $(a+c)-(b+d) = (q_3+q_4)m$ (e $(a-c)-(b-d) = (q_3-q_4)m$); daí segue-se que $a \pm c \equiv b \pm d(mod\ m)$.
De $(*)$ também temos $a = q_3 m + b$ e $c = q_4 m + d$. Multiplicando membro a membro e pondo m em evidência, obtemos $ac = (q_3 q_4 m + q_3 d + q_4 b)m + bd$. Então $ac - bd \in m\mathbb{Z}$ e, daí, segue-se o resultado.
(v) Por hipótese $a - b = q_5 m$ para algum $q_5 \in \mathbb{Z}$. Então $c(a-b) = c.q_5 m$ qualquer que seja $c \in \mathbb{Z}$, ou seja, m divide $ac - bc$. Daí $ac \equiv bc(mod\ m)$.
(vi) Segue-se por indução sobre n, usando (iv) com c (respectivamente d) uma potência de a (respectivamente de b).
(vii) De $a = qm + r$, $0 \leq r < m$, tem-se que $a \equiv r(mod.m)$. $\square$

2.5 Aplicações da Aritmética

A teoria dos números tem muitas aplicações em muitas áreas das ciências. Como aplicações de congruência e divisibilidade, daremos um método para se criptografar mensagens de um modo seguro e faremos um breve estudo de representação de números inteiros em uma base b, em especial quando $b = 2, 4, 8$ ou 16, muito útil na teoria de computação.

2.5.1 (I) Criptografia

Congruência e funções podem ser usadas para designar locação de memória para arquivos de computação, gerar variáveis falsas e criptografar, etc.

Um dos primeiros métodos conhecidos de criptografar é devido a Julius Caesar. O método conhecido de *Caesar* consiste em codificar uma mensagem trocando cada letra da sentença pela letra que está três posições adiante desta no alfabeto. Isto é feito ciclicamente, de modo que as três últimas letras do alfabeto passam a ser, respectivamente, as três primeiras letras do alfabeto, na codificação. Assim, nesta codificação A, é enviada para D, B é enviada para E e X é enviada para A, por exemplo.

Para simplificar vamos identificar cada letra com sua posição no alfabeto.

a	b	c	d	e	f	g	h	i	j	k	l	m	n
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
1	2	3	4	5	6	7	8	9	10	11	12	13	14

o	p	q	r	s	t	u	v	w	x	y	z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
15	16	17	18	19	20	21	22	23	24	25	26.

Exemplo Vamos codificar segundo Caesar a sentença "*Abacaxi é uma fruta tropical*".

Trocando as letras pelos números correspondentes de suas posições, temos:
1 2 1 3 1 24 9 - 5 - 21 13 1 - 6 18 21 20 1 - 20 18 15 16 9 3 1 12.

Somando 3($mod.$26) temos:
4 5 4 6 4 1 12 - 8 - 24 16 4 - 9 21 24 23 4 - 23 21 18 19 12 6 4 15.
Assim, a palavra que codifica "Abacaxi é uma fruta" é

dedfdal h xpd iuxwd wurslfdo.

No caso de enviar para alguém a mensagem codificada "abacaxi é uma fruta tropical", se envia a sequência: "dedfdal h xpd iuxwd wurslfdo". E para saber qual é a mensagem enviada, o receptor deve ter a "chave" para decriptografar que neste caso é:

$$f^{-1}(y) = y + 23(mod.\ 26),$$

onde $y = f(x)$ é a função $f(x) = x + 3(mod.26)$.

Existem vários meios de generalizar a codificação de Caesar. Por exemplo, em vez de trocar cada letra pela terceira letra ($mod.$26) adiante dela no alfabeto, podemos trocá-la pela k-ésima letra ($mod.$26) adiante dela no alfabeto. Caso $f(x)$ seja uma função bijetora sobre $A = \{1, 2, 3, \ldots, 26\}$, podemos usá-la para codificar. Particularmente, se $f(x) = \overline{ax+b}$ é definida sobre $A = \{1, 2, \ldots, 26\}$ ($\overline{ax+b}$ é o resto da divisão Euclidiana de $ax + b$ por 26), para a, b inteiros convenientes, podemos codificar sentenças usando $f(x)$. A função $f(x)$ deve ser bijetora para que **(i)** cada letra seja enviada em uma única letra, **(ii)** letras distintas sejam enviadas em letras distintas e, finalmente, **(iii)** toda letra seja imagem de outra letra. As condições necessárias e suficientes sobre a para que f satisfaça as condições acima são:

Lema 2.21 *Sejam $a,\ b \in \mathbb{Z},\ a \neq 0$ e $A = \{1, 2, 3, \ldots, 26\}$. A função $f : A \to A$ definida por $f(x) = \overline{ax+b}$ é bijetora se, e somente se, $mdc(a, 26) = 1$.*

Demonstração: Como o resto da divisão Euclidiana de $ax + b$ por 26 é único, a função f está bem definida. Sejam $x, y \in A$, tais que $f(x) = f(y)$. Então $\overline{ax+b} = \overline{ay+b}$, ou seja,

$$a(x - y) \equiv 0(mod\ 26). \qquad (*)$$

Como $mdc(a, 26) = 1$, pela identidade de Bezout (Teo.2.14) existem $r, s \in \mathbb{Z}$, tais que $1 = s.a + r.26$, ou seja,

$$1 \equiv s.a(mod\ 26) \qquad (**)$$

Multiplicando ambos os membros de $(*)$ por s, tem-se $as(x-y) \equiv s.0(mod\ 26)$. Por $(**)$ temos $x - y \equiv 0(mod\ 26)$. Como $x, y \in A$, vem que $|x - y| < 26$. Logo, $x = y$ e então f é injetora. Como A é um conjunto finito, segue-se que f é bijetora.

Reciprocamente, suponhamos que $f(x)$ é bijetora e seja $b = 26.q + r$, onde $0 \leq r < 26$. Então $r + 1 \in A$ e portanto existe $x_0 \in A$, tal que $f(x_0) = \overline{ax_0 + b} = r + 1$. Substituindo b e fazendo as reduções módulo 26, obtemos $ax_0 \equiv 1(mod\ 26)$. Logo existe $s \in \mathbb{Z}$, tal que $26.s + a.x_0 = 1$. Seja $d = mdc(a, 26)$. Como d divide 26 e d divide a, concluímos que d divide $26.s + a.x_0 = 1$. Logo $d = 1$. □

Exemplo Como $mdc(3, 26) = 1$, a função $g(x) = \overline{3x + 3}$ pode ser usada para dar uma boa "embaralhada" nas letras do alfabeto. Usando $g(x)$ para codificar "A lua é bela" temos:

Primeiro substituímos as letras por suas posições no alfabeto.

a	l	u	a	é	b	e	l	a
↕	↕	↕	↕	↕	↕	↕	↕	↕
1	12	21	1	5	2	5	12	1

Esta seqüência de números é levada pela $g(x)$ em $g(1), g(12), g(21), \ldots, g(12), g(1)$. De $3.12 + 3 = 39 \equiv 13(mod\ 26)$ e $3.21 + 3 = 66 \equiv 14(mod\ 26)$, segue que $g(12) = 13$ e $g(21) = 14$. Além destes, temos $g(1) = 3.1 + 3 = 6$, $g(5) = 3.5 + 3 = 18$, $g(2) = 3.2 + 3 = 9$. Conseqüentemente, a seqüência de números é levada pela função g na seguinte seqüência codificada:

6 - 13 14 6 - 18 - 9 18 13 6,

que corresponde à seqüência de letras "f mnf r irmf".

A função inversa de g é a chave para a decodificação. Ela é dada por

$$h(y) = \overline{9y + 25}.$$

De fato, $g \circ h = h \circ g = 1_A$. Portanto, a seqüência

6 - 13 14 6 - 18 - 9 18 13 6

é levada em

1 - 12 21 1 - 5 - 2 5 12 1,

que corresponde a "a lua é bela".

Uma outra boa aplicação da teoria dos números na computação vem da representação de um número em uma base b, $b > 1$.

2.5.2 (II) Representação de Números em Bases e as Quatro Operações Básicas

Representação de Números em Bases

No dia a dia, usamos a notação decimal para representar números. Por exemplo, a seqüência 234 é usada para denotar $2.10^2 + 3.10 + 4$. No entanto, muitas vezes é conveniente usar bases diferentes de 10. O termo *algoritmo* originalmente se refere a procedimentos, ou programas, para executar operações aritméticas, e foram desenvolvidos originalmente usando a representação decimal de números inteiros. Usualmente os computadores estão preparados para o uso da notação binária (base 2) quando se faz operações aritméticas, e notações octal (base 8) ou hexadecimal (base 16) quando se lida com caracteres, tais como letras ou dígitos.

O sistema de numeração decimal é composto de 10 dígitos, e os mais usados são: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, cujos valores numéricos dependem da posição de cada dígito na seqüência em relação a um ponto de referência chamado vírgula decimal. Por exemplo, 474,54 representa o número $4.10^2+7.10+4.10^0+5.10^{-1}+4.10^{-2}$, e o primeiro dígito 4, a partir da esquerda, em 474,54, tem o valor numérico 400 (quatrocentos), o segundo dígito 4 na seqüência tem o valor numérico 4, enquanto o terceiro dígito 4 tem o valor numérico $\frac{4}{100}$ (quatro centésimos). A representação em seqüência com valores dos dígitos dependendo da posição nos permite representar qualquer número usando apenas os 10 dígitos acima. Qualquer que seja a base $b > 1$ usada, o sistema de numeração é também posicional e funciona exatamente igual ao sistema decimal. No caso binário (base 2) usamos 2 dígitos: 0 e 1. Os algoritmos adaptados para o uso com representação binária de números são a base para a aritmética de computadores, porque estes algoritmos são mais

fáceis de se implementar eletronicamente, além da base binária permitir relações com a lógica clássica. No entanto, como a base 2 é a menor possível, a grande desvantagem do sistema binário é que em geral são necessárias grandes seqüências de dígitos "zeros"e "uns"para representar números. Por exemplo, 9990 na base decimal tem representação 10011100000110 na base binária, e foram necessários 14 dígitos binários para representar um número com apenas 4 dígitos decimais.

Para explorar melhor a expansão de um número numa base b, vamos desenvolver as 4 operações básicas efetuadas sobre números em diferentes bases. Fixaremos nossa atenção nas bases decimal e binária, octal e hexadecimal, devido ao uso e à importância computacional. Comecemos com um teorema que dá a representação única de um número inteiro em uma dada base. Os números fracionários serão explorados mais tarde.

Teorema 2.22 *Seja b um inteiro positivo maior que 1. Então cada inteiro positivo n maior que zero pode ser representado de modo único na forma*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

com $a_1,\ a_2, \ldots, a_k$ positivos menores que b e $a_k \neq 0$.

Demonstração: Se $n = 1$, então $k = 0$ e $a_k = 1$, qualquer que seja $b > 1$. Suponha, como hipótese de indução, a validade do teorema para todos $q \in \mathbb{Z}$, $0 < q < n$. Pelo algoritmo da divisão existem $q_1,\ a_0 \in \mathbb{Z}$: únicos, com $0 \leq a_0 < b$, tais que $n = bq_1 + a_0$. Como n e b são estritamente positivos com $b > 1$ e $a_0 \geq 0$, vem que $q_1 < n$. Logo, por hipótese de indução, existem $a_{k+1},\ a_k,\ \ldots,\ a_1$ menores que b e $a_{k+1} \neq 0$, tais que $q_1 = a_{k+1} b^k + a_k b^{k-1} + \cdots + a_2 b + a_1$. Daí $n = a_{k+1} b^{k+1} + a_k b^k + \cdots + a_1 b + a_0$.
A unicidade segue da hipótese de indução e do algoritmo da divisão. □

Notação. Denotaremos o número $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$ por $(a_k a_{k-1} \cdots a_1 a_0)_b$ ou $a_k a_{k-1} \cdots a_1 a_{0_b}$ quando a base b for, em geral, distinta de 10, e diremos que n está escrito na base b. Quando a base b for a base decimal usual, escreveremos simplesmente $n =$

$a_k a_{k-1} \ldots a_1 a_0$. Dizemos que a expressão $(a_k a_{k-1} \cdots a_1 a_0)_b$ é a *expansão* do número n na base b.

Note que são necessários b números a_i's para escrever qualquer número na base b; por isso usamos os algarismos $0,\ 1, \ldots, 9$ para escrever qualquer número na base decimal, 0, 1 no caso da expansão de n na base binária, etc.

Para o sistema hexadecimal, além dos algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, usados no sistema decimal, usaremos também as letras A, B, C, D, E, F, que representam os números decimais de 10 a 15, respectivamente.

Exemplo 1. $(234)_5$ representa o número $2.5^2 + 3.5 + 4 = 69$.

Exemplo 2. Para obter 91 na base 5, aplicamos divisões sucessivas como sugere o Teorema 2.22, do seguinte modo:
$91 = (18).5 + 1 = (3.5 + 3).5 + 1 = 3.5^2 + 3.5 + 1$. Logo $91 = (331)_5$.

Exemplo 3. O número b tem sempre a expressão $b = (10)_b$. Mais geralmente a potência b^n tem a expressão $(10 \ldots 0)_b$ (n zeros) na base b.

Exemplo 4. $200 = (21102)_3$.

De fato, dividindo 200 por 3, podemos escrever $200 = (66).3+2$, e a demonstração do Teorema 2.22 sugere dividir o quociente por 3 sucessivamente até este ficar menor que 3. Assim,

$$\begin{array}{rcll} 200 & = & (66).3+2, & (a_0 = 2) \\ 66 & = & (22).3+0, & (a_1 = 0) \\ 22 & = & (7).3+1, & (a_2 = 1) \\ 7 & = & (2).2+1, & (a_3 = 1) \\ 2 & = & 0.3+2, & (a_4 = 2) \end{array}$$

Daí, $200 = (a_4 a_3 a_2 a_1 a_0)_3 = (21102)_3$

Note que $200 = (66).3+2 = [(22).3+0].3+2 = [(7.3+1).3+0].3+2 =$
$[((2.3 + 1).3 + 1).3 + 0].3 + 2 = 2.3^4 + 1.3^3 + 1.3^2 + 0.3 + 2 =$
$(21102)_3$.

Exemplo 5. -200 na base 3 tem a expansão: $-(21102)_3$.

Exemplo 6. Dê a expansão de 3073 na base hexadecimal.

Fazendo a divisão de 3073 por 16, e depois dividindo sucessivamente os quocientes obtidos até o último ficar menor que 16, temos:

$$\begin{aligned} 3073 &= (192).16+1, \quad (a_0 = 1) \\ 192 &= (12).16+0, \quad (a_1 = 0) \\ 12 &= (0).16+12, \quad (a_2 = 12 = C) \end{aligned}$$

Logo $3073 = (C01)_{16}$, ou seja

$$3073 = (192).16 + 1 = [(12).16 + 0].16 + 0 = C.16^2 + 0.16 + 1.$$

Note que, no caso de não se acrescentar os dígitos A, B, C, D, E, F, teríamos que escrever $3073 = \big((12)01\big)_{16}$ para não confundir com $(1201)_{16} = 1.16^3 + 2.16^2 + 0.16^1 + 1$; um número bem diferente de 3073.

Observação (1) Se $n < 0$, então $n = -m$ com $m > 0$. Pelo Teorema 2.22, $m = \sum_{i=0}^{k} a_i b^i$ e, portanto, $n = -(a_k a_{k-1} \cdots a_1 a_0)_b$. **(2)** A prova do Teorema 2.22 nos dá um processo prático para determinar a representação de um número n numa base b, que é o seguinte: 'Dividimos n por b, obtendo quociente q e resto a_0. Se $q > b$, dividimos q por b, obtendo quociente q_1 e resto a_1. Se q_1 for maior que b, novamente dividimos o quociente obtido (agora q_1) por b, obtendo quociente q_2 e resto a_2. Procedemos assim até obter quociente q_{k+1} igual a zero. Portanto, o resto $a_k = q_k < b$, pois os quocientes obtidos vão decrescendo, desde que $a_i \geq 0$ e $b > 1$. Daí basta considerar a seqüência de restos na ordem inversa a que foram gerados, $(a_k a_{k-1} \cdots a_1 a_0)_b$. Esta seqüência é a representação de n na base b.

Exemplo Determine a expansão de 211 na base 4.

$$\begin{aligned} 211 &= (52).4 + 3 \\ 52 &= (13).4 + 0 \\ 13 &= 3.4 + 1 \\ 3 &= 0.4 + 3 \end{aligned}$$

$$\begin{array}{rlll} 211 & \big|\overline{4} & & \\ 3 & 52 & \big|\overline{4} & \\ & 0 & 13 & \big|\overline{4} \\ & & 1 & 3 \quad \big|\overline{4} \\ & & & 3 \quad 0 \end{array}$$

Daí $211 = (52).4 + 3 = [(13).4 + 0].4 + 3 = (13).4^2 + 0.4 + 3 = ((3).4 + 1).4^2 + 0.4 + 3 = 3.4^3 + 1.4^2 + 0.4 + 3 = (3103)_4$.

Vamos representar os 17 primeiros inteiros positivos nas bases decimal, binária, quaternária, octal e hexadecimal. Para a base hexadecimal, as letras A, B, C, D, E, F representam os números decimais de 10 a 15, respectivamente.

BASES

dec.	0	1	2	3	4	5	6	7	8	9
bin.	0	1	10	11	100	101	110	111	1000	1001
quat.	0	1	2	3	10	11	12	13	20	21
oct.	0	1	2	3	4	5	6	7	10	11
hex.	0	1	2	3	4	5	6	7	8	9

BASES

decimal	10	11	12	13	14	15	16
binária	1010	1011	1100	1101	1110	1111	10000
quatern.	22	23	30	31	32	33	100
octal	12	13	14	15	16	17	20
hexadec.	A	B	C	D	E	F	10

As Quatro Operações Básicas

Começamos observando que os processos de adição, subtração, multiplicação e divisão de números em uma base b qualquer são os mesmos processos que usamos na base decimal.

(a) - Adição

Para somar 2 números escritos na base b, soma-se os coeficientes de mesma potência de b, ou seja, faz-se uma soma posicional; não esquecendo que pode haver 'excesso'. O 'excesso' ocorre quando somamos os coeficientes de b^i, a_i e c_i, com $a_i + c_i > b$. Neste caso, $a_i + c_i < 2b$ e, então, $a_i + c_i = b + d_i$ com $0 \leq d_i < b$.

No processo prático dado abaixo, ocorre o 'vai um'. Observe que $(a_i + c_i)b^i = (b + d_i)b^i = 1.b^{i+1} + d_i.b^i$ e, portanto, vai acrescentar uma potência aos coeficientes de b^{i+1}, justificando assim o 'vai um'. Por exemplo, para somar $x = (22)_3$ com $y = (120)_3$, temos: escrevemos x e y nas formas $x = 2.3^1 + 2.3^0$ e $y = 1.3^2 + 2.3 + 0.3^0$. Somamos $(0+1)$ (coef. de 3^2), $(2+2) = (11)_3$ (coef. de 3^1), $(2+0)$ (coef. de 3^0.). Daí $x + y = 1.3^2 + \big((11)_3\big)3 + 2 = 1.3^2 + (1.3 + 1)3 + 2 =$

$(1+1)3^2 + 1.3^1 + 2 = (212)_3$.

Resumidamente temos:

$$\begin{array}{cccc} {\scriptstyle 1} & & 2 & 2 \\ 1 & & 2 & 0 \\ \hline 2 & & 1 & 2 \end{array} +$$

Observe que usamos a seguinte tábua para soma

+	0	1	2
0	0	1	2
1	1	2	10
2	2	10	11

Exemplo Para $b = 3$, façamos a adição $202_3 + 101_3 + 120_3$. Usando o algoritmo e a tábua acima:

$$\begin{array}{cccc} {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & \\ & 2 & 0 & 2 \\ + & 1 & 0 & 1 \\ & 1 & 2 & 0 \\ \hline 1 & 2 & 0 & 0 \end{array}$$

(b) - Subtração

Para a subtração de números em uma mesma base, subtrai-se os coeficientes de uma mesma potência de b. Quando o coeficiente a ser subtraido é maior, é preciso subtrair 1 do coeficiente da potência de b imediatamente maior para acrescentar naquela que tem falta. Este é o motivo do 'cai um' visto no ensino fundamental. Assim, $a_i b^i = (a_i - 1)b^i + b.b^{i-1}$, ou seja, ficamos com coeficiente $a_i - 1$ para b^i e, no nível b^{i-1}, ficamos com coeficiente $b = (10)_b$, mais a_{i-1} que já existia, totalizando $(1a_{i-1})_b$. Agora $(1a_i)_b \geq b > c_{i-1}$, sendo possível efetuar a subtração.

Exemplo 1 Sejam $x = (1011)_2$ e $y = (101101)_2$, calculemos $x - y$.

Como $x < y$, façamos $-(y - x)$, que é a mesma coisa. Então calculamos primeiro $y - x$ e trocamos o sinal do resultado obtido. Observe que, para os coeficientes de 2^1, é necessário retirar 1 do

coeficiente de 2^2 para fazer $y - x$. Daí $1.2^2 = 2.2 = (10)_2.2$ e, portanto, $y - x = 1.2^5 + 1.2^3 + (10)_2.2 + 1 - (1.2^3 + 1.2 + 1) = 1.2^5 + (1-1).2^3 + \big((10)_2 - 1\big).2^1 + (1-1) = 1.2^5 + 1.2^1 = 100010_2$. Logo, $x - y = -100010_2$.

Observe no processo prático como se *empresta um* e como *se subtrai um*.

$$\begin{array}{cccccccc} 1 & 0 & 1 & {}^{0}\not{2} & {}^{1} & 0 & 1 & \\ & & 1 & 0 & & 1 & 1 & - \\ \hline 1 & 0 & 0 & 0 & & 1 & 0 & \end{array}$$

Assim, $x - y = -(100010)_2$.

Exemplo 2 Vamos obter $x - y$, para $x = 1012_3$ e $y = 121_3$, por etapas. Primeiro "emprestaremos 1"do coeficiente de 3^3 para o coeficiente de 3^2 de x, pois este é menor que o coeficiente correspondente de y. Depois faremos a mesma coisa para as potências imediatamente inferiores, pelas mesmas razões.

$$\begin{array}{cccc} 1^{\rightarrow} & 0 & 1 & 2 \\ & 1 & 2 & 1 \\ \hline \end{array} - \quad \Rightarrow \quad \begin{array}{cccc} (10)_3^{\rightarrow} & 1 & 2 & \\ 1 & & 2 & 1 \\ \hline \end{array} - \quad \Rightarrow \quad \begin{array}{ccc} 2 & (11)_3 & 2 \\ 1 & 2 & 1 \\ \hline 1 & 2 & 1 \end{array} -$$

(c) - Multiplicação

Para fazer a multiplicação de $x = a_s b^s + a_{s-1} b^{s-1} + \cdots + a_1 b + a_0$ por $y = c_j b^j + c_{j-1} b^{j-1} + \cdots + c_1 b + c_0$, usamos a propriedade distributiva e a regra: $a_i b^i . c_k b^k = (a_i . c_k) b^{i+k}$.

Como $0 \leq a_i,\ c_k < b$ então $0 \leq a_i . c_k < b^2$. Logo, $a_i . c_k = qb + d_{i+k},\ 0 \leq d_{i+k},\ q < b$ e, portanto, $a_i b^i . c_k b^k = (qb + d_{i+k}) b^{i+k} = q . b^{i+k+1} + d_{i+k} b^{i+k}$. Ou seja, acrescenta-se 'q' ao coeficiente da potência b^{i+k+1} e o coeficiente de b^{i+k} é d_{i+k} = resto da divisão de $a_i . c_k$ por b.

Para o exemplo que segue, precisaremos das tábuas da multiplicação e adição de números na base 4,

+	0	1	2	3
0	0	1	2	3
1	1	2	3	10
2	2	3	10	11
3	3	10	11	12

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	10	12
3	0	3	12	21

Exemplo Para efetuarmos o produto de $(23)_4$ por $(32)_4$, precisaremos de $2_4.3_4 = 12_4$ e $3_4.3_4 = 21_4$. Daí a multiplicação de 23 por 32 na base 4 é:

$$\begin{array}{cccc}
 & {\scriptstyle 2} & & \\
 & {\scriptstyle 1} & & \\
 & 2 & 3 & \\
 & \times & 3 & 2 \\
\hline
 & 1 & 1 & 2 \\
2 & 0 & 1 & + \\
\hline
2 & 1 & 2 & 2
\end{array}$$

Observe que $3_4.3_4 = (21)_4$, logo fica 1 e "vai"o 2. Também $3_4.2_4 + 2_4$ (2_4 que foi) totalizam $(20)_4$ e assim por diante. Faça, agora, também o produto polinomial $(2.4 + 3)(3.4 + 2)$ e observe o vai 1 e vai 2. Finalmente, justifique porque temos a casa vazia, onde aparece o símbolo de $+$.

(d) - Divisão

Consideremos os números $a = (a_n a_{n-1} \cdots a_1 a_0)_b$ e $c = (c_m c_{m-1} \cdots c_1 c_0)_b$. Para dividirmos o número a pelo número c, vejamos se $x = a_n a_{n-1} \cdots a_{n-m-1}$ é maior ou igual a c; se não for, consideremos $x = a_n a_{n-1} \cdots a_{n-m-2}$ e dividamos x por c. Então $x = qc + r$, onde $0 \leq r < c$. Sejam $q = (q_k q_{k-1} \cdots q_1 q_0)_b$ e $r = (r_s r_{s-1} \cdots r_1 r_0)_b$. Daí juntamos a r o próximo a_j da esquerda para a direita que não aparece na seqüência x e ficamos com $R = r_s r_{s-1} \cdots r_1 r_0 a_j$. Dividimos R por c obtendo q'_1 como quociente e resto $R_1 = (d_1 \cdots d_t)_b$. Novamente juntamos, a R_1, a_{j-1} e ficamos com $R_2 = d_1 \cdots d_t a_{j-1}$ e dividimos R_2 por c, obtendo q'_2 como quociente e resto $R_3 = (u_1 \cdots u_v)_b$. Assim sucessivamente até chegar a a_0 e concluir a divisão. Neste caso, o quociente da divisão será $Q = q_k q_{k-1} \cdots q_1 q_0 q'_1 q'_2 \cdots q'_l$ e, o resto, o último resto obtido. Então, para efetuar a divisão usaremos os conceitos de multiplicação e subtração já vistos.

Exemplo Dividir 231003 por 302 na base 4.

Solução Precisaremos das tábuas na base 4, dadas anteriormente. Observe que a 1ª sequência de números da esquerda para a direita

em 231003 que é maior ou igual a 302 é 2310. Então $x = 2310$. Dividindo 2310 por 302, encontramos quociente 3. Daí $2310_4 - 3_4.(302)_4 = (132)_4$. A seguir, juntamos $a_1 = 0$ a 132, ficando com 1320, e dividimos novamente por 302, etc. O processo pode ser resumido da seguinte forma:

$$\begin{array}{rcccccc|ccc}
 & 2 & 3 & {}^{1}1 & {}^{1}0 & 0 & 3 & 3 & 0 & 2 \\
- & 2 & 1^{1} & 1^{1} & 2 & \downarrow & \downarrow & 3 & 2 & 1 \\
\cline{2-7}
 & 0 & 1 & 3 & 2 & 0 & \downarrow & & & \\
 & - & 1 & 2 & 1 & 0 & \downarrow & & & \\
\cline{3-6}
 & & 0 & 1 & 1 & 0 & 3 & & & \\
 & & & - & 3 & 0 & 2 & & & \\
\cline{4-6}
 & & & & 2 & 0 & 1 & & &
\end{array}$$

Para fazer conversão de um número n de uma base b para uma base c, um método é escrever n na base decimal e aplicar divisões sucessivas por c, como foi exemplificado. Considerando os restos $c_0, c_1, \ldots, c_s$ das divisões, segue que $n = (c_s c_{s-1} \cdots c_1 c_0)_c$. No entanto, quando uma base é potência da outra, existe um processo prático para a conversão de um número de uma base à outra, dado na proposição a seguir para as bases binária e hexadecimal. Façamos um exemplo antes.

Exemplo

(i) Seja $a = 1010111_2$. Escreva a na base octal e na base hexadecimal.

(ii) Como se escreve o número $B6_{16}$ nas bases 2 e 4?

Solução **(i)** Como $8 = 2^3$, agrupamos os números de 3 em 3 a partir da direita para a esquerda, isto é: $1010111_2 = ((1)_2(010)_2(111)_2)_8 = 127_8$, pois $111_2 = 7_8$, $010_2 = 2_8$ e $1_2 = 001_2 = 1_8$.

Para a base hexadecimal, como $16 = 2^4$, agrupamos os números que aparecem em 1010111 de 4 em 4 a partir da direita para esquerda, para obter $1010111_2 = ((0101)_2(0111)_2)_{16} = (57)_{16}$. Note que $1010111 = 1.2^6 + 1.2^4 + 1.2^2 + 1.2 + 1 = (1.2^2 + 1)2^4 + 7 = 5.(16) + 7 = 57_{16}$.

(ii) Para escrever $B6_{16}$ na base 2, tomam-se as representações binárias dos dígitos B (=onze) e 6 *com 4 dígitos 0's e 1's, pois*

$16 = 2^4$, para obter:

$B6_{16} = ((1011)_2(0110)_2) = 10110110_2$.

Note que $B6_{16} = B.(16) + 6 = B.2^4 + 6 = (1.2^3 + 0.2^2 + 1.2 + 1).2^4 + 2^2 + 2 = 1.2^7 + 0.2^6 + 1.2^5 + 1.2^4 + 0.2^3 + 1.2^2 + 1.2 + 0.2^0 = 10110110_2$.

Para passar $B6_{16}$ para a base 4, além do processo acima, podemos fazer também: $B6_{16} = B.(16) + 6 = (2.4 + 3)4^2 + 1.4 + 2 = 2.4^3 + 3.4^2 + 1.4 + 2 = 2312_4$.

Pode-se ver que, para a conversão de um número da base hexadecimal para a base binária, basta converter cada dígito do número dado para a base binária, obtendo uma seqüência de 4 0's e 1's, guardando suas posições. Reciprocamente, para a conversão de um número da base binária para a base hexadecimal, basta agrupar os dígitos de 4 em 4 da direita para a esquerda e passar cada grupo para a base 16, guardando as posições dos números obtidos. Em símbolos temos:

Proposição 2.23 *Seja* $a = (a_k a_{k-1} \dots a_1 a_0)_{16}$, $0 \leq a_i \leq 15$ *a representação de* $a \in \mathbb{Z}$ *na base 16, e suponhamos que a representação de* a_i *na base 2 seja* $a_i = a_{i3}a_{i2}a_{i1}a_{i0}$, $a_{ij} = 0$ *ou 1. Então*

$a = (a_{k3}a_{k2}a_{k1}a_{k0} \cdots a_{13}a_{12}a_{11}a_{10}a_{03}a_{02}a_{01}a_{00})_2$, *isto é:*

$$\begin{array}{ccccccc} (a_k & & a_{k-1} & \cdots & a_1 & & a_0\ )_{16} \\ \downarrow & & \downarrow & \downarrow & \downarrow & & \downarrow \\ (a_{k3}a_{k2}a_{k1}a_{k0} & \cdots & \cdots & & a_{13}a_{12}a_{11}a_{01} & & a_{03}a_{02}a_{01}a_{00})_2 \end{array}$$

Reciprocamente se $a = (a_s a_{s-1} \dots a_1 a_0)_2$, *então* $a = (c_k\ c_{k-1} \cdots c_1 c_0)_{16}$ *onde* $c_j = (2^3 a_{4j+3} + 2^2 a_{4j+2} + 2a_{4k+1} + a_{4j})_{16}$, *isto é:*

$$\begin{array}{ccccc} a = (\cdots & \cdots a_8 & a_7a_6a_5a_4 & & a_3a_2a_1a_0)_2 \\ a = (\cdots & \cdots & c_1 & & c_0\ )_{16} \end{array}$$

Demonstração: Seja $a = (a_k a_{k-1} \dots a_1 a_0)_{16}$. Então $a = a_k 16^k + a_{k-1}16^{k-1} + \cdots + a_1 16 + a_0$, $0 \leq a_i \leq 15$. Escrevemos a_i e 16 na forma $a_i = (a_{i3}a_{i2}a_{i1}a_{i0})_2$ e $16 = 2^4$. Substituindo e fazendo as contas, temos: $a = a_{k3}2^{4k+3} + a_{k2}2^{4k+2} + a_{k1}2^{4k+1} + a_{k0}2^{4k} +$

$\cdots + a_{11}2^5 + a_{10}2^4 + a_{03}2^3 + a_{02}2^2 + a_{01}2^1 + a_{00}$, isto é: $a = (a_{k3}a_{k2}a_{k1}a_{k0}\cdots a_{13}a_{12}a_{11}a_{03}a_{02}a_{01}a_{00})_2$.
O problema inverso é mais simples ainda e deixaremos como exercício. □

Exemplo
(i) Dado a=$2F9_{16}$, convertê-lo para a base binária.
Como $2 = 0010_2$, $F = 1111_2$ e $9 = 1001_2$, temos
$a = \underset{2}{(0010} \quad \underset{F}{1111} \quad \underset{9}{1001)_2} = 1011111001_2$.

(ii) Dado $b = 110001110111101_2$, convertê-lo para a base hexadecimal.

Temos $b = (0110\ 0011\ 1011\ 1101)_2$. Como $0110_2 = 6_{16}$, $0011_2 = 3_{16}$, $1011_2 = B_{16}$ e $1101_2 = D_{16}$, concluímos que $b = 63BD_{16}$.

Representação de Números Fracionários

Vimos que todo número inteiro tem uma representação posicional na base b para qualquer $b > 1$. O mesmo princípio vale para números fracionários. Por exemplo, $0,351$ (3 décimos 5 centésimos e 1 milésimo) se escreve como $3.10^{-1}+5.10^{-2}+1.10^{-3} = \frac{3}{10}+\frac{5}{100}+\frac{1}{1000}$.

Todo número racional se escreve na forma $I + F$, onde I é um número inteiro e F é um número racional compreendido entre zero e um. Claro que, estas quantidades independem da base escolhida para representar o número. Com isto podemos enunciar.

Teorema 2.24 *Todo número racional a se escreve de modo único na forma $a = \pm(I + F)$ em qualquer base b fixada, onde I é um número inteiro positivo e F um número racional, $0 \leq F < 1$. Em outras palavras, podemos escrever o número a de modo único como uma seqüência*

$$a = \pm(b_m b_{m-1}\cdots b_1 b_0 b_{-1} b_{-2}\cdots)_b,$$

onde $I = (b_m b_{m-1}\cdots b_1 b_0)_b$ e $F = b_{-1}b^{-1} + b_{-2}b^{-2} + \cdots$ □

Notação 2.25 O número a será denotado por $\pm(b_m b_{m-1} \cdots b_1 b_0, b_{-1} b_{-2} \cdots)_b$ e F será denotado por $(0, b_{-1} b_{-2} \cdots)_b$. Note a necessidade da vírgula para diferir por exemplo os números $2.(10)^1+1$ e $2+1.(10)^{-1}$. Sem usar a vírgula ambos tem a representação: 21_{10}, desde que não se conhece m. A vírgula nos informa disto.

Com isto temos a representação de um número racional qualquer em uma base qualquer, previamente fixada.

Como podemos escrever um número racional dado em uma base fixada diferente da base dez? Como já temos feito isto no caso de números inteiros, devido ao teorema acima basta ver como isto é feito no caso de números fracionários. Este é o assunto do próximo item.

Conversão de Fração de uma Base à Outra

Seja F um número racional, $0 < F < 1$, dado no base b por $F = (0, b_{-1} b_{-2} \ldots)_b$, e suponhamos que queremos escrever F na base c. Então $F = (0, b_{-1} b_{-2} \ldots)_b = (0, c_{-1} c_{-2} \ldots)_c$ onde c_{-i} deve ser determinado, para cada i. Multiplicando ambos os lados da igualdade por c, movemos a vírgula uma casa para a direita no segundo membro da igualdade. Com isto, ficaremos com c_{-1} como parte inteira (no 2º membro), e é possível determiná-lo. Ou seja: $(c)_b(0, b_{-1} b_{-2} \ldots)_b = (c_{-1}, c_{-2} \ldots)_c$, e, igualando as partes inteiras, tem-se o valor de c_{-1}. Para obter c_{-2}, iguala-se as partes fracionárias de $(c)_b(0, b_{-1} b_{-2} \ldots)_b$ e $(c_{-1}, c_{-2} \ldots)_c$ e repete-se o processo. Os outros c_{-i}, $i \geq 3$ são obtidos de maneira semelhante.

Exemplos 2.26 (A) Seja $F = b_{-1}.10^{-1} + b_{-2}.10^{-2} + \cdots = 0, b_{-1} b_{-2} \cdots$, acharemos $c_{-j} \in \{0, 1\}$ $j = 1, 2, \ldots$, tais que $F = (0, c_{-1} c_{-2} \cdots)_2$.
De $(0, b_{-1} b_{-2} \ldots)_{10} = (0, c_{-1} c_{-2} \ldots)_2$, multiplicando por 2, obtemos:
$2(0, b_{-1} b_{-2} \cdots)_{10} = (c_{-1}, c_{-2} c_{-3} \cdots)_2$ (pois $(I + F)_{10} = I' + F')_2$), igualando as partes inteiras obtemos c_{-1} (pois $I_{10} = I'_2$). Igualando as partes fracionárias de $2(0, b_{-1} b_{-2} \cdots)_{10}$ e $(0, c_{-2} c_{-3} \cdots)_2$ (pois $F_{10} = F'_2$), e repetindo o processo, obteremos c_{-2}. Assim por diante, até obter todos os c_{-j}. Façamos dois exemplos:

(i) $(0,75)_{10} = (0, c_{-1}c_{-2}\cdots)_2$.
Multiplicando por 2, temos $1,5 = c_{-1}, c_{-2}\cdots$. Então $c_{-1} = 1$ e $0,5 = (0, c_{-2}\cdots)_2$. Multiplicando por 2 obtemos $1,0 = (c_{-2}, c_{-3}\cdots)_2$, o que implica que $c_{-2} = 1$ e $0 = c_{-j}$, para todo $j \geq 3$. Então $0,75 = (0,11)_2 \qquad (= \frac{1}{2} + \frac{1}{4})$.

(ii) $0,6 = (0, c_{-1}c_{-2}\cdots)_2$. Usemos o processo prático:

$0,$	6		$0,$	4
$\times$	2		$\times$	2
$c_{-1} = 1,$	2		$c_{-3} = 0,$	8
$\times$	2		$\times$	2
$c_{-2} = 0,$	4		$c_{-4} = 1,$	6

e tudo volta a repetir infinitamente a partir de c_{-4}. Logo $0,6 = (0, \overline{1001})_2$.

A notação $0, b_{-1}b_{-2}\cdots b_{-k}\overline{b_{k+1}\cdots b_t}$ significa que, a partir de b_{-k}, a seqüência $b_{k+1}\cdots b_t$ vai se repetir infinitamente.

(iii) $0,22\cdots = (0, c_{-1}c_{-2}\cdots)_2$.

Como a fração na base dez é uma série infinita, se multiplicarmos por 2, pode ficar complicado para efetuar o produto. Mas se fizermos $x = 0,22\cdots$ e multiplicarmos por dez, temos: $10x = 2 + x$ e daí $9x = 2$. Portanto, $x = \frac{2}{9}$. Então, $\frac{2}{9} = (0, c_{-1}c_{-2}\cdots)_2$. Multiplicando por 2, $\frac{4}{9} = (c_{-1}, c_{-2}\cdots)_2$. Logo, $c_{-1} = 0$ e, multiplicando por 2, $\frac{8}{9} = (c_{-2}, c_{-3}\cdots)_2$. Novamente $c_{-2} = 0$ e, multiplicando por 2, $\frac{16}{9} = 1 + \frac{7}{9} = (c_{-3}, c_{-4}\cdots)_2$. Encontramos $c_{-3} = 1$ e $\frac{7}{9} = (0, c_{-4}\cdots)_2$. Continuando, encontramos: $0,22\cdots = 0,\overline{001110}_2$.

(B) Para a conversão de uma fração binária para uma fração decimal, existem 2 processos pelo menos. O mesmo processo anterior, só que agora multiplicamos por dez. Se temos $a = (0, a_{-1}a_{-2}\cdots)$ na base dois, e queremos escrever $a = (0, b_{-1}b_{-2}\cdots)$ na base dez, se multiplicarmos por dez, b_{-1} fica sendo a parte inteira do número $10a$. Assim, $10a = (b_{-1}, b_{-2}\cdots)_{10}$, ou seja, $(1010)_2(0, a_{-1}a_{-2}\cdots)_2 = (b_{-1}, b_{-2}\cdots)_{10}$. Igualando as partes inteiras, obtém-se b_{-1}. Igualam-se as partes fracionárias e continua-se o processo para achar os outros $b_{-j},\ j = 2, \ldots$

Para o segundo processo basta escrever $a = (0, a_{-1}a_{-2}\cdots)$ na forma $a = a_{-1}2^{-1} + a_{-2}2^{-2} + \cdots = \sum_{i\geq 0} a_{-i}2^{-i}$ e calcular esta série convergente.

Exemplo **(i)** Dado $a = (0,11)_2$, escrevemos $a = (0, b_{-1}b_{-2}\cdots)$ na base dez. Multiplicando a por dez, ficamos com $(1010)_2(0,11)_2 = (10)(0, b_{-1}\cdots)$. Portanto, $(111,10)_2 = (b_{-1}, b_{-2}\cdots)_{10}$. Logo, $b_{-1} = (111)_2 = 7_{10}$ e $(0,1)_2 = (0, b_{-2}\cdots)_{10}$. Repetindo o processo, multiplicando a última igualdade por "dez", ficamos com $(1010)_2(0,1)_2 = (b_{-2}, b_{-3}\cdots)_{10}$, ou seja, $(101)_2 = 5_{10} = b_{-2}$ e $b_{-j} = 0,\ j = 3, 4\cdots$. Encontramos $a = 0,75$.

(ii) Usando o segundo processo temos: $a = (0,11)_2 = \frac{1}{2} + \frac{1}{4}$ (na base "dez"). Logo, $a = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}$. Efetuando a divisão encontramos: $a = 0,75$.

(iii) Para exemplificar o segundo processo, mais uma vez, considere $c = (0, \overline{101})_2$, ou seja, $c = (0, 101101101\cdots)_2$. Podemos escrever $c = 2^{-1}+2^{-3}+2^{-4}+2^{-6}+2^{-7}+2^{-9}+2^{-12}+\cdots$ Como a seqüência é absolutamente convergente, podemos escrever $c = (2^{-1} + 2^{-4} + 2^{-7} + 2^{-10} + \cdots) + (2^{-3} + 2^{-6} + 2^{-9} + 2^{-12} + \cdots)$. Usando a soma de uma progressão geométrica, concluímos que

$$c = \frac{2^{-1}}{1-2^{-3}} + \frac{2^{-3}}{1-2^{-3}} = \frac{2^{-1}}{7/8} + \frac{2^{-3}}{7/8} = \frac{5}{7} = 0, \overline{7142857}.$$

Seja $d = 0,101_2$. Então $d = 2^{-1} + 2^{-3} = \frac{1}{2} + \frac{1}{8} = \frac{5}{8} = 0,625$.

Exercícios

(1) Prove as seguintes fórmulas por indução matemática: **(i)** $n < 2^n,\ \forall n \in \mathbb{N}$, **(ii)** $n^3 - n$ é divisível por 3, para todo inteiro n. Sugestão Considere $n \geq 0$ e depois $n < 0$. **(iii)** $2^n < n!,\ n \geq 4$.

(2) Considere os números de Fibonacci: $F_1 = F_2 = 1,\ F_n = F_{n-1} + F_{n-2},\ n \geq 3$.

(a) Calcule F_i, para $i = 1, 2, \ldots, 12$.

(b) Prove por indução que: **(i)** A soma dos n primeiros números de Fibonacci é igual a $F_{n+2} - 1$, isto é, $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

(ii) A soma dos n primeiros números de Fibonacci com índices ímpares é igual a F_{2n}, isto é: $F_1 + F_3 + \cdots + F_{2(n-1)+1} = F_{2n}$.

(iii) A soma dos n primeiros números de Fibonacci de índices pares é $F_{2n+1} - 1$.

(iv) Para $n \geq 1$, $\quad F_1^2 + F_2^2 + \cdots + F_n^2 = F_n.F_{n+1}$.

(3) Os números de Stirling de primeira espécie, denotados por $S_1(m,n)$ são definidos pela equação

$$\sum_{n=0} mS_1(m,n)x^n = x(x-1)\ldots(x-m+1).$$

Mostre que $S_1(m,n)$ satisfaz a relação:

$$S_1(m+1,n) = S_1(m,n-1) - mS_1(m,n)$$

com

$$S_1(0,0) = 1, \quad S_1(k,0) = S_1(0,k) = 0$$

para $k > 0$.

(4) Prove por indução que:

(a) $a + ar + ar^2 + \ldots + ar^n = \dfrac{a(r^{n+1}-1)}{r-1}$, para qualquer $a \in \mathbb{R},\ r > 0,\ r \neq 1$.

(b) Defina $P(0) = 1$ e $P(n) = n.P(n-1),\ n \geq 1$. Prove que $P(n)$ define recursivamente $n!$

(c) Se $|A| = n$, então $|\wp(A)| = 2^n$.

(d) $2^n - 1 = 2^0 + \cdots + 2^{n-1},\ n \geq 1$.

(e) $1^2 + 2^2 + \cdots n^2 = \dfrac{n(n+1)(2n+1)}{6},\ n \geq 1$.

(f) $2^{2n-1}.3^{n+2} + 1$ é divisível por 11, $\forall n \geq 1$.

(g) $17|3^{4n+2} + 2.4^{3n+1}, n \in \mathbb{N}$.

(h) $a_0 + a_1 r + a_2 r^2 + \ldots + a_j r^j < r^{j+1},\ \forall j \in \mathbb{N}$; onde $r \in \mathbb{N}$ e $a_0, a_1 \ldots, a_j \in \mathbb{N}$, tais que $a_i < r,\ \forall i = 0, \ldots, j$.

(i) $(A_1 \cup \ldots \cup A_r)^c = A_1^c \cap \ldots \cap A_r^c$, e $(A_1 \cap \ldots \cap A_r)^c = A_1^c \cup \ldots \cup A_r^c$, para todo $r \in \mathbb{N}$.

(j) $\sum_{i=1}^{n}(2i-1) = n^2,\ (n \geq 1)$. **(k)** $\sum_{i=1}^{n} i^3 = [\frac{1}{2}n(n+1)]^2$.

(l) $\sum_{i=1}^{n} i(i!) = (n+1)!-1,\ (n \geq 1)$. **(m)** $\forall a,\ 0 < a < 1;\ (1-a)^n \geq 1 - na,\ (n \geq 1)$. **(n)** $2^n > n^3,\ (\forall n \geq 10)$.

(5) Sendo $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ a função de Ackermann, calcule $A(2,3)$ e, na tabela de dupla entrada,

	0	1	2	3	4	...
0	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$	...
1	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$	...
2	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$(2,4)$	...
3	$(3,0)$	$(3,1)$	$(3,2)$	$(3,3)$	$(3,4)$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

faça um caminho usando setas para indicar os passos dados, necessários no cálculo de $A(2,3)$.

(6) Defina as seguintes seqüências de números usando recorrência:
(a) $1, 2, 2^2, \ldots, 2^n, \ldots$ **(b)** $0, 1^2, 2^2, \ldots, k^2, \ldots$
(c) $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

(7) Defina recursivamente: $E(i) = \binom{n}{i} \quad (i \geq 0)$.

(8) Determine os quocientes e os restos (q, r) da divisão euclidiana de a por b, onde: **(a)** $a = 18$ e $b = 5$, **(b)** $a = 121$ e $b = 10$, **(c)** $a = 3512$ e $b = 91$, **(d)** $a = 55$ e $b = 5$,
(e) $a = -63$ e $b = 8$, **(f)** $a = -2764$ e $b = 3$.

(9) **(A)** Encontre os $mdc(a, b)$ e expresse-os na forma $ra + sb$, onde
(a) $a = 14,\ b = 7684$ **(b)** $a = 4148,\ b = 7684$
(c) $a = 180,\ b = 252$ **(d)** $a = 1144,\quad b = -351$
(e) $a = 8024,\quad b = 412$.
(B) Expresse o $mdc(6, 10, 14)$ na forma $6r + 10s + 14t,\ r, s, t \in \mathbb{Z}$.

(10) **(i)** Seja $n \in \mathbb{Z},\ n > 1$. Mostre que, se não existe um primo $p \leq \sqrt{n}$, tal que p divide n, então n é um número primo.
(ii) Verifique se 1943 e 1891 são números primos.

(11) **(i)** Use o crivo de Eratostenes para calcular todos os números primos até 200.
(ii) Por que os números compostos da tabela são cancelados até múltiplo de 13 e daí para frente não se cancelam mais?

(12) Obtenha a fatoração de 144 e 162 em produto de primos e utilize-as para obter $mdc(144, 162)$ e o $mmc(144, 162)$.

(13) Ache $a \in \mathbb{Z}$, $48 < a \leq 384$, tal que $mdc(a,\ 384) = 48$. Quantos $a \in \mathbb{Z}$ existem nestas condições?

(14) Se a, b, c são inteiros positivos, prove que:
(a) $a|b$ e $a|c$, então $a|(b+c)$, **(b)** $mdc(a,b) = mdc(b,a)$,
(c) $mdc(a,a) = a$, **(d)** $mdc(ba,bc) = b.mdc(a,c)$,
(e) $mdc(mdc(a,b),c) = mdc(a,mdc(b,c))$,
(f) Se $a > b$, então $mdc(a,b) = mdc(a-b,b)$.
(g) Se $ab = l^2$ para algum $l \in \mathbb{Z}$, e $mdc(a,b) = 1$, então $a = l_1^2$ e $b = l_2^2$ para l_1 e l_2 convenientes.
Sugestão para (d): Mostre que $b|d_1$, onde $d_1 = mdc(ab,cb)$.

(15) Utilize o Lema 2.13 e calcule $mdc(1935, 30)$.

(16) Enuncie e prove o critério de divisibilidade por 5, 9 e por 11.

(17) **(i)** Prove que quaisquer números da forma $abcabc$ são divisíveis por 13, 11, e 7. **(ii)** Use o teorema fundamental da aritmética e escreva 310310 como produto de primos. **(iii)** 997 é primo? Por que?

(18) **(i)** Ache o resto de divisão de $u = (531)^6.(31)^2.2$ por 7.
(ii) Ache o resto da divisão de $7^{7^{1321}}$ por 11.
(iii) Ache os 2 últimos algarismos de $7^{7^{1000}}$.

(19) Escolha a, k em $\mathbb{Z}$ com $a > 1$, a e 26 relativamente primos, para criptografar a sentença "*A terra é azul*" usando a função $f(x) = ax + k(mod.26)$.
Dê a função inversa de $f(x)$ para decriptografar.

(20) Faça a tábua da adição na base 2 e efetue a soma: $1111_2 + 11_2 + 10111_2$.

(21) **(i)** Escolha $b > 2$ e faça a conversão de números da base dez para a base b e vice-versa.
(ii) Dê alguns exemplos.
(iii) Para a base b escolhida em **(i)**, faça conversão de números da base b para a base dois e vice-versa, sem passar pela base dez.

(22) Resolver na base dada:
(i) $23010_4 - 1231_4$ **(ii)** $120301_4 + 21130_4$ **(iii)** $223_4 - 2132_4$.
(iv) $23010_4 \div 1231_4$ **(v)** $2121_4 \div 22_4$. **(vi)** $1011_2 \div 11_2$.

(23) Escreva o número 621 nas bases **(i)** 2, **(ii)** 3, **(iii)** 7 e **(iv)** 11.

(24) Escreva na base decimal os números: $(12011)_3$, $(22210)_3$.

(25) **(i)** Escreva nas bases 2 e 8 os seguintes números dados na notação decimal: 74, 149, 19, 101, 144, 225.
(ii) Represente os números 35 e e 155 nas bases 6 e 8.
(iii) Represente os números dados em **(i)** e **(ii)** na base hexadecimal.

(26) O que está errado nas representações: $(1532)_4$, $(2193)_7$ e $(1013)_2$?

(27) Converter 9,421875 e 0,3333 de decimal para binário.

(28) **(a)** Represente na base 2 as frações **(i)** 0,8125 **(ii)** $\frac{3}{4}$ **(iii)** $0,6875$ **(iv)** $\frac{5}{8}$ **(v)** 0,7 **(vi)** $24,625$ **(vii)** $29,1875$ **(viii)** $0,222\cdots$.
(b) Represente na base "dez" as frações binárias **(i)** $0,1101_2$ **(ii)** $0,111_2$ **(iii)** $0,101101_2$.

(29) **(i)** Verifique que a série: $2^{-1}+2^{-3}+2^{-4}+2^{-7}+2^{-8}+2^{-11}+2^{-12}+\cdots=\frac{1}{2}+(2^{-3}+2^{-7}+2^{-11}+\cdots)+(2^{-4}+2^{-8}+2^{-12}+\cdots)$ converge. **(ii)** Compare com **(28)(v)**.

(30) **(a)** Justifique porque $B3_{16}=10110011_2$. **(b)** Represente $a=6D_{16}$ e $b=3A_{16}$ na base 2, calcule $a-b$ na base 16. **(c)** Dados $x=7C_{16}$ e $y=A2_{16}$, faça as contas $x+y$ e $x-y$ na base hexadecimal e binária.

(31) **(i)** Faça a conversão dos números fracionários binários $(101111,01)_2$ e $(111010,1001)_2$ para as bases octal e hexadecimal.
(ii) Idem de $A85E,16_{16}$ e $761F,98_{16}$ para octal e binário.

(32) Faça as tabuadas para a base 16 e 8.

(33) Faça os cálculos: **(i)** $23089_{16}\div 13A_{16}$, **(ii)** $2142_8\bullet 34_8$, **(iii)** $2307,02_8\div 125,2_8$.

(34) **(i)** Enuncie, prove e dê exemplos de um processo prático para converter um número da base 4 para a base 16 e vice-versa.
(ii) Idem para as bases 3 e 9. Qual a diferença dos processos obtidos entre si e destes para o processo prático dado na Proposição 2.23?

Capítulo 3

CONJUNTOS

Segundo dicionários, um *axioma* é uma premissa imediatamente evidente, universalmente aceita como verdade sem exigência de demonstração; um *postulado* é um princípio, proposição não evidente nem demonstrável, que se admite como princípio de um sistema dedutível e um *paradoxo* é um contra-senso, um absurdo.

Bem, do ponto de vista matemático, não estamos totalmente de acordo com estas definições, principalmente devido aos adjetivos "*imediatamente evidente*" e "*proposição evidente*", que são discutíveis. Mas aceitaremos estes conceitos como estão para não entrar numa discussão semântica e/ou filosófica.

Como acontece em qualquer teoria matemática, o ponto de partida são sempre os conceitos não definidos, denominados *conceitos primitivos* e o conjunto de axiomas ou postulados. Uma Teoria é dita consistente se não se deriva contradições ou paradoxos dos seus conceitos primitivos.

A idéia intuitiva de conjunto desenvolvida pelo matemático germânico Georg Cantor, em 1895, leva a paradoxos. Um deles foi proposto pelo matemático Bertrand Russell em 1902 (será visto a seguir). Uma teoria de conjunto baseada em axiomas e consistente resolve este problema, no entanto, fica bastante complexa. Um meio de evitar ambas as formas de abordagem é considerar a teoria de conjunto de G. Cantor reduzida, também chamada *Teoria Ingênua de Conjuntos,* onde se admite, a priori, um conjunto dito *Conjunto Universo* que contém todos os elementos do discurso. Isto evita os paradoxos, a teoria fica consistente e, para nossos

propósitos, é suficiente.

São *Conceitos Primitivos* da Teoria dos Conjuntos: conjuntos, elementos, igualdade de conjuntos, relações de pertinência e continência.

Não há nenhuma razão aparente para o uso de determinados tipos de letras para indicar conjuntos ou elementos, assim, convencionaremos o seguinte:

- Letras latinas minúsculas representarão elementos;
- Letras latinas maiúsculas ou retorcidas denotarão conjuntos
- $\in$ indica pertence
- $=$ indica igual.

Por exemplo, a sentença "$x \in A$" lê-se: "o elemento x pertence ao conjunto A". E "$A \in \mathcal{C}$" lê-se: "o conjunto A é um elemento de $\mathcal{C}$".

Para sabermos qual é o conjunto a que estamos nos referindo, usamos o

Axioma da Determinação - "Um Conjunto fica bem determinado por seus elementos". De forma mais "ingênua", pode-se dizer que dois conjuntos são iguais se possuem os mesmos elementos.

Já que basta conhecermos os elementos de um conjunto para reconhecê-lo, por vezes, podemos representá-lo apresentando uma listagem de seus elementos colocados entre chaves. Por exemplo, $\{1, 2, 3\}$ é o conjunto constituído pelos números 1, 2, 3 e por nenhum outro elemento.

Observe que o Axioma da Determinação nos garante que os conjuntos $\{1, 3, 5\}$ e $\{1, 5, 3, 3\}$ são iguais; o que significa também que a ordem e o número de vezes que um determinado elemento é listado no conjunto não é relevante.

Definição 3.1 Se A e B são dois conjuntos, e se todo elemento de A pertence a B, dizemos que A *é um subconjunto de* B, ou que B *inclui* A, e denotamos por: $A \subseteq B$ ou $B \supseteq A$. Neste caso, dizemos também que A *está contido em* B ou que B *contém* A.

A inclusão entre conjuntos $A \subseteq B$ corresponde à proposição na álgebra de proposições $p \longrightarrow q$, onde p pode ser visto como a proposição "$x \in A$", onde x é fixo e q : "$x \in B$". Portanto suas propriedades são as mesmas de $p \longrightarrow q$. Para A, B e C subconjuntos de um conjunto universo U, tem-se:

(1) $A \subseteq A$ (reflexiva)

(2) $A \subseteq B$ e $B \subseteq C \Longrightarrow A \subseteq C$ (transitiva)

(3) $A \subseteq B$ e $B \subseteq A \Longrightarrow A = B$, (anti-simétrica).

Estas propriedades correspondem, respectivamente, às implicações lógicas
(1') $p \Longrightarrow p$, **(2')** $[(p \longrightarrow q)$ e $(q \longrightarrow r)] \Longrightarrow [p \longrightarrow r]$ e **(3')** $[(p \longrightarrow q) \wedge (q \longrightarrow p)] \Longrightarrow [p \longleftrightarrow q]$, e todas são de demonstrações simples e imediatas.

Observações:
1. O fato de $A \subseteq B$ não exclui a possibilidade de termos $B \subseteq A$.
2. Com a notação $A \not\subseteq B$ indicamos que "*o conjunto A não está contido no conjunto B*". Assim, $A \not\subseteq B \Longleftrightarrow (\exists x)(x \in A$ e $x \notin B)$. Por exemplo: $\{2,3\} \not\subseteq \{1,3,5,6,7\}$, pois $2 \in \{2,3\}$ e $2 \notin \{1,3,5,6,7\}$, $[1,3] \not\subseteq \mathbb{Q}$, pois $\sqrt{2} \in [1,3]$ e $\sqrt{2} \notin \mathbb{Q}$. Para os conjuntos numéricos temos a seqüência de inclusões $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Uma outra forma de reconhecer um conjunto é dada pelo

Axioma 3.2 *(Axioma da Separação) Seja A um conjunto e $P(x)$ uma sentença aberta definida sobre A. Então existe um subconjunto B de A que consiste exatamente daqueles elementos x de A que satisfazem $P(x)$.*

Costumamos indicar o conjunto B por

$$B = \{x \in A \mid P(x)\}.$$

Observamos que, para especificarmos um conjunto, não é suficiente termos uma sentença aberta $P(x)$, é necessário, também, um conjunto para cujos elementos verificaremos a validade $P(x)$. O conjunto dos elementos com os quais estaremos trabalhando é chamado *conjunto universo* e indicado por U. Este universo é usado no sentido de "*universo de discurso*".

Decorre do axioma da separação a existência de um conjunto sem nenhum elemento. Vejamos: se A é um conjunto qualquer, considere $B = \{x \in A : x \neq x\}$. Este conjunto, evidentemente, não possui elementos e é chamado *conjunto vazio*. Para indicá-lo usaremos os seguintes símbolos: $\emptyset$ ou $\{\ \}$.

Observações: (1) O conjunto vazio é subconjunto de qualquer conjunto, ou seja, $\emptyset \subseteq A$, para todo A. A prova deste fato é por vacuidade. De fato precisamos demonstrar que:

$$\forall x, (x \in \emptyset \longrightarrow x \in A).$$

Desde que, se a proposição "$x \in \emptyset$" é falsa, a proposição "$x \in \emptyset \longrightarrow x \in A$" é verdadeira, podemos concluir que $\emptyset \subseteq A$. □

(2) A teoria geral de conjuntos proposta por G. Cantor apresenta alguns paradoxos. Por exemplo, veja o seguinte paradoxo apresentado por Bertrand Russell: Seja Y o conjunto constituído pelos conjuntos B que não contêm a si mesmo como elemento. Em símbolos: $Y = \{B \mid B \notin B\}$.

Como um conjunto pode ser definido por uma propriedade, segue que Y é um conjunto bem definido. Agora a pergunta que se põe é: $Y \in Y$?

Resposta: Caso $Y \in Y$, então Y satisfaz a propriedade: $Y \notin Y$, absurdo. Caso $Y \notin Y$, então Y tem a propriedade que o define como conjunto e portanto $Y \in Y$, absurdo também!!

Este paradoxo nos diz que não podemos considerar a existência de um conjunto Universo no sentido absoluto da palavra, e daí surge a expressão "universo de discurso" usada anteriormente.

Para representarmos um conjunto por meio da listagem de seus elementos, às vezes podemos usar pontos de reticências quando o padrão dos elementos do conjunto é evidente. Por exemplo $S = \{0, 1, 2, 3, \ldots, 100\}$ denota o conjunto dos números naturais de 0 até 100, inclusive. Para conjuntos constituído de infinitos elementos, seguem algumas notações:

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ o conjunto dos números naturais.

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \{0, \pm 1, \pm 2, \ldots\}$ o conjunto dos números inteiros.

(3) Como já vimos, os símbolos $\in$ (*pertence*) $\notin$ (*não pertence*) relacionam elemento e conjunto, enquanto $\subseteq$ (*está contido*) $\not\subseteq$ (*não está contido*) ou $\supseteq$ (*contém*) $\not\supseteq$ (*não contém*) relacionam conjuntos. Por exemplo, sejam: $U = \{a, \{a\}, b, c, d, e, f\}$, $A = \{\{a\},\ b\}$, $B = \{a, b, c, d\}$. Então: $a \in B$, pois o elemento a e o conjunto B se relacionam. Temos também que $\{a\} \in A$ e $\{a\} \notin B$, pois o elemento $\{a\}$ se relaciona com o conjunto A e não se relaciona com o conjunto B. Também por isso $A \not\subseteq B$, ou $B \not\supseteq A$. Ainda temos:

$1 \in \{1, 2, 3\}$, $\{1\} \notin \{1, 2, 3\}$ e, portanto, $\{\{1\}\} \not\subseteq \{1, 2, 3\}$; $\{\{1\}\} \subseteq \{\{1\}, 2, 3\}$, pois $\{1\} \in \{\{1\}, 2, 3\}$.

Outros exemplos de conjuntos são:

(a) *Conjunto Unitário*: É qualquer conjunto constituido de um único elemento. São exemplos $\{a\}$, $\{3\}$, $\{\emptyset\}$.

(b) *Conjunto das Partes* - Dado um conjunto B, o conjunto das partes de B, denotado por $\wp(B)$ ou 2^B, é o conjunto definido por:

$$\wp(B) := \{X \mid X \subseteq B\}.$$

Logo, $X \in \wp(B) \Longleftrightarrow X \subseteq B$. Observe também que este conjunto nunca é vazio, pois pelo menos $\emptyset$ é um elemento de $\wp(B)$.

Exemplos $\wp(\emptyset) = \{\emptyset\}$, $\wp(\{1, 2\} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$, $\wp(\{a, \{a\}\}) = \{\emptyset, \{a\}, \{\{a\}\}, \{a, \{a\}\}\}$.

3.1 Diagrama de Venn-Euler

Uma boa ajuda para pensar sobre conjuntos é dada pelo "diagrama de Venn-Euler", em que regiões fechadas do plano são usadas para representar conjuntos.

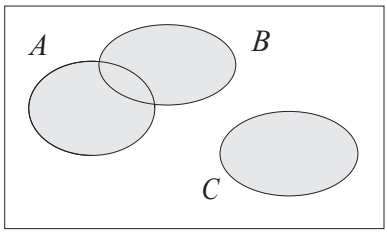


Figura 3.1: Diagrama de Venn

Na Figura 3.1, o retângulo representa o conjunto universo e as regiões cercadas pelas curvas representam os conjuntos A, B e C.

Observações: Freqüentemente um diagrama de Venn pode sugerir um argumento formal, por exemplo evidenciar o fato que, se A e B são dois conjuntos quaisquer, não se tem necessariamente $A \subseteq B$ ou $B \subseteq A$. Porém, devemos ter cuidado, pois um diagrama pode representar um caso muito particular da situação em questão e não servir para mostrar que, em geral, vale uma determinada propriedade.

3.2 Operações entre Conjuntos

3.2.1 Reunião ou União de Conjuntos

Definição 3.3 Dados A, $B \subseteq U$ a *união de A e B* é o conjunto constituído pelos elementos de U que são elementos de A ou de B. Denotando por $A \cup B$ este conjunto tem-se, $A \cup B := \{x \in U \mid x \in A \vee x \in B\}$, que se lê: "$A$ reunião (ou união) B".

Representando no diagrama de Venn-Euler, temos:

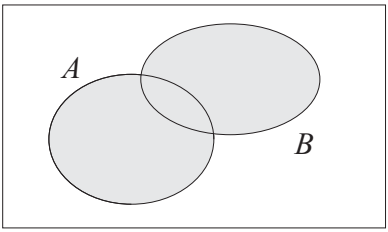


Figura 3.2: União

Exemplos: Sejam $A = \{-12, 1, 2, 6\}$ e $B = \{x \in \mathbb{R} : 0 \leq x \leq 8\}$. Então $A \cup B := \{-12\} \cup B$.

Seja $C = \{-1, 3, 7, 8\}$, então $A \cup C = \{-12, -1, 1, 2, 3, 6, 7, 8\}$.

Propriedades da Reunião: Sejam A, B, C conjuntos contidos em um conjunto universo U. Então:

(a) $A \cup B = B \cup A$,

(b) $A \subseteq A \cup B$ e $B \subseteq A \cup B$,

(c) $A \cup A = A$,

(d) $A \cup \emptyset = A$,

(e) $A \cup U = U$,

(f) $(A \cup B) \cup C = A \cup (B \cup C)$.

Como $A \cup B$ é definido em função de A e B usando o conectivo *ou*, nota-se que as propriedades da reunião e a sua tabela verdade (de $x \in A \cup B$ em função de $x \in A$ e $x \in B$) são as mesmas de $p \vee q$. Cada uma das propriedades acima correspondem, respectivamente, a:

(a') $p \vee q \equiv q \vee p$ **(b')** $p \Longrightarrow (p \vee q)$, **(c')** $p \vee p \equiv p$, **(d')** $p \vee C \equiv p$, **(e')** $p \vee T \equiv T$, **(f')** $(p \vee q) \vee r \equiv p \vee (q \vee r)$.

Observações: (1) Como vale $(A \cup B) \cup C = A \cup (B \cup C)$, podemos simplesmente suprimir or parênteses.

(2) Um elemento y não pertence a $A \cup B$ se, e somente se, $y \notin A$ e $y \notin B$.

A definição de reunião pode ser estendida para uma quantidade não enumerável de conjuntos, como segue

Definição 3.4 A reunião de uma coleção de conjuntos contidos em um conjunto universo U é o conjunto constituído dos elementos de U que pertencem a pelo menos um dos conjuntos da coleção.

Em particular, se temos um número finito n de conjuntos A_i podemos, escrever:

$$A_1 \bigcup A_2 \bigcup \cdots \bigcup A_n \;=\; \bigcup_{i=1}^{n} A_i$$

para $n \in \mathbb{N}, n \geq 1$.

Observação: No caso particular, em que cada A_i é um conjunto unitário $\{a_i\}$ com a_i em U, indicaremos sua união $\{a_1\} \cup \{a_2\} \cup \ldots \cup \{a_n\}$ simplesmente por $\{a_1, a_2, \ldots, a_n\}$. Note que estes elementos não são necessariamente distintos dois a dois. Se os elementos $a_1, a_2, \ldots, a_n$ são dois a dois distintos, diremos que o conjunto $A = \{a_1, a_2, \ldots, a_n\}$ tem n elementos, ou que n é o número de elementos de A, e usaremos a notação $n = |A|$. Assim, se $B = \{b_1, b_2, \ldots, b_n\}$ com $b_i \in U$ $(i = 1, \ldots, n)$, então $|B| \leq n$.

Exemplo Seja $A_i = \{i, i+1, i+2, \ldots\}$, i um número natural não nulo. Então

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} \{i, i+1, i+2, \ldots\} = \{1, 2, 3, \ldots\}.$$

3.2.2 Interseção de Conjuntos

Definição 3.5 Dados $A,\ B \subseteq U$, a *interseção de A e B* é o conjunto constituído pelos elementos de U que são elementos de A e de B. Denotando por $A \cap B$ este conjunto, tem-se:

$$A \bigcap B := \{x \in U \mid x \in A \wedge x \in B\},$$

que se lê: "A interseção B" ou "A inter B".

No diagrama de Venn-Euler temos:

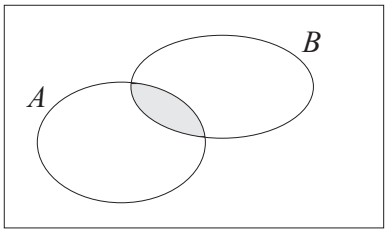


Figura 3.3: Interseção

Exemplo Sejam $A = \{-12, 1, 2, 6\}$, $B = \{x \in \mathbb{R} : 0 \leq x \leq 8\}$ e $C = \{-1, 3, 7, 8\}$.

Então, $A \cap B = \{1, 2, 6\}$ e $A \cap C = \emptyset$.

Propriedades da Interseção - Para A, B, C conjuntos contidos em um conjunto universo U, temos:

(a) $A \cap B = B \cap A$,

(b) $A \cap B \subseteq A$ e $A \cap B \subseteq B$,

(c) $A \cap A = A$,

(d) $A \cap \emptyset = \emptyset$,

(e) $A \cap U = A$,

(f) $(A \cap B) \cap C = A \cap (B \cap C)$.

Pode-se notar as propriedades da interseção, sendo definida pelo conectivo e, são as mesmas da proposição $p \wedge q$. As demonstrações ficam como exercícios.

A definição de interseção também pode ser estendida para uma quantidade não enumerável de conjuntos.

Definição 3.6 A interseção de uma coleção de conjuntos contidos em um conjunto universo U é o conjunto constituído dos elementos de U que são membros de todos os conjuntos da coleção.

Em particular, se temos um número finito n de conjuntos A_i, podemos escrever:

$$A_1 \bigcap A_2 \bigcap \cdots \bigcap A_n \;=\; \bigcap_{i=1}^{n} A_i$$

para $n \in \mathbb{N}, n \geq 1$.

Exemplo: Seja $A_i = \{i, i+1, i+2, \ldots\}$, i um número natural. Então,

$$\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i, i+1, i+2, \ldots\} = \{n, n+1, n+2, \ldots\}$$

e

$$\bigcap_{i=1}^{\infty} A_i = \bigcap_{i=1}^{\infty} \{i, i+1, i+2, \ldots\} = \emptyset.$$

Observações: (1) Um elemento y não pertence a $A \cap B$ se, e somente se, $y \notin A$ ou $y \notin B$.

(2) Dizemos que os conjuntos A e B são *disjuntos* se $A \cap B = \emptyset$. No exemplo dado anteriormente, A e C são conjuntos disjuntos.

3.2.3 Diferença de Dois Conjuntos e Conjunto Complementar

Definição 3.7 Dados os conjuntos $A,\ B \subseteq U$, chamamos de *diferença* de A por B o conjunto dos elementos que pertencem a A, mas não a B, e denotamos por $A - B$ ou $A \backslash B$, ou seja, $A - B := \{x \in U \mid x \in A \wedge x \notin B\}$.

Veja a representação no diagrama de Venn-Euler:

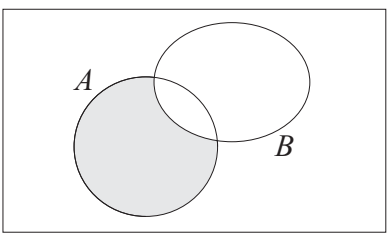


Figura 3.4: Diferença

Exemplos: (1) $\{1,2,3\} - \{3,4,5\} = \{1,2\}$
(2) $\{1,2\} - \{3,4\} = \{1,2\}$.
(3) $\{1,2,3\} - \{1,2,3,5\} = \emptyset$.
(4) Sendo $A = \{1,2,3,4,5\}$ e $B = \{2,4,6,8,10\}$, temos: $A - B = \{1,3,5\}$ e $B - A = \{6,8,10\}$.
(5) Se $A = \mathbb{N}$ e $B = \{x \in \mathbb{N} \mid x \text{ é ímpar }\}$, então $A - B = \{x \in \mathbb{N} \mid x \text{ é par }\}$ e $B - A = \emptyset$.

Propriedades da Diferença: Sejam A, B conjuntos contidos em um conjunto universo U. Então:

(a) $A - A = \emptyset$,

(b) $A - B \subseteq A$,

(c) $A - \emptyset = A$,

(d) $A - U = \emptyset$.

Definição 3.8 (Conjunto Complementar) No caso em que $B \subseteq A$, a diferença $A - B$ é chamada o *complementar de B em relação a A* e é denotada por $\mathcal{C}_A B := \{x \in U \mid x \in A \wedge x \notin B\}$. No caso em que $A = U$, denotaremos apenas por $\overline{B}$ ou por $B^c := \{x \in U \mid x \notin B\}$.

Veja as representações nos diagramas a seguir:

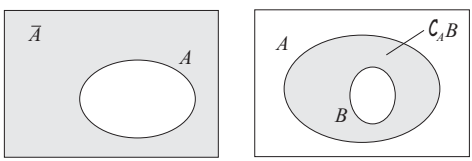


Figura 3.5: Complementar

Exemplos: Sejam $U = \mathbb{R}$, $A = \{x \in \mathbb{R} : x \leq 1\}$ e $B = \{x \in \mathbb{R} : x \geq 0\}$. Então
$\overline{A} = \{x \in \mathbb{R} \mid x \notin A\} = \{x \in \mathbb{R} : \neg(x \leq 1)\} = \{x \in \mathbb{R} \mid x > 1\}$.
$\overline{B} = \{x \in \mathbb{R} : x \notin B\} = \{x \in \mathbb{R} : \neg(x \geq 0)\} = \{x \in \mathbb{R} : x < 0\}$.

$A \cap B = \{x \in \mathbb{R} : x \in A \wedge x \in B\} = \{x \in \mathbb{R} : (x \leq 1) \wedge (x \geq 0)\} =$
$= \{x \in \mathbb{R} : 0 \leq x \leq 1\}.$

$A \cup B = \{x \in \mathbb{R} : x \in A \vee x \in B\} = \{x \in \mathbb{R} : (x \leq 1) \vee (x \geq 0)\} = \mathbb{R}.$

$A - B = \{x \in \mathbb{R} : x \in A \wedge x \notin B\} = \{x \in \mathbb{R} : (x \leq 1 \ \wedge x < 0)\} =$
$\{x \in \mathbb{R} : x < 0\} = \overline{B}.$

$B - A = \{x \in \mathbb{R} \mid x \in B \wedge x \notin A\} = \{x \in \mathbb{R} : (x \geq 0) \wedge (x > 1)\} =$
$\{x \in \mathbb{R} : x > 1\} = \overline{A}.$

Propriedades do Complementar. Para A e B partes de um conjunto universo U, temos:

(a) $\overline{B} \cap B = \emptyset$

(b) $\overline{\emptyset} = U$

(c) $\overline{U} = \emptyset$

(d) $\overline{B} \cup B = U$

(e) $\overline{(\overline{B})} = B$

(f) Dualidade ou Leis de De-Morgan: $\begin{cases} \text{(i) } \overline{(A \cap B)} = \overline{A} \cup \overline{B} \\ \text{(ii) } \overline{(A \cup B)} = \overline{A} \cap \overline{B} \end{cases}$

Nota: A complementação de conjunto em relação ao conjunto universo corresponde exatamente a negação de uma proposição e, portanto, suas propriedades são análogas. Verifique isto como exercício.

Reuniremos algumas das identidades mais importantes da teoria de conjuntos na tabela que segue:

TABELA (1) Identidades de Conjuntos

Identidades	Nomes
$A \cup \emptyset = A$ $A \cap U = A$	Identidades
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Dominação
$A \cup A = A$ $A \cap A = A$	Idempotentes
$\overline{(\overline{A})} = A$	Complementação
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Comutativa
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associativa
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributiva
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	DeMorgan
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorção
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complementação

Como exemplo, faremos a demonstração de que $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

$$\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} \\
&= \{x \mid \neg(x \in A \cap B)\} \\
&= \{x \mid x \notin A \vee x \notin B\} \\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} \\
&= \{x \mid x \in \overline{A} \cup \overline{B}\} \\
&= \overline{A} \cup \overline{B}.
\end{aligned}$$

Agora, construiremos a tábua desta propriedade, indicando por 1, na coluna de cada conjunto X, quando um elemento genérico x de

U pertence ao conjunto X, e 0 caso contrário. Os valores na coluna de A e B são independentes e temos quatro combinações possíveis para formar os pares constituídos de "zeros"e "uns", conforme $x \in A$ ou $x \notin A$, e $x \in B$ ou $x \notin B$. As outras colunas (é claro) dependem destas duas primeiras, do mesmo modo quando se faz uma tabela-verdade para uma proposição composta genérica.

A	B	A^c	B^c	$A \cap B$	$(A \cap B)^c$	$A^c \cup B^c$
1	1	0	0	1	0	0
1	0	0	1	0	1	1
0	1	1	0	0	1	1
0	0	1	1	0	1	1

Segue-se, pela tabela, que um elemento genérico $x \in U$, se $x \in A$ e $x \in B$, então $x \notin (A \cap B)^c$ e $x \notin A^c \cup B^c$ (primeira linha). Por todas as linhas, concluímos que um elemento genérico x de U pertence a $(A \cap B)^c$ e a $A^c \cup B^c$, sempre que, ou x não pertence a A, ou x não pertence a B. Veja, também, as linhas dois, três e quatro da tabela. Em outras palavras,

$$\forall x \in U : [x \in (A \cap B)^c \iff x \in A^c \cup B^c].$$

Logo, $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

A demonstração de que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ pode ser feita usando a teoria e as definições de intersecções e de reuniões. No entanto, também pode ser feita usando a tabela de "zeros" e "uns" associada, como segue (onde denotamos $A \cap B$ por D e $A \cap C$ por E para reduzir espaço).

A	B	C	$B \cup C$	$A \cap (B \cup C)$	$D \cup E$	$A \cap B$	$A \cap C$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	1	0
1	0	1	1	1	1	0	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Como $A \cap (B \cup C)$ e $(A \cap B) \cup (A \cap C)$ têm a mesma tabela de

"zeros" e "uns", significa que

$$\forall x \in U : \ [x \in A \cap (B \cup C) \Longleftrightarrow x \in (A \cap B) \cup (A \cap C)].$$

Isto prova a igualdade: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

3.3 Número de Elementos de um Conjunto

Muitas vezes estamos interessados em calcular o número de elementos da reunião $A \cup B$. Denotando por $|X|$ ou $n(X)$ o número de elementos do conjunto X, quando A e B são disjuntos temos que $|A \cup B| = |A| + |B|$, mas quando $A \cap B \neq \emptyset$ a soma $|A| + |B|$ conta duas vezes os elementos de $A \cap B$. De um modo geral, temos:

Proposição 3.9 *Sejam A, B subconjuntos finitos de um conjunto universo U. Então, $A \cup B$ também é finito e $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.*

Demonstração: O ponto de partida é que para A e B disjuntos define-se: $n(A \cup B)$ como sendo $n(A) + n(B)$. Agora, para quaisquer A, $B \subseteq U$ temos $A \cup B = A \cup (B - A)$, com A e $B - A$ conjuntos disjuntos. Logo,

$$n(A \cup B) = n(A) + n(B - A) \qquad (*)$$

Como $B = (B - A) \cup (A \cap B)$ com $B - A$ e $A \cap B$ disjuntos, segue-se que $n(B) = n(B - A) + n(A \cap B)$. Daí $n(B - A) = n(B) - n(A \cap B)$. Substituindo $n(B - A)$ em $(*)$ tem-se o resultado. □

Esta fórmula se generaliza para uma reunião genérica qualquer $\bigcup_{i=1}^{n} A_i$ e é chamada de *princípio de inclusão-exclusão.* Veja exercício 23.

Exemplo Sejam $A = \{1, 2, \ldots, 30\}$, $\quad B = \{21, 22, \ldots, 50\}$.

Então: $\quad A \cup B = \{1, 2 \ldots, 50\}$ e $A \cap B = \{21, 22, \ldots, 30\}$. Conseqüentemente $n(A \cup B) = 50 = 30 + 30 - 10 = n(A) + n(B) - n(A \cap B)$.

3.4 Produto Cartesiano e Gráficos

Definição 3.10 Uma *n-upla ordenada* $(a_1, a_2, \ldots, a_n)$, $(n > 1)$ é uma coleção ordenada que tem a_1 como seu primeiro elemento, a_2 seu segundo elemento, ..., a_n seu n-ésimo elemento. Diz-se que duas n-uplas $(a_1, a_2, \ldots, a_n)$ e $(b_1, b_2, \ldots, b_n)$ são iguais quando $a_i = b_i$, $i = 1, 2, \ldots, n$. A dupla (a_1, a_2) é dita *par ordenado*. Assim, $(a, b) = (c, d)$ quando $a = b$ e $c = d$. Em particular, se $a \neq b$, então $(a, b) \neq (b, a)$.

Nota: O conceito de par ordenado formado por a e b, nesta ordem, foi definido por Georg Cantor como sendo o conjunto $\{a, \{a, b\}\}$. Com esta definição tem-se que $(a, b) = (c, d)$ se, e somente se, $a = b$ e $c = d$. Prove isto.

Definição 3.11 Dados A, $B \subseteq U$, define-se o *produto cartesiano* de A por B e denota-se por $A \times B$ (A cartesiano B) como sendo o conjunto de todos os pares ordenados (a, b), onde $a \in A$ e $b \in B$. Assim

$$A \times B := \{(a, b) \mid a \in A \text{ e } b \in B\}.$$

Caso $A = \emptyset$ ou $B = \emptyset$, define-se $A \times B$ como sendo $\emptyset$.

Mais geralmente, se são dados os conjuntos A_1, $A_2, \ldots, A_n$, denota-se por $A_1 \times A_2 \times \cdots \times A_n$ o conjunto de todas as n-uplas $(a_1, a_2, \ldots, a_n)$ onde $a_i \in A_i$, $i = 1, 2, \ldots, n$. Também, escreve-se

$$A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\ i = 1, 2, \ldots, n\}$$

O conjunto $\{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\ i = 1, 2, \ldots, n\}$ também é denotado por $\prod_{i=1}^{n} A_i$.

Exemplo Sejam $A = \{a, r, \star\}$ e $B = \{2, 3\}$. Então $A \times B = \{(a, 2), (a, 3), (r, 2), (r, 3), (\star, 2), (\star, 3)\}$.

Caso A e B sejam subconjuntos de $\mathbb{R}$, podemos representar o produto cartesiano $A \times B$ no plano cartesiano. Nesta representação os elementos de A são representados na reta horizontal (eixo dos

x) e os elementos de B na reta vertical (eixo dos y). Assim, se o par $(x, y) \in A \times B$, ele é representado por

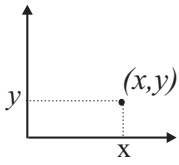


Figura 3.6: Representação do par (x, y)

Exemplo 1 $A = \{1, 2\}$ e $B = \{1, 2, 3\}$
$A \times B = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$

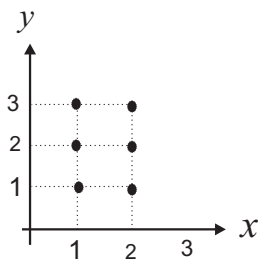


Figura 3.7: Produto Cartesiano $A \times B$

Exemplo 2 Se $C = \{x \in \mathbb{R} : -1 \leq x \leq 1\}$ e $D = \{1, 2\}$, então $C \times D = \{(x, 1), (z, 2),\ x, z \in C\} = \{(x, 1), x \in C\} \cup \{(x, 2), x \in C\}$, onde $[a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}$.

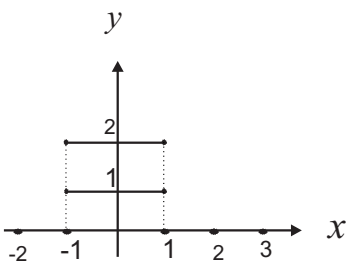


Figura 3.8: Produto Cartesiano $C \times D$

3.5 Representação Computacional de Conjuntos

Existem vários métodos de representar conjuntos usando um computador. Um método é armazenar os elementos de um conjunto de uma maneira não ordenada. Entretanto, se isto for feito, os cálculos computacionais para se obter uniões, intersecções, ou diferença entre conjuntos leva um tempo enorme, pois estas operações exigem uma grande pesquisa de elementos.

No caso em que o conjunto universo é finito com poucos elementos, podemos ordenar seus elementos e assim os cálculos de operações de conjuntos por computador ficam mais fáceis. Suponhamos por exemplo que $U = \{a_1, a_2, \ldots, a_n\}$, com $n \geq 1$ e não muito grande para que o computador a ser usado tenha memória suficiente para realizar as operações. Agora considere A um subconjunto de U. Identifique A com uma seqüência de comprimento n do tipo $x_1x_2 \ldots x_n$, onde $x_i = 1$, se $a_i \in A$, e $x_i = 0$, se $a_i \notin A$. Note que esta identificação é uma correspondência bijetora entre todos os subconjuntos de U e o conjunto de todas as n-uplas de "*zeros*" e "*uns*", dita *função característica de A*. Por exemplo, a seqüência de *bits* (do inglês binary digits): $11\cdots1$ corresponde ao conjunto universo U; a n-upla de bits $00\cdots0$ corresponde ao conjunto vazio $\emptyset$; a seqüência de n bits $1010\cdots0$ corresponde ao conjunto $\{a_1, a_3\}$; enquanto que, ao conjunto $\{a_1, a_2\}$, associamos a seqüência de n bits $110\cdots0$. Para o que segue precisaremos das *operações booleanas* "*ou*" e "*e*" sobre o conjunto $\{0, 1\}$. Elas são dadas pela tabela

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

Além destas operações, a *complementação booleana* também será usada: $\overline{0} = 1$ e $\overline{1} = 0$.

Agora, se são dados dois conjuntos A e B contidos em U, sejam $x_1x_2 \ldots x_n$ e $y_1y_2 \ldots y_n$ as seqüências de bits que representam os

conjuntos A e B, respectivamente. Então a seqüência $z_1 z_2 \dots z_n$ representa o conjunto $A \cup B$, onde $z_i = x_1 \vee y_i$, para $i = 1, 2, \dots, n$. Do mesmo modo a seqüência $t_1 t_2 \dots t_n$ representa o conjunto $A \cap B$, onde $t_i = x_i \wedge y_i$, para $i = 1, 2 \dots, n$, e $\bar{x}_1 \bar{x}_2 \dots \bar{x}_n$ é a seqüência de bits que representa o conjunto $\bar{A}$. Em outras palavras temos:

Definição 3.12 Dadas duas seqüências de bits $a = x_1 x_2 \cdots x_n$ e $b = y_1 y_2 \cdots y_n$ sobre o conjunto $\{0, 1\}$, definimos as operações booleanas $a \vee b$, $a \wedge b$ e $\bar{a}$ por:

$$a \vee b := (x_1 \vee y_1)(x_2 \vee y_2) \cdots (x_n \vee y_n),$$

$$a \wedge b := (x_1 \wedge y_1)(x_2 \wedge y_2) \cdots (x_n \wedge y_n), \quad \text{e}$$

$$\bar{a} := \bar{x}_1 \bar{x}_2 \cdots \bar{x}_n.$$

Lema 3.13 *Sejam A, B subconjuntos de $\{a_1, a_2, \dots, a_n\}$ e $a = x_1 x_2 \cdots x_n$, $b = y_1 y_2 \cdots y_n$ suas seqüências de bits associadas. Então a seqüência de bits correspondente aos conjuntos $A \cup B$, $A \cap B$ e $\bar{A}$ são, respectivamente, $a \vee b$, $a \wedge b$ e $\bar{a}$.*

Demonstração: De fato o elemento genérico $x_i \vee y_i$ de $a \vee b$ é 1 se, e somente se, $x_i = 1$ ou $y_i = 1$. Logo, $x_i \vee y_i = 1$ se, e somente se, $a_i \in A$ ou $a_i \in B$. Portanto $x_i \vee y_i = 1$ se, e somente se, $a_i \in A \cup B$. Por definição, a seqüência de bits $a \vee b$ é a seqüência de bits associada ao conjunto $A \cup B$.

Com um argumento semelhante, prova-se que a seqüência correspondente a $A \cap B$ é $a \wedge b$.

Agora, seja $u_1 u_2 \cdots u_n$ a seqüência de bits associada ao conjunto $\bar{A}$. Então o elemento a_i pertence a $\bar{A}$ se, e somente se, $a_i \notin A$. Em termos de seqüências de bits isto se traduz por: $u_i = 1$ se, e somente se, $x_i = 0$, $i = 1, 2, \dots, n$. Logo, $u_i = \bar{x}_i$ e, portanto, $u_1 u_2 \cdots u_n = \bar{x}_1 \bar{x}_2 \dots \bar{x}_n = \bar{a}$. □

Exemplo Sejam $U = \{1, 2, \dots, 10\}$, $A = \{1, 3, 5, 7, 9\}$ e $B = \{1, 2, 3, 4, 5\}$.

Então: $a = x_1 x_2 \cdots x_{10} = 1010101010$ e $b = y_1 y_2 \dots y_n = 1111100000$. Daí, $a \vee b = 1111101010$, $a \wedge b = 1010100000$ e

$\bar{a} = 0101010101$, e estas seqüências correspondem respectivamente aos conjuntos $A \cup B = \{1,2,3,4,5,7,9\}$, $A \cap B = \{1,3,5\}$ e $A^c = \{2,4,6,8,10\}$.

Exercícios

(1) Coloque verdadeiro ou falso: **(a)** $3 = \{3\}$, **(b)** $0 \in \emptyset$, **(c)** $3 \in \{3\}$, **(d)** $0 = \emptyset$, **(e)** $5 \in \{\{5\}\}$, **(f)** $4 \in \{\{4\},4\}$, **(g)** $3 \subseteq \{3\}$, **(h)** $\emptyset \in \{3\}$, **(i)** Se $A \neq B$ e $B \neq C$, então $A \neq C$, **(j)** $A \subseteq B$ e $B \not\subseteq C$, então $A \not\subseteq C$, **(l)** $x \in B$ e $B \subseteq C$, então $x \in C$, **(m)** $a \in B$ e $B \not\subseteq C \Rightarrow a \in C$.

Para o que se segue S é um conjunto não vazio.

(n) $S \in \wp(S)$, **(o)** $S \subseteq \wp(S)$, **(p)** $\{S\} \in \wp(S)$, **(q)** $\{S\} \subseteq \wp(S)$.

(2) Coloque *pertence* ou *está contido* nos campos pontilhados.

(a) $\{3,4\} \ldots \{\{3,4\},\{5,6\}\}$, **(b)** $\{2,8\} \ldots \{2,8,9\}$,

(c) $\emptyset \ldots \{3\}$, **(d)** $\{\{3,4\}\} \ldots \{\{3,4\},\{5,6\}\}$.

(3) Dados os conjuntos $A = \{1,2,3,4,5\}$, $B = \{2,3,4\}$ e $C = \{2,4,5\}$, verifique e justifique quais das seguintes sentenças são verdadeiras ou falsas: **(a)** $A \subseteq B$, **(b)**$A \subseteq C$, **(c)** $B \subseteq C$, **(d)** $C \subseteq B$, **(e)** $C \subseteq C$, **(f)** $\emptyset \subseteq B$.

(4) Dados os conjuntos $X = \{1,2,3,4,5\}$, $Y = \{1,2,3\}$ e $Z = \{4,6,8\}$ do conjunto universo $U = \{1,2,3,4,5,6,7,8\}$, obter: **(a)** $X \cap Y$, **(b)** $X \cap Z$, **(c)** $Y \cap Z$, **(d)** $(X \cap Y)^c$, **(e)** $X \cup Y$, **(f)** $X \backslash Y$, **(g)** $X \cup (Y \cup Z)$.

(5) Para $A = \{1,3,4,6,9,10,11,12,15\}$, enumere os elementos dos seguintes conjuntos:

a) $\{x \in A \mid x \neq 16\}$, **b)** $\{x \in A \mid x + 5 = 9\}$,

c) $\{x \in A \mid x$ é par$\}$, **d)** $\{x \in A \mid x$ é primo$\}$,

e) $\{x \in A \mid x^2 - 5x + 4 = 0\}$ **f)** $\{x \in A \mid (x+1) \in A\}$,

g) $\{x \in \mathbb{Z} \mid |x - 6| < 2\}$, **h)** $\{x \in \mathbb{N} \mid x$ é par$\}$,

i) $\{x \in \mathbb{N} \mid 4 < x < 9\}$.

(6) Prove cada uma das afirmações a seguir, onde A, B e C são subconjuntos de um conjunto universo U.

(a) Se $A \subseteq C$ e $B \subseteq C$, então $A \cup B \subseteq C$. **(b)** $A \cap B = \emptyset \iff A \cap B^c = A$.

(c) Se $A \subseteq B$ e $C \subseteq D$, então $A \cap C \subseteq B \cap D$.
(d) Se $A \cap B = A$ e $A \cap C \neq \emptyset$, então $B \cap C \neq \emptyset$.
(e) $A \cup (A^c \cap B) = A \cup B$. **(f)** $A \cap (A^c \cup B) = A \cap B$.
(g) $A \subseteq B \subseteq C \Longleftrightarrow A \cup B = B \cap C$. **(h)** $A \cup B = U \Rightarrow A^c \subseteq B$.
(i) $A \cup B = \emptyset \Rightarrow A = \emptyset$ e $B = \emptyset$. **(j)** $A \subseteq B$ se, e somente se, $B^c \subseteq A^c$ se, e somente se, $A \cap B = A$ se, e somente se, $A \cup B = B$ se, e somente se, $A \cap B^c = \emptyset$ se, e somente se, $A^c \cup B = U$.
(k) Se existe C, tal que $A \cup C = B \cup C$ e $A \cap C = B \cap C$, então $A = B$.
(l) Se $A \cup B = B$ e $A^c \cap B = \emptyset$, então $A = B$.
(m) Se $A \cup B = U$ e $A \cap B = \emptyset$. então $A = B^c$.
(n) Se $A \cap B = A$ e $B \cup C = C$, então $A \cap C^c = \emptyset$.
(o) Se $A \cap B = A$ e $B \cup C = B$, então $(A \cup C) \cap B = A \cup C$.
(p) Se $A \cap B^c = \emptyset$ e $A \neq \emptyset$, então $B \neq \emptyset$.
(q) Se $A \cap B^c = \emptyset$ e $A \cap B = \emptyset$, então $A = \emptyset$.
(r) $A = \emptyset$ se, e somente se, existe B, tal que $(A \cap B^c) \cup (A^c \cap B) = B$.
(s) Se $A \cup B = A$ para todo A, então $B = \emptyset$.
(t) Se $A \subseteq B$ e $A^c \subseteq B$, então $B = U$.
(u) Se $A \cup B \subseteq C$, então $A \subseteq C$ e $B \subseteq C$.
(v) Se $A \cup X = A \cup B$ e $A \cap X = \emptyset$, então $X = A^c \cap B$.

(7) Faça diagramas de Venn que representem as seguintes situações: **(a)** $A \cup B \subseteq A \cup C$ e $B \not\subseteq C$. **(b)** $A \cup B = C \cup B$, mas $A \neq C$. **(c)** $A \cap B \subseteq A \cap C$, mas $B \not\subseteq C$. **(d)** $A \cap B = C \cap B$, mas $A \neq C$.

(8) Prove ou apresente um contra-exemplo para as seguintes afirmações, onde A, B e C representam conjuntos quaisquer:
(a) $(A - B) - C = A - (B - C)$. **(b)** $A - (B - C) = (A \cup B) \cap C$.
(c) $A \cup (B \cap C) = (A \cup B) \cap C$. **(d)** $A - B = A - (B \cap A)$.

(9) Usando a definição $A \triangle B := (A \backslash B) \cup (B \backslash A)$, prove que:
(a) $A \triangle B = (A \cap B^c) \cup (A^c \cap B)$ e $A \triangle B = \mathcal{C}_{A \cup B} A \cap B$.
(b) $A \triangle B = B \triangle A$, **(c)** $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.
(d) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$. **(e)** $A \triangle A = \emptyset$.
(f) $A \cup B = A \triangle B \triangle (A \cap B)$ e $A^c = A \triangle U$. **(g)** $A \cap \emptyset = \emptyset$.
(h) $A \cap U = A$. **(i)** $A \triangle B = A \cup B \Longleftrightarrow A \cap B = \emptyset$.

(10) Para conjuntos A, B e C contidos em U, mostre que **(i)** $(A - B) - C \subseteq A - C$, **(ii)** $(A - C) \cap (C - B) = \emptyset$ e **(iii)** $(B-A) \cup (C-A) = (B \cup C) - A$.

(11) Dados $A = \{x \in \mathbb{R} : x^2 - 1 > 0\}$ e $B = \{x \in \mathbb{R} : x + 1 > 0\}$, determine:

(a) $A \cup B$, **(b)** $A^c \cap B$, **(c)** $A \backslash B$ e **(d)** $A^c \cap B^c$.

(12) Seja $U = \mathbb{R} \times [-10, 10]$ o conjunto universo e $A = \{(x, y) \in U : x + 2y = 1\}$, $B = \{(x, y) \in U : x^2 + x = y^2 + y\}$. **(i)** Ache $A \cap B$ e **(ii)** Ache $A \cap B^c$.

(13) Prove que $A \subseteq B \iff \wp(A) \subseteq \wp(B)$.

(14) **(i)** Prove que $A \subseteq B \iff A \cap B = A$ e que esta equivalência lógica corresponde a $(p \longrightarrow q) \equiv (p \wedge q \longleftrightarrow p)$ na álgebra das proposições.

(ii) Mais geralmente relacione as leis da álgebra de proposições com as leis da álgebra de conjunto.

(15) **(i)** Se A e B são conjuntos finito, verifique se $\wp(A \times B) = \wp(A) \times \wp(B)$.

(ii) Dê um exemplo que confirma a resposta em **(i)**.

(16) Calcule $\wp(A)$ onde $A = \{a, b, \{a, b\}\}$ e $a \neq b$.

(17) Calcule $B \times B$, sabendo-se que $|B \times B| = 16$ e $(0, 3)$ e $(7, 5)$ pertencem a $B \times B$.

(18) Calcule: **(i)** $\{1, 2, 3\} - \{3, 4, 5\}$, **(ii)** $\{1, 2, 4, 6, 7\} - \{3, 4, 5, 7, 9\}$, **(iii)** $\{1, 2, 3\} - \{1, 2, 3, 5\}$, **(iv)** $A - B$ e $B - A$, sendo $A = \{1, 2, 3, 4, 5\}$ e $B = \{2, 4, 6, 8, 10\}$ e **(v)** $A - B$ e $B - A$, sendo $A = \mathbb{N}$ e $B = \{x \in \mathbb{N} \mid x \text{ é ímpar}\}$.
Em que condições sobre os conjuntos A e B, tem-se $A-B = B-A$?

(19) Verifique as propriedades:

P1 $(A \cup B) \times C = (A \times C) \cup (B \times C)$,
P2 $(A \cap B) \times C = (A \times C) \cap (B \times C)$,
P3 $(A - B) \times C = (A \times C) - (B \times C)$,
P4 Se $A \subseteq B$, então $(A \times C) \subseteq (B \times C)$ e $(C \times A) \subseteq (C \times B)$,
P5 Se $|A| = m$ e $|B| = n$, então $|A \times B| = m.n$

(20) Construir o diagrama cartesiano de cada um dos seguintes produtos:
(a) $[1,4]\times[-2,3]$, **(b)** $[-2,3]\times[-1,2]$ e **(c)** $[-2,3]\times[-3,\infty[$.

(21) Dados os conjuntos $A=\{a,b\}$, $B=\{2,3\}$ e $C=\{3,4\}$, obter:
(a) $A\times(B\cup C)$, **(b)** $A\times(B\cap C)$, **(c)** $A\times(B-C)$,
(d) $(A\times B)\cup(A\times C)$ e **(e)** $A\times(B\triangle C)$, onde $X\triangle Y=(X\backslash Y)\cup(Y\backslash X)$.

(22) Sejam A e C dois conjuntos não vazios. Mostre que $A\subseteq B$ e $C\subseteq D$ se, e somente se, $A\times C\subseteq B\times D$.

(23) Sejam A,B,C partes finitas de um conjunto universo U.
(i) Mostre que:
$n(A\cup B\cup C)=n(A)+n(B)+n(C)-n(A\cap B)-n(A\cap C)-n(B\cap C)+n(A\cap B\cap C)$,
(ii) Generalize para um número m de conjuntos finitos de U, ou seja, para $A_1,A_2,\ldots,A_m$ conjuntos finitos; prove o princípio de inclusão-exclusão:
$$n(A_1\cup A_2\cup\cdots\cup A_m)=\sum_{i=1}^{m}n(A_i)-\sum_{i\neq j}^{m}n(A_i\cap A_j)+\sum_{i\neq j\neq k\neq i}^{m}n(A_i\cap A_j\cap A_k)-\cdots+(-1)^{m+1}n(A_1\cap A_2\cap\cdots\cap A_m),$$
(iii) Mostre que $n(A\times B)=n(A).n(B)$ e, a partir daí e da definição de $A\times B\times C$, mostre que $n(A\times B\times C)=n(A).n(B).n(C)$,
(iv) Se $A\subseteq B$, então $n(B-A)=n(B)-n(A)$ e **(v)** $n(\wp(A))=2^{n(A)}$.

(24) Determine condições necessárias e suficientes sobre os conjuntos A e B para que: **(a)** $|A\times B|=|A|$, e **(b)** $|A\cup B|=|A\times B|$.

(25) Numa cidade há 1.000 pessoas: 470 assinam o Estado, 420 assinam a Folha, 315 assinam a Gazeta, 140 assinam a Gazeta e a Folha, 220 assinam a Gazeta e o Estado, 110 a Folha e o Estado e 75 assinam os três jornais. Pede-se: **(a)** Quantas pessoas não assinam jornal? **(b)** Quantas pessoas assinam um dos jornais? **(c)** Quantas pessoas assinam exatamente dois jornais?

(26) Sejam $A_i=\{(x,ix),x\in\mathbb{R},\ i\in\mathbb{R}\}$. Determine a reunião e a

interseção desta coleção de conjuntos A_i.

(27) O *sucessor* de um conjunto A é o conjunto $A \cup \{A\}$.
(i) Ache os sucessores dos conjuntos: **(a)** $\{1, 2, 3\}$, **(b)** $\emptyset$, **(c)** $\{\emptyset\}$, **(d)** $\{\emptyset, \{\emptyset\}\}$.
(ii) Quantos elementos tem o sucessor de um conjunto com n elementos?

(28) Dê a seqüência de bits correspondente a cada um dos conjuntos dos ítens dos exercícios (4) e dos ítens a), b), c), d) e f) do exercício (5).

(29) Prove que, se $a = x_1 x_2 \cdots x_n$ e $b = y_1 y_2 \cdots y_n$ são seqüências de bits associadas aos conjuntos A e B, respectivamente, então $\overline{A \cap B} = \overline{a \wedge b}$, onde $\overline{a \wedge b} = \overline{x_1 \wedge y_1} \cdots \overline{x_n \wedge y_n}$.

(30) Dados os conjuntos A e B contidos em $U = \{z_1, \ldots, z_n\}$, $n \geq 1$, pede-se: Quais seqüências de bits estão associadas aos conjuntos $A - B$ e $A \Delta B := (A \cup B) - (A \cap B)$, relativamente às seqüências de bits associadas aos conjuntos A e B?

Capítulo 4

RELAÇÕES

4.1 Relações

Definição 4.1 Sejam A e B conjuntos quaisquer, não necessariamente distintos. Uma relação binária de A em B é um subconjunto do produto cartesiano $A \times B$.

Assim, se R é uma relação binária de A em B, então $\mathsf{R} \subseteq (A \times B)$ e usaremos a notação $a\mathsf{R}b$ para indicar que o par $(a, b) \in \mathsf{R}$. Neste caso, A e B são chamados, respectivamente, *conjunto de partida* e *conjunto de chegada* da relação R.

Observação: O adjetivo "binária"usado na definição indica que a relação está definida entre dois conjuntos, uma vez que é possível definir, mais geralmente, relações n-árias ($n \in \mathbb{N}$) entre n conjuntos $A_1, \ldots, A_n$ como sendo um subconjunto do produto cartesiano $A_1 \times \cdots \times A_n$. A relação binária é apenas um caso particular desta última definição.

4.1.1 Representações

Representação por meio de Matrizes

Sejam $A = \{a_1, a_2, \ldots, a_n\}$ e $B = \{b_1, b_2, \ldots, b_m\}$ conjuntos finitos com n e m elementos, respectivamente. Uma relação binária R definida de A em B pode ser representada por uma matriz

$M_{\mathsf{R}} = [r_{ij}]_{n\times m}$, onde :

$$r_{ij} = \begin{cases} 1, & \text{se } (a_i, b_j) \in \mathsf{R} \\ 0, & \text{se } (a_i, b_j) \notin \mathsf{R} \end{cases}$$

Observação: A escolha 0 e 1 é puramente técnica, quaisquer outros símbolos poderiam ser usados, como por exemplo \$ e $*$.

Exemplo 4.2 *Sejam* $A = \{a, b, c, d\}$, $B = \{2, 3\}$ *e* $\mathsf{R} = \{(a, 2), (b, 2), (b, 3), (d, 3)\}$. *A representação de* R *por meio de matriz é dada por:*

$$M_{\mathsf{R}} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Representação Gráfica

Quando uma relação binária está definida entre dois conjuntos finitos com poucos elementos podemos, ainda, representá-la por meio de diagrama de setas que é particularmente atraente pelos recursos visuais. Nesta representação, os elementos dos conjuntos são representados em diagramas de Venn-Euler, e um par ordenado é representado por uma flecha conectando os elementos do par, sendo que a ponta da mesma indica a segunda coordenada. Esta representação é também chamada *representação sagital* ou *por arcos*. A relação é, simplesmente, uma coleção de arcos. É claro que, a cada arco da relação, corresponde exatamente um símbolo "1" da representação matricial e vice-versa. Assim, dada uma representação, é fácil obter a outra. A representação sagital da relação R, é dada na figura 4.1.

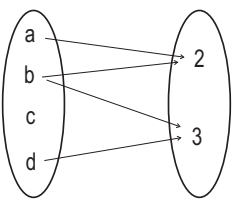


Figura 4.1: Representação de uma relação e os arcos dos pares ordenados

Representação Cartesiana

No caso em que a relação está definida entre subconjuntos de números reais, podemos representá-la através de um gráfico cartesiano. No caso em que a relação é constituída de um número finito de elementos, sua representação cartesiana é constituída de um número finito de pontos isolados do plano cartesiano. A seguir temos dois exemplos de representação de relações com um número infinito de elementos:

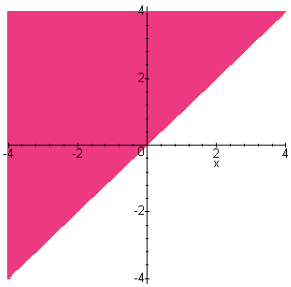


Figura 4.2: $\mathsf{S} = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$

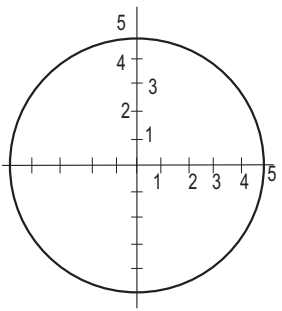


Figura 4.3: $\mathsf{T} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 25\}$

4.1.2 Comentários e Observações

Dados dois conjuntos A e B, sendo $U = A \times B$, temos:
(1) O conjunto $R(A \times B)$ de todas as relações de A em B é, simplesmente, $\mathcal{P}(U)$.

(2) O subconjunto vazio de U é chamado *relação vazia de A em B*. Nesta relação, é claro, nenhum elemento de A está relacionado com qualquer elemento de B. Se A e B são conjuntos finitos com poucos elementos, sua representação matricial corresponde à matriz nula.
(3) A relação U consiste de todos os pares ordenados possíveis e é chamada *relação universal de A em B*. Nesta relação, todos os elementos de A estão relacionados com todos os elementos de B, logo, na sua representação matricial, (se existir), todas as entradas são iguais a 1.
(4) A relação complementar de uma relação R, R^c, é um subconjunto de $A \times B$, a saber: $(A \times B) - \mathsf{R}$ constituído pelos pares ordenados $A \times B$ que não pertencem a R.
(5) A união de duas relações R_1 e R_2, definidas de A em B, é a relação $\mathsf{R}_1 \cup \mathsf{R}_2$, consistindo da união dos conjuntos R_1 e R_2, e a intersecção de R_1 e R_2 é a relação $\mathsf{R}_1 \cap \mathsf{R}_2$, que consiste da intersecção dos conjuntos R_1 e R_2. Se existirem as matrizes das relações R_1 e R_2, então as matrizes correspondentes à união e à intersecção das relações R_1 e R_2 são dadas por:

$$M_{\mathsf{R}_1 \cup \mathsf{R}_2} = [(r_{ij} \vee s_{ij})]_{n \times m} \quad \text{e} \quad M_{\mathsf{R}_1 \cap \mathsf{R}_2} = [(r_{ij} \wedge s_{ij})]_{n \times m}$$

onde: $M_{\mathsf{R}_1} = [r_{ij}]$ e $M_{\mathsf{R}_2} = [s_{ij}]$. Além disso, $\vee$ e $\wedge$ representam as *operações booleanas* sobre o conjunto $\{0, 1\}$ definidas por:

$$0 \vee 0 = 0, \quad 0 \vee 1 = 1, \quad 1 \vee 0 = 1, \quad 1 \vee 1 = 1 \quad \text{e}$$
$$0 \wedge 0 = 0, \quad 0 \wedge 1 = 0, \quad 1 \wedge 0 = 0, \quad 1 \wedge 1 = 1.$$

(6) Uma relação de um conjunto A em si mesmo (isto é, um subconjunto de A^2) é chamada *relação sobre A*, ou ainda, *relação em A*. Por exemplo,

$$\mathsf{R} = \{(0,0), (0,3), (2,0), (2,1), (2,3), (3,2)\}$$

é uma relação sobre $\{0, 1, 2, 3\}$, ou relação em $A = \{0, 1, 2, 3\}$.
(7) A relação idêntica sobre A, denotada por I_A, é definida por

$$I_A = \{(a, a); a \in A\}.$$

Por exemplo, para $A = \{0, 1, 2\}$, $I_A = \{(0, 0), (1, 1), (2, 2)\}$.
(8) Quando uma relação está definida sobre um conjunto finito A, podemos representá-la, também, por meio de um *grafo.* Por exemplo, seja: $A = \{a, b, c\}$ e $R = \{(a, a), (a, b), (b, a), (c, c)\}$. Sua representação por meio de um grafo é dada na figura 4.4.

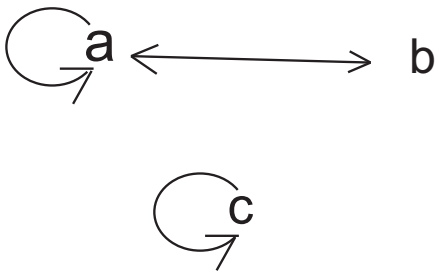


Figura 4.4: Representação de uma relação utilizando-se um grafo

4.1.3 Domínio e Imagem

Seja R uma relação de A em B.

Definição 4.3 Chama-se *domínio de* R o subconjunto de A constituído dos elementos x para os quais existe algum $y \in B$, tal que $(x, y) \in \mathsf{R}$. Simbolicamente temos:

$$D(\mathsf{R}) := \{x \in A \mid \exists y \in B : (x, y) \in \mathsf{R}\}.$$

Definição 4.4 Chama-se *imagem de* R o subconjunto de B constituído pelos elementos y para os quais existe algum x em A, tal que $(x, y) \in \mathsf{R}$. Simbolicamente:

$$Im(\mathsf{R}) := \{y \in B \mid \exists x \in A : (x, y) \in \mathsf{R}\}.$$

Por exemplo, para $A = \{0, 1, 2\}$, $B = \{-2, -1, 0, 1, 2\}$, considere as relações $\mathsf{R}_1 = \{(0, 0), (1, -1), (1, 1)\}$, $\mathsf{R}_2 = \{(0, 1), (1, 2), (2, -2), (0, -1), (1, 0)\}$, $\mathsf{R}_3 = \{(2, -2)\}$ e $\mathsf{R}_4 = \emptyset$. Então

$$\begin{array}{ll} D(\mathsf{R}_1) = \{0,1\} & Im(\mathsf{R}_1) = \{0,-1,1\} \\ D(\mathsf{R}_2) = \{0,1,2\} & Im(\mathsf{R}_2) = \{1,2,-2,-1,0\} \\ D(\mathsf{R}_3) = \{2\} & Im(\mathsf{R}_3) = \{-2\} \\ D(\mathsf{R}_4) = \emptyset & Im(\mathsf{R}_4) = \emptyset \end{array}$$

4.1.4 Inversa de uma Relação

Definição 4.5 Seja R uma relação de A em B. Chama-se *relação inversa* de R e indica-se por R^{-1} a seguinte relação de B em A.

$$\mathsf{R}^{-1} := \{(y,x) \in B \times A : (x,y) \in \mathsf{R}\}.$$

Por exemplo, num grupo de pessoas, a inversa da relação "é um dos pais de" é a relação "é filho de".

Exemplo 4.6 Sejam $A = \{a,b,c,d\}$, $B = \{0,1\}$ e $\mathsf{R} = \{(a,0), (b,0), (b,1), (c,1)\}$. Então

$$\mathsf{R}^{-1} = \{(0,a), (0,b), (1,b), (1,c)\}.$$

Exemplo 4.7 Se $A = B = \mathbb{R}$ e $\mathsf{R} = \{(x,y) \in \mathbb{R}^2 \mid y \leq 2x\}$, então

$$\mathsf{R}^{-1} = \{(y,x) \in \mathbb{R}^2 \mid y \leq 2x\} = \{(x,y) \in \mathbb{R}^2 \mid \frac{x}{2} \leq y\}.$$

Propriedades:

(1) Se $\mathsf{R} \subseteq A \times B$, então $\mathsf{R}^{-1} \subseteq B \times A$.

(2) Para toda relação R temos:

$$D(\mathsf{R}^{-1}) = Im(\mathsf{R}), \qquad Im(\mathsf{R}^{-1}) = D(\mathsf{R}) \qquad \text{e} \qquad (\mathsf{R}^{-1})^{-1} = \mathsf{R}.$$

(3) Dada a representação gráfica de $\mathsf{R} \subseteq A \times B$, obtemos a representação de R^{-1} apenas invertendo o sentido das flechas.

(4) Se existe representação matricial para R, então $M_{\mathsf{R}^{-1}} = (M_{\mathsf{R}})^t$.

(5) Sabendo que $(x, y) \in \mathsf{R} \iff (y, x) \in \mathsf{R}^{-1}$ fica evidente que, quando existe representação cartesiana para R, a representação cartesiana de R^{-1} é simétrica a ela em relação à reta $y = x$.

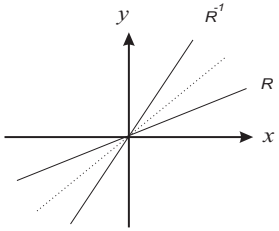


Figura 4.5: Simetria entre R e R^{-1}

4.1.5 Composição de Relações

Considere agora o seguinte caso: João é filho de Paulo e Paulo é irmão de Pedro. Podemos concluir que João é sobrinho de Pedro, combinando as duas relações dadas. Esta situação faz parte de um caso mais geral, que consiste em obter uma nova relação a partir da combinação de outras duas, o qual formalizaremos agora:

Definição 4.8 Sejam A, B e C conjuntos quaisquer, R e S relações binárias definidas de A em B e de B em C, respectivamente. A *composta de* S com R é definida por $\mathsf{S} \circ \mathsf{R} := \{(x, z) \in A \times C \mid \exists y \in B$ com, $(x, y) \in \mathsf{R}$ e $(y, z) \in \mathsf{S}\}$.

Observe que esta definição condiciona a existência da relação composta $\mathsf{S} \circ \mathsf{R}$, ao fato de que o conjunto de chegada de R seja igual ao conjunto de partida de S. Assim, se $A \neq C$, então podemos ter $\mathsf{S} \circ \mathsf{R}$ e não conseguiremos definir $\mathsf{R} \circ \mathsf{S}$, pois aqui o conjunto de chegada de S deve ser igual ao conjunto de partida de R.

Agora, examinaremos como construir $\mathsf{S} \circ \mathsf{R}$ dados S e R, isto é, como construir uma representação para $\mathsf{S} \circ \mathsf{R}$ a partir das representações de S e R. Consideraremos, primeiramente, a seguinte representação gráfica: segundo a definição de composição, um arco de $\mathsf{S} \circ \mathsf{R}$ existe se, e só se, existe pelo menos um caminho ligando um vértice de A a um vértice de C, passando através de algum vértice intermediário de B. Por exemplo, na figura 4.6 existe um caminho de a_5 para c_2, pois existe um arco de a_5 a b_3 e de b_3 a c_2. Observe que existem dois caminhos de a_5 a c_2, mas apenas um é suficiente para estabelecer $a_5(\mathsf{S} \circ \mathsf{R})c_2$.

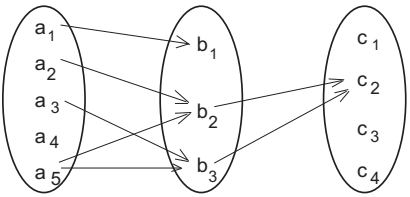


Figura 4.6: Representação de duas relações

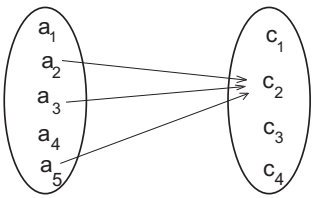


Figura 4.7: Representação de $S \circ R$

O procedimento adotado para construir a representação sagital de $\mathsf{S} \circ \mathsf{R}$ nos dá uma idéia para a construção de sua representação matricial. Sejam M_{R} e M_{S} as representações matriciais de S e R, de ordem $n \times m$ e $m \times p$, respectivamente. Consideremos agora uma linha (ou coluna) qualquer de M_{R} (ou M_{S}). Cada linha (ou coluna) é uma seqüência de símbolos 1's e 0's, ordenados da esquerda para a direita para as linhas (de cima para baixo para as colunas). Um caminho de a_i a c_k existe se, e só se, para algum b_j ocorrem simultaneamente:

(a) um caminho de a_i a b_j e
(b) um caminho de b_j a c_k.
Observe que:

(i) cada linha de M_{R} contém o mesmo número de entradas que as colunas de M_{S}, e o número dessas entradas é o mesmo que $n(B)$;

(ii) observemos, mais ainda, que a condição (a) indica a existência de 1 na j-ésima posição da linha de M_{R} correspondente ao elemento a_i, e a condição (b) é satisfeita por um elemento 1 na k-ésima posição da coluna de M_{S} correspondente a c_k.

A matriz $M_{\mathsf{S}\circ\mathsf{R}}$ pode ser obtida de M_{R} e M_{S} com o seguinte

Teorema 4.9 *Sejam A, B e C conjuntos com n, m e p elementos, respectivamente, R e S relações definidas do conjunto A em B e de B em C, respectivamente. Se $M_{\mathsf{R}} = [r_{ik}]$ e $M_{\mathsf{S}} = [s_{kj}]$, então a matriz de $\mathsf{S}\circ\mathsf{R}$ é*

$$M_{\mathsf{S}\circ\mathsf{R}} = \left[\bigvee_{k=1}^{n} (r_{ik} \wedge s_{kj})\right]_{m\times p}.$$

Demonstração: De fato, a i,j-entrada expandida é:

$$(r_{i1} \wedge s_{1j}) \vee (r_{i2} \wedge s_{2j}) \vee \cdots \vee (r_{in} \wedge s_{nj}),$$

que tem valor de 1 se, e só se, para pelo menos um valor de k, $r_{ik} = s_{kj} = 1$. Em termos das relações, isto significa que o par $(a_i, c_j) \in (\mathsf{S}\circ\mathsf{R})$ se, e somente se, existe $b_k \in B$, tal que $(a_i, b_k) \in \mathsf{R}$ e $(b_k, c_j) \in \mathsf{S}$. Isto demonstra o teorema. □

Nota: Podemos escrever $M_{\mathsf{S}\circ\mathsf{R}} = M_{\mathsf{R}}.M_{\mathsf{S}}$, onde o produto de matrizes é o *produto booleano* conforme visto na demonstração do Teorema 4.9.

Exemplo 4.10 Considerando as relações dadas pela figura 4.6, a matriz $M_{\mathsf{S}\circ\mathsf{R}}$ pode ser obtida da seguinte forma:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \bullet \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Suponha agora que são dados quatro conjuntos A, B, C e D e 3 relações binárias: R de A em B, S de B em C e T de C em D. Então a composta $\mathsf{T} \circ (\mathsf{S} \circ \mathsf{R})$ está definida e também $(\mathsf{T} \circ \mathsf{S}) \circ \mathsf{R}$. Além disso , vale o seguinte resultado:

Teorema 4.11 *Para relações binárias* R, S, T, *tais que existem* $\mathsf{T} \circ (\mathsf{S} \circ \mathsf{R})$, *tem-se que existe também* $(\mathsf{T} \circ \mathsf{S}) \circ \mathsf{R}$ *e*

$$\mathsf{T} \circ (\mathsf{S} \circ \mathsf{R}) = (\mathsf{T} \circ \mathsf{S}) \circ \mathsf{R}.$$

Demonstração: Desde que existe $\mathsf{T} \circ (\mathsf{S} \circ \mathsf{R})$ então o conjunto de chegada de R é igual ao conjunto de partida de S e o conjunto de chegada de $\mathsf{S} \circ \mathsf{R}$ é igual ao conjunto de partida de T. Logo a situação apresentada é $\mathsf{R} \subseteq A \times B$, $\mathsf{S} \subseteq B \times C$ e $\mathsf{T} \subseteq C \times D$. Consequentemente existe a relação composta $(\mathsf{T} \circ \mathsf{S}) \circ \mathsf{R}$. Agora consideremos $(a, d) \in A \times D$. Então:
$(a, d) \in (\mathsf{T} \circ \mathsf{S}) \circ \mathsf{R} \iff \exists b \in B : (a, b) \in \mathsf{R}$ e $(b, d) \in (\mathsf{T} \circ \mathsf{S})$. E $(b, d) \in (\mathsf{T} \circ \mathsf{S}) \iff \exists c : (b, c) \in \mathsf{S}$ e $(c, d) \in \mathsf{T}$. Mas, de $(a, b) \in \mathsf{R}$ e $(b, c) \in \mathsf{S}$ segue-se, por definição, que $(a, c) \in (\mathsf{S} \circ \mathsf{R})$. De $(a, c) \in (\mathsf{S} \circ \mathsf{R})$ e $(c, d) \in \mathsf{T}$ temos que $(a, d) \in \mathsf{T} \circ (\mathsf{S} \circ \mathsf{R})$ e portanto

$$(\mathsf{T} \circ \mathsf{S}) \circ \mathsf{R} \subseteq \mathsf{T} \circ (\mathsf{S} \circ \mathsf{R}).$$

Analogamente, demonstra-se que $\mathsf{T} \circ (\mathsf{S} \circ \mathsf{R}) \subseteq (\mathsf{T} \circ \mathsf{S}) \circ \mathsf{R}$. Assim, podemos concluir que:

$$(\mathsf{T} \circ \mathsf{S}) \circ \mathsf{R} = \mathsf{T} \circ (\mathsf{S} \circ \mathsf{R}).$$

□

Nota: Esta última igualdade nos mostra que a composição de relações é associativa e, assim, podemos omitir os parênteses quando escrevemos as composições $(\mathsf{T} \circ \mathsf{S}) \circ \mathsf{R}$ ou $\mathsf{T} \circ (\mathsf{S} \circ \mathsf{R})$ e escrever simplesmente $\mathsf{T} \circ \mathsf{S} \circ \mathsf{R}$.

4.1.6 Propriedades de Relações Sobre Conjuntos

Uma relação R definida sobre um conjunto A pode apresentar várias propriedades, algumas das quais passaremos a estudar a seguir.
Reflexiva: Uma relação R definida sobre um conjunto A é *reflexiva* se $[(\forall a)\ (a \in A \Longrightarrow (a, a) \in \mathsf{R})]$, ou ainda $[\forall a, (a \in A \Longrightarrow a\mathsf{R}a]$.
Observe que:
(i) A representação matricial de uma relação reflexiva apresenta 1's em todas as posições da diagonal principal, isto é, $r_{ii} = 1$ para todo i.
(ii) a representação por grafo de uma relação reflexiva é caracterizada por um laço em torno de cada vértice.
(iii) Se R é uma relação reflexiva, então $I_A \subseteq \mathsf{R}$, onde $I_A := \{(x, x),\ x \in A\}$ também é representado por Δ_A e dizemos ser a *diagonal de A.*
Simétrica: Uma relação R definida sobre um conjunto A é *simétrica* se $\forall a, b \in A : (a, b) \in \mathsf{R} \Longrightarrow (b, a) \in \mathsf{R}$.
Observe que:
(i) a representação por meio de um gráfico cartesiano é uma figura simétrica em relação à reta $y = x$.
(ii) na representação sagital, os arcos ocorrem aos pares, ou seja, cada seta tem dupla ponta;
(iii) Se M_{R} é a representação matricial de R, então $M_{\mathsf{R}} = M_{\mathsf{R}^{-1}} = M_{\mathsf{R}}^t$, uma vez que se R é uma relação simétrica, então $\mathsf{R} = \mathsf{R}^{-1}$.

Quando nem todos os arcos de uma representação gráfica de R formam pares simétricos, R é chamada assimétrica. Entretanto, quando nenhum par simétrico existe, temos a anti-simetria:
Anti-simétrica: Uma relação R definida sobre um conjunto A é *anti-simétrica* se, quaisquer que sejam a e b em A, $\big((a, b) \in \mathsf{R}$ e $(b, a) \in \mathsf{R} \Longrightarrow a = b\big)$. Um exemplo simples de relação anti-simétrica é a relação "menor ou igual" definida sobre o conjunto dos inteiros.

Transitiva: Uma relação R definida sobre um conjunto A é *transitiva* quando para quaisquer $a,\ b,\ c \in A$ $\big((a,b) \in \mathsf{R}$ e $(b,c) \in \mathsf{R}$ implicam $(a,c) \in \mathsf{R}\big)$.

A característica da representação gráfica de uma relação transitiva é uma estrutura de três arcos, como na figura a seguir.

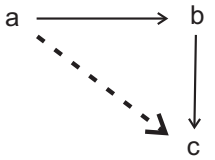


Figura 4.8: Relação Transitiva

Isto significa que, se existe um caminho constituído de dois arcos consecutivos ligando os vértices a e c através de um vértice intermediário b, então existe um arco de a para c.

Observe que todos os caminhos constituídos de dois arcos podem ser encontrados aplicando-se a relação R duas vezes, ou seja, pela composta $\mathsf{R} \circ \mathsf{R}$. Note ainda que R é transitiva se, e só se, R contém $\mathsf{R} \circ \mathsf{R}$ e que para a transitividade de R podem ocorrer arcos na representação gráfica de R que não são arcos da representação de $\mathsf{R} \circ \mathsf{R}$. Isto acontece, por exemplo, quando um vértice da representação de R não tem nenhum arco "saindo"dele.

Exemplo 4.12 A relação definida sobre $\{1,2,3,4\}$ por:

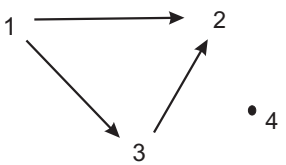


Figura 4.9:

não é reflexiva, não é simétrica e é anti-simétrica e transitiva.

Exemplo 4.13 A relação definida sobre $\{1,2,3,4\}$ por

$$1 \quad 2 \longleftrightarrow 3 \longleftrightarrow 4$$

é simétrica, não é reflexiva, nem transitiva e nem anti-simétrica.

Exemplo 4.14 A relação dada por:

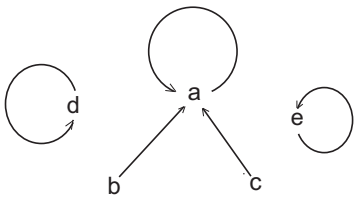


Figura 4.10:

é anti-simétrica, transitiva, não é reflexiva e nem simétrica.

Exemplo 4.15 A relação de igualdade: $\Delta_{\{a,b,c\}} = \{(a,a),(b,b),(c,c)\}$ é reflexiva, simétrica, anti-simétrica e transitiva.

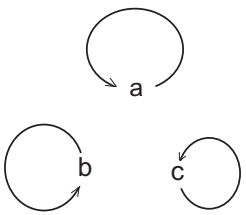


Figura 4.11:

Exemplo 4.16 Considere sobre o conjunto dos números inteiros a seguinte relação:

$$(a,b) \in \mathsf{R} \Longleftrightarrow |a-b| = 1.$$

Esta relação é simétrica, não é reflexiva, não é transitiva nem anti-simétrica.

Exemplo 4.17 Em $\mathcal{P}(U)$ (U qualquer), consideremos R a relação de inclusão. R é reflexiva, anti-simétrica e transitiva.

Exemplo 4.18 Em $\mathcal{P}(U),\ U \neq \emptyset$ a relação dada por

$$(A, B) \in \mathsf{R} \Longleftrightarrow A \cap B = \emptyset$$

é simétrica, não é reflexiva, não transitiva nem anti-simétrica.

Exemplo 4.19 (1) A relação R_1 sobre $E = \{a, b, c\}$, cujo diagrama de flechas é:

$$a \longrightarrow b \longleftarrow c,$$

não é reflexiva, não é simétrica, não é transitiva nem anti-simétrica.

Exemplo 4.20 A relação de divisibilidade sobre $\mathbb{Z}$ definida por: $\mathsf{R}_2 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x|y\}$ é reflexiva, transitiva, não é simétrica e não é anti-simétrica.

De fato, para qualquer $a \in \mathbb{Z},\ a$ divide a. Logo, $(a, a) \in \mathsf{R}_2$ qualquer que seja $a \in \mathbb{Z}$. Se a divide b e b divide c, então a divide c. Logo, a relação R_2 é transitiva. Como 2 divide 4 e 4 não divide 2 em $\mathbb{Z}$, temos que a relação R_2 não é simétrica. Finalmente, R_2 também não é anti-simétrica pois 2 divide -2 e -2 divide 2, ou seja, $(2, -2) \in \mathsf{R}_2,\ (-2, 2) \in \mathsf{R}_2$ e $2 \neq -2$.

Note que a relação de divisibilidade sobre $\mathbb{N}$ é anti-simétrica.

Exemplo 4.21 Considere o conjunto T de retas no plano e R_3 a seguinte relação sobre T, $\mathsf{R}_3 = \{(r, s) \in T^2 : r \perp s\}$, onde $r \perp s$ significa "r é perpendicular a s".

Como $r \not\perp r,\ \forall r \in T$ então R_3 não é reflexiva. Se $r \perp s$, então $s \perp r$, para todos $r,\ s \in T$. Então R_3 é simétrica. R_3 não é anti-simétrica, pois se r e s são perpendiculares, então $r \perp s$ e $s \perp r$, e, no entanto, $r \neq s$. Também não é transitiva pois: $r \perp s$ e $s \perp t$ não implica que $r \perp t$; basta tomar $t = r$.

Exemplo 4.22 Seja $\mathsf{R}_4 = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$, ou seja, R_4 é a relação de ordem usual $\leq$ sobre $\mathbb{R}$.

A relação $\leq$ é reflexiva, anti-simétrica, transitiva e não é simétrica, pois $2 \leq 4$ e $4 \not\leq 2$.

Dois tipos particularmente interessantes de relações são:

(i) as que são simultaneamente reflexivas, simétricas e transitivas chamadas *relações de equivalência* e;
(ii) as que são simultaneamente reflexivas, anti-simétricas e transitivas, tecnicamente chamadas de *relações de ordem parcial*.

Essas relações induzem estruturas especiais nos conjuntos nos quais estão definidas e serão estudadas, com detalhes, posteriormente.

Uma pergunta que ocorre naturalmente neste ponto é se as propriedades são independentes uma das outras. A resposta é afirmativa, uma vez que podemos encontrar relações que sejam:

(1) não simétrica, não anti-simétrica e transitiva,
(2) não simétrica e transitiva,
(3) simétrica e não transitiva,
(4) simétrica e transitiva,
(5) reflexiva, não simétrica e não transitiva,
(6) reflexiva, não simétrica e transitiva,
(7) reflexiva, simétrica e não transitiva,
(8) reflexiva, simétrica e transitiva.

Deixamos ao leitor interessado o trabalho de exibir exemplos destas situações!
Uma outra pergunta que ocorre naturalmente é: Qual é a relação entre as propriedades apresentadas por R e R^{-1}?
O seguinte teorema (que apresentaremos sem demonstração) nos garante que:

Teorema 4.23 *As propriedades reflexiva, simétrica, anti-simétrica e transitiva de uma relação* R *definida sobre um conjunto* A *são preservadas pela inversão, ou seja, se* R *é uma relação definida sobre* A *e tem uma destas propriedades, então o mesmo acontece com* R^{-1}. *Além disso, temos:*

(i) R *é reflexiva se, e somente se,* $\Delta_A \subseteq \mathsf{R}$,
(ii) R *é simétrica se, e somente se,* $\mathsf{R}^{-1} = \mathsf{R}$,
(iii) R *é transitiva se, e somente se,* $\mathsf{R} \circ \mathsf{R} \subseteq \mathsf{R}$ *e*
(iv) R *é anti-simétrica se, e somente se,* $\mathsf{R} \cap \mathsf{R}^{-1} \subseteq \Delta_A$.

Exercícios

(1) Determine quais as propriedades de cada uma das relações a seguir definidas sobre o conjunto dos números inteiros positivos:
(a) m é divisível por n.
(b) $m + n$ é par.
(c) $m.n$ é par.
(d) $m + n$ é múltiplo de 3.
(e) $m + n$ é ímpar.
(f) $m + n \geq 50$.
(g) m é uma potência de n.
(h) $m \geq n$.

(2) Seja A um conjunto não vazio. Mostre que o conjunto $\emptyset$, considerado como uma relação sobre A, não é reflexiva, mas é simétrica e transitiva.

(3) Determine quais propriedades são preservadas pela composição de relações definidas sobre um conjunto A, $A \neq \emptyset$.

(4) Se I_A representa a relação idêntica de A, $A \neq \emptyset$, mostre que uma relação R definida sobre A é reflexiva se, e somente se, $I_A \subseteq \mathsf{R}$.

(5) Mostre que uma relação R definida sobre A, $A \neq \emptyset$, é anti-simétrica se, e somente se, $(\mathsf{R} \cap \mathsf{R}^{-1}) \subseteq I_A$.

(6) Prove o resto dos ítens do Teorema 4.23.

(7) Considere uma relação representada pela matriz:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Esta relação é reflexiva? É simétrica? É anti-simétrica? É transitiva? (Justifique cada uma de suas respostas).

(8) Por meio de uma matriz (ou outro) mostre que, se R e S são ambas relações simétricas definidas sobre um conjunto não vazio A, o mesmo pode não ocorrer com $\mathsf{R} \circ \mathsf{S}$.

(9) Seja R uma relação simétrica e transitiva, definida sobre um conjunto não vazio A. Suponha que $(a, b) \in \mathsf{R}$. Pela simetria devemos ter $(b, a) \in \mathsf{R}$ e então, usando a transitividade, devemos ter $(a, a) \in \mathsf{R}$, ou seja, R é reflexiva. Assim, toda relação simétrica

e transitiva é reflexiva. Existe alguma falha nesta argumentação? Explique.

(10) Mostre que quando R é uma relação simétrica, definida sobre um conjunto não vazio A, o mesmo ocorre com R^k ($\forall k \in \mathbb{N},\ k \geq 1$).

(11) Sejam R e S relações simétricas definidas sobre um conjunto não vazio A. Mostre que $(\mathsf{R} \circ \mathsf{S}) \subseteq (\mathsf{S} \circ \mathsf{R})$ implica em $(\mathsf{R} \circ \mathsf{S}) = (\mathsf{S} \circ \mathsf{R})$.

(12) Seja R uma relação reflexiva, definida sobre um conjunto não vazio A, que não é, necessariamente, simétrica ou transitiva. Mostre que as relações $\mathsf{R} \circ \mathsf{R}^{-1}$ e $\mathsf{R}^{-1} \circ \mathsf{R}$ são reflexivas e simétricas. Pergunta-se: $\mathsf{R} \circ \mathsf{R}^{-1}$ é transitiva?

(13) Mostre que:

(a) Se R e S são relações simétricas definida sobre A, $A \neq \emptyset$ então $\mathsf{S} \circ \mathsf{R}$ é simétrica se, e somente se, $\mathsf{R} \circ \mathsf{S} = \mathsf{S} \circ \mathsf{R}$;

(b) A composição de duas relações simétricas não é, necessariamente, simétrica (Sugestão: encontre um contra-exemplo).

(14) Descreva um algoritmo para checar se uma relação é transitiva.

(15) Quantas relações podem ser definidas de A em B, quando $n(A) = m$ e $n(B) = r$.

(16) Quantas relações reflexivas podemos definir sobre um conjunto A com $n(A) = m$? Nas mesmas condições, quantas relações simétricas? Quantas anti-simétricas?

(17) Sejam R e S relações definidas de $A = \{1, 2, 3, 4\}$ em $B = \{2, 3, 4\}$ e de B em A, respectivamente, por:

$\mathsf{R} = \{(a, b) \mid a + b = 6\}$ e $\mathsf{S} = \{(b, c) \mid b - c = 1\}$. Obter: $\mathsf{S} \circ \mathsf{R}$, $I_B \circ \mathsf{R}$, $\mathsf{R} \circ I_A$ e $\mathsf{R} \circ \mathsf{S}$, além das matrizes que representam R, S, $\mathsf{S} \circ \mathsf{R}$, $\mathsf{R} \circ \mathsf{S} \circ \mathsf{R}$.

(18) Dados $A = \{0, 1, 2, 3\}$, R e S relações definidas em A por $\mathsf{R} = \{(i, j) \mid j = i + 1 \text{ ou } j = \frac{i}{2}\}$ e $\mathsf{S} = \{(i, j) \mid i = j + 2\}$. Determine: $\mathsf{S} \circ \mathsf{R}$, $\mathsf{R} \circ \mathsf{S}$, $\mathsf{R} \circ \mathsf{S} \circ \mathsf{R}$ e R^3.

(19) Dadas R, S e T relações definidas sobre um conjunto A, mostre que $\mathsf{R} \subseteq \mathsf{S}$ implica que:

$\mathsf{T} \circ \mathsf{R} \subseteq \mathsf{T} \circ \mathsf{S}$, $\mathsf{R} \circ \mathsf{T} \subseteq \mathsf{S} \circ \mathsf{T}$ e $\mathsf{S}^{-1} \supseteq \mathsf{R}^{-1}$.

(20) Dados $\mathsf{R} = \{(0, 1), (1, 2), (3, 4)\}$ e $\mathsf{D} \circ \mathsf{R} = \{(1, 3), (1, 4), (3, 3)\}$, encontrar uma relação de menor cardinalidade que satisfaça as condições dadas. Em geral, dados R e $\mathsf{D} \circ \mathsf{R}$, D fica univocamente determinado? E D com a menor cardinalidade possível, é

univocamente determinado?
(21) Dado $\mathsf{R} = \{(i,j) : i,j \in \mathbb{Z} \mid j - i = 1\}$. Obter R^r, $(\forall r, r \in \mathbb{N}^*)$.
(22) Mostre que, se $\mathsf{S} \circ \mathsf{R}$ está definida, então $(\mathsf{S} \circ \mathsf{R})^{-1} = \mathsf{R}^{-1} \circ \mathsf{S}^{-1}$.
(23) Dadas as relações R, S e T definidas sobre $A = \{1,2,3,4\}$ por:

$$M_{\mathsf{R}} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad M_{\mathsf{S}} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$M_{\mathsf{T}} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

determine as relações e as matrizes correspondentes a:

(a) $\mathsf{S} \cup \mathsf{R}$ (d) $\mathsf{R} \cup \mathsf{T}^c$ (g) $\big(\mathsf{R} \cup (\mathsf{S} \cap \mathsf{T}^c)\big)^c$
(b) $\mathsf{R} \cap \mathsf{S}$ (e) $(\mathsf{R} \cup \mathsf{S}) \cap \mathsf{T}$ (h) $(\mathsf{S} \cup \mathsf{T}) \cap (\mathsf{R} \cup \mathsf{T}^c)$
(c) T^c (f) $\mathsf{R} \cup \mathsf{S}^c$

(24) Prove que, para quaisquer relações R e S definidas sobre um conjunto A, tem-se:

(a) $(\mathsf{R} \cup \mathsf{S})^{-1} = \mathsf{R}^{-1} \cup \mathsf{S}^{-1}$
(b) $(\mathsf{R} \cap \mathsf{S})^{-1} = \mathsf{R}^{-1} \cap \mathsf{S}^{-1}$

4.2 Relação de Equivalência

Definição 4.24 Uma relação R sobre um conjunto A, não vazio, é uma *relação de equivalência* sobre A se for reflexiva, simétrica e transitiva, isto é, são verdadeiras as seguintes sentenças:
(i) $\forall x,\ [x \in A \Longrightarrow (x,x) \in \mathsf{R}]$,
(ii) $\forall x, \forall y \in A,\ [(x,y) \in \mathsf{R} \Longrightarrow (y,x) \in \mathsf{R}]$ e
(iii) $\forall x, \forall y, \forall z \in A,\ [(x,y) \in \mathsf{R}\ \text{ e }\ (y,z) \in \mathsf{R} \Longrightarrow (x,z) \in \mathsf{R}]$.

Exemplo 4.25 A relação de igualdade sobre um conjunto A é uma relação de equivalência, pois:
$\forall x,\ [x \in A \Longrightarrow x = x]$,
$\forall x, y,\ [x = y \Longrightarrow y = x]$ e
$\forall x, y, z,\ [x = y\ \text{ e }\ y = z \Longrightarrow x = z]$.

Exemplo 4.26 A relação universal definida sobre um conjunto A é uma relação de equivalência, pois:
$\forall x,\ x \in A \Longrightarrow (x,x) \in A \times A$,
$\forall x, y,\ (x,y) \in A \times A \Longrightarrow (y,x) \in A \times A$, e
$\forall x, y, z,\ (x,y) \in A \times A\ \text{ e }\ (y,z) \in A \times A \Longrightarrow (x,z) \in A \times A$.

Exemplo 4.27 A relação R definida sobre $\mathbb{Z}$ por: $\forall x, y \in \mathbb{Z}$, $x\mathsf{R}y \iff \exists q \in \mathbb{Z} : x - y = mq$ (onde $m \geq 0$ é um inteiro fixo) é uma relação de equivalência, pois: (i) $a - a = 0 = 0.m$, $\forall a \in \mathbb{Z}$. Logo $a\mathsf{R}a,\ \forall a \in \mathbb{Z}$,
(ii) $a - b = mq \Rightarrow b - a = m(-q)$. Logo $a\mathsf{R}b \Longrightarrow b\mathsf{R}a,\ \forall a, b \in \mathbb{Z}$, e (iii) se existem inteiros p e q, tais que $a - b = mq$ e $b - c = mp$, então

$$a - c = (a - b) + (b - c) = mq + mp = m(q + p).$$

Logo $a\mathsf{R}b$ e $b\mathsf{R}c \Longrightarrow a\mathsf{R}c,\ \forall a, b, c \in \mathbb{Z}$.

Esta relação é chamada *congruência módulo m.*

Exemplo 4.28 A relação de paralelismo entre as retas de um espaço euclidiano (definida como tendo mesma direção) $x\mathsf{R}y \Leftrightarrow x//y$ é uma relação de equivalência, pois, se x, y e z são retas do espaço, temos:

(i) $x//x$,
(ii) $x//y \Rightarrow y//x$, e
(iii) $x//y$ e $y//z \Rightarrow x//z$.

Definição 4.29 Dada uma relação de equivalência R definida sobre A ($A \neq \emptyset$), dizemos que b *é equivalente a* c (pela R) se $(b, c) \in \mathsf{R}$.

Note que, se b é equivalente a c, então, pela simetria de R, temos $(c, b) \in \mathsf{R}$, ou seja, c é equivalente a b e podemos dizer então que b e c são equivalentes.

Definição 4.30 Dada uma relação de equivalência R sobre um conjunto A, chama-se *classe de equivalência determinada por* a, módulo R, o subconjunto $[a]_{\mathsf{R}}$ de A constituído pelos elementos x, tais que $(x, a) \in \mathsf{R}$. Em símbolos

$$[a]_{\mathsf{R}} = \{x \in A : (x, a) \in \mathsf{R}\}.$$

Quando não houver possibilidade de confusão, denotaremos $[a]_{\mathsf{R}}$ simplesmente por $[a]$.

Considere a relação de congruência módulo 4, por exemplo. Então temos as seguintes classes de equivalência:

$$\begin{aligned}
[0] &= \{\ldots, -4, 0, 4, 8, 12, \ldots\} \\
[1] &= \{\ldots, -3, 1, 5, 9, 13, \ldots\} \\
[2] &= \{\ldots, -2, 2, 6, 10, 14, \ldots\} \\
[3] &= \{\ldots, -1, 3, 7, 11, 15, \ldots\}
\end{aligned}$$

Observe que $[4] = [0]$, $[5] = [1]$, $[6] = [2]$, etc.

Lema 4.31 *Dada uma relação de equivalência* R *definida sobre um conjunto não vazio* A, *temos* $[a] = [b]$ *se, e somente se,* $(a, b) \in \mathsf{R}$.

Demonstração: De fato,
(i) Vamos supor $(a, b) \in \mathsf{R}$. Se $x \in [a]$, então, por definição, $(x, a) \in \mathsf{R}$. Como por hipótese, $(a, b) \in \mathsf{R}$ e R é transitiva $(x, b) \in \mathsf{R}$, ou seja, $x \in [b]$. Com isso mostramos que $[a] \subseteq [b]$. De forma análoga podemos mostrar que $[b] \subseteq [a]$, o que completa a prova de que "se $(a, b) \in \mathsf{R}$, então $[a] = [b]$".
(ii) Agora, se $[a] = [b]$, então $a \in [b]$, o que é o mesmo que $(a, b) \in \mathsf{R}$. □

Ainda temos:

Lema 4.32 *Seja* R *uma relação de equivalência definida sobre um conjunto não vazio* A*. Temos então que* $[a] \cap [b] \neq \emptyset \Longrightarrow [a] = [b]$*, ou equivalentemente* $[a] \neq [b] \Longrightarrow [a] \cap [b] = \emptyset$*.*

Demonstração: Como $[a] \cap [b] \neq \emptyset$, existe $x \in [a] \cap [b]$, ou seja, existe $x \in A$ tal que $(x, a) \in \mathsf{R}$ e $(x, b) \in \mathsf{R}$. Então pela simetria e transitividade, temos $(a, b) \in \mathsf{R}$, ou seja, $[a] = [b]$, pelo Lema 4.31. □

Podemos concluir dos Lemas 4.31 e 4.32, e pelo fato de R ser reflexiva que todo elementos de A está em uma, e apenas uma, classe de equivalência, ou seja, com as classes de equivalência definidas por R em A, obtemos uma subdivisão de A conforme a seguinte definição:

Definição 4.33 Uma *partição de um conjunto* A é uma coleção de subconjuntos de A tal que cada $a \in A$ está exatamente em um desses subconjuntos, e a intersecção de dois subconjuntos distintos da coleção é vazia.

Toda relação de equivalência definida sobre um conjunto A define uma partição de seu domínio. Mais ainda, podemos também estabelecer um resultado recíproco deste:

Teorema 4.34 *Seja* $\prod = \{A_i\}_{i \in I}$ *uma partição de um conjunto* A*. Então existe uma relação de equivalência definida sobre* A *que induz a partição* $\prod$*.*

Demonstração: Definindo $\mathsf{R} \subseteq A \times A$ por

$$(a, b) \in \mathsf{R} \Leftrightarrow a \text{ e } b \quad \text{pertencem a um mesmo elemento de} \prod.$$

temos:
(i) Como $\bigcup_{i \in I} A_i = A$, então para todo $x \in A$ existe $i \in I$ tal que $x \in A_i$. Portanto para todo $x \in A$, $(x, x) \in \mathsf{R}$;
(ii) Para todos $x, y \in A$ tais que $(x, y) \in \mathsf{R}$, existe $j \in I \mid x, y \in A_j$, ou seja, $y, x \in A_j$. Portanto $(y, x) \in \mathsf{R}$;

(*iii*) Para todos $x, y, z \in A$ tais que $(x, y) \in \mathsf{R}$ e $(y, z) \in \mathsf{R}$, existe $A_i \in \prod$, tal que $x, y \in A_i$, e existe $A_j \in \prod$, tal que $y, z \in A_j$. Assim, $y \in (A_j \cap A_i)$, de onde segue-se que $A_i \cap A_j \neq \emptyset$. Portanto, $A_i = A_j = A_i \cap A_j$, ou seja, $x, z \in A_i$ para um mesmo i. Então $(x, z) \in \mathsf{R}$.
Por (*i*), (*ii*) e (*iii*) segue que R é uma relação de equivalência. É claro que a partição induzida sobre A por R é $\prod$! □

Exemplo 4.35 Considere a relação R definida sobre $A = \{0, 1, 2, 3, 4, 5\}$ cuja matriz é:

$$M_{\mathsf{R}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

R induz sobre A a seguinte partição: $\prod = \{\{0\}, \{1, 2, 3\}, \{4, 5\}\}$.

Proposição 4.36 *Sejam m um inteiro maior que 1 e R a relação de congruência módulo m definida sobre $\mathbb{Z}$. Se $\mathbb{Z}_m$ é a partição definida por R sobre $\mathbb{Z}$ então $\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$.*

Demonstração: (*i*) Para cada a pertencente a $\mathbb{Z}$, efetuando a divisão euclidiana por m, obtemos:

$$a = qm + r,$$

onde q é o quociente e r é o resto. Portanto, $0 \leq r \leq m - 1$. Logo, $a - r = qm$, ou seja, $(a, r) \in \mathsf{R}$, ou ainda, $\bar{a} = \bar{r}$. (No caso da congruência módulo m é costume indicar $[a]$ por $\bar{a}$).
(*ii*) Supondo, agora, que existam duas classes iguais em $\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$, isto é, $\bar{r} = \bar{s}$. Segue que $r \equiv s \pmod{m}$, ou seja, $r - s = km$. Portanto, $m|(r - s)$ e, como $0 \leq r, s \leq m - 1$, concluímos que $r = s$. Logo, $\mathbb{Z}_m$ tem exatamente m elementos. □

Alguns comentários e observações

Os resultados dos Lemas 4.31 e 4.32 mostram que uma dada classe de equivalência pode ser descrita de diferentes modos; mais precisamente, $[x] = [y]$ para cada $y \in [x]$. Diremos que fizemos uma escolha do representante x ou y, conforme denotemos a classe por $[x]$ ou $[y]$. Assim, $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{-3}, \overline{-2}, \overline{-1}\} = \{\overline{6}, \overline{19}, \overline{-4}, \overline{-3}, \overline{10}, \overline{23}\}$.

Se R e S são relações de equivalência definidas sobre um mesmo conjunto A, já vimos que $\mathsf{R} \cap \mathsf{S}$ é também uma relação. A pergunta que fazemos agora é: nestas condições $\mathsf{R} \cap \mathsf{S}$, é uma relação de equivalência? Vejamos um exemplo:

Em $\mathbb{Z}$, consideremos as relações de congruência módulo 2 e 3, que chamaremos de R e S, respectivamente. Então $\mathsf{R} \cap \mathsf{S}$ é a congruência módulo 6 (Verifique!), que também é uma relação de equivalência. De fato, isto faz parte de um caso mais geral, cuja demonstração fica a cargo do leitor interessado.

Proposição 4.37 *Se* R *e* S *são relações de equivalência definidas sobre um conjunto* A*, então* $\mathsf{R} \cap \mathsf{S}$ *também é.*

Agora, como são as classes de equivalência determinadas por $\mathsf{R} \cap \mathsf{S}$ em A? Como $(x, y) \in (\mathsf{R} \cap \mathsf{S})$ se, e somente se, $(x, y) \in \mathsf{R}$ e $(x, y) \in \mathsf{S}$, as classes de equivalência determinadas por $\mathsf{R} \cap \mathsf{S}$ são exatamente resultados das intersecções de cada uma das classes determinadas por R com cada uma das classes determinada por S. Por exemplo, considere $A = \mathbb{Z}$, R a congruência módulo 2 e S a congruência módulo 3. Então,

$$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\} \quad \text{e} \quad \mathbb{Z}_3 = \{\hat{0}, \hat{1}, \hat{2}\},$$

onde

$$\begin{aligned}
\overline{0} &= \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} \\
\overline{1} &= \{\ldots, -7, -5, -3, -1, 1, 3, 5, 7, \ldots\} \\
\hat{0} &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\
\hat{1} &= \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\
\hat{2} &= \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, \ldots\}.
\end{aligned}$$

Temos, portanto, $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$, onde:

$$\begin{aligned}
[0] &= \hat{0} \cap \bar{0} = \{\ldots, -12, -6, 0, 6, 12, \ldots\} \\
[1] &= \hat{1} \cap \bar{1} = \{\ldots, -5, 1, 7, \ldots\} \\
[2] &= \hat{2} \cap \bar{0} = \{\ldots, -4, 2, 8, \ldots\} \\
[3] &= \hat{0} \cap \bar{1} = \{\ldots, -3, 3, 9, \ldots\} \\
[4] &= \hat{1} \cap \bar{0} = \{\ldots, -8, -2, 4, \ldots\} \\
[5] &= \hat{2} \cap \bar{1} = \{\ldots, -7, -1, 5, 11, \ldots\}.
\end{aligned}$$

Exercícios

(1) Descreva a partição de $\mathbb{Z}$ induzida pelas relações de congruência:

(a) módulo 5 (b) módulo 2

(c) módulo 10 (d) módulo 12

(2) Sobre o conjunto $\mathbb{Q}$ dos números racionais, defina $a\mathsf{R}b$ se, e somente se, $a - b \in \mathbb{Z}$. Mostre que R é uma relação de equivalência e descreva as classes de equivalência resultantes.

(3) Dado $\mathbb{Q}$ conjunto dos números racionais, definimos para cada $q \in \mathbb{Q}$ fixo:

$$A_q = \{q + n; n \in \mathbb{N}\}.$$

Mostre que $\prod = \{A_q : q \in \mathbb{Q},\ 0 \leq q < 1\}$ é uma partição de $\mathbb{Q}$ e mostre que a relação obtida coincide com aquela dada no exercício (2).

(4) Determine a partição definida pelas relações (de equivalência, é claro!) descritas pelas matrizes:

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

(5) Mostre que, se R é uma relação de equivalência definida sobre um conjunto A, então $\mathsf{R} \circ \mathsf{R} = \mathsf{R}$.

(6) Sejam $A = \{1,2,3\} \times \{1,2,3,4\}$, R e S relações definidas sobre A por: (a) $(x,y)\mathsf{R}(u,v) \Leftrightarrow x+y = u+v$ e
(b) $(x,y)\mathsf{S}(u,v) \Leftrightarrow |x-y| = |u-v|$.
Verifique que R e S são relações de equivalência e obtenha as partições de A induzidas por elas.

(7) Obtenha todas as partições possíveis do conjunto $\{a,b,c,d\}$.

(8) Descreva um algoritmo para obter o número de partições de um conjunto finito. Obtenha o número de partições de conjuntos contendo $3, 4$ e 5 elementos.

(9) Dada a partição $\prod = \{\{1,2\},\{3,4\},\{5\}\}$, obtenha a correspondente relação de equivalência.

(10) Quais das seguintes relações são relações de equivalência?

	Conjunto	Relação
(a)	Pessoas	é irmão de
(b)	Pessoas	tem o mesmo pai que
(c)	Pontos de um mapa	é unido por uma estrada
(d)	Retas do plano euclidiano	é perpendicular a
(e)	Inteiros positivos	para algum $k \in \mathbb{N}$ é igual a 10^k vezes

(11) A figura a seguir mostra duas relações definidas sobre o conjunto $\{a,b,c\}$. Essas relações são relações de equivalência?

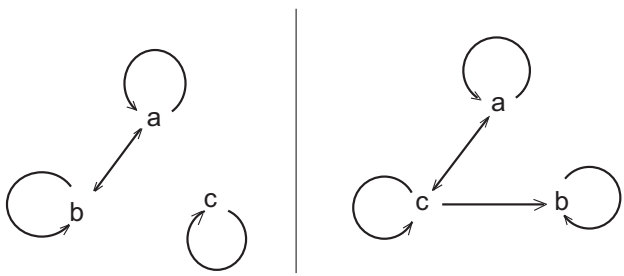


Figura 4.12:

(12) Dada uma representação gráfica de uma relação de equivalência, como podemos identificar as classes de equivalência?

(13) Definindo R sobre $\mathbb{N}$ por $x\mathsf{R}y \Leftrightarrow \frac{x}{y} = 2^m$ para algum inteiro m.
(a) Mostre que R é uma relação de equivalência.
(b) Quais são as classes de equivalência definidas pela relação R sobre $\mathbb{N}$.

(14) Uma relação R, definida sobre um conjunto não vazio A, é chamada circular se é verdadeira a sentença: $[\forall a, b, c \in A,\ a\mathsf{R}b$ e $b\mathsf{R}c \longrightarrow c\mathsf{R}a]$. Mostre que uma relação R será reflexiva e circular se, e somente se, for uma relação de equivalência.

(15) Sejam R e S relações de equivalência definidas sobre um conjunto A. Prove que $\mathsf{R} \subseteq \mathsf{S}$ se, e somente se, toda classe de equivalência definida por R está contida em alguma classe de equivalência definida por S.

(16) Dada uma relação de equivalência R definida sobre um conjunto não vazio A, se a partição determinada por R sobre A for uma família finita, chamamos de *posto de* R o número de distintas classes de equivalência de A determinada por R. Se R e S são relações de equivalência com postos r e s respectivamente, mostre que $\mathsf{R} \cap \mathsf{S}$ é uma relação de equivalência de posto no máximo rs. Mostre também que $\mathsf{R} \cup \mathsf{S}$ pode não ser, necessariamente, uma relação de equivalência.

(17) Sejam α e β relações de equivalência sobre um conjunto não vazio A. Mostre que a composta $\alpha \circ \beta$ é uma relação de equivalência se, e somente se, $\alpha \circ \beta = \beta \circ \alpha$. Dar exemplos de relações α e β, tais que $\alpha \circ \beta = \beta \circ \alpha$, e outros, tais que $\alpha \circ \beta \neq \beta \circ \alpha$.

(18) Seja R uma relação definida sobre os inteiros positivos por:

$$a\mathsf{R}b \Leftrightarrow a^2 \equiv b^2 \pmod 7.$$

Mostre que R é uma relação de equivalência. Qual é o posto de R?

4.3 Relações de Ordens - Conjuntos Ordenados

Outro tipo particularmente interessante de relações são as de ordem parcial que definiremos a seguir.

Definição 4.38 Uma relação binária R, definida sobre um conjunto não-vazio E, é chamada *relação de ordem parcial* (ou simplesmente *relação de ordem*) se for, simultaneamente, reflexiva, anti-simétrica e transitiva, isto é, se tivermos as seguintes implicações:
(i) $\forall x \in E \Longrightarrow (x,x) \in \mathsf{R}$,
(ii) $\big(\forall x, y \in E\big)\ \big((x,y) \in \mathsf{R}\ \text{ e }\ (y,x) \in \mathsf{R}\big) \Longrightarrow (x = y)$, e
(iii) $\big(\forall x, y, z \in E\big)\ \big((x,y) \in \mathsf{R}$ e $(y,z) \in \mathsf{R}\big) \Longrightarrow (x,z) \in \mathsf{R}$.

Notação 4.39 *:* Quando R for uma relação de ordem parcial sobre um conjunto não vazio E, para exprimirmos que $(a,b) \in \mathsf{R}$, usaremos a notação $a \preceq_{\mathsf{R}} b$, que se lê "*a precede b na relação* R", e a notação $x \prec_{\mathsf{R}} y$, que se lê: "*a precede estritamente b na relação* R" para indicar que $x \preceq_{\mathsf{R}} y$ e $x \neq y$. Quando a relação de ordem parcial R estiver clara no contexto, escreveremos simplesmente $a \preceq b$ ("*a precede b*") quando $(a,b) \in \mathsf{R}$, em vez da notação mais carregada $a \preceq_{\mathsf{R}} b$.

Definição 4.40 Se sobre um conjunto não vazio E estiver definida uma relação de ordem parcial $\preceq$, diremos que E é um *conjunto parcialmente ordenado* por $\preceq$ e indicaremos este fato por $(E, \preceq)$.

Exemplos 4.41 **(a)** A relação "menor ou igual: $\leq$", definida sobre o conjunto dos números naturais.
(b) Se $E = \{x_1, x_2, x_3, x_4\}$ e R é a relação descrita pela matriz

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

então R é uma relação de ordem parcial. (Verifique!)
(c) A relação de inclusão definida sobre uma família E de subconjuntos de um dado conjunto. De fato: todo conjunto está contido

em si mesmo; dados dois conjuntos, A e B, quaisquer, se $A \subseteq B$ e $B \subseteq A$, então $A = B$; e, além disso, para quaisquer conjuntos A, B, C, se $A \subseteq B$ e $B \subseteq C$, então, como já vimos, $A \subseteq C$).
(d) A relação de divisibilidade definida sobre o conjunto dos números naturais. Para a verificação das propriedades indicaremos a relação entre dois elementos por $x|y \iff (\exists q \in \mathbb{Z} : y = xq)$. Assim,
(i) $n|n$, $\forall n \in \mathbb{N}$ pois $n = n1$ (inclusive para $n = 0$),
(ii) Se $n|m$ e $m|n$, então existem $p, q \in \mathbb{Z}$ tais que $n = pm$ e $m = qn$. Substituindo, $m = (qp)m$. Logo, $p = q = \pm 1$, se $m \neq 0$. Como n e m são números naturais, $p = q = 1$, ou seja, $m = n$. Se $m = 0$, de $n = pm$ vem que $n = 0$. Logo $n = m$ também, e
(iii) Se $n|m$ e $m|k$, então existem $p, q \in \mathbb{Z}$, tais que $m = pn$ e $k = pm$. Substituindo, vem que $k = (pq)n$. Logo, $n|k$.

Pelos ítens (i), (ii) e (iii) a relação de divisibilidade sobre $\mathbb{N}$ é uma relação de ordem parcial.

Assim, por exemplo, se $S = \{a, b, c\}$, pela ordem de inclusão do item (c) podemos escrever: $\{a, b\} \not\preceq \{b, c\}$, pois $\{a, b\} \not\subseteq \{b, c\}$. Considerando a ordem parcial $\preceq$ do item (d), podemos escrever $5 \not\preceq 6$ e $6 \not\preceq 5$, pois 5 não divide 6 e 6 também não divide 5.

Em geral, num conjunto parcialmente ordenado, existem pares de elementos x, y incomparáveis, isto é, para os quais

$$x \not\preceq y \qquad \text{e} \qquad y \not\preceq x$$

são ambas verdadeiras. É o caso dos elementos 5 e 6 com a ordem de divisibilidade do exemplo 4.41 (d). No entanto, tal situação não ocorre no item (a) do Exemplo 4.41, porque $\mathbb{N}$ é *totalmente* (ou *linearmente*) *ordenado* pela relação "menor ou igual a", isto é, para cada par (x, y) de elementos, ou $x \leq y$, ou $y \leq x$. Isto explica o uso da palavra "parcial"ao nos referirmos a conjuntos ordenados em geral. Considerando os números 5 e 6, os ítens (a) e (d) do exemplo anterior também mostram que dois elementos a e b de um conjunto E podem ser *comparáveis* (isto é, $x \preceq y$ ou $y \preceq x$) segundo uma ordem e ser incomparáveis segundo outra ordem, ambas definidas sobre E.

Definição 4.42 Seja $(E, \preceq)$ um conjunto parcialmente ordenado. Dizemos que dois elementos a e b de E são comparáveis se $a \preceq b$ ou $b \preceq a$. Se dois elementos quaisquer de E forem comparáveis por $\preceq$, dizemos que $\preceq$ é uma *ordem total* de E e o conjunto E juntamente com $\preceq$ é chamado *conjunto totalmente ordenado* ou *cadeia*.

Observações
(i) Claramente, a relação inversa de uma relação de ordem é, também, uma relação de ordem. Denotemos a relação inversa de $\preceq$ por $\succeq$ (lê-se: "*sucede*"). Assim, $a \preceq b$ se, e somente se, $b \succeq a$. Por exemplo, sobre o conjunto dos números inteiros, a relação inversa da relação de ordem *menor ou igual* é *maior ou igual*, cuja notações são, respectivamente $\leq$ e $\geq$, como é de praxe. Assim, $a \leq b$ se, e somente se, $b \geq a$.
(ii) Se R é uma relação de ordem $(\preceq)$ definida sobre um conjunto E, e A é um subconjunto não vazio de E, então $\mathsf{R}_A = (A \times A) \cap \mathsf{R}$ também é uma relação de ordem parcial sobre A. (Prove!). Esta ordem é denotada por $\preceq_A$ e é dita *ordem restrita a* A, ou *ordem induzida sobre* A por $\preceq$. Mais ainda, se $(E, \preceq)$ é totalmente ordenado, o mesmo ocorre com $(A, \preceq_A)$, mas, mesmo quando $(E, \preceq)$ não é totalmente ordenado, podemos ter $A \subseteq E$, com $(A, \preceq_A)$ totalmente ordenado. Por exemplo, tome $\preceq$ a ordem parcial de divisibilidade sobre $\mathbb{N}$ e $A = \{1, 2, 4, 8\}$. Então $1 \preceq_A 2 \preceq_A 4 \preceq_A 8$.

Definição 4.43 Definimos uma relação de ordem sobre $\{0, 1\}$, por $0 \leq 0$, $0 \leq 1$, $1 \leq 1$. Se $M = (a_{ij})$, $N = (b_{ij})$ são matrizes de ordem $m \times n$ com a_{ij}, $b_{ij} \in \{0, 1\}$, diz-se que "M *precede* N e denota-se por $M \preceq N$, se $a_{ij} \leq b_{ij}$ para todos i, j.

Lema 4.44 *Sejam* $B = \{0, 1\}$ *e* $M_{m\times n}(B)$ *o conjunto de todas as matrizes retangulares* $m \times n$ *com entradas zero ou 1. Então* $\big(M_{m\times n}(B), \preceq\big)$ *é um conjunto parcialmente ordenado. Além disso, se* R, S *são relações contidas em* $E \times F$ *com* E *e* F *conjuntos finitos com* m *e* n *elementos, respectivamente, então* $\mathsf{R} \subseteq \mathsf{S}$ *se, e somente se,* $M_{\mathsf{R}} \preceq M_{\mathsf{S}}$.

Demonstração: Sejam $M_{\mathsf{R}} = (a_{ij})$ e $M_{\mathsf{S}} = (b_{ij})$. Temos $\mathsf{R} \subseteq \mathsf{S}$ se, e somente se, $[a_{ij} = 1 \Longrightarrow b_{ij} = 1]$. Assim $\mathsf{R} \subseteq \mathsf{S}$ se, e somente

se, $a_{ij} \leq b_{ij}$, ou $M_{\mathsf{R}} \preceq M_{\mathsf{S}}$. A demonstração de que $M_{m\times n}(B)$ é parcialmente ordenado também é imediata e fica como exercício. □

Note que, para qualquer relação R, tem-se que $M_{\emptyset} \preceq M_{\mathsf{R}} \preceq M_{E\times F}$.

Para finalizar, apresentamos a versão matricial de algumas propriedades de relações definidas sobre um conjunto finito. Estas propriedades são as mesmas propriedades enunciadas no Teorema 4.23.

Teorema 4.45 *Seja* R *uma relação definida sobre* $E = \{x_1, x_2, \ldots, x_n\}$, $n \geq 1$. *Então:*

(i) R *é reflexiva se, e somente se,* $I_n \preceq M_{\mathsf{R}}$, *onde* I_n *é a matriz identidade* $n \times n$;

(ii) R *é simétrica se, e somente se,* $M_{\mathsf{R}^{-1}} = M_{\mathsf{R}}$, *ou* $M_{\mathsf{R}}^t = M_{\mathsf{R}}$, *(onde* M^t *é a matriz transposta de* M*);*

(iii) R *é transitiva se, e somente se,* $M_{\mathsf{R}\circ\mathsf{R}} \preceq M_{\mathsf{R}}$;

(iv) R *é anti-simétrica se, e somente se,* $M_{\mathsf{R}} \wedge M_{\mathsf{R}}^t \preceq I_n$, *onde o produto de matrizes* $(a_{ij})_{m\times n} \wedge (b_{ij})_{m\times n}$ *é* $(a_{ij}.b_{ij})_{m\times n}$.

Demonstração: Seja $M_{\mathsf{R}} = (a_{ij})$.

(i) R é reflexiva se, e somente se, $\Delta = \{(a_i, a_i),\ a_i \in E\} \subseteq \mathsf{R}$. Logo, R é reflexiva se, e somente se, $a_{ii} = 1,\ i = 1, 2, \ldots, n$; se, e somente se, $I_n \preceq M_{\mathsf{R}}$.

(ii) R é simétrica se, e somente se, $(x_i, x_j) \in \mathsf{R}$ implica $(x_j, x_i) \in \mathsf{R}$. Então R é simétrica quando se tem a equivalência: $[a_{ij} = 1 \iff a_{ji} = 1]$. Em outras palavras: R é simétrica se, e somente se, M_{R} é simétrica.

(iii) Por definição, R é transitiva se $[(x_i, x_j),\ (x_j, x_k) \in \mathsf{R} \implies (x_i, x_k) \in \mathsf{R}]$. Em termos matriciais, R é transitiva quando $[(a_{ij} = a_{jk} = 1) \implies a_{ik} = 1]$. Isto é equivalente a: $[\sum_{j=1}^{n} a_{ij}a_{jk} = 1 \implies a_{ik} = 1]$. Como $(a_{ik}) = (a_{ij}).(a_{jk})$, segue-se que R é transitiva se, e somente se, $M_{\mathsf{R}}.M_{\mathsf{R}} \preceq M_{\mathsf{R}}$, ou $M_{\mathsf{R}\circ\mathsf{R}} \preceq M_{\mathsf{R}}$.

(iv) Por definição, R é anti-simétrica quando $(x_i, x_j) \in \mathsf{R},\ i \neq j$ implica $(a_j, a_i) \notin \mathsf{R}$. Em termos matriciais, R é anti-simétrica se $a_{ij} = 1,\ i \neq j$ implica $a_{ji} = 0$, ou seja, quando $a_{ij}.a_{ji} = 0$, se $i \neq j$.

Portanto, R é anti-simétrica se, e somente se, $(a_{ij}) \wedge (a_{ji}) \preceq I_n$, ou $M_{\mathsf{R}} \wedge M_{\mathsf{R}}^t \preceq I_n$. □

4.3.1 Diagrama de Hasse

Quando o conjunto sobre o qual está definida uma relação de ordem (total ou parcial) é finito, podemos representar a relação por meio de um diagrama de setas (ou segmentos) com as seguintes características:

- as propriedades reflexiva e transitiva não são indicadas (sendo admitidas a priori);

- se a, b são elementos, tais que $a\mathsf{R}b$, indica-se b numa posição relativamente acima da de a.

Tal diagrama é chamado *Diagrama de Hasse* de R.

Vejamos alguns exemplos:

Exemplos 4.46 (a) Seja R a relação dada por: $\mathsf{R} = \{(0,0), (1,1), (2,2), (3,3), (4,4), (0,1), (0,2), (1,2), (0,3), (0,4), (1,4), (3,2), (4,2)\}$. O diagrama de Hasse que a representa é:

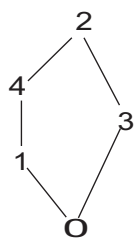


Figura 4.13:

(b) $\mathsf{R} = \{(a,a), (b,b), (c,c), (d,d), (e,e), (a,b), (a,c), (a,d), (a,e), (d,c), (e,c), (b,c)\}$

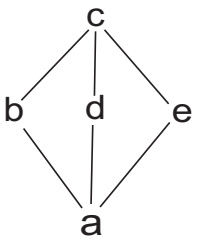


Figura 4.14:

(c) O diagrama de Hasse da relação de ordem | definida sobre o conjunto $\{3, 5, 7\}$ é dado por:

(d) Considerando o conjunto dos divisores positivos 18, $D^+(18)$, com relação à ordem de divisibilidade temos: $\mathsf{R} = \{(1,1), (1,2), (1,3), (1,6), (1,9), (1,18), (2,6), (2,18), (3,6), (3,9), (3,18), (6,18), (9,18), (2,2), (3,3), (6,6), (9,9), (18,18)\}$.

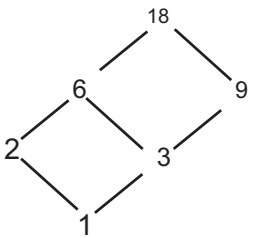
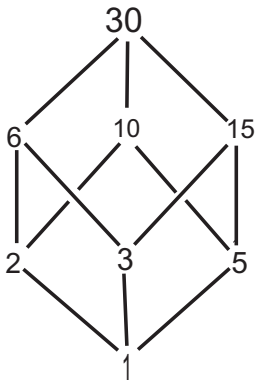


Figura 4.15:

(e) O diagrama de Hasse da relação de ordem | sobre o conjunto dos divisores positivos de 30, $D^+(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$ e o diagrama de Hasse da relação de inclusão definida sobre o conjunto das partes de $S = \{a, b, c\}$, $\wp(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ são idênticos. Veja os diagramas



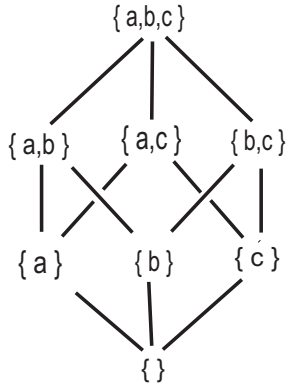


Figura 4.16:

4.3.2 Elementos Especiais de Conjuntos Parcialmente Ordenados

Nesta parte, consideraremos E um conjunto parcialmente ordenado por $\preceq$ e $A \subseteq E$, $A \neq \emptyset$.

Definição 4.47 Diremos que um elemento L de E é um *limite superior* de A se $[(\forall x \in E), (x \in A \rightarrow x \preceq L)]$ for uma sentença verdadeira.

Definição 4.48 Um elemento $l \in E$ é um *limite inferior* de A se $[(\forall x \in E),\ (x \in A \rightarrow l \preceq x)]$ for uma sentença verdadeira.

Exemplo Consideremos sobre o conjunto $\{1, 2, \ldots, 10\}$ a relação de ordem $\preceq$ com o diagrama de Hasse, a seguir. Se $A = \{5, 6, 7\}$, então

os limites superiores de A são: 9 e 10 e

os limites inferiores de A são: 1, 2, 3 e 5.

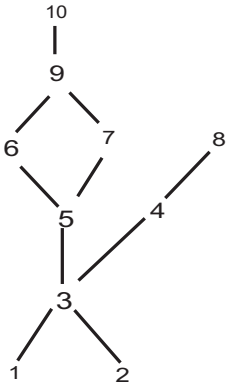


Figura 4.17:

Definição 4.49 Seja A um subconjunto não vazio de um conjunto parcialmente ordenado $(E, \preceq)$. Um elemento $M \in A$ é um *máximo* de A quando $[(\forall x \in E),\ (x \in A \Longrightarrow x \preceq M)]$, isto é, M é um limite superior e pertence ao conjunto A. Analogamente, diremos que $m \in A$ é um *mínimo* de A quando $[(\forall x \in E),\ (x \in A \Longrightarrow m \preceq x)]$. Denota-se $m = \min A$ e $M = \max A$.

Observe que, se um conjunto A possui dois elementos máximos M_1 e M_2, então, por definição, $M_1 \preceq M_2$ (M_2 sendo máximo e $M_1 \in A$) e $M_2 \preceq M_1$ ($M_2 \in A$ e M_1 é máximo). Portanto, $M_1 = M_2$. Analogamente para o mínimo. Com isto, acabamos de demonstrar a seguinte proposição:

Proposição 4.50 *Seja A um subconjunto não vazio de um conjunto parcialmente ordenado $(E, \preceq)$. Se A possui máximo (mínimo), então ele é único.* □

Observe, ainda, que um conjunto pode não ter máximo ou mínimo.

Exemplos 4.51 **(a)** $\mathbb{N}$ com a relação $|$ (divisibilidade) tem como mínimo 1 e máximo 0.
(b) $\mathbb{N}$ com a relação $\leq$ tem como mínimo 0 e não possui máximo.
(c) $\mathbb{N}$ com a relação $\geq$ tem como máximo 0 e não possui mínimo.

Outros elementos importantes nos conjuntos parcialmente ordenados são:

Definição 4.52 Dado um subconjunto não vazio A de um conjunto E parcialmente ordenado, chama-se *supremo* de A o mínimo (caso exista) do conjunto dos limites superiores de A, e *ínfimo* de A o máximo (caso exista) do conjunto dos limites inferiores de A. Indicaremos estes elementos por $\sup A$ e $\inf A$, respectivamente.

Note que o $\sup A$ é o limite superior "mais próximo" de A. Então, se existe $\max A$, tem-se que existe $\sup A$ e eles são iguais, desde que $\max A$ pertence à A. O mesmo vale com relação ao $\inf A$ e $\min A$.

Considerando a relação de ordem parcial dada pelo diagrama de Hasse a seguir, sobre o conjunto $E = \{a_1, a_2, \cdots, a_{10}\}$ e $A = \{a_5, a_6, a_7\}$, temos:

Os limites superiores de A são a_9 e a_{10}. Como $a_9 \preceq a_{10}$, então $a_9 = \sup A$. A não possui máximo.

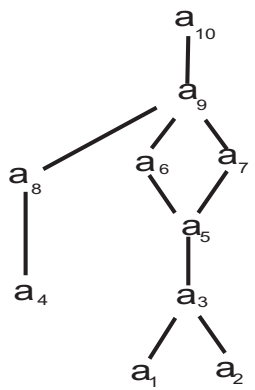


Figura 4.18:

Os limites inferiores de A são a_1, a_2, a_3, e a_5. Como $a_5 \in A$, então $\min A = a_5$. Além disso, $a_5 = \max\{a_1, a_2, a_3, a_5\}$. Portanto, $\inf A = a_5$.

Agora, considerando $B = \{a_5, a_6, a_8\}$, temos $\sup B = a_9$ e, como não existem limites inferiores, não existe $\inf B$.

Se $C = \{a_1, a_2, a_3\}$, então não existem limites inferiores e portanto não existe ínfimo. Os limites superiores de C são a_3, a_5, a_6, a_7, a_9 e a_{10}, sendo $a_3 = \min\{a_3, a_5, a_6, a_7, a_9, a_{10}\} = \sup C = \max C$.

Definição 4.53 Seja A um subconjunto não vazio de um conjunto E parcialmente ordenado. Um elemento $m_1 \in A$ é um *elemento minimal de* A quando ocorrer $[(\forall x \in A),\ (x \preceq m_1 \Rightarrow x = m_1)]$, isto é, quando o único elemento de A que precede m_1 é ele próprio. Analogamente, um elemento $m_0 \in A$ é *um elemento maximal de* A, quando $[(\forall x \in A), (m_0 \preceq x \Rightarrow x = m_0)]$, isto é, o único elemento de A que m_0 precede é ele mesmo; ou então, (usando a ordem inversa *sucede*) podemos dizer: "o único elemento de A que sucede m_0 é ele mesmo.

Exemplos 4.54 (1) Considere o conjunto E e os subconjuntos A=$\{a_5, a_6, a_7\}$ e $B = \{a_5, a_6, a_8\}$ do exemplo anterior. Então, a_5 é o único elemento minimal de A e a_6 e a_7 são elementos maximais de A.

Os elementos a_5 e a_8 são os elementos minimais de B, enquanto a_6 e a_8 são os elementos maximais de B.

Quando A é o próprio E então a_1, a_2, a_4 são os elementos minimais de E e a_{10} é o único elemento maximal de E.
(2) $(\mathbb{Z}, \leq)$ não possui elemento maximal nem minimal.

Observação
Observe que $(\mathbb{Z}, \leq) \subseteq (\mathbb{R}, \leq)$ não possui mínimo, nem máximo, nem limites superiores, ou inferiores, isto é, não possui elementos especiais. O mesmo ocorre com outros conjuntos infinitos. No entanto, este fato não ocorre com conjuntos finitos não vazios, como pode ser visto no que segue:

Proposição 4.55 *Seja E um conjunto parcialmente ordenado, finito e não vazio. Então E tem pelo menos um elemento maximal e um elemento minimal. Além disso, se E possui um único elemento maximal (minimal), este elemento é o máximo (mínimo) de E.*

Demonstração: De fato:
Seja p_1 um elemento qualquer de E. Se p_1 não é maximal, então existe $p_2 \in E : p_1 \prec p_2$. Agora, se p_2 não é maximal, então existe $p_3 \in E : p_2 \prec p_3$ e assim por diante. Como E é finito, a cadeia $p_1 \prec p_2 \prec p_3 \prec \cdots$ deve terminar em algum elemento p_k de E. Assim, não existe elemento $a \in E : p_k \prec a$, portanto p_k é maximal. Um argumento semelhante mostra que existe, pelo menos, um elemento minimal. Vejamos, agora, a demonstração da segunda parte da proposição

Seja m_0 o único elemento maximal de E. Se $a_1 \neq m_0$, então a_1 não é maximal. Logo existe $a_2 \in E : \ a_1 \prec a_2$. Se $a_2 \neq m_0$, então a_2 não é maximal. Logo existe $a_3 \in E$ tal que $a_2 \prec a_3$. Com este raciocínio construiremos uma cadeia de elementos de $E : a_1 \prec a_2 \prec a_3 \cdots$ Como E é finito, esta seqüência termina num elemento maximal. Como este elemento maximal deve ser m_0, então $\forall a_1 \in E$, $a_1 \preceq m_0$ e, portanto, m_0 é o máximo. De modo análogo se demonstra para o mínimo. □

Observe que a hipótese de E ser finito é muito importante, pois o conjunto $\mathbb{N}$ com a relação definida pelo diagrama:

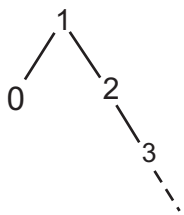


Figura 4.19:

possui um único elemento minimal: 0, que não é o mínimo de $\mathbb{N}$ com a ordem estabelecida.

Uma *cadeia* em um conjunto parcialmente ordenado é um subconjunto não vazio que é totalmente ordenado em relação à ordem induzida. O subconjunto $\{0, 2, 3\}$ não é uma cadeia em $\mathbb{N}$ com a ordem dada acima. Os subconjuntos $\{0, 1\}$ e $\{4, 2, 1\}$ são cadeias no exemplo acima. Para conjuntos parcialmente ordenados $(E, \preceq)$,

em geral temos o seguinte:

Lema 4.56 Lema de Zorn. *Seja* $(E, \preceq)$ *um conjunto parcialmente ordenado. Se toda cadeia em* E *admite limite superior em* E*, então* E *possui, pelo menos, um elemento maximal.* □

Definição 4.57 Uma relação de ordem parcial, definida sobre um conjunto E, é uma *boa ordem* se todo subconjunto não vazio de E possui mínimo. Neste caso, dizemos que E é *bem ordenado.*

Um exemplo de boa ordem é a ordem "menor ou igual" definida sobre o conjunto dos números naturais, embora $\leq$ não seja uma boa ordem sobre o conjunto dos números inteiros.

Observe também que todo conjunto E bem ordenado também é totalmente ordenado, pois, para quaisquer $x,\ y \in E$, tem-se que $\{x, y\}$ possui mínimo (que é x ou y). Logo, $x \preceq y$ ou $y \preceq x$. Vejamos alguns exemplos de elementos especiais de conjuntos.

Exemplos 4.58 Se $E = \mathbb{R}$ e $A = \{x \in \mathbb{R} : 0 < x \leq 1\}$, temos:
(a) $\forall x \in \mathbb{R},\ x \geq 1$ é um limite superior de A,
(b) $\forall x \in \mathbb{R},\ x \leq 0$ é um limite inferior de A,
(c) $\max A = 1$,
(d) não existe mínimo de A,
(e) $\sup A = 1$,
(f) $\inf A = 0$,
(g) 1 é o único elemento maximal de A,
(h) A não tem elementos minimais.

(2) Sejam $E = D^+(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\},\ A = \{2, 4, 6\}$ e R a relação "divide".
(a) os limites superiores de A são 12 e 36,
(b) os limites inferiores de A são 1 e 2,
(c) não existe $\max A$,
(d) mínimo de $A = 2$,
(e) $\sup A = 12$,
(f) $\inf A = 2$,
(g) 2 é o único elemento minimal de A,
(h) 4 e 6 são os elementos maximais de A.

Exercícios

(1) Desenhe todos os diagramas de Hasse possíveis para conjuntos com $1, 2, 3$ e 4 elementos. Em cada caso identifique o máximo e o mínimo (se existirem).

(2) (i) Verifique que a relação de divisibilidade sobre $\mathbb{N}$ não é ordem total e dê uma cadeia em $\mathbb{N}$.

(ii) Para $A = \{2, 3, 6\} \subseteq \mathbb{N}$, determine os limites superiores e inferiores; $\max A$ e $\min A$; $\sup A$ e $\inf A$; elementos maximais e minimais de A.

(3) Seja $B = \{0, 1\}$ com a ordem usual e sobre $B^2 = B \times B$:

(i) Defina $(a, b) \preceq_1 (c, d)$ se, e somente se, $a \leq c$ e $b \leq d$. Verifique que $\preceq_1$ é uma ordem não linear;

(ii) Defina $(a, b) \preceq_2 (c, d)$ se, e somente se, $a < c$ ou ($a = c$ e $b \leq d$). Verifique que $(B^2, \preceq_2)$ é totalmente ordenado;

(iii) Generalize (i) e (ii) para o conjunto $E \times E$, onde E é um conjunto ordenado qualquer.

(4) Considere a ordem usual sobre $B = \{0, 1\}$ e verifique que $[(a, b, c) \preceq (a_1, b_1, c_1) \iff a \leq a_1,\ b \leq b_1$ e $c \leq c_1]$ definida em $B = \{0, 1\}$ é uma relação de ordem parcial sobre B^3. Faça o diagrama de Hasse desta ordem e verifique que este diagrama é idêntico aos diagramas dado no exemplo 4.46(e).

(5) Sejam $(E, \preceq_1)$ e $(F, \preceq_2)$ conjuntos ordenados. Verifique que $E \times F$ pode ser ordenado por $[(a, b) \preceq (c, d) \iff a \preceq_1 c$ e $b \preceq_2 d]$.

(6) Seja $A = \{3, 5, 6\}$ contido em $D^+(30)$, ordenado pela divisibilidade. Determine os limites inferiores e superiores, elementos maximais e minimais de A. E determine $\sup A$, $\inf A$ e $\max A$, $\min A$.

(7) Em $\mathbb{N} \times \mathbb{N}$ defina $(a, b) \preceq (c, d)$ se, e somente se, $a|c$ e $b \leq d$.

(i) Mostre que esta relação binária é de ordem.

(ii) Ela é total? Por que?

(iii) Qual é a ordem inversa desta ordem?

(iv) Dado $A = \{(2, 1), (1, 2)\}$, ache os limites superiores e inferiores de A, $\sup A$, $\inf A$; $\max A$, $\min A$ e os elementos maximais e minimais de A.

(8) Mostre que $(\mathbb{R}, \leq)$ não possui máximo, nem elementos maximais.

(9) Dado um conjunto parcialmente ordenado $(E, \preceq)$ e $p_1 \preceq p_2 \preceq \cdots \preceq p_k \preceq p_1$, onde $p_i \in E$, prove que $p_1 = p_2 = \cdots = p_k$, isto é, nenhum conjunto parcialmente ordenado pode conter cadeias fechadas.

(10) Desenhe o diagrama de Hasse para $(D^+(72), |)$. Qual será a natureza dos diagramas de Hasse para os conjuntos dos divisores inteiros positivos de:
(a) $p_1^{k_1} p_2^{k_2}$ **(b)** $p_1^{k_1} p_2^{k_2} p_3^{k_3}$, onde p_1, p_2, p_3 são primos distintos?

(11) A intersecção de duas relações de ordem parcial definidas sobre um mesmo conjunto é uma relação de ordem? Justifique sua resposta. E a união?

(12) Em $\mathbb{N} \times \mathbb{N}$ defina $\{(a,b)\mathsf{R}(c,d) \Leftrightarrow [a < c \text{ ou } (a = c \text{ e } b \leq d)]\}$. Mostre que $(\mathbb{N} \times \mathbb{N}, \mathsf{R})$ é totalmente ordenado.

(13) Seja $\mathsf{R} \subseteq E \times E$. Mostre que R é relação de ordem se, e somente se, $\mathsf{R} \cap \mathsf{R}^{-1} = I_E$ e $\mathsf{R} \circ \mathsf{R} = \mathsf{R}$.

(14) Seja $(X, \preceq)$ um conjunto totalmente ordenado. Em X^n introduzimos a ordem lexicográfica:

$(x_1, \ldots, x_n) \preceq_1 (y_1, \ldots, y_n) \iff [(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$, ou para algum k, $1 \leq k \leq n$ tem-se: $x_i = y_i$, $(i < k)$ e $x_k \prec y_k]$.

Mostre que esta é uma relação de ordem parcial definida sobre X^n. Esta ordem é total?

(15) Verifique se as matrizes, a seguir, representam relações de ordem parcial

$$M_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad M_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(16) Liste todos os pares de elementos incomparáveis dos conjuntos parcialmente ordenados do Exercício anterior.

4.4 Funções ou Aplicações

O caso mais importante de relações binárias definidas de um conjunto não vazio A num conjunto não vazio B ocorre quando A é o domínio da relação, e cada elemento de A aparece apenas uma vez como abscissa de pares ordenados da relação. Numa representação sagital de uma tal relação, de cada elemento de A sai um e apenas um arco; na representação matricial, em cada linha aparece um e apenas um 1.

Este tipo de relação é chamado *transformação, aplicação* ou *função* e, devido a unicidade do 1^o elemento de cada par, as notações $f \subseteq A \times B$ e afb usadas para relações também são representadas por

$$f : A \longrightarrow B \quad \text{e} \quad \Big(f : a \longmapsto b \quad \text{ou} \quad b = f(a)\Big),$$

respectivamente. Nesta notação, b é chamado de "*valor de f em a*" ou "*a imagem de a dada pela f*". Mais precisamente temos:

Definição 4.59 Seja f uma relação de A em B. Dizemos que f é uma *aplicação* (*função* ou *transformação*) de A em B se:
(i) $D(f) = A$, isto é, para todo $a \in A$ existe $b \in B$, tal que $(a, b) \in f$.
(ii) Para todos $a \in A,\ b,\ c \in B$, $[\big((a, b) \in f \text{ e } (a, c) \in f\big) \Longrightarrow b = c]$.

É claro que o conjunto A é o *domínio* de f e o conjunto B *contradomínio*, além disso, como já vimos antes, o conjunto dos

elementos de B associados a elementos de A é chamado conjunto *imagem* de f e denotado por $f(A)$. Então $f(A) = \{b \in B \mid b = f(a) \text{ para algum } a \in A\}$.

Observações:
(a) O termo função, em geral, é usado quando A e B são subconjuntos de $\mathbb{R}$ e, neste caso, podemos fazer a representação cartesiana de f.
(b) Se $f : A \longrightarrow B$ e $g : A \longrightarrow B$, é claro que $f = g$ se, e somente se, $f(x) = g(x)$ para todo $x \in A$.
(c) Se A é um conjunto de n-uplas, digamos $(a_1, \ldots, a_n)$, a expressão $f((a_1, \ldots, a_n))$ é simplificada para $f(a_1, \ldots, a_n)$.
(d) A definição de função particulariza o conceito de relação binária em dois aspectos:

- um elemento qualquer do domínio A está relacionado com um único elemento do conjunto B;

- cada elemento de A está relacionado com algum elemento de B.

Quando esta última condição é relaxada e um subconjunto não vazio A' de A é o domínio de f, a relação resultante é uma função de A' em B, a qual é chamada *função parcial* de A em B.
(e) Para enfatizar que todo elemento no domínio de uma função tem exatamente uma imagem no contradomínio, dizemos que a função está bem definida.

Exemplos 4.60 (1) $A = \{a, b, c, d\}$, $B = \{0, 1, 2, 3\}$ e $f : A \longrightarrow B$ dada por $f = \{(a, 0), (b, 1), (c, 2), (d, 2)\}$.
(2) A relação $\mathsf{R} = \{(x, y) \in \mathbb{R}^2 : y = x^2\}$ é uma função, cujo domínio é $\mathbb{R}$ e o conjunto imagem é $\mathbb{R}_+$.
(3) Às vezes, a função é definida por meio de uma sentença, por exemplo $f \subseteq \mathbb{R} \times \mathbb{R}$ definida por $f(x) = x + 1$. Com esta definição, podemos denotar f por: $f = \{(x, x + 1),\ x \in \mathbb{R}\}$.
(4) Dados $A = \{a, b, c\}$, $B = \{0, 1\}$ e $f = \{(a, 1), (b, 0)\}$, então f não é função de A em B, pois $c \in A$ e $c \notin Dom(f)$.
(5) A relação $\mathsf{S} = \{(x, y) \in \mathbb{R}^2 : x^2 = y^2\}$ não é uma função, pois $(1, 1) \in \mathsf{S}$; $(1, -1) \in \mathsf{S}$ e $1 \neq -1$.

(6) A relação $\mathsf{T} = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ não é função pois $(0, 1)$ e $(0, -1) \in \mathsf{T}$ e $1 \neq -1$.
(7) Seja $f : \mathbb{Z} \longrightarrow \mathbb{N}$, tal que $f(i) = |2i| + 1$. f é uma função definida do conjunto dos números inteiros no conjunto dos números naturais. Sua imagem é o conjunto de todos os naturais ímpares.
(8) Seja $f : \mathcal{P}(U) \times \mathcal{P}(U) \longrightarrow \mathcal{P}(U)$ definida por $f(A, B) = A \cap B$. Esta relação é uma função do conjunto de todos os pares ordenados de subconjuntos de U nas partes de U. Neste caso o contra-domínio e a imagem de f são iguais. Como você justificaria esta última afirmação?
(9) Dados conjuntos não vazios A, B e $b \in B$ fixo, a função $f : A \longrightarrow B$, tal que $f(x) = b$ para todo x em A, é chamada *função constante*.
(10) Dado um conjunto não vazio A, a função de A em A definida por $f(x) = x$, isto é, $f = \{(x, x),\ x \in A\}$ é dita *função identidade* ou *função identidade sobre* A e é denotada por $I_A : A \longrightarrow A$, ou por $1_A : A \longrightarrow A$.

4.4.1 Imagem Direta e Imagem Inversa

Definição 4.61 Seja $f : A \longrightarrow B$. Dado $C \subseteq A$, chama-se *imagem direta* de C, segundo f, e indica-se por $f(C)$ o seguinte subconjunto de B:

$$f(C) := \{f(x) \mid x \in C\},$$

isto é, $f(C)$ é o conjunto das imagens dos elementos de C pela f.

Definição 4.62 Seja $f : A \longrightarrow B$. Dado $D \subseteq B$, chama-se *imagem inversa* de D, segundo f, e indica-se por $f^{-1}(D)$ o seguinte subconjunto de A:

$$f^{-1}(D) := \{x \in A \mid f(x) \in D\},$$

isto é, $f^{-1}(D)$ é o subconjunto de A formado pelos elementos cujas imagens estão em D.

Exemplos 4.63 (a) Sejam $A = \{1, 3, 5, 7, 9\}$, $B = \{n \in \mathbb{N} : 0 \leq n \leq 10\}$ e $f : A \longrightarrow B$ dada por $f(x) = x + 1$. Então

$$f(\{3, 5, 7\}) = \{f(3), f(5), f(7)\} = \{4, 6, 8\},$$
$$f(A) = \{f(1), f(3), f(5), f(7), f(9)\} = \{2, 4, 6, 8, 10\},$$
$$f(\emptyset) = \emptyset,$$
$$f^{-1}(\{2, 4, 9\}) = \{1, 3\},$$
$$f^{-1}(\{0, 1, 3, 5, 7, 9\}) = \emptyset.$$

(b) Sejam $A = B = \mathbb{R}$ e $f : \mathbb{R} \longrightarrow \mathbb{R}$, tal que $f(x) = x^2$. Então

$$f(\{1, 2, 3\}) = \{1, 4, 9\},$$
$$f([0, 2]) = [0, 4],$$
$$f(]-1, 3]) = \{x^2 \mid -1 < x \leq 3\} = [0, 9],$$
$$f^{-1}(\{0, 4, 9\}) = \{0, 2, -2, 3, -3\},$$
$$f^{-1}([1, 9]) = \{x \in \mathbb{R} \mid 1 \leq x^2 \leq 9\} = [-3, -1] \cup [1, 3].$$

(c) Sejam $A = B = \mathbb{R}$ e

$$f(x) = \begin{cases} 0, & \text{se} \quad x \in \mathbb{Q} \\ 1, & \text{se} \quad x \in \mathbb{R} \setminus \mathbb{Q}, \end{cases}$$

então $f(Q) = \{0\}$, $f(\mathbb{R} \setminus \mathbb{Q}) = \{1\}$, $f([0, 1]) = \{0, 1\}$, $f^{-1}(\{0\}) = \mathbb{Q}$ e $f^{-1}([4, 5]) = \emptyset$.

Observação: Se $|S| = m$ e $|T| = n$, podemos definir n^m funções diferentes de S em T. Observe que, para cada um dos m elementos $s \in S$, podemos escolher como imagem qualquer um dos n elementos de T como $f(s)$, independentemente da escolha efetuada para os outros elementos. Assim, temos n^m opções. Em linguagem técnica, para T e S conjuntos não vazios temos: $T^S := \{f : S \to T\}$, e então $|T^S| = |T|^{|S|}$.

4.4.2 Restrição e Prolongamento de Funções

Definição 4.64 Considere uma função $f : A \longrightarrow B$ e C um subconjunto não vazio de A. Uma função $g : C \to B$ é chamada *restrição de f a C* se para todo $x \in C$, $g(x) = f(x)$. Usualmente, denota-se a função g por $f_{|A}$. Assim, $f_{|A}(x) = f(x)$, $\forall x \in C$.

Definição 4.65 Considere novamente uma função $f : A \longrightarrow B$ e sejam $C \supseteq A$ e $D \supseteq B$. Uma função $h : C \longrightarrow D$ é dita *prolongamento de f ao conjunto D* se $h(x) = f(x),\ \forall x \in A$.

Exemplos 4.66 **(1)** Considere $f : \mathbb{Z} \to \mathbb{N}$, tal que $f(x) = |2x|+1$. A função $g : \mathbb{N} \longrightarrow \mathbb{N}$ dada por $g(n)=2n+1$ é a restrição de f a $\mathbb{N}$.

(2) Seja $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = |x|$, e $\mathbb{C}$ o conjunto dos números complexos.

A função $h : \mathbb{C} \to \mathbb{R}$ definida por $h(x + yi) = \sqrt{x^2 + y^2}$, para todo $x+yi \in \mathbb{C}$ é uma extensão de f. Note que $h_1 : \mathbb{C} \to \mathbb{R}$, definida por $h_1(x+yi) = |x| + |y|$, também estende a função f. Isto mostra que uma função pode ter várias extensões, mas qualquer função só admite uma única restrição a um subconjunto não vazio de seu domínio.

4.4.3 Funções Injetoras e Sobrejetoras

Quando algumas condições são impostas sobre as funções, obtemos classes interessantes. Vejamos algumas delas.

Definição 4.67 Dizemos que uma função $f : A \to B$ é *sobrejetora* se para todo $y \in B$ existe pelo menos um $x \in A$, tal que $f(x) = y$. Em outras palavras temos: para todo y em B, $f^{-1}(\{y\}) \neq \emptyset$ ou ainda $Im(f) = B$.

Exemplos 4.68 **(a)** Sejam $A = \{1, 2, 3\},\ B = \{a, b\}$ e $f : A \longrightarrow B$ dada por $f = \{(1, b), (2, a), (3, b)\}$. Como $Im(f) = B,\ f$ é sobrejetora.

(b) Sejam $A = \{1, 2, 3\}$ e $f : A \longrightarrow B$ dada por $f = \{(1, 0), (2, 0), (3, 0)\}$. Então f só será sobrejetora se B for o conjunto unitário $\{0\}$.

Observação: Uma função $f : A \to B$ não é sobrejetora se

$$\exists b \in B \mid f^{-1}(\{b\}) = \emptyset.$$

Definição 4.69 Dizemos que uma função $f : A \to B$ é *injetora* quando

$$(\forall x, y \in A), \big(x \neq y \Longrightarrow f(x) \neq f(y)\big),$$

isto é, quando elementos distintos em A possuem imagens distintas em B.

Observe que:

(i) Uma condição equivalente à condição de injetividade dada é: $\big(\forall\ x,\ y \in A\big),\ \big(f(x) = f(y) \Longrightarrow x = y\big)$

(ii) Uma função $f : A \to B$ não é injetora quando $\exists x, y \in A$, tais que $f(x) = f(y)$ e $x \neq y$.

Definição 4.70 Dizemos que uma função $f : A \longrightarrow B$ é *bijetora* se f é injetora e sobrejetora.

Exemplos 4.71 (1) $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = x + 3$ é bijetora.

De fato: $\forall x, y \in \mathbb{R}$ se $f(x) = f(y)$, então $x + 3 = y + 3$. Logo $x = y$ e então f é injetora. Além disso, para qualquer $z \in \mathbb{R}$, existe $x = z - 3$ em $\mathbb{R}$, tal que $f(x) = f(z - 3) = (z - 3) + 3 = z$.

(2) $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $f(x) = x^2$ não é sobrejetora nem injetora, pois $f(1) = f(-1)$ e $1 \neq -1$. Além disso, $Im(f) = \mathbb{N} \neq \mathbb{Z}$.

(3) $f : \mathbb{N} \longrightarrow \mathbb{N}$ definida por $f(x) = x^2$ é injetora, mas não é sobrejetora, uma vez que, por exemplo, $2 \notin Im(f)$.

(4) Seja $f : \mathbb{N} \longrightarrow \{0, 1\}$ definida por:

$$f(x) = \begin{cases} 0, & \text{se } n \text{ for par} \\ 1, & \text{se } n \text{ for ímpar} \end{cases}$$

Esta função é, claramente, sobrejetora, mas não é, obviamente, injetora.

(5) Para X e Y conjuntos não vazios, $p : X \times Y \longrightarrow X$, definida por $p(x, y) = x$, é sobrejetora, mas só será injetora se Y for um conjunto unitário.

Nota: As funções

$$\begin{array}{rccc} p_i: & A_1 \times \ldots \times A_i \times \ldots \times A_n & \longrightarrow & A_i \\ & (x_1, \ldots, x_i, \ldots, x_n) & \longmapsto & x_i \end{array}$$

para $i = 1, 2, \ldots, n$ são chamadas de i-ésima projeção e sempre são sobrejetoras. Deixamos a justificativa para esta última afirmação a cargo do leitor.

4.4.4 Função Inversa

Como uma função f é uma relação binária, podemos considerar a relação inversa f^{-1}. Pode ocorrer que, mesmo f sendo uma função, f^{-1} não seja uma função. Por exemplo, consideremos $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d, e\}$ e $f : A \to B$ definida por:

$$f = \{(1, a), (2, a), (3, b), (4, e)\},$$

então

$$f^{-1} = \{(a, 1), (a, 2), (b, 3), (e, 4)\}$$

não é uma função uma vez que $c \notin D(f^{-1})$ e $c \in B$.

Definição 4.72 Seja f uma função de A em B. Diremos que f é uma *função invertível* ou (*inversível*) se a relação inversa $f^{-1} \subseteq B \times A$ é uma função.

Vejamos quais são as condições para que dada $f : A \longrightarrow B$, f^{-1} seja, também, uma função.
(1) $D(f^{-1}) = Im(f) = B$, ou seja, f deve ser sobrejetora
(2) Cada elemento de B deve ser imagem de um único elemento de A pela função f, caso contrário, em f^{-1}, um mesmo elemento teria duas imagens distintas, o que não pode ocorrer. Resumindo, f deve ser injetora.

Note que essas condições acima são necessárias e suficientes, ou seja, temos:

Proposição 4.73 *Seja $f : A \longrightarrow B$ uma função. Uma condição necessária e suficiente para que f^{-1} seja uma função de B em A é que f seja bijetora.*

Demonstração: De fato:
($\Longleftarrow$) Vamos supor que f^{-1} é uma função de B em A e mostremos que f é bijetora.
(i) Se $y \in B$, como $f^{-1} : B \longrightarrow A$ é uma função, existe $x \in A$, tal que $f^{-1}(y) = x$ e, portanto, $f(x) = y$, ou seja, f é sobrejetora.
(ii) Sejam $x_1, x_2 \in A$, tais que $f(x_1) = y = f(x_2)$. Então, por definição, $(x_1, y) \in f$ e $(x_2, y) \in f$, ou seja, $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$, de onde se segue que $x_1 = x_2$, uma vez que f^{-1} é função. Portanto, f é injetora. De (i) e (ii) concluímos que f é bijetora.

($\Longrightarrow$) Vamos mostrar que, se f é bijetora, então f^{-1} é uma função.
(i) Dado y em B, como f é sobrejetora, existe x em A, tal que $y = f(x)$ e, portanto, $f^{-1}(y) = x$. Assim, temos $D(f^{-1}) = B$.
(ii) Se x_1, x_2 são tais que $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$, então $(x_1, y) \in f$ e $(x_2, y) \in f$, de onde se segue que $x_1 = x_2$, uma vez que f é uma função injetora. De (i) e (ii) podemos concluir que f^{-1} é uma função de B em A. □

Exemplos 4.74 (1) Sejam $A = \{a, b, c\}$, $B = \{1, 2, 3\}$ e f definida por $f = \{(a, 2), (b, 1), (c, 3)\} \subseteq A \times B$. Temos f bijetora e $f^{-1} = \{(2, a), (1, b), (3, c)\}$.

(2) $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $f(n) = n^2$ não admite inversa (como função) pois f não é bijetora.

(3) $f : \mathbb{N} \longrightarrow \mathbb{Z}$ definida por $f(n) = \begin{cases} \frac{n}{2}, & \text{se } n \text{ for par} \\ -\frac{n+1}{2}, & \text{se } n \text{ for ímpar} \end{cases}$ é uma função bijetora, logo f^{-1} é função.

De fato, para todo m, $n \in \mathbb{N}$, se $f(n) = f(m)$, então temos $n/2 = m/2$ ou $-(m+1)/2 = -(n+1)/2$ (pois a situação $n/2 = -(m+1)/2$ não ocorre, já que um é positivo e o outro é negativo). Assim, em qualquer caso, $m = n$ e f é injetora.

Vejamos agora que f também é sobrejetora: se $m \in \mathbb{Z}$ e $m \geq 0$, então $m = f(2m)$; e, se $m < 0$, tomando $n = -2m - 1 \in \mathbb{Z}$, tem-se $n \geq 0$ e $f(n) = f(-2m-1) = -\dfrac{-2m-1+1}{2} = \dfrac{2m}{2} = m$.

Assim, f é bijetora e sua inversa é $f^{-1} : \mathbb{Z} \longrightarrow \mathbb{N}$ definida por

$$f^{-1}(n) = \begin{cases} 2n & \text{se } n \geq 0, \\ -2n-1, & \text{se } n < 0. \end{cases}$$

Observação: Observe que o fato de $\mathbb{N} \subsetneq \mathbb{Z}$ não impediu a existência de uma bijeção entre os dois conjuntos. Compare este fato com o exercício (7) da última lista.

(4) A função $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = 2x + 3$ é bijetora e $f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$ é dada por $f^{-1}(x) = \dfrac{x-3}{2}$.

Observe que, se f é uma função bijetora, o mesmo ocorre com f^{-1}, além disso, a relação inversa de f^{-1} é f. Assim, podemos afirmar que f e f^{-1} são aplicações inversas entre si.

4.4.5 Composição de Funções

Definição 4.75 Dadas duas funções $f : A \to B$ e $g : B \longrightarrow C$, a *composta* de f e g, indicada por $g \circ f$, é a função $g \circ f : A \longrightarrow C$ definida por $(g \circ f)(x) = g(f(x))$, $\forall x \in A$.

Assim, se $b \in B$ é imagem de $a \in A$ pela f e $c \in C$ é imagem de b pela g, então c é imagem de a pela $g \circ f$.

Vejamos uma representação em diagrama de uma composição de funções.

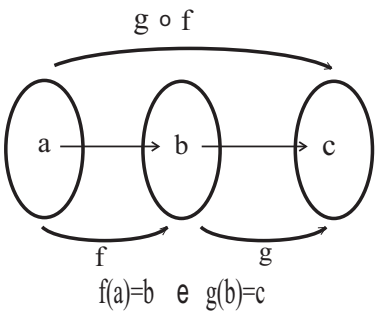


Figura 4.20:

Exemplos 4.76 (1) Considere U um conjunto finito qualquer e f e g as funções definidas por:

$$\begin{array}{rccc} f: & \mathcal{P}(U) & \longrightarrow & \mathbb{Z} \\ & A & \longmapsto & |A| \end{array} \quad \text{e} \quad \begin{array}{rccc} g: & \mathbb{Z} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \dfrac{x-5}{2}. \end{array}$$

Então a composta $g \circ f : \mathcal{P}(U) \longrightarrow \mathbb{R}$ é definida por $(g \circ f)(A) = \dfrac{|A|-5}{2}$.

De fato, $\big(g \circ f\big)(A) = g\big(f(A)\big) = g(|A|) = \dfrac{|A|-5}{2}$.

(2) Considere f e g representadas no diagrama a seguir

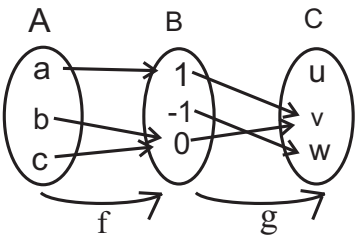


Figura 4.21:

Então $g \circ f = \{(a,v),(b,v),(c,v)\}$, pois

$$\begin{array}{l} \big(g \circ f\big)(a) = g\big(f(a)\big) = g(1) = v \\ \big(g \circ f\big)(b) = g\big(f(b)\big) = g(0) = v \\ (g \circ f)(c) = g\big(f(c)\big) = g(0) = v. \end{array}$$

(3) Sejam $f : \mathbb{R} \longrightarrow \mathbb{R}$ e $g : \mathbb{R} \longrightarrow \mathbb{R}$ definidas por $f(x) = x^2$ e $g(x) = 2x + 1$. Então, $g \circ f : \mathbb{R} \longrightarrow \mathbb{R}$ é definida por $\big(g \circ f\big)(x) = g\big(f(x)\big) = g(x^2) = 2x^2 + 1$.

(4) Sejam $A = \{a_1, a_2, a_3, a_4\}$, $B = \{b_1, b_2, b_3, b_4, b_5\}$ e $C = \{c_1, c_2, c_3\}$. Consideremos as funções $f : A \longrightarrow B$ e $g : B \longrightarrow C$ definidas por:

$$\begin{array}{c} f = \{(a_1,b_1),(a_2,b_2),(a_3,b_4),(a_4,b_3)\} \\ g = \{(b_1,c_1),(b_2,c_1),(b_3,c_2),(b_4,c_2),(b_5,c_3)\} \end{array}$$

A função composta de f e g, por definição, é $g \circ f : A \longrightarrow C$, tal que

$$\begin{aligned}(g \circ f)(a_1) &= g(f(a_1)) = g(b_1) = c_1\\ (g \circ f)(a_2) &= g(f(a_2)) = g(b_2) = c_1\\ (g \circ f)(a_3) &= g(f(a_3)) = g(b_4) = c_2\\ (g \circ f)(a_4) &= g(f(a_4) = g(b_3) = c_2,\end{aligned}$$

isto é,

$$g \circ f = \{(a_1, c_1), (a_2, c_1), (a_3, c_2), (a_4, c_2)\}.$$

(5) Sendo $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = 3x$ e $g : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $g(x) = x^2$, a função composta $g \circ f : \mathbb{R} \to \mathbb{R}$ é definida por

$$(g \circ f)(x) = g(f(x)) = g(3x) = (3x)^2 = 9x^2.$$

(6) Sejam

$$f: \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R}\\ x & \longmapsto & 2^x\end{array} \quad \text{e} \quad g: \begin{array}{ccc}\mathbb{R}_+ & \longrightarrow & \mathbb{R}\\ x & \longmapsto & \sqrt{x}+1.\end{array}$$

Então, $g \circ f: \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R}\\ x & \longmapsto & \sqrt{2^x}+1\end{array}$ é a função composta de f e g.

Observações 4.77 :
(i) Para f e g definidas no exemplo (5) anterior é possível obter também $f \circ g$. Esta é uma função de $\mathbb{R}$ em $\mathbb{R}$, tal que $\big(f \circ g\big)(x) = f\big(g(x)\big) = f(x^2) = 3x^2$,
(ii) A composta $f \circ g$ só pode ser definida quando o contradomínio da função f coincide com o domínio da função g.
(iii) A composta $g \circ f$ tem domínio e contradomínio iguais, respectivamente, ao domínio da f e contradomínio da g.
(iv) Se $f : E \longrightarrow F$ e $g : F \longrightarrow E$, então existem $g \circ f$ e $f \circ g$, porém, em geral, temos $g \circ f \neq f \circ g$.
(v) Se são dadas as funções $f : A \longrightarrow B$, $g : B \longrightarrow C$, $h : C \to D$, então, da definição de composição, temos as funções compostas $(h \circ g) \circ f : A \longrightarrow D$ e $h \circ (g \circ f) : A \longrightarrow D$. Além disso, $\forall a \in A$ tem-se: $[(h \circ g) \circ f](a) = \big(h \circ g\big)\big(f(a)\big) = h\Big(g\big(f(a)\big)\Big) =$

$h[(g\circ f)(a)] = [h\circ(g\circ f)](a)$. Assim, as funções compostas $h\circ(g\circ f)$ e $(h\circ g)\circ f$ são iguais. Portanto, podemos escrever, sem ambiguidade, $h\circ g\circ f$ para indicá-las. Mais geralmente, dadas as funções

$$f_1 : A_1 \longrightarrow A_2, \quad f_2 : A_2 \longrightarrow A_3\ , \quad \ldots\ , \quad f_r : A_r \longrightarrow A_{r+1}$$

a expressão $f_r \circ f_{r-1} \circ \cdots \circ f_1$ representa uma única função de A_1 em A_{r+1}. Além disso, quando $A_i = A_j$, para todo $i, j \in \{1, \ldots, r+1\}$ e $f_1 = \cdots = f_r = f$, a função composta $f_r \circ f_{r-1} \circ \cdots \circ f_1$ será indicada por f^r.

Por exemplo, se $f : \mathbb{Z} \to \mathbb{Z}$ é a função definida por $f(x) = 2x+1$. Então $f^2 : \mathbb{Z} \longrightarrow \mathbb{Z}$ é definida por

$f^2(x) = f\big(f(x)\big) = f(2x+1) = 2(2x+1)+1 = 4x+3$.

E $f^3 : \mathbb{Z} \longrightarrow \mathbb{Z}$ é definida por

$$f^3(x) = f^2\big(f(x)\big) = f^2(2x+1) = 4(2x+1)+3 = 8x+7.$$

(vi) Uma função $f : A \longrightarrow A$, tal que $f^2 = f$, é chamada *idempotente*. Um exemplo de função idempotente é $f : \mathbb{Z}_6 \to \mathbb{Z}_6$, onde $f(\overline{x}) = 4\overline{x}$. Ainda, quando f é idempotente, temos:

$$\begin{gathered} f^3 = f^2 \circ f = f \circ f = f \\ f^4 = f^3 \circ f = f \circ f = f \\ \vdots \\ f^k = f^{k-1} \circ f = f \circ f = f, \forall k \geq 1. \end{gathered}$$

No que segue, a função identidade de um conjunto A, denotada por 1_A, é, como já vimos, definida por $1_A : A \to A$, tal que $1_A(a) = a$. É claro que, para uma função qualquer $f : A \longrightarrow B$, temos:

Lema 4.78 *Seja $f : A \to B$ uma função. Então $f \circ 1_A = f = 1_B \circ f$, onde 1_A e 1_B indicam as funções identidades dos conjuntos A e B, respectivamente, como visto acima. Em particular, se $B = A$, temos $f \circ 1_A = f = 1_A \circ f$.* □

Proposição 4.79 *Se $f : A \longrightarrow B$ é uma função bijetora, então $f \circ f^{-1} = 1_B$ e $f^{-1} \circ f = 1_A$.*

Demonstração: De fato: já sabemos que, se f é bijetora, o mesmo ocorre com f^{-1}. Agora, para todo $x \in A$, temos

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x = 1_A(x),$$

portanto, $f^{-1} \circ f = 1_A$. Analogamente, para todo $x \in B$, tem-se

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = x = 1_B(x),$$

portanto, $f \circ f^{-1} = 1_B$. □

Lema 4.80 *Sejam $f : A \longrightarrow B$ e $g : B \longrightarrow A$, tais que $g \circ f = 1_A$. Então f é injetora e g é sobrejetora.*

Demonstração: De fato, sejam $x,\ x_1 \in A$, tais que $f(x) = f(x_1)$. Então, $g\big(f(x)\big) = g\big(f(x_1)\big)$; ou $1_A(x) = 1_A(x_1)$. Logo, $x = x_1$ e, então, f é injetora. Para demonstrar que g é sobrejetora tome um elemento x em A. Então $x = g\big(f(x)\big)$. Assim, para $y = f(x)$, tem-se que $g(y) = x$. Logo, g é sobrejetora. □

Proposição 4.81 *Sejam $f : A \longrightarrow B$ e $g : B \longrightarrow A$. Se $f \circ g = 1_B$ e $g \circ f = 1_A$, então f e g são bijetoras e $g = f^{-1}$.*

Demonstração: Que f e g são bijetoras, segue do Lema 4.80. Resta demonstrar que $g = f^{-1}$.

Por hipótese, $D(f^{-1}) = B = D(g)$ e $f \circ g = 1_B = f \circ f^{-1}$. Portanto, $f(g(x)) = f(f^{-1}(x)), \forall x \in F$ e, como f é injetora, $g(x) = f^{-1}(x), \forall x \in F$. Portanto, $g = f^{-1}$. □

Observações:
(i) O fato de que $f \circ g = 1_B$ nos garantiu pelo Lema 4.80 a injetividade de g e, de $g \circ f = 1_A$, a sobrejetividade de g, ou seja, as duas condições juntas garantem que g é invertível. Além disso, a parte final da demonstração garante a unicidade da inversa.
(ii) Apesar da condição $f \circ g = 1_B$ nos garantir a sobrejetividade de f e a injetividade de g, as funções g ou f podem não ser bijetora. Por exemplo, considere $f : \mathbb{N} \longrightarrow \mathbb{N}$, definida por $f(n) = n + 1$, e $g : \mathbb{N} \longrightarrow \mathbb{N}$, definida por $g(n) = n - 1$, se $n \geq 1$ e $g(0) = 0$. Então, $g \circ f = 1_{\mathbb{N}}$, mas nem f nem g são bijetoras, uma vez que $0 \notin Im(f)$ e $g(0) = g(1)$, com $0 \neq 1$.

4.4.6 Algumas Funções Importantes:

(A) Função fatorial

É a função $f : \mathbb{N} \longrightarrow \mathbb{Z}$ denotada por $f(n) = n!$ e definida recursivamente por $f(0) = 1$ e $f(n-1) := n.f(n-1),\ n \geq 1$.

Esta função não é injetora, desde que $f(0) = f(1) = 1$, e também não é sobrejetora, desde que, por exemplo, $3 \notin Im(f)$.

(B) Função escolha

Seja $A_i,\ i \in I \quad (I \neq \emptyset)$ uma família de conjuntos, com $A_i \neq \emptyset$. Uma função escolha definida sobre esta família é uma função $f : \{A_i,\ i \in I\} \longrightarrow D$ com $D \supseteq A_i,\ \forall i$, tal que $f(A_i) \in A_i$.

Exemplo: Sejam $A_1 = \{0\},\ A_2 = \{a, b, c\},\ A_3 = \{x, y\}$ e $D = A_1 \cup A_2 \cup A_3$. Então, $f : \{A_1,\ A_2,\ A_3\} \longrightarrow D$, tal que $f(A_1) = 0,\ f(A_2) = a,\ f(A_3) = y,$ é uma função escolha. Essa função se identifica com a "*escolha*"ou terna ordenada $(0, a, y) \in A_1 \times A_2 \times A_3$. De maneira mais geral, o conjunto de todas as funções escolha definidas sobre a família $\{A_i,\ i \in I\}$ pode ser identificado com o produto cartesiano $\prod_{i \in I} A_i$.

(C) Função característica

Seja A um subconjunto de um conjunto universo U. A *função característica de* A é a função $c_A : U \longrightarrow \{0, 1\}$ definida por

$$c_A(x) = \begin{cases} 1, & \text{se } x \in A \\ 0, & \text{se } x \notin A. \end{cases}$$

Esta função tem as seguintes propriedades que são facilmente verificadas:

Propriedades:

(i) Dois subconjuntos A_1 e A_2 de U são iguais se, e somente se, $c_{A_1} = c_{A_2}$,

(ii) $c_{\overline{A}} = 1 - c_A$,

(iii) $c_{A \cup B} = c_A + c_B - c_A.c_B$,

(iv) $c_{A \cap B} = c_A.c_B$ e

(v) Toda função $f : U \longrightarrow \{0,1\}$ é a função característica de algum subconjunto de U. De fato, sendo $S = \{x \in U : f(x) = 1\}$, tem-se que $f = c_S$.

Usando essas identidades, outras identidades mais complexas podem ser obtidas. Por exemplo, desde que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, segue-se de (i) que $c_{A\cap(B\cup C)} = c_{(A\cap B)\cup(A\cap C)}$.

Exemplos: **(1)** Seja $A = \{a, b, c, d, e, f\}$ e $S = \{b, d\}$. Então

$$c_S = \{(a,0), (b,1), (c,0), (d,1), (e,0), (f,0)\}.$$

(2) A função $f : \mathbb{N} \longrightarrow \{0,1\}$ definida por

$$f(n) = \begin{cases} 0, & \text{se } n \text{ é par} \\ 1, & \text{se } n \text{ é ímpar} \end{cases}$$

é a função característica dos números ímpares, conforme propriedade (v).

No que segue, veremos uma outra forma de demonstrar que, se A é finito, com n elementos, então $|\wp(A)| = 2^n$.

Lema 4.82 *Sejam $\{0,1\}^U$ o conjunto de todas as funções de U em $\{0,1\}$ e $\psi : \{0,1\}^U \longrightarrow \wp(U)$ definida por $\psi(f) = A$, onde $A = \{x \in U \mid f(x) = 1\}$. Então ψ é uma função bijetora.*

Demonstração: Sejam f, $g \in \{0,1\}^U$, tais que $\psi(f) = \psi(g) = A$. Então, $f(x) = 1$ e $g(x) = 1$ se, e somente se, $x \in A$. Pela propriedade (v) temos que $f = g$ e, portanto, ψ é injetora. Para cada $S \in U$, considere c_S a função característica de S. Então, $\psi(c_S) = S$ e, portanto, ψ é sobrejetora. □

Segue-se que os conjuntos $\{0,1\}^U$ e $\wp(U)$ têm o mesmo número de elementos. Em particular, se U é finito

$$|\{0,1\}^U| = |\wp(U)|.$$

Sabendo que

$$|\{0,1\}^U| = |\{0,1\}|^{|U|} = 2^{|U|}.$$

Concluímos que $|\wp(U)| = 2^{|U|}$, o que havíamos visto anteriormente.

Dada uma função $f : A \longrightarrow B$, a relação R_f definida sobre A por $a\mathsf{R}b \Longleftrightarrow f(a) = f(b)$ é claramente uma relação de equivalência e, portanto, induz uma partição Π_{R}, sobre A, onde cada classe de equivalência consiste de todos os elementos de A que têm por imagem um dado elemento do contra-domínio da f. Assim, existe uma bijeção entre Π_{R_f} e $Im(f)$ (Prove).

Devido a este fato, a função característica pode ser usada para dar uma representação conveniente para as funções, cujo conjunto imagem $Im(f)$, é finito. Vejamos: Considere $f : A \longrightarrow B$ onde $B = \{b_1, b_2, \ldots, b_k\}$ e $\Pi_{\mathsf{R}_f} = \{A_1, A_2, \ldots, A_k\}$, a partição definida por f sobre A. Portanto,

$$A_i = \{a \in A \mid f(a) = b_i\}.$$

Como para cada $a \in A$ exatamente um dos k valores

$$c_{A_1}(a),\ c_{A_2}(a), \ldots, c_{A_k}(a)$$

é 1 (digamos $c_{A_i}(a)$), enquanto todos os demais são 0, podemos representar $f : A \longrightarrow B$ por

$$f(a) = \sum_{i=1}^{k} b_i c_{A_i}(a).$$

Exemplo 4.83 Considere a função $f : \mathbb{Z} \longrightarrow \mathbb{Z}_m$, onde $f(j) = j(mod\, m)$. Então, $A_i = \{j \in \mathbb{Z} \mid j \equiv i(mod\, m)\}$ $(i = 0, 1, \ldots, m-1)$. Então podemos escrever

$$f(j) = \sum_{i=0}^{m-1} i c_{A_i}(j).$$

Por exemplo, quando $m = 3$,

$$f(j) = \sum_{i=0}^{2} i c_{A_i}(j) = 0.c_{A_0}(j) + 1.c_{A_1}(j) + 2.c_{A_2}(j) =$$

$$= c_{A_1}(j) + 2.c_{A_2}(j).$$

(D) Função escada

As *funções assoalho* e *teto* (Floor and Ceiling functions) são duas funções importantes em matemática discreta. Observando que todo número real x é da forma $x = m + f$, onde m é um inteiro e f é um número real com $0 \leq f < 1$, definimos

Definição 4.84 A *função assoalho*, também dita *função maior inteiro*, é a função que, quando aplicada à $x = m + f$, dá como resultado m : o maior inteiro contido em x, (ou o maior inteiro menor ou igual a x). A *função teto*, quando aplicada à $x = m + f$, toma o menor inteiro maior ou igual a x, ou seja, arredonda x para cima.

Notações: $\lfloor x \rfloor$ ou $[x]$ para a função assoalho, e $\lceil x \rceil$ para a função teto.

Assim, se $x = m + f$, $m \in \mathbb{Z}$ e $0 \leq f < 1$, então $\lfloor x \rfloor = m$ e $\lceil x \rceil = \begin{cases} m, & \text{se } f = 0 \\ m+1, & \text{se } 0 < f < 1. \end{cases}$

Por exemplo, $\lfloor 1/2 \rfloor = 0$ e $\lceil 1/2 \rceil = 1$; $\lfloor -\frac{1}{2} \rfloor = -1$ e $\lceil -\frac{1}{2} \rceil = 0$; $\lfloor 3,2 \rfloor = 3$ e $\lceil 3,2 \rceil = 4$; $\lfloor 7 \rfloor = 7$ e $\lceil 7 \rceil = 7$. Veja os gráficos destas funções.

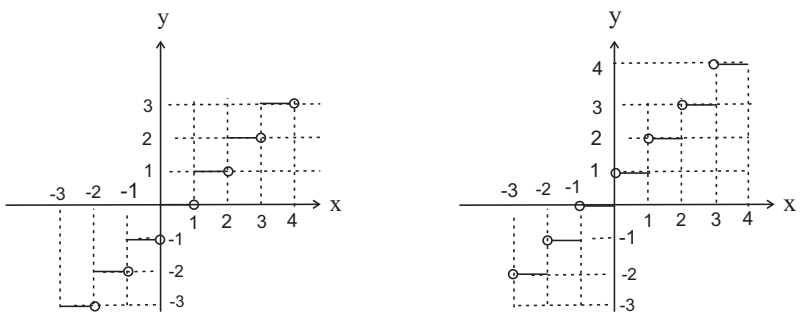


Figura 4.22: Funções $\lfloor x \rfloor$ e $\lceil x \rceil$

Exemplos (a) Em uma caderneta de poupança, em que são depositados juros mensais sobre o montante atualizado, quantos depósitos de juros foram feitos pelo banco se o poupador retirou toda a aplicação em 88 dias?

Solução - Como o depósito em juros é feito com mês vencido, o número de depósitos em juros feito pelo banco é $\lfloor \frac{88}{30} \rfloor = 2$.

(b) Uma pessoa física ficou em atraso com o imposto de renda por 88 dias. Sendo que os juros sobre a dívida também são cobrados mensalmente, quantos meses de juros a pessoa física pagará?

Solução: - Neste caso, a cobrança pela receita federal é feita usando a função teto. Portanto, o resultado é $\lceil \frac{88}{30} \rceil = 3$.

(c) Os dados armazenados em um disco rígido ou transmitidos por rede usualmente são representados como uma seqüência de bytes. Cada byte é composto de 8 bits. Quantos bytes são necessários para codificar 100 bits de dados?

Solução: - É claro que é o menor inteiro que é maior ou igual a $\frac{100}{8}$, ou seja, são necessários $\lceil \frac{100}{8} \rceil = 13$ bytes.

(E) Permutações:

Definição 4.85 Seja A um conjunto finito $A = \{a_1, \ldots, a_n\}$. Uma função bijetora de A em si mesma é chamada uma *permutação* sobre A. O número $|A| = n$ é chamado ordem de permutação.

Representamos uma permutação $p : A \longrightarrow A$ de ordem n da seguinte forma:

$$p = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ p(a_1) & p(a_2) & \ldots & p(a_n) \end{pmatrix}.$$

Observe que:
(i) O número total de permutações de ordem n distintas que podemos obter é $n!$
(ii) Dada uma permutação sobre A

$$p = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ p(a_1) & p(a_2) & \ldots & p(a_n) \end{pmatrix},$$

a inversa de p é a permutação

$$p^{-1} = \begin{pmatrix} p(a_1) & p(a_2) & \ldots & p(a_n) \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}.$$

Exemplo 4.86 Seja $A = \{a, b, c\}$. Como $|A| = 3$ e $3! = 6$, existem 6 permutações distintas definidas sobre A. São elas:

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix},$$

$$\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix},$$

onde a primeira delas é a permutação idêntica. A inversa de $\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$, por exemplo, é $\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$.

Seja p uma permutação definida sobre $A = \{a_1, \ldots, a_n\}$. Para cada $a_i \in A$, consideremos a seguinte seqüência de elementos:

$$a_i, p(a_i), p^2(a_i), p^3(a_i), \ldots.$$

Como A é finito, a seqüência infinita deve conter repetições, isto é, existem l e $k \in \mathbb{N}$ tais que $p^k(a_i) = p^l(a_i)$. Assim, se l e k são os menores inteiros, tais que $0 \leq l < k \leq n$ e $p^k(a_i) = p^l(a_i)$ (p^0 denota a identidade), escrevendo p^{-l} como sendo $(p^{-1})^l$ temos

$$p^{-l}(p^k(a_i) = p^{-l}(p^l(a_i)),$$

que implica em $p^{k-l}(a_i) = a_i$. Fazendo $k - l = r$, temos $p^r(a_i) = a_i$. Portanto, a seqüência inicial $a_i, p(a_i), p^2(a_i), p^3(a_i), \ldots$ pode ser reescrita de forma periódica

$$a_i, p(a_i), p^2(a_i), p^3(a_i), \ldots, p^{r-1}(a_i), a_i, p(a_i), p^2(a_i), p^3(a_i), \ldots$$

Os r primeiros elementos desta seqüência são dois a dois distintos e são freqüentemente indicados na forma da r-upla

$$\begin{pmatrix} a_i & p(a_i) & p^2(a_i) & \cdots & p^{r-1}(a_i) \end{pmatrix}, \tag{4.1}$$

que é denominada *r-ciclo* ou *ciclo de ordem r*.

Podemos observar que a permutação p quando aplicada r vezes "leva a_i em si mesmo", o mesmo ocorrendo para qualquer outro

elemento que aparece no mesmo ciclo que a_i. Quando $r < n$, pelo menos um elemento $a_j \in A$ não foi incluído no r-ciclo 4.1. Podemos agora repetir o processo e determinar o ciclo que contém a_j, digamos

$$\left(a_j \quad p(a_j) \quad \cdots \quad p^{t-1}(a_j)\right). \tag{4.2}$$

Notemos que os ciclos 4.1 e 4.2 não possuem elementos comuns, pois de $p^s(a_i) = p^m(a_j)$ para algum s e $m \in \mathbb{N}$, então

$$p^{t-m}(p^s(a_i)) = p^{t-m}(p^m(a_j)),$$

ou seja,

$$p^{t+s-m}(a_i) = p^t(a_j) = a_j,$$

mas $p^{t+s-m}(a_i)$ está no ciclo 4.1 enquanto a_j não. Dois ciclos com esta propriedade são chamados ciclos disjuntos.

Pode-se repetir o processo anterior, tantas vezes quantas se fizerem necessárias, e partir o conjunto A em subconjuntos, cada um dos quais constituídos pelos elementos de diferentes ciclos. Essa partição é freqüentemente chamada produto de ciclos disjuntos e expressa da forma

$$\big(a_i\ p(a_i)\ \cdots\ p^{r-1}(a_i)\big)\big(a_j\ p(a_j)\ \cdots\ p^{t-1}(a_j)\big)\cdots \\ \cdots\big(a_m\ p(a_m)\ \cdots\ p^{l-1}(a_m)\big),$$

onde a ordem em que os ciclos são escritos são arbitrárias e os ciclos de ordem 1 são omitidos. Esta forma especifica perfeitamente a permutação p.

Exemplo 4.87 Considere a permutação

$$\begin{pmatrix} a & b & c & d & e & f & g & h \\ h & g & b & f & e & d & a & c \end{pmatrix}.$$

O ciclo contendo o elemento a, isto é, $(a\ p(a)\ p^2(a)\ \ldots)$ é $(a\ h\ c\ b\ g)$.

Qualquer elemento deste ciclo é aplicado nele mesmo por p^5. O ciclo contendo d é dado por $(d\ f)$ e, finalmente, o ciclo contendo e é (e). Então, p pode ser escrita da seguinte forma: $(a\ h\ c\ b\ g)(d\ f)(e)$ onde (e) pode ser omitida.

(F) Princípio da Casa do Pombo

Este princípio e sua generalização, que veremos a seguir, tem muitas aplicações interessantes e surpreendentes. Ele afirma o seguinte:

"*Se $k+1$ objetos são colocados em k caixas, pelo menos uma caixa conterá mais de um objeto*"

Vejamos algumas aplicações:

Exemplos (1) Em um grupo de 367 pessoas, pelo menos duas fazem aniversário em um mesmo dia do ano.

(2) Para qualquer $n > 1$ existe um número formado apenas dos dígitos 0 e 1 que é divisível por n.

Solução: tome os $n+1$ números 1, 11, 111, ..., $111\cdots1$($n+1$ vezes). Como temos $n+1$ números, então dividindo estes números por n, pelo menos dois deles têm o mesmo resto. Logo, a diferença deles é um número constituído de "zeros"e "uns"e é divisível por n.

Agora veremos o

Teorema 4.88 (Princípio da Casa do Pombo Generalizado). *Se n objetos são colocados em k caixas, pelo menos uma caixa conterá pelo menos $\lceil \frac{n}{k} \rceil$ objetos.*

Demonstração: (Por contradição). Suponhamos que nenhuma caixa conterá mais que $\lceil \frac{n}{k} \rceil - 1$ objetos. Como todos os objetos estão contidos nas k caixas, temos: $n \leq k\big(\lceil \frac{n}{k} \rceil - 1\big) < k\big((\frac{n}{k}+1)-1\big) = n$, absurdo. □

Exemplos (i) Em um grupo de 100 pessoas, pelo menos $\lceil \frac{100}{12} \rceil = 9$ nasceram no mesmo mês.

(ii) Qual é o número mínimo necessário de jogadores para se ter certeza que existe pelo menos um time de futebol (11 jogadores), sendo que estes jogadores podem escolher aleatoriamente as equipes A, B ou C?

Solução: Equipe com 10 jogadores ainda não é um time. Tendo 3 equipes, 3.(10)=30 jogadores pode não ser suficiente. Logo, é $\lceil \frac{n}{3} \rceil > 10$, ou seja, $n = 3(10) + 1 = 31$.

(iii) Assuma que todos os telefones fixos do estado de São Paulo sejam do tipo $0-1B-YZ-X_1X_2X_3X_4X_5X_6X_7$, onde $1B$ é o código de área e B é um dos dígitos de 1 à 9. O número YZ é o código da operadora para interurbanos e $X_1X_2X_3X_4X_5X_6X_7$ é o número do telefone individual fixo. Cada X_i é um dos dígitos de 0 à 9 e X_1 é diferente de zero. Pede-se:

Qual é o número mínimo de códigos de área necessário para garantir que 25 milhões de telefones fixos no estado de São Paulo tenham os números de telefones distintos?

Solução: Como YZ é o código da operadora ele não influi nos cálculos e no resultado final. O número do telefone fixo é $X_1X_2X_3X_4X_5X_6X_7$ com X_1 um dos dígitos de 1 à 9. Logo, há 9 possibilidades para X_1. Para $X_i,\ i=2,\ldots,7$ há 10 possibilidades. Pelo princípio da contagem, podemos ter $9.10.10\cdots10 = 9.10^6 = 9.000.000$ de telefones fixos distintos. Como se quer 25 milhões de telefones fixos, pelo menos $\left\lceil \frac{25.000.000}{9.000.000} \right\rceil = \left\lceil \frac{25}{9} \right\rceil = 3$ deles terá o mesmo número. Portanto, vamos precisar de pelo menos 3 códigos de área para que todos os telefones fixos do estado de São Paulo sejam diferentes.

(iv) Mostre que dentre quaisquer $n+1$ inteiros positivos, não excedendo $2n$, existe um inteiro que divide um dos outros.

Solução: Sejam $a_1, a_2, \ldots, a_{n+1}$ inteiros quaisquer entre 1 e $2n$. Pelo Teorema Fundamental da Aritmética 2.17, podemos escrever $a_i = 2^{\alpha_i}.q_i$, com q_i : ímpar. Como $1 \leq q_i \leq 2n$, temos $n+1$ números ímpares no intervalo $[1, 2n]$. Logo, dois deles são iguais: digamos $q_i = q_j = q$. Assim, $a_i = 2^{\alpha_i}q$ e $a_j = 2^{\alpha_j}q$. Portanto, a_i divide a_j (se $\alpha_i \leq \alpha_j$, ou a_j divide a_i (se $\alpha_j \leq \alpha_i$).

(v) Mostre que em qualquer $n+1$ escolha distinta feita no conjunto de $2n$ elementos $B = \{1, 2, \ldots, 2n\},\ (n \geq 1)$ existem 2 elementos escolhidos, cuja soma é $2n+1$.

Solução: Considere os seguintes n pares $(1, 2n),\ (2, 2n-1), \ldots,$ $(n, n+1)$, cuja soma é $2n+1$. Como vamos fazer $n+1$ escolha de elementos distintos em B e temos n pares, pelo princípio da casa do pombo vamos acabar escolhendo um destes pares.

Exercícios

(1) Quais das seguintes relações constituem uma função:
(a) $\{(x,y) \in \mathbb{N} \times \mathbb{N} : x + y < 10\}$
(b) $\{(x,y) \in \mathbb{R} \times \mathbb{R} : x = y\}$
(c) $\{(x,y) \in \mathbb{R} \times \mathbb{R} : y^2 = x\}$
(d) $\{(x,y) \in \mathbb{N} \times \mathbb{N} : y$ é o número de primos menores que $x\}$.
(2) Considere a função $f : A \longrightarrow B$, onde $A = \{-1,0,1\} \times \{-1,0,1\}$, $B = \{-1,0,1\}$ e

$$f(x,y) = \begin{cases} 0 & \text{se } xy > 0 \\ x.y & \text{nos outros casos} \end{cases}$$

(a) Qual a relação definida por f?
(b) Qual o domínio de f?
(c) Defina a restrição de f a $\{0,1\} \times \{0,1\}$
(d) Quantas funções distintas existem com mesmo domínio e mesma imagem de f?
(3) Seja $f : \mathbb{R}_+ \longrightarrow \mathbb{R}$ definida por

$$f(x) = \begin{cases} x+5 & \text{se } x \in \mathbb{R}_+ \setminus \mathbb{Q}_+ \\ x^2 & \text{se } x \in \mathbb{Q}_+ \end{cases}$$

(a) f é função injetora?
(b) f é bijetora?
(4) Para cada uma das funções a seguir, determine o conjunto imagem e identifique se são injetoras, sobrejetoras e/ou bijetoras.

$$(a)\ f_1 : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x \end{array} \qquad (b)\ f_2 : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x+y \end{array}$$

$$(c)\ f_3 : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{N} \\ x & \longmapsto & x^2 \end{array} \qquad (d)\ f_4 : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x-y \end{array}$$

$$(e)\ f_5 : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & xy \end{array} \qquad (f)\ f_6 : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \cos x \end{array}$$

$$(g)\ f_7: \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \qquad (h)\ f_8: \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & x^2+1 \end{array}$$

$$(i)\ f_9: \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ x & \longmapsto & x+1 \end{array} \qquad (j)\ f_{10}: \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^3 \end{array}$$

$(k)\ f_{11} : A \longrightarrow A$, onde $A = \{1, 2, \ldots, k\}$ e

$$f_{11}(n) = \begin{cases} n+1 & \text{se } 1 \leq n < k \\ 1 & \text{se } n = k \end{cases}$$

(5) Quantas funções sobrejetoras de um conjunto de 3 elementos num conjunto de 2 elementos existem? Quantas funções injetoras de um conjunto de 3 elementos num conjunto de 4 elementos existem?

(6) Mostre que existe uma bijeção entre $A \times B$ e $B \times A$.

(7) Sejam A e B dois conjuntos com $|A| = m$ e $|B| = n$ com $m \neq n$.
(a) Sob quais condições uma função $f : A \longrightarrow B$ é injetora? E sobrejetora?
(b) Qual é o número mínimo de elementos que um subconjunto de $A \times B$ deve ter para definir uma função?

(8) Mostre que $f : A \longrightarrow B$ é sobrejtora se, e somente se, a relação f^{-1} satisfaz a condição: para cada $b \in B$, existe pelo menos um $a \in A$, tal que $b = f^{-1}(a)$.

(9) Mostre que, se $f : A \longrightarrow B$ é uma função dada e $A_1 \subseteq A_2 \subseteq A$, então $f(A_1) \subseteq f(A_2)$.

(10) Sejam $f : A \longrightarrow B$ uma função dada, e $A' \subseteq A$ e $B' \subseteq B$. Mostre que
(a) $A' \subseteq f^{-1}(f(A'))$ e $A' = f^{-1}(f(A'))$ quando f é injetora,
(b) $f(f^{-1}(B')) \subseteq B'$, e $f(f^{-1}(B')) = B'$ quando f é sobrejetora.

(11) Prove que, se S e T são conjuntos finitos com $|S| = |T| = n$ e se $f : S \longrightarrow T$ é uma função, as seguintes afirmações são equivalentes:
(a) f é injetora.
(b) f é sobrejetora.

(12) Dada $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por

$$f(x) = \begin{cases} 2x + 5, & \text{quando} \quad x < -1 \\ x^2 - 1, & \text{quando} \quad -1 \leq x \leq 1 \\ 5x, & \text{quando} \quad x > 1. \end{cases}$$

Determine:
(a) $f(0)$, $f(\frac{5}{3})$, $f(\frac{-7}{2})$, $f(\sqrt{2})$, $f(\frac{2\pi}{5})$
(b) $f([-1, 5])$
(c) $f^{-1}(\mathbb{R}_+)$
(d) $f^{-1}(\{10, -7\})$
(e) $f^{-1}(]-2, 3[)$
(13) Considere $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = |x|$. Determinar: $f(1)$, $f(-3)$, $f(1 - \sqrt{2})$, $f([-1, 1])$, $f(]-1, 2[)$, $f(\mathbb{R})$, $f^{-1}([0, 3])$, $f^{-1}([-1, 3])$ e $f^{-1}(\mathbb{R}^*_-)$.
(14) Seja $f : \mathbb{R} \longrightarrow \mathbb{R}$ a função definida por

$$f(x) = \begin{cases} x^2 & \text{se} \quad x \leq 0 \\ \sqrt[3]{x} & \text{se} \quad x > 0. \end{cases}$$

Determinar: $f([-1, 8])$, $f(\mathbb{R}_-)$, $f^{-1}([-1, 16])$ e $f^{-1}(\mathbb{R}^*_-)$.
(15) Provar que a função $f :]-1, 1[\longrightarrow \mathbb{R}$ definida por $f(x) = \frac{x}{1 - |x|}$ é bijetora.
(16) Seja $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ definida por $f(x, y) = xy$.
(a) f é injetora?
(b) f é sobrejetora?
(c) Obter $f^{-1}(\{0\})$.
(d) Obter $f([0, 1] \times [0, 1])$.
(e) Obter $f(\Delta_{\mathbb{R}})$, onde $\Delta_{\mathbb{R}} = \{(x, y) \mid x = y\}$.
(17) Dizemos que dois conjuntos A e B são equipotentes quando $A = B = \emptyset$, ou existe $f : A \longrightarrow B$ bijetora. Em cada caso a seguir, mostre que A e B são equipotentes:
(a) $A = \mathbb{N}$ e $B = \mathbb{N}^*$
(b) $A = \mathbb{Z}$ e $B = \mathbb{N}$
(c) $A = \mathbb{R}$ e $B = \mathbb{R}^*_+$
(d) $A =]-\frac{\pi}{2}, \frac{\pi}{2}[$ e $B = \mathbb{R}$
(e) $A =]-1, 1[$ e $B =]a, b[$ com $a < b$, $a, b \in \mathbb{R}$

(f) $A =]-1,1[$ e $B = [-1,1]$
(g) $A =]-1,1[$ e $B = \mathbb{R}$

(18) Prove que duas pessoas em São Paulo devem ter as mesmas letras iniciais no primeiro nome.

(19) Prove que, se S e T são conjuntos finitos com $|S| = |T| = n$ e $f : S \longrightarrow T$ é uma função, as seguintes afirmações são equivalentes:
(a) f é injetora.
(b) f é sobrejetora.
(c) f é invertível.

(20) Obter a inversa da função $f :]-1,1[\longrightarrow \mathbb{R}$ definida por $f(x) = \frac{x}{1-|x|}$, $\forall x \in]-1,1[$.

(21) Prove que, se uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$ é invertível e seu gráfico é uma curva simétrica em relação à reta $y = x$, então $f = f^{-1}$. Dar exemplos de funções, tais que $f = f^{-1}$.

(22) Dadas

$$f : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & n+1 \end{array} \quad \text{e} \quad g : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & 2n, \end{array}$$

mostre que $f \circ g \neq g \circ f$.

(23) Mostre que a composição de duas funções injetoras é injetora. E que o mesmo acontece para funções sobrejetoras.

(24) Considere duas funções $f : A \longrightarrow B$ e $g : B \longrightarrow C$ quaisquer e prove as seguintes afirmações:
(a) se $g \circ f$ é injetora, então f é injetora;
(b) se $g \circ f$ é sobrejetora, então g é sobrejetora;
(c) se $g \circ f$ é bijetora, então f é injetora e g é sobrejetora.

(25) Mostre que, se $f : A \longrightarrow B$ e $g : B \longrightarrow C$ são bijetoras, então existe $(g \circ f)^{-1}$ e, além disso, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(26) Sejam f, g, h funções definidas sobre o conjunto dos números reais por $f(x) = x - 1$, $g(x) = x^2 + 2$ e $h(x) = x + 1$, $\forall x \in \mathbb{R}$.
(a) Determine $f \circ g$, $f \circ h$, $h \circ f$, $g \circ f$ e $h \circ g$;
(b) Verifique que $(f \circ g) \circ h = f \circ (g \circ h)$.

(27) Dadas $f = \{(x,y) \in \mathbb{R}^2 : y = x^3 + 1\}$ e $g = \{(x,y) \in \mathbb{R}^2 : y = x^2 + 1\}$. Determine as compostas $f \circ g$, $g \circ f$, $f \circ f$ e $g \circ g$.

(28) Considere as funções $f(x) = \cos x$ e $g(x) = |x|$, definidas sobre o conjunto dos números reais. Esboce os gráficos das compostas $f \circ g$ e $g \circ f$.

(29) Para cada par de funções reais f e g dados a seguir, determine as compostas: $f \circ g$ e $g \circ f$.

$(a)\quad f(x) = \begin{cases} x+1, & \text{se } x \geq 0 \\ x-1, & \text{se } x < 0 \end{cases} \qquad g(x) = 3x - 2$

$(b)\quad f(x) = \begin{cases} x^2, & \text{se } x < 0 \\ 2x, & \text{se } x \geq 0 \end{cases} \qquad g(x) = \begin{cases} 1-x, & \text{se } x < 1 \\ 1+x, & \text{se } x \geq 1 \end{cases}$

$(c)\quad f(x) = \begin{cases} x^2+1, & \text{se } x < 0 \\ 2x+1, & \text{se } x \geq 0 \end{cases} \qquad g(x) \text{ dada por}$

$$g(x) = \begin{cases} 3x, & \text{se } x < 1 \\ 7x+1, & \text{se } 1 \leq x \leq 5 \\ 2+x, & \text{se } x > 5 \end{cases}$$

(30) Determine $f \circ f$ para $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por

$$f(x) = \begin{cases} x+1, & \text{se} \quad x \leq 0 \\ 1-2x, & \text{se} \quad x > 0. \end{cases}$$

(31) Dadas as funções definidas sobre $\mathbb{R}$ por $f(x) = 2x + 7$ e $(f \circ g)(x) = 4x^2 - 2x + 3$. Determinar a lei de definição de g.

(32) Mostre que uma função $f : A \longrightarrow B$ $(A \neq \emptyset)$ é injetora se, e somente se, existe uma função parcial $g : B \to A$, tal que $g(f(a)) = a$, $\forall a \in A$.

(33) Considere $f : A \longrightarrow B$ e $g : A \longrightarrow C$ com $\prod_{\mathsf{R}_f} = \{A_1,\ A_2\}$ e $\prod_{\mathsf{R}_g} = \{A_3,\ A_4,\ A_5\}$, $f(a) = 0.c_{A_1}(a) + 1.c_{A_2}(a)$ e $g(a) = 0.c_{A_3}(a) + 1.c_{A_4}(a) + 3.c_{A_5}(a)$. Mostre que

$$\begin{aligned} f(a) + g(a) \quad = \quad & 0.c_{A_1 \cap A_3}(a) + 1.c_{A_1 \cap A_4}(a) + c_{A_2 \cap A_3}(a) + \\ & + 2.c_{A_2 \cap A_4}(a) + 3.c_{A_1 \cap A_5}(a) + 4.c_{A_2 \cap A_5}(a). \end{aligned}$$

(34) Prove que para todo $u \in U$ tem-se:

(a) $c_A(u) \leq c_B(u)$ se, e somente se, $A \subseteq B$,

(b) $c_{A \cap B}(u) = \min\{c_A(u),\ c_B(u)\}$,

(c) $c_{A \cup B}(u) = \max\{c_A(u),\ c_B(u)\}$,

(d) $c_{A-B}(u) = c_A(u) - c_{A \cap B}(u)$.

(35) A cada subconjunto A de $U = \{u_1, \ldots, u_n\}$ associe o número binário com n dígitos $\beta_1, \ldots, \beta_n$, onde $\beta_i = c_A(u_i)$. Baseado nesta associação, prove (mais uma vez) que $|\wp(U)| = 2^{|U|}$.

(36) Expressar as seguintes permutações como produto de ciclos disjuntos. Encontre também as inversas dessas permutações:

$$p_1 = \begin{pmatrix} a & b & c & d & e & f & g \\ g & f & e & d & c & b & a \end{pmatrix}$$

$$p_2 = \begin{pmatrix} a & b & c & d & e & f & g \\ e & g & f & b & a & c & d \end{pmatrix}$$

$$p_3 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j \\ h & d & b & a & c & f & j & i & g & e \end{pmatrix}$$

(37) Considere as permutações p_1 e p_2 do exercício anterior e encontre as permutações:

(a) p_1p_2, (b) p_2p_1 e (c) $(p_1p_2p_1)^2$.

(38) Encontre as permutações correspondentes aos seguintes produtos de ciclos:

(i) $(a, c, b, f)(d, h, i, j)(e)(g)$ (ii) $(a, g)(f, e)(b, i)(h, c)(d, j)$

(iii) $(a, h, c, d, j, f, g, i, b, e)$

(39) Uma *transposição* é uma permutação que troca dois elementos deixando os demais fixos. Por exemplo: $\begin{pmatrix} a & b & c & d & e \\ d & b & c & a & e \end{pmatrix}$ é uma transposição sobre $\{a, b, c, d, e\}$, que pode ser denotada como produto de ciclos por $(a\ d)$. Mostre que toda permutação pode ser expressa como a composição de um número finito de transposições. Expresse a permutação

$$p = \begin{pmatrix} a & b & c & d & e & f & g & h \\ h & g & b & f & e & d & a & c \end{pmatrix}$$

desta maneira.

Capítulo 5

ANÉIS E ÁLGEBRAS DE BOOLE

O objetivo principal deste capítulo é fazer um breve estudo sobre as álgebras booleanas de um ponto de vista computacional. Usaremos a estrutura natural de ordem de uma álgebra booleana e demonstraremos o Teorema de Stone para álgebras booleanas finitas. Em seguida, trataremos das funções booleanas, como álgebras booleanas. Exemplo destas álgebras são as álgebras de proposições exploradas em capítulos anteriores. A seguir daremos as formas canônicas de funções booleanas e finalizaremos representando funções booleanas por circuitos, muito útil em aplicações na área de engenharia.

5.1 Operações

Definição 5.1 Uma *operação* sobre um conjunto não vazio E é simplesmente uma função $f : E \times E \longrightarrow E$. Em geral, denota-se f por $*$, $\triangle$, etc e $f(x, y)$ por $x * y$, $x \triangle y$, etc, que se lê: 'x *estrela* y,', ' x delta y', etc.

Exemplos 5.2 (1) Se a função f é a adição de números naturais $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, geralmente se escreve $x+y$ para a imagem de f em (x, y) e se diz "soma"de x e y. Como a soma de números naturais é sempre um número natural, segue-se que f é uma operação sobre $\mathbb{N}$. Pode-se verificar que a adição também é uma operação sobre quaisquer dos conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Verifique!

(2) A subtração de números naturais: $f(n,m) = n - m$ não é uma operação sobre $\mathbb{N}$, pois $f(2,3) = 2 - 3$ não é um número natural. No entanto $f(n,m) = n - m$ é um número inteiro para todos $n,\ m \in \mathbb{Z}$. Portanto, a subtração é uma operação sobre $\mathbb{Z}$.

(3) $* : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ dada por $x * y = x^y$ não é operação sobre $\mathbb{R}$ porque não é função. Por exemplo, $(-2) * \frac{1}{2} = (-2)^{\frac{1}{2}} = \sqrt{-2} \notin \mathbb{R}$. Pela mesma razão não é uma operação sobre $\mathbb{Q}$. Esta relação é uma operação sobre $\mathbb{N}$, pois quaisquer que sejam os números naturais x e y, x^y é um número natural.

(4) Adição e multiplicação de matrizes sobre o conjunto das matrizes quadradas de ordem n sobre $\mathbb{R}$ são operações sobre este conjunto de matrizes.

(5) Dados $A = \{f : \mathbb{R} \longrightarrow \mathbb{R}\}$, a operação de composições de funções de A é uma operação sobre A.

(6) A função $f(n,m) = mdc(n,m)$ é uma função sobre $\mathbb{Z}$ pois para todo par $(m,n) \in \mathbb{Z} \times \mathbb{Z}$, tem-se que $mdc(m,n) \in \mathbb{Z}$.

(7) Seja L um alfabeto com pelo menos dois símbolos e L^* é o conjunto de todas as palavras (= seqüências finitas de letras) do alfabeto L. A concatenação de palavras:

$$x_1x_2 \ldots x_n * y_1y_2 \ldots y_m = x_1x_2 \ldots x_ny_1y_2 \ldots y_m,$$

onde $n > 0,\ m > 0$ e $x_i,\ y_j$ pertencem a L, é uma operação sobre L^*, pois junções de duas palavras sobre L é uma palavra sobre L.

Propriedades

Uma operação $*$ definida sobre um conjunto não vazio E pode satisfazer as seguintes propriedades:

(a) *Associativa*

$* : E \times E \longrightarrow E$ é dita *associativa* se, para todos $x,\ y,\ z \in E$, $x * (y * z) = (x * y) * z$.

Observação: Pelas leis do cálculo proposicional podemos afirmar que $*$ não é associativa se existem $x,\ y,\ z \in E$, tais que $x * (y * z) \neq (x * y) * z$.

(b) *Comutativa*

$* : E \times E \longrightarrow E$ é dita *comutativa* se, para todos $x,\ y \in E$, $x * y = y * x$.

Observação: Podemos afirmar que $*$ não é comutativa se existem $x,\ y \in E$, tais que $x * y \neq y * x$.

(c) *Existência do elemento neutro*

Dizemos que $* : E \times E \longrightarrow E$ admite *elemento neutro* $e \in E$ se, para todo $x \in E$, tem-se: $x * e = x = e * x$.

Observação: O elemento neutro $e \in E$ é um elemento fixo e a propriedade acima deve ser satisfeita para todo $x \in E$.

(d) *Elemento simetrizável e Elemento simétrico*

Seja $* : E \times E \longrightarrow E$ uma operação que admite elemento neutro 'e'. Dizemos que $a \in E$ é *simetrizável* se existe $b \in E$, tal que $a * b = b * a = e$. O elemento $b \in E$ com esta propriedade é dito o *simétrico do elemento* $a \in E$ (para a operação $*$) e será denotado por a'.

Notação 5.3 Denotaremos por $U_*(E)$ o conjunto dos elementos simetrizáveis de E para a operação $*$. Assim, $U_*(E) = \{a \in E : a * b = e = b * a,\ \text{para algum } b \in E\} = \{a \in E \text{ tal que } \exists a' \in E\}$.

No caso em que $*$ é denotada pelo símbolo aditivo $+$, a' será indicado por $-a$ e chamado *oposto de* a. Quando a operação $*$ é denotada por $\bullet$, sugerindo a operação multiplicativa, também mudamos a notação de a', neste caso, para a^{-1}, e dizemos *inverso de* a em vez de simétrico de a.

Observação: Pode acontecer de existirem dois elementos diferentes a' e a'' em E que são simétricos de $a \in E$. Veja o exercício (1) da próxima lista de exercícios.

(e) *Distributiva*

Nada impede que existam duas ou mais operações sobre um conjunto não vazio E. Vamos supor que $*$ e $\triangle$ sejam operações sobre um conjunto não vazio E. Dizemos que a operação $*$ é *distributiva em relação a* $\triangle$ se:

$$x * (y \triangle z) = (x * y) \triangle (x * z)$$
e
$$(y \triangle z) * x = (y * x) \triangle (z * x),$$

para todos $x,\ y,\ z \in E$.

(f) *Elementos Regulares*

Dizemos que um elemento $a \in E$ é *regular* para $* : E \times E \longrightarrow E$ se, para todos $x,\ y \in E$,

$$\left\{ \begin{array}{l} a * x = a * y \\ \text{ e } \\ x * a = y * a \end{array} \right. \Longrightarrow \quad x = y.$$

Notação: Denotaremos por $R_*(E)$ o conjunto dos elementos regulares de E para a operação $*$. Assim, $R_*(E) = \{a \in E : a \text{ é regular}\}$.

Observe que um elemento $a \in E$ não será regular para a operação $*$ se existirem $x,\ y \in E$, tais que $a * x = a * y, \quad x * a = y * a$ e $x \neq y$.

Exemplos 5.4 As operações de adição e multiplicação sobre os campos numéricos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ obedecem várias propriedades que enumeraremos a seguir. Ressaltamos que na demonstração destas propriedades, precisaremos considerar as definições tratando da construção desses conjuntos, coisa que não faremos aqui.

(a) A operação de adição sobre $\mathbb{N}$ obedece as propriedades associativa, comutativa e admite elemento neutro 0 (zero). Todo elemento é regular para a adição, e o único elemento simetrizável é zero.

(b) A operação de adição sobre $\mathbb{Z},\ \mathbb{Q},\ \mathbb{R}$, ou $\mathbb{C}$ satisfaz todas as propriedades, todos os elementos são regulares e todos os elementos admitem opostos.

(c) A operação de multiplicação sobre $\mathbb{N}$ é comutativa, associativa, admite 1 como elemento neutro, que é o único elemento inversível (simétrico para a multiplicação), e todos os elementos não nulos são regulares para a multiplicação. Observe que 0 (zero) não é regular para a multiplicação, pois $0.2 = 0.3$ e $2 \neq 3$.

(d) A operação de multiplicação sobre os números inteiros admite as mesmas propriedades e $R_\bullet(\mathbb{Z}) = \mathbb{Z} \setminus \{0\}$, pois, para todo $a \in \mathbb{Z}, \quad a \neq 0$ se $ax = ay \quad (xa = ya)$, então $x = y$. O conjunto dos elementos inversíveis é $U_\bullet(\mathbb{Z}) = \{1, -1\}$ com $(-1)^{-1} = -1$ e

$1^{-1} = 1$. Se $a \neq 1$ ou -1, então não existe $b \in \mathbb{Z}$, tal que $ab = 1$, ou seja, se $a \neq 1$ e $a \neq -1$, então a não é inversível.

(e) A operação de multiplicação sobre $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ satisfazem todas as propriedades vistas e $U_\bullet(\mathbb{Q}) = R_\bullet(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$, $U_\bullet(\mathbb{R}) = R_\bullet(\mathbb{R}) = \mathbb{R} \setminus \{0\}$. O mesmo vale para o conjunto dos números complexos.

Como exemplo, vamos mostrar que $U_\bullet(\mathbb{C}) = \mathbb{C} \setminus \{0\}$. Dado $x = a + bi$ em $\mathbb{C}$, queremos condições sobre x para que exista $x^{-1} \in \mathbb{C}$. Seja $x^{-1} = c + di$, $c, d \in \mathbb{R}$ a determinar. Desde que $(a + bi)(a - bi) = a^2 + b^2$, e este elemento é não-nulo, se x é não-nulo, vem que $(a + bi)\Big(\dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2}i\Big) = 1$. Logo, $x^{-1} = \dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2}i$. Para existir $x^{-1} \in \mathbb{C}$ é preciso que $a^2 + b^2 \neq 0$ em $\mathbb{R}$, ou seja, $a \neq 0$ ou $b \neq 0$ em $\mathbb{R}$. Logo existe x^{-1} se, e somente se, $x \neq 0$.

Exemplos 5.5 (1). Verifique quais das propriedades dadas as operações abaixo satisfazem

A. $*$ = potenciação e $E = \mathbb{N}$.

(i) $(x * y) * z = x * (y * z)$ se, e somente se, $x^y * z = x * y^z$ se, e somente se, $(x^y)^z = x^{(y^z)}$, ou seja, $x^{yz} = x^{(y^z)}$. Para os valores $x = 4$, $y = 3$, $z = 2$, temos $4^6 \neq 4^9$. Logo a operação de potenciação não é associativa.

(ii) $x * y = y * x$ se, e somente se, $x^y = y^x$. Ocorre que, para $x = 2$, $y = 3$, temos que $8 \neq 9$. Logo, a operação de potenciação não é comutativa.

(iii) Elemento neutro. Queremos $e \in \mathbb{N}$ fixo, tal que $x^e = e^x$ para todo $x \in \mathbb{N}$. Então, se existe $e \in \mathbb{N}$ nestas condições, deve valer para $x = 1$ e aí temos $1^e = e^1 = e$. Logo, $e = 1$ (se existir). Voltando na equação geral, ficamos com: $x = x^1 = 1^x = 1$ para todo $x \in \mathbb{N}$ (absurdo). Logo, não existe elemento neutro para a operação de potenciação sobre $\mathbb{N}$.

(iv) Elementos regulares. Seja $a \in \mathbb{N}$ fixado.

Se $a = 0$; de $0^1 = 0^2 = 1$ e $1 \neq 2$, vem que 0 não é regular.

Se $a \neq 0$, as equações $a * x = a * y$, $(x * a = y * a)$ significam que $a^x = a^y$, $x^a = y^a$. Logo, $x = y$ e, portanto, $R_*(\mathbb{N}) = \mathbb{N} \setminus \{0\}$.

B. $*$ = multiplicação de matrizes 2×2 sobre $\mathbb{R}$.

Para quaisquer $A,\ B,\ C \in M_2(\mathbb{R})$, tem-se:

(i) $(AB)C = A(BC)$, ou seja, a operação de multiplicação de matrizes é associativa (verifique!).

(ii) A operação de multiplicação de matrizes não é comutativa pois, por exemplo, para

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \text{ temos: } AB \neq BA.$$

(iii) O elemento neutro é a matriz $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, pois para toda matriz quadrada 2×2 A, temos que $A.I_2 = I_2.A$.

(iv) A matriz inversa da $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ é a matriz $A^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Portanto, A é inversível se, e somente se, $det(A) = ad - bc \neq 0$, ou então $U_{\bullet}\big(M_2(\mathbb{R})\big) = \{A \in M_2(\mathbb{R}) : det(A) \neq 0\}$.

(v) Para o cálculo de $R_{\bullet}\big(M_2(\mathbb{R})\big)$, veja a propriedade (5) adiante.

C. $*$ = composição de funções de $\mathbb{R}$ em $\mathbb{R}$.

(i) A composição de funções é associativa e não é comutativa, veja observação 4.77. O elemento neutro é a função identidade de $\mathbb{R}$, denotada por $1_{\mathbb{R}}$, veja Lema 4.78. Os elementos inversíveis de $\mathbb{R}^{\mathbb{R}}$ são as funções bijetoras, conforme visto na Proposição 4.73.

2. Sobre a distributividade.

(a) A operação de multiplicação é distributiva em relação a operação de adição definidas sobre quaisquer dos conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, pois $a(b+c) = ab + ac$ e $(b+c)a = ba + ca$.

(b) Como $2 + 3.1 \neq (2+3)(2+1)$, a adição não é distributiva em relação a multiplicação sobre quaisquer dos campos numéricos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(c) A exponenciação não é distributiva em relação a multiplicação, pois existem $x,\ y,\ z \in \mathbb{N}$, tais que $x^{yz} \neq x^y.x^z$, isto é, $x*(y\triangle z)$ em geral é diferente de $(x*y)\triangle(x*z)$. Por exemplo, tome $x = 2,\ y = 3,\ z = 4$.

(d) Apesar de que $(g+h) \circ f = g \circ f + h \circ f$ para todas funções $f,\ g,\ h \in \mathbb{R}^{\mathbb{R}}$, a operação de composição de funções não é dis-

tributiva em relação a adição de funções, pois nem sempre vale a igualdade $f \circ (g+h) = f \circ g + f \circ h$. Obtenha $f,\ g,\ h \in \mathbb{R}^{\mathbb{R}}$ convenientes.

(e) A multiplicação de matrizes é distributiva em relação a adição de matrizes em $M_n(\mathbb{R})$, pois: para todas as matrizes $A,\ B,\ C$ de $M_n(\mathbb{R})$ tem-se $A.(B+C) = A.B + A.C$ e $(B+C).A = B.A + C.A$.

Propriedades de Operações

1. Se uma operação $*$ sobre um conjunto não vazio E admite elemento neutro e, então ele é único.

Demonstração: Seja $e' \in E$ outro elemento neutro. Então: $e * e' = e'$, pois e é elemento neutro de E, e $e * e' = e$, pois e' também é elemento neutro de E. Sendo assim, $e = e'$.

2. Se a operação $*$ sobre E é associativa e admite elemento neutro, então todo elemento simetrizável admite um único simétrico.

Demonstração: Observe que $U_*(E) \neq \emptyset$, pois e é simetrizável. Suponhamos que $x \in E$ seja simetrizável com simétrico x' e seja $y \in E$ outro simétrico de x. Então, $x * x' = x' * x = e$ e $x * y = y * x = e$. Daí $x' = x' * e = x' * (x * y) = (x' * x) * y = e * y = y$. Note que usamos a associatividade de $*$.

3. Se $x \in E$ é simetrizável para a operação $*$, então x' também é simetrizável e $(x')' = x$.

Demonstração: Basta ver que $x * x' = x' * x = e$. Daí, por definição, temos que o simétrico de x' é x, ou seja, $(x')' = x$. Note que, se $*$ é associativa, x é o único simétrico de x'.

4. Se a operação $*$ é associativa e $x,\ y$ são simetrizáveis, então $x * y$ também é simetrizável e $(x * y)' = y' * x'$.

Demonstração: Basta usar a associativa para provar que $(x * y) * (y' * x') = (y' * x') * (x * y) = e$. Daí, por definição, segue-se o resultado.

5. Se a operação $*$ é associativa, admite elemento neutro e e $a \in E$ é simetrizável, então a é regular (ou seja: $U_*(E) \subseteq R_*(E)$).

Demonstração: Sejam $x,\ y \in E$, tais que $a * y = a * x$. Multiplicando por a' pela esquerda, temos: $a' * (a * y) = a' * (a * x)$. Usando a associatividade de $*$ ficamos com $(a' * a) * y = (a' * a) * x$

e, portanto, $x = y$. Se multiplicarmos a equação $y * a = x * a$ pela direita por a' e usarmos a hipótese, chegaremos também que $x = y$. Agora podemos concluir que $a \in R_*(E)$.

Exemplos 5.6 (i) Seja $*$ a operação de multiplicação sobre os números reais. Então $e = 1 \in \mathbb{R}$ é o único elemento neutro para a multiplicação. Temos que $3 \in U_\bullet(\mathbb{R})$ e $(3^{-1})^{-1} = 3$.

Como 2, 3 são simetrizáveis, temos que $(2.3)^{-1} = 3^{-1}.2^{-1} = 2^{-1}.3^{-1}$ (pois, neste caso, $*$ é comutativa).

Neste caso, temos a igualdade $U_\bullet(\mathbb{R}) = R_\bullet(\mathbb{R}) = \mathbb{R} \setminus \{0\}$.

(ii) Verifiquemos a validade de todos os conceitos vistos sobre a seguinte operação definida sobre $\mathbb{Z}$: $x * y = x + y + xy$.

É fácil ver que $*$ é comutativa.

Seja $e \in \mathbb{Z}$ o elemento neutro de $*$, se existir. Então, para todo $x \in \mathbb{Z}$, $x*e = x+e+xe = x$. Podemos escrever $x+(e+ex) = x+0$ e, como todo elemento de $\mathbb{Z}$ é regular para a operação de adição, ficamos com $e + ex = 0$, para todo $x \in \mathbb{Z}$. Como $e \in \mathbb{Z}$ deve ser fixo, esta equação só é possível para $e = 0$.

A associativa também vale e fica como exercício.

Calculemos os elementos simetrizáveis. Seja $x \in U_*(\mathbb{Z})$. Então existe $x' \in \mathbb{Z}$ a determinar, tal que $x*x' = e = 0$. Daí $x+x'+xx' = 0$, ou seja, $x'(1 + x) = -x \in \mathbb{Z}$. Logo, $x' = \dfrac{-x}{1+x} \in \mathbb{Z}$. Ou seja, queremos $x \in \mathbb{Z}$, tal que $x' = \dfrac{-x}{1+x}$ pertença a $\mathbb{Z}$. Para que isto ocorra, é necessário e suficiente que $x+1$ divida x. Como x e $x+1$ são dois números consecutivos, e queremos o maior dividindo o menor, isto só é possível para $x + 1 \in U_\bullet(\mathbb{Z}) = \{-1, 1\}$. Logo, $U_*(\mathbb{Z}) = \{0,\ 2\}$, com $0' = 0$ e $(-2)' = -2$.

Cálculo de $R_*(\mathbb{Z})$:

Como $*$ é associativa e existe e, já sabemos que $\{0, 2\} \subseteq R_*(\mathbb{Z})$. Seja $a \in \mathbb{Z}$ e queremos condições sobre a para que de $a * x = a * y$ tenhamos $x = y$. Mas de $a + x + ax = a + y + ay$ ficamos com $x(1 + a) = y(1 + a)$, pois a é regular para a operação de adição sobre $\mathbb{Z}$. Daí $(x - y)(1 + a) = 0 \in \mathbb{Z}$. Como um produto é zero em $\mathbb{Z}$ quando um dos fatores é nulo, vem que $x - y$ é sempre nulo

para $1 + a$ não nulo. Assim, $x = y$ sempre que $a \neq -1$, ou seja, $R_*(\mathbb{Z}) = \mathbb{Z} \setminus \{-1\}$.

5.1.1 Tabela de uma Operação

Quando o conjunto E é finito, digamos $E = \{a_1, a_2, \ldots, a_n\}$, com poucos elementos, podemos representar a operação em uma 'matriz' onde o elemento da (ij)-posição é o "produto" $a_i * a_j$.

$*$	a_1	a_2	$\cdots$	a_i	$\cdots$	a_j	$\cdots$	a_n
a_1	$a_1{*}a_1$	$a_1{*}a_2$	$\cdots$	$a_1{*}a_i$	$\cdots$	$a_1{*}a_j$	$\cdots$	$a_1{*}a_n$
$\vdots$	$\cdots$	$\cdots$	$\ddots$	$\cdots$	$\ddots$	$\cdots$	$\ddots$	$\cdots$
a_i	$a_i{*}a_1$	$a_i{*}a_2$	$\cdots$	$a_i{*}a_i$	$\cdots$	$a_i{*}a_j$	$\cdots$	$a_i{*}a_n$
$\vdots$	$\cdots$	$\cdots$	$\ddots$	$\cdots$	$\ddots$	$\cdots$	$\ddots$	$\cdots$
a_j	$a_j{*}a_1$	$a_j{*}a_2$	$\cdots$	$a_j{*}a_i$	$\cdots$	$a_j{*}a_j$	$\cdots$	$a_j{*}a_n$
$\vdots$	$\cdots$	$\cdots$	$\ddots$	$\cdots$	$\ddots$	$\cdots$	$\ddots$	$\cdots$
a_n	$a_n{*}a_1$	$a_n{*}a_2$	$\cdots$	$a_n{*}a_i$	$\cdots$	$a_n{*}a_j$	$\cdots$	$a_n{*}a_n$

Exemplo 5.7 Seja $E = \{0, 1, \sqrt{2}, \pi\}$ e $x * y = min\{x, y\}$. Então

$*$	0	1	$\sqrt{2}$	π
0	0	0	0	0
1	0	1	1	1
$\sqrt{2}$	0	1	$\sqrt{2}$	$\sqrt{2}$
π	0	1	$\sqrt{2}$	π

Observações 5.8 (1) Observe a simetria em relação à diagonal principal existente na tabela do exemplo acima. Isto ocorre na tabela se, e somente se, a operação $*$ é comutativa.

(2) Observando a tabela do exemplo acima podemos dizer que o elemento π é o elemento neutro, porque na sua linha e coluna são repetidos os elementos do conjunto E, postos na 1ª linha e 1ª coluna, sem fazer permutação na ordem dada. Sempre que isto

ocorre para um elemento $a \in E$ em vez de π, como é o caso, este elemento será o elemento neutro para a operação $*$ sobre E.

(3) O elemento π, no exemplo dado acima, é regular para a operação $* = min$ sobre o conjunto E dado; isto porque na sua linha e coluna não repete elementos de E. Já o elemento $1 \in E$ não é regular, porque na sua linha ou coluna repete elementos de E. Por exemplo, $1 * 1 = 1 * \sqrt{2}$ e $1 \neq \sqrt{2}$. De um modo geral, se $E = \{a_1, \ldots, a_n\}$, $n > 1$ e $a_i * a_j = a_i * a_k$ ou $a_j * a_i = a_k * a_i$ com $j \neq k$ então o elemento $a_i \in E$ não é regular para $*$.

(4) Se a operação $*$ admite elemento neutro e, um elemento $a_i \in E$ é simetrizável com simétrico $a_j \in E$ se aparecer o elemento neutro e nas posições simétricas i-ésima linha $\times$ j-ésima coluna e j-ésima linha $\times$ i-ésima coluna em relação a diagonal principal. Por exemplo, na tabela do exemplo anterior temos que π é o único elemento simetrizável, com simétrico π, pois $\pi * \pi = \pi$ enquanto os outros elementos não têm em suas linhas e colunas o elemento neutro π em posições simétricas em relação a diagonal principal. A associatividade é mais difícil de ver pela tabela.

Exercícios

(1) Faça uma tabela de uma operação $*$ sobre um conjunto E, de modo que exista um elemento simetrizável e seu simétrico não seja único.

(2) Verifique se $*$ definida sobre E é associativa, comutativa, se admite elemento neutro e, neste caso, obtenha os elementos simetrizáveis e os elementos regulares.

(a) $E = \mathbb{R}^+$ e $x * y = \frac{x+y}{1+xy}$. **(b)** $E = \mathbb{Q}$, $x * y = x + xy$. **(c)** $E = \mathbb{R}$ e $x * y = x^2 + y^2 + 2xy$. **(d)** $E = \mathbb{N}$ e $x * y = min\{x,\ y\}$. **(e)** $E = \mathbb{N}$ e $x * y = mdc(x, y)$. **(f)** $E = \mathbb{Z} \times \mathbb{Z}$ e $(a, b) * (c, d) = (ac, 0)$. **(g)** $E = \mathbb{Z} \times \mathbb{Z}$ e $(a, b) * (c, d) = (ac, ad + bc)$.

(3) Para $E = \{a,\ b\}$: **(i)** Construir as tábuas de todas as operações possíveis sobre E;

(ii) Verificar quais propriedades possuem cada uma das operações obtidas em **(i)**.

(4) Construir a tábua de uma operação $*$ sobre $E = \{e, a, b, c\}$, tal

que
(i) seja comutativa, **(ii)** e seja o elemento neutro, **(iii)** $x * a = a,\ \forall x \in E$ e **(iv)** $R_*(E) = E \setminus \{a\}$.

(5) Defina sobre $\mathbb{R}$: $x * y = x + y - 3$. Mostre que $*$ satisfaz as propriedades associativa, comutativa, existência do elemento neutro e que $U_*(\mathbb{R}) = \mathbb{R}$. Calcule $(1^3)^{-1}$, ou seja, $(1 * 1 * 1)'$ e resolva $x^2 * (1^3)' = 1$.

(6) Seja $G = \{e, a, b, c, d, f\}$ com uma operação $*$ que satisfaz: **(i)** $*$ é associativa, **(ii)** $*$ é comutativa, **(iii)** e é o elemento neutro, **(iv)** $U_*(G) = G$, **(v)** $a * f = b * d = e$, **(vi)** $a * d = b * c = f$, **(vii)** $a * c = b * b = d$, **(viii)** $c * d = a$.

Faça a tábua de $(G, *)$ e resolva a equação: $b * c * x * a * b = b$.

5.2 Anéis

Definição 5.9 Sejam A um conjunto não vazio, $\oplus$ e $\odot$ duas operações sobre A. Dizemos que $(A, \oplus, \odot)$ (ou simplesmente A, se as operações estiverem claras no contexto) é um *anel* se as seguintes propriedades estiverem satisfeitas:

1. $x \oplus (y \oplus z) = (x \oplus y) \oplus z$, para todos $x,\ y,\ z \in A$ (associativa).

2. $x \oplus y = y \oplus x$, para todos $x,\ y \in A$ (comutativa).

3. Existe $e \in A$ (denotado por 0_A), tal que $e \oplus x = x \oplus e = x$ para todo $x \in A$ (Elemento neutro para $\oplus$).

4. Para todo $x \in A$, existe $y \in A$, tal que $x \oplus y = y \oplus x = 0_A$ (existência do elemento simétrico, para todo elemento de A). O elemento y será denotado por $\ominus x$. Observe que exige-se $U_\oplus(A) = A$.

5. $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$ e $(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$ para todos $x,\ y,\ z \in A$ (distributiva de $\odot$ em relação a $\oplus$).

6. $(x \odot y) \odot z = x \odot (y \odot z)\ \ \forall x, y, z \in A$ (Associativa de $\odot$).

Exemplos 5.10 Daremos alguns exemplos, deixando as propriedades para serem verificadas pelo leitor.

a. $(\mathbb{Z}, +, .)$ e $\big(M_n(\mathbb{Q}), +, .\big)$ são anéis.

b. Seja $A = \{f : \mathbb{R} \longrightarrow \mathbb{R}\}$ e definimos $(f+g)(x) = f(x)+g(x)$,

$(f.g)(x) = f(x)g(x)$ e $(f \circ g)(x) = f\big(g(x)\big)$ para todas funções $f,\ g \in A$ e para todo $x \in A$.

Então $(A, +, .)$ é anel e $(A, +, \circ)$ não é anel (de fato, nem sempre $f \circ (g + h) = (f \circ g) + (f \circ h)$).

c. Seja $A = 2\mathbb{Z} := \{2q,\ q \in \mathbb{Z}\} = \{0, 2, -2, 4, -4, 6, -6, \ldots\}$ com as operações usuais de adição e multiplicação de $\mathbb{Z}$. Então $(2\mathbb{Z}, +, .)$ é um anel.

Observe que as operações '+' e '$\bullet$' são operações sobre $2Z$ porque soma e produto de números pares continuam pares, ou seja, para todos $a,\ b \in \mathbb{Z}$, $\quad 2a + 2b = 2(a + b) \in 2\mathbb{Z}$ e $2a.2b = 2(2ab) \in 2\mathbb{Z}$.

d. $A = \mathbb{R} \times \mathbb{R} = \{(a, b) :\ a,\ b \in \mathbb{R}\}$ com as operações $(a, b) + (c, d) = (a + b, c + d)$ e $(a, b).(c, d) = (ac, bd)$. Então $(A, +, .)$ é um anel.

Agora, enunciaremos algumas propriedades de anéis. A maioria destas propriedades foram feitas no item anterior e as demonstrações das propriedades restantes deixamos como exercícios.

Propriedades de Anéis

Seja $(A, \oplus, \odot)$ um anel. Então

(i) 0_A é único.

(ii) Para todo $a \in A$, o oposto de $a : \ominus a$ é único.

(iii) Para todos $a_1,\ a_2,\ \ldots, a_n \in A,\ n \geq 2$, $\quad \ominus(a_1 \oplus a_2 \oplus \cdots \oplus a_n) = (\ominus a_1) \oplus (\ominus a_2) \oplus \cdots \oplus (\ominus a_n)$. Por exemplo, $-(2+3+5) = (-2) + (-3) + (-5)$ em $(Z, +, .)$.

(iv) Para todo $a \in A$, tem-se: $\ominus(\ominus a) = a$

(v) Para todos $a,\ b \in A$ tem-se: $(\ominus a) \odot b = a \odot (\ominus b) = \ominus(a \odot b)$.

(vi) $R_{\oplus}(A) = A$, isto é, para todo $a \in A$ fixado e $x,\ y \in A$, se $a \oplus x = a \oplus y$, então $x = y$.

(vii) Para todos $a,\ b \in A$, a equação $a \oplus x = b$ tem solução única, a saber: $x = (\ominus a) \oplus b$.

Definição 5.11 Um anel $(A, \oplus, \odot)$ é dito ser *comutativo* se para todos $x,\ y \in A$, $x \odot y = y \odot x$. O anel A é dito *unitário* se existe elemento neutro 1_A para a operação de multiplicação $\odot$, ou seja: existe $1_A \in A$, tal que para todo $x \in A$ tem-se: $x \odot 1_A = 1_A \odot x$.

Observação: Geralmente exige-se que $1_A \neq 0_A$ para que não se tenha $A = \{0_A\}$ (de fato: se $0_A = 1_A$, então $x = x \odot 1_A = x \odot 0_A = x \odot (0_A \ominus 0_A) = (x \odot 0_A) \ominus (x \odot 0_A) = x \odot 1_A \ominus x \odot 1_A = x \ominus x = 0_A$. Justifique cada passagem).

Exemplo 5.12 O anel $(\mathbb{Z}, +, .)$ é comutativo, pois $x.y = y.x$ para todos $x,\ y \in \mathbb{Z}$ e unitário com $1_{\mathbb{Z}} = 1 \in \mathbb{Z}$; o anel $(2\mathbb{Z}, +, .)$ é comutativo e não é unitário, pois não existe elemento da forma $2q \in 2\mathbb{Z}$, tal que $2q.x = x.2q = x$, para todo $x \in 2\mathbb{Z}$.

O anel das matrizes de ordem $n \geq 2$ sobre $\mathbb{Z}$ $(M_n(\mathbb{Z}), +, .)$ não é comutativo e é unitário com $1_{M_n(\mathbb{Z})}$ =matriz identidade.

5.2.1 O Anel de Inteiros Módulo m

Para esta subseção, é interessante recordar os tópicos 2.4 e 4.2 que tratam, respectivamente, de congruência e relação de equivalência. Nestes tópicos foram visto que a relação de congruência módulo m (m um inteiro maior que 1) é uma relação de equivalência e, como tal, ela particiona o conjunto $\mathbb{Z}$, dos números inteiros, em classes de equivalência. O número de classes é exatamente m, veja Proposição 4.36. Se $a \in \mathbb{Z}$, denotamos a classe de equivalência determinada por a módulo m por $[a]$ ou por $\overline{a}$. Vimos que $[a] = \{x \in \mathbb{Z} : x \equiv a(mod.m)\}$, e então $[a]$ é precisamente o seguinte subconjunto de $\mathbb{Z}$: $[a] = \{a + qm,\ q \in \mathbb{Z}\}$. O subconjunto $\{a+qm,\ q \in \mathbb{Z}\}$ é denotado por: $a+m\mathbb{Z}$. Consequentemente, $[a] = a + m\mathbb{Z}$.

Exemplo 5.13 Para $m = 5$ e $a = 2$, temos: **(i)** $[2] = 2 + 5\mathbb{Z} = \{2 + 5q, q \in \mathbb{Z}\}$. Então, $2+5\mathbb{Z} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$. **(ii)** $\overline{5} = \overline{0}$.

De fato, por definição, $5 + 5\mathbb{Z} = \{5 + 5q',\ q' \in \mathbb{Z}\} = \{5(1 + q'),\ 1 + q' \in \mathbb{Z}\} = \{5q,\ q = 1 + q' \in \mathbb{Z}\} = \{0, \pm 5, \pm 10, \pm 15, \ldots\}$.

Outro modo de ver que $\overline{5} = \overline{0}$ é observar que $5 \equiv 0(mod.5)$. Pelo Lema 4.31, segue que $[5] = [0]$.

(iii) Vamos descrever todas as classes de equivalência módulo 5, ou seja, descrever todos os elementos de $\mathbb{Z}_5$.

Pela Proposição 4.36, basta considerar os representantes de classes 0, 1, 2, 3, 4 (os possíveis resto da divisão euclidiana de um número por 5).

$\overline{0} = 0+5\mathbb{Z} = \{0, \pm 5, \pm 10, \ldots\}$. Os elementos deste conjunto e só eles são os inteiros congruentes a zero módulo 5. E só eles são congruentes entre si. Do mesmo modo $\overline{1} = 1 + 5\mathbb{Z} = \{1+5q,\ q \in \mathbb{Z}\} = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$. Pela mesma razão, $\overline{2} = 2 + 5\mathbb{Z} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$,

$$\overline{3} = 3 + 5\mathbb{Z} = \{\ldots, -12, -7, -2, 3, 8, 13, \ldots\} \quad \text{e}$$
$$\overline{4} = 4 + 5\mathbb{Z} = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}.$$

Notemos que qualquer número inteiro a, $a = 5q + r$ com q, $r \in \mathbb{Z}$ e $0 \leq r < 5$, ou seja, $a \in r + 5\mathbb{Z}$ com $r = 0, 1, 2, 3$ ou 4. Logo, $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Podemos representar geometricamente o conjunto $\mathbb{Z}_5$ (mais geralmente $\mathbb{Z}_m$) considerando um círculo dividido em 5 (m) partes iguais. Isto porque, para obter a classe $a + 5\mathbb{Z}$ ($a + m\mathbb{Z}$) a partir de a, basta ir saltando para frente e também para trás de 5 em 5 (de m em m) números no conjunto ordenado $\mathbb{Z}$.

Considerando os 5 (m) vértices no círculo com o 1º vértice no pólo norte, podemos ir enrolando $\mathbb{Z}$ no círculo do seguinte modo: colocamos 0 no polo norte e, percorrendo o sentido horário vamos colocando 1 no 2º vértice, 2 no 3º vértice, 3 no 4º vértice, assim por diante. A partir do polo norte, no sentido anti-horário, colocamos 0 no polo norte, -1 no próximo vértice (portanto vai ficar junto com 4), -2 no próximo vértice (portanto vai ficar junto com 3), etc. Veja a figura 5.1.

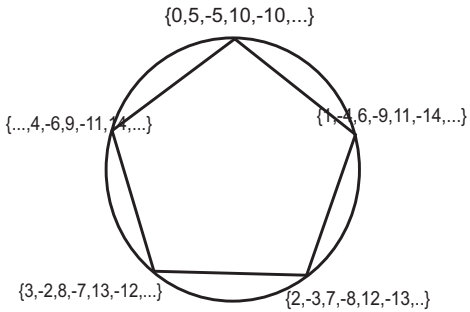


Figura 5.1: As classes de restos módulo 5

A seguinte proposição resume algumas propriedades de congruência e reescreve os Lemas 4.31 e 4.32 para o caso em que a relação R é de equivalência. Ela será útil para o que segue.

Proposição 5.14 *Fixado* $m \in \mathbb{Z},\ m \geq 2$, *vale:*
(a) *Para todo* $a \in \mathbb{Z},\ a \equiv r(mod\ m)$, *onde* r *é o resto da divisão de* a *por* m.
(b) *Para quaisquer* $b,\ c \in \mathbb{Z}$ *são equivalentes:*
(i) $c \equiv b(mod\ m)$, **(ii)** $c \in \overline{b}$, **(iii)** $b \in \overline{c}$, **(iv)** $\overline{c} = \overline{b}$. □

Exemplo. No exemplo anterior todos os números que estão no vértice que contém o 1 deixam resto 1 quando divididos por 5. Eles são todos côngruos módulo 5. Podemos ver que $\overline{1} = \overline{-4} = \overline{-9} = \overline{11} = \cdots$

Agora vamos definir as operações de adição e multiplicação sobre o conjunto $\mathbb{Z}_m$ de modo a torná-lo um anel. Observe que, se tivermos uma operação $*$ sobre um conjunto não vazio E, nada impede de definirmos a seguinte operação sobre $\wp(E)$ (conjunto das partes de E) : $A * B = \{x * y,\ x \in A,\ y \in B\}$. Como $x * y \in E$ para todo $x \in A$, e $y \in B$, vem que $A * B \in \wp(E)$, ou seja, $*$ é de fato uma operação sobre $\wp(E)$, pois o domínio desta função é $\wp(E) \times \wp(E)$ e o contradomínio é $\wp(E)$. Como $\mathbb{Z}_m \subseteq \wp(\mathbb{Z})$, o que se faz é usar as operações de adição e multiplicação definidas sobre $\mathbb{Z}$ para definir as operações de adição e multiplicação módulo m, ou sobre $\mathbb{Z}_m$.

Definição 5.15 Fixado $m > 1,\ m \in \mathbb{Z}$, e dados $\overline{a},\ \overline{b} \in \mathbb{Z}_m$, define-se adição e multiplicação em $\mathbb{Z}_m$ por:

$$\overline{a} \oplus \overline{b} := \overline{a+b}$$
e
$$\overline{a} \odot \overline{b} := \overline{a.b},$$

para todos $\overline{a},\ \overline{b} \in \mathbb{Z}_m$.

Observações 5.16 (1) Para definir estas duas operações, preferimos as notações $\oplus$ e $\odot$ para ficar claro quais operações estamos definindo, e não haver confusão com o símbolo de adição usado nas classes $a + m\mathbb{Z}$. Por exemplo, desde que $\overline{a} = a + m\mathbb{Z}$ e $\overline{b} = b + m\mathbb{Z}$ poderíamos ter escrito:

$$(a+m\mathbb{Z}) + (b+m\mathbb{Z}) = (a+b)+m\mathbb{Z} \quad \text{e} \quad (a+m\mathbb{Z}).(b+m\mathbb{Z}) = ab+m\mathbb{Z},$$

em vez da notação usada anteriormente. Note que $[a] \oplus [b] = [a+b]$ e $[a] \odot [b] = [a.b]$ é outra maneira de denotar a adição e a multiplicação, a qual será descrita simplesmente por $[a]+[b] = [a+b]$ e por $[a].[b] = [ab]$, respectivamente.
(2) Observe que, para somar as classes $\overline{a}$ e $\overline{b}$, soma-se os representantes a e b em $\mathbb{Z}$, resultando em $a + b$, e toma-se a classe da soma obtida, $\overline{a+b}$, em $\mathbb{Z}_m$. O mesmo vale para a multiplicação de classes de equivalência; multiplica-se os representantes e depois volta-se para $\mathbb{Z}_m$, tomando-se as classes do produto obtido.

Antes de passar a alguns exemplos, verifiquemos que estas relações são de fato operações. Porque temos que fazer isto? É porque, para somar ou multiplicar, usam-se os particulares representantes das classes de equivalência e, como as classes de equivalência podem ser representadas por vários elementos, esses representantes não podem influenciar no resultado final (soma ou produto). Por exemplo, em $\mathbb{Z}_4$ como $\overline{1} = \overline{5}$ e $\overline{2} = \overline{6}$ (pois $1 \equiv 5(mod\ 4)$ e $2 \equiv 6(mod\ 4)$), então $\overline{1} + \overline{2}$ deve ser igual a $\overline{5} + \overline{6}$. Ou seja, $\overline{3}$ deve ser igual a $\overline{11}$. Como $3 \equiv 11(mod\ 4)$, pela Proposição 5.14(b) temos que $\overline{3} = \overline{11}$.

O que, exatamente, estamos fazendo, aqui, é somando particulares subconjuntos de $\mathbb{Z}$, ou seja,

$\{\ldots,-7,-3,1,5,9,\ldots\} + \{\ldots,-6,-2,2,6,10,\ldots\} =$
$= \{\ldots,-5,-1,3,7,11,\ldots\}$.

O que foi feito no exemplo acima deve valer sempre e não apenas para as classes $\overline{1}$ e $\overline{2}$ envolvidas e $m = 4$, e sim para todas as classes $\overline{a}, \overline{b} \in \mathbb{Z}_m$, onde $m > 1$ é um inteiro qualquer fixado. Em outras palavras,

Proposição 5.17 *As operações* $+$ *e* $.$ *estão bem definidas sobre* $\mathbb{Z}_m$, *ou seja, dados* $\overline{a} = \overline{c}$, $\overline{b} = \overline{d} \in \mathbb{Z}_m$, *então* $\overline{a} + \overline{b} = \overline{c} + \overline{d}$ *e* $\overline{a}.\overline{b} = \overline{c}.\overline{d}$.

Demonstração: Sejam $\overline{a}$, $\overline{b}$, $\overline{c}$, $\overline{d} \in \mathbb{Z}_m$ com $\overline{a} = \overline{c}$ e $\overline{b} = \overline{d}$. Então, $a \equiv c(mod\ m)$ e $b \equiv d(mod\ m)$ pela Proposição 5.14. Por definição $a = qm + c$. Então $\overline{a} + \overline{b} = \overline{a + b} = \overline{qm + c + b} \stackrel{def}{=} \overline{qm} + \overline{c + b} = \overline{qm} + (\overline{c} + \overline{b})$. Como $\overline{qm} = \overline{0}$, pois $qm \equiv 0(mod\ m)$ vem que $\overline{a}+\overline{b} = \overline{c}+\overline{b}$. Ou seja, fixada a 2^a parcela (da soma), podemos trocar a 1^{a} parcela. Do mesmo modo, prova-se que, fixada a 1^{a} parcela da soma, podemos trocar a 2^{a} parcela. Assim $\overline{a} + \overline{b} = \overline{c} + \overline{b} = \overline{c} + \overline{d}$. Do mesmo modo prova-se que $\overline{a}.\overline{b} = \overline{c}.\overline{d}$. □

Exemplo 5.18 Em $\mathbb{Z}_6$ $\overline{4} + \overline{5} = \overline{9} = \overline{3}$ (pois $9 \equiv 3(mod\ 6)$.) Também podemos proceder assim: $\overline{5} = \overline{-1}$ (pois $5 \equiv -1(mod\ 6)$), então $\overline{4} + \overline{5} = \overline{4} + \overline{-1} = \overline{4 - 1} = \overline{3}$.

Também $\overline{4}.\overline{5} = \overline{4.5} = \overline{20} = \overline{2}$ (pois $20 - 2 = 3.6 \in 6\mathbb{Z}$).

Convém fazer as tabuadas de adição e multiplicação de $\mathbb{Z}_3$.

Já vimos que $\mathbb{Z}_3 = \{\overline{0},\ \overline{1},\ \overline{2}\}$.

Por definição

$\overline{0} + \overline{0} = \overline{0 + 0} = \overline{0}$, $\quad \overline{0} + \overline{1} = \overline{1}$

e

$\overline{1} + \overline{0} = \overline{1 + 0} = \overline{1}$, $\quad \overline{0} + \overline{2} = \overline{0 + 2} = \overline{2}$,

$\overline{2} + \overline{0} = \overline{2}$, $\quad \overline{1} + \overline{1} = \overline{1 + 1} = \overline{2}$,

$\overline{1} + \overline{2} = \overline{2} + \overline{1} = \overline{3} = \overline{0}$ (pela Proposição 5.14(b)),

$\overline{2} + \overline{2} = \overline{2 + 2} = \overline{4} = \overline{1}$ (pois $4 \equiv 1(mod.3)$.

Observe que $\overline{a}+\overline{b}=\overline{r}$, onde r é o resto da divisão de $a + b$ por 3.

Os produtos em $\mathbb{Z}_3$ ficam assim:

$\overline{0}.\overline{0} = \overline{0.0} = \overline{0}$, $\quad \overline{0}.\overline{1} = \overline{1}.\overline{0} = \overline{1.0} = \overline{0}$,
$\overline{1}.\overline{1} = \overline{1.1} = \overline{1}$, $\quad \overline{0}.\overline{2} = \overline{2}.\overline{0} = \overline{0.2} = \overline{0}$,
$\overline{1}.\overline{2} = \overline{2}.\overline{1} = \overline{2.1} = \overline{2}$, $\quad \overline{2}.\overline{2} = \overline{2.2} = \overline{4} = \overline{1}$, (pois $4 \equiv 1(mod\ 3)$).

Como antes temos, também, que $\overline{a}.\overline{b} = \overline{s}$, onde s é o resto da divisão de ab por 3. Daí temos as tábuas

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Observação 5.19 De um modo geral, podemos afirmar que $\overline{a}+\overline{b} = \overline{r}$ em $\mathbb{Z}_m$, onde r é o resto da divisão de $a+b$ por m. Do mesmo modo $\overline{a}.\overline{b} = \overline{s}$, onde s é o resto da divisão de ab por m. Procedendo assim sempre vamos tomar os representantes das classes $\overline{a}+\overline{b}$ e $\overline{a}.\overline{b}$ no conjunto $\{0, 1, 2, \ldots, m-1\}$, pois são estes elementos os possíveis restos da divisão de um número por m.

Teorema 5.20 *Para* $m \geq 2$, $(\mathbb{Z}_m, +, .)$ *é um anel comutativo e unitário com* $U_\bullet(\mathbb{Z}_m) = R_\bullet(\mathbb{Z}_m) = \{\overline{a} \in \mathbb{Z}_m$ tal que $mdc(a, m) = 1\}$.

Demonstração: **(i)** - Associativa: Para todo $\overline{a}$, $\overline{b}$, $\overline{c} \in \mathbb{Z}_m$, $(\overline{a}+\overline{b})+\overline{c} \overset{def}{=\!=} \overline{a+b}+\overline{c} \overset{def}{=\!=} \overline{(a+b)+c} \overset{\text{assoc. em } \mathbb{Z}}{=\!=\!=} \overline{a+(b+c)} \overset{def}{=\!=} \overline{a}+(\overline{b+c}) = \overline{a}+(\overline{b}+\overline{c})$.

(ii) - As propriedades comutativa para a adição e para a multiplicação ficam como exercícios. Também são simples como **(i)** acima, e basta usar as definições e as propriedades de $\mathbb{Z}$.

(iii) - $\overline{0} \in \mathbb{Z}_m$ é o elemento neutro para a adição, pois: $\overline{a}+\overline{0} = \overline{a+0} = \overline{a} = \overline{0+a} = \overline{0}+\overline{a}$, para todo $\overline{a} \in \mathbb{Z}_m$.

(iv) - O oposto de um elemento $\overline{a} \in \mathbb{Z}_m$ é o elemento $\overline{m-a}$, pois $\overline{a}+\overline{m-a} = \overline{a+(m-a)} = \overline{m} = \overline{0} = \overline{(m-a)}+\overline{a}$, para todo $\overline{a} \in \mathbb{Z}_m$.

(v) - A propriedade distributiva também fica como exercício. Basta usar as definições e propriedades de $\mathbb{Z}$.

(vi) - O elemento neutro para a operação de multiplicação é $\overline{1}$, pois $\overline{a}.\overline{1} = \overline{a.1} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_m$. Logo, $\overline{1} = 1_{\mathbb{Z}_m}$.

(vii) - Cálculo de $U_\bullet(\mathbb{Z}_m)$.

Mostraremos que $U_\bullet(\mathbb{Z}_m) = \{\overline{a} \in \mathbb{Z}_m, \text{ tal que } mdc(a,m) = 1\}$.

Seja $A := \{\overline{a} \in \mathbb{Z}_m, \text{ tal que } mdc(a,m) = 1\}$. Se $\overline{a} \in U_\bullet(\mathbb{Z})$, existe $\overline{b} \in \mathbb{Z}_m$, tal que $\overline{a}.\overline{b} = \overline{1}$. Isto significa que $ab \equiv 1(mod\ m)$, ou seja, existe $q \in \mathbb{Z}$, tal que $ab - 1 = qm$, ou ainda, $ab + (-q)m = 1$. Assim, se $d = mdc(a,m)$, então d divide a e d divide m. Daí d divide ab e d divide $(-q)m$. Conseqüentemente, d divide $1 = ab + (-q)m$, ou seja, $d = 1$ (pois $d \geq 0$). Isto mostra que $\overline{a} \in A$.

Reciprocamente, se $\overline{a} \in A$, pela identidade de Bezout existem r e s em $\mathbb{Z}$, tais que $1 = ra + sm$. Considerando esta igualdade em $\mathbb{Z}_m$ e tendo em vista que $\overline{m} = \overline{0}$, temos: $\overline{1} = \overline{ra + sm} = \overline{ra} + \overline{sm} = \overline{r}.\overline{a} + \overline{s}.\overline{m} = \overline{r}.\overline{a} + \overline{s}.\overline{0} = \overline{s}.\overline{a}$. Assim, $\overline{a} \in U_\bullet(\mathbb{Z}_m)$, com $(\overline{a})^{-1} = \overline{s}$. Logo, $U_\bullet(\mathbb{Z}) = A$.

(viii) - Cálculo de $R_\bullet(\mathbb{Z}_m)$. Pela propriedade (5) de operações, sabemos que $U_\bullet(\mathbb{Z}_m) \subseteq R_\bullet(\mathbb{Z}_m)$ e já sabemos que propriedades devem ter os elementos de $U_\bullet(\mathbb{Z}_m)$: seus representantes devem ser primos com m.
Considere então $\overline{a} \in \mathbb{Z}_m$, tal que $d = mdc(a,m) > 1$ e $1 < a \leq m - 1$. Então existem $b, c \in \mathbb{Z}$, tais que $a = bd$ e $m = cd$, com $1 < a,\ c < m$. Daí $\overline{a} \notin R_\bullet(\mathbb{Z}_m)$, pois $\overline{a}.\overline{c} = \overline{a.c} = \overline{b.d.c} = \overline{b.m} = \overline{0} = \overline{a}.\overline{0}$ e $\overline{c} \neq \overline{0}$. Conclusão, se $\overline{a} \notin U_\bullet(\mathbb{Z}_m)$, então $\overline{a} \notin R_\bullet(\mathbb{Z}_m)$, o que equivale à: $a \in R_\bullet(\mathbb{Z}_m)$, então $a \in U_\bullet(\mathbb{Z}_m)$. Logo, $R_\bullet(\mathbb{Z}_m) \subseteq U_\bullet(\mathbb{Z}_m)$. Portanto $U_\bullet(\mathbb{Z}_m) = R_\bullet(\mathbb{Z}_m)$. □

Exemplos 5.21 (1) O anel $(\mathbb{Z}_4, +, .)$ tem como elemento neutro para a adição $\overline{0} = 4\mathbb{Z}$, pois: $\overline{a} + \overline{0} = \overline{a}$ para todo $a \in \{0,1,2,3\}$. Temos que o oposto de $\overline{1} \in \mathbb{Z}_4$ é $\overline{3}$, pois $\overline{1} + \overline{3} = \overline{0}$. Escrevemos $-\overline{1} = \overline{3}$.

Do mesmo modo verifica-se que $-\overline{2} = \overline{2}, \quad -\overline{3} = \overline{1}$.

O elemento neutro para a operação de multiplicação é $\overline{1}$, pois para todo $\overline{a}$ em $\mathbb{Z}_4$, $\quad \overline{a}.\overline{1} = \overline{a}$.

$U_\bullet(\mathbb{Z}_4) = R_\bullet(\mathbb{Z}_4) = \{\overline{1}, \overline{3}\}$ com inversos $(\overline{1})^{-1} = \overline{1}$ e $(\overline{3})^{-1} = \overline{3}$, pois: $\overline{1}.\overline{1} = \overline{1}$ e $\overline{3}.\overline{3} = \overline{9} = \overline{1} \in \mathbb{Z}_4$. O elemento $\overline{2} \notin U_\bullet(\mathbb{Z}_4)$, pois não existe $\overline{x} \in \mathbb{Z}_4$, tal que $\overline{2}.\overline{x} = \overline{1}$ e também não é um elemento regular, pois: $\overline{2}.\overline{0} = \overline{2}.\overline{2} = \overline{0}$ e, no entanto, $\overline{0} \neq \overline{2}$.

(2) Em $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ temos $\overline{0}+\overline{0} = \overline{0}$, $\overline{1}+\overline{4} = \overline{0}$, $\overline{2}+\overline{3} = \overline{0}$. Assim $-\overline{0} = \overline{0}$, $-\overline{1} = \overline{4}$, $-\overline{2} = \overline{3}$, $-\overline{3} = \overline{2}$, $-\overline{4} = \overline{1}$.

O elemento $\overline{1} = \{..., -9, -4, 1, 6, ...\}$ é o elemento neutro para a multiplicação (ele é diferente de $\overline{1}$ em $\mathbb{Z}_4$, por que?)

Como os números 1,2,3,4 são todos primos com o número 5, temos que $U_\bullet(\mathbb{Z}_5) = \mathbb{Z}_5 \setminus \{0\}$, com $(\overline{1})^{-1} = \overline{1}$, $(\overline{2})^{-1} = \overline{3}$ e vice-versa, $(\overline{4})^{-1} = \overline{4}$, pois $\overline{1}^2 = \overline{1}$, $\overline{2}.\overline{3} = \overline{3}.\overline{2} = \overline{1}$, $\overline{4}^2 = \overline{1}$. Veja isto nas tabelas a seguir

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Finalmente, reforçamos que as classes $\overline{a} \in \mathbb{Z}_m$ e $\overline{a} \in \mathbb{Z}_n$ não são as mesmas se $m \neq n$; não têm relação nenhuma uma com a outra, a não ser o fato de que tomamos os mesmos representantes para denotá-las. Por exemplo, a classe de 2 módulo 4 não é inversível módulo 4, enquanto a classe de 2 módulo 5 já o é. Também $-\overline{2} = \overline{2}$ em $\mathbb{Z}_4$ e $-\overline{2} = \overline{3}$ em $\mathbb{Z}_5$.

(3) **(i)** Calcule $U_\bullet(\mathbb{Z}_{15})$ e calcule o inverso de cada elemento de $U_\bullet(\mathbb{Z}_{15})$;

(ii) Resolva o sistema $\begin{cases} \overline{2}x + \overline{6}y &= \overline{5}, \\ \overline{3}x + \overline{4}y &= \overline{0}. \end{cases}$

Solução **(i)** $U_\bullet(\mathbb{Z}_{15}) = \{\overline{a} \in \mathbb{Z}_{15} : mdc(a, 15) = 1\}$. Como 15=3.5, então $\overline{a} \in U_\bullet(\mathbb{Z}_{15})$ se, e somente se, nem 3 nem 5 dividem a. Logo, $\overline{a} \in \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$.

Para calcular o inverso de $\overline{2}$, basta achar x, $1 \leq x \leq 14$, tal que $\overline{2}.\overline{x} = \overline{1}$. A solução é $x = 8$, pois $2.8 = 16 \equiv 1(mod.15)$.

De $(\overline{4})^2 = \overline{16} = \overline{1}$, temos que $(\overline{4})^{-1} = \overline{4}$. As classes $\overline{7}$ e $\overline{13}$ são inversas uma da outra, pois $\overline{7}.\overline{13} = \overline{1}$. Finalmente, $(\overline{14})^{-1} = \overline{14}$ e $(\overline{11})^{-1} = \overline{11}$.

(ii) Da 2ª equação temos: $\overline{4}y = -\overline{3}x = \overline{12}x$ (pois $-\overline{3} = \overline{12}$). Multiplicando por $\overline{4}$ (para isolar y), ficamos com: $\overline{y} = \overline{48}x = \overline{3}x$ (pois $48 \equiv 3(mod\ 15)$). Substituindo na 1ª equação, temos: $\overline{2}x + \overline{18}x = \overline{5}$, ou $\overline{5}x = \overline{5}$. Como $\overline{5}$ não admite inverso, não podemos isolar x a princípio. Mas da equação acima, temos que $5x \equiv 5(mod\ 15)$, ou seja, $5x - 5 = 15q$ para algum $q \in \mathbb{Z}$. Isto equivale à $x - 1 = 3q$ para algum $q \in \mathbb{Z}$, ou seja, $x = 3q + 1 \in \mathbb{Z}$ e basta tomar $1 \leq x \leq 14$. Variando q para obter x neste intervalo, encontramos as soluções: $(\overline{1}, \overline{3})$, $(\overline{4}, \overline{12})$, $(\overline{7}, \overline{6})$, $(\overline{10}, \overline{0})$, $(\overline{13}, \overline{9})$.

(4) Calcular $\sqrt{4}$ em $\mathbb{Z}_{12}$ e resolver $x^2 + \overline{2}x + \overline{9} = \overline{0}$.

Solução $\sqrt{a}$ é o número b do anel $\mathbb{Z}_m$, tal que $b^2 = a$. Então calculemos b^2 para todos $b \in \mathbb{Z}_{12}$. Como $\overline{b^2} = (-b)^2$ qualquer que seja o elemento b de um anel, e $-\overline{b} = \overline{m - b}$ no anel $\mathbb{Z}_m$ temos: $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = (\overline{11})^2 = \overline{1}$, $\overline{2}^2 = (\overline{10})^2 = \overline{4}$, $\overline{3}^2 = \overline{9}^2 = \overline{9}$, $\overline{4}^2 = \overline{8}^2 = \overline{4}$, $\overline{5}^2 = \overline{7}^2 = \overline{1}$, $\overline{6}^2 = \overline{0}$. Logo $\sqrt{\overline{4}} = \overline{2}, -\overline{2}, \overline{4}, -\overline{4}$, ou seja, $\overline{2}$, $\overline{10}$, $\overline{4}$, $\overline{8}$, respectivamente.

Agora $x^2 + \overline{2}x + \overline{9} = \overline{0}$ podemos escrever $(x + \overline{1})^2 + \overline{8} = \overline{0}$, ou seja, $(x + \overline{1})^2 = -\overline{8} = \overline{4}$. Portanto $x + \overline{1} \in \{\overline{2}, \overline{4}, \overline{8}, \overline{10}\}$ e o conjunto solução é $\{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$.

5.2.2 Aritmética Binária Módulo 2^n

Considere o anel $\left(\dfrac{\mathbb{Z}}{2^n\mathbb{Z}}, +, \bullet\right)$, com cada um de seus elementos representados por um elemento r, $0 \leq r \leq 2^n - 1$. Por simplicidade de notação, denotaremos por $\mathbb{Z}_{2^n} = \{0, 1, 2, \ldots, 2^n - 1\}$.

A *representação binária* dos elementos de $\mathbb{Z}_{2^n}$ são as seguintes seqüências de n dígitos "zeros"ou "uns":

$$
\begin{array}{lll}
0 = 00\cdots000 & 1 = 00\cdots001 & 2 = 00\cdots010 \\
3 = 00\cdots011 & 4 = 0\cdots0100 & 5 = 0\cdots0101 \\
6 = 0\cdots0110 & 7 = 0\cdots0111 & \cdots \\
2^n - 1 = 11\cdots11. & &
\end{array}
$$

Então podemos representar todos elementos de $\mathbb{Z}_{2^n}$ como uma n-upla de números $a_{n-1}a_{n-2}\cdots a_1a_0$, onde a_i é zero ou um para todo $i = 1, 2, \ldots$. Em particular, $2^n - 1$ é representado na base 2 por n números 1; $11\cdots1$.

Exemplos 5.22 Os elementos de $\mathbb{Z}_2$ têm a seguinte representação binária: $0 = 0$, $1 = 1$. Os elementos de $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, $(n = 2)$ têm representações binárias

$$0 = 00, \quad 1 = 01, \quad 2 = 10, \quad 3 = 11.$$

Os elementos de $\mathbb{Z}_8 = \{0, 1, \ldots, 7\}$, $(n = 3)$, têm representação binária

$$\begin{array}{llll} 0 = 000, & 1 = 001, & 2 = 010, & 3 = 011, \\ 4 = 100, & 5 = 101, & 6 = 110, & 7 = 111. \end{array}$$

Isto mostra que podemos identificar $\mathbb{Z}_{2^n}$ com B^n, desde que identifiquemos cada elemento de $\mathbb{Z}_{2^n}$ com uma seqüência de 0´s e 1´s, $a_{n-1}a_{n-2}\cdots a_1a_0 \in B^n$, como descrito anteriormente. Vejamos como se traduz as operações do anel $\mathbb{Z}_{2^n}$ quando seus elementos são escritos como seqüências de zeros e uns.

Adição. Efetuemos a adição $110 + 011$ em $\mathbb{Z}_8 \equiv B^3$.

Temos $110 + 011 = 1001 = 1.2^3 + 0.2^2 + 0.2 + 1 = 001$, pois $2^3 = 0$ em $\mathbb{Z}_8$.

Então, para somar n-uplas em $\mathbb{Z}_{2^n}$, somamos normalmente como se fosse números inteiros na base 2, depois reduzimos módulo 2^n, ou seja:

$a_{n-1}a_{n-2}\cdots a_1a_0 + b_{n-1}b_{n-2}\cdots b_1b_0 = c_nc_{n-1}c_{n-2}\cdots c_1c_0 = c_{n-1}c_{n-2}\cdots c_1c_0$, pois $c_n2^n = 0 \in \mathbb{Z}_{2^n}$.

Multiplicação. Para a multiplicação de dois elementos $a = a_{n-1}a_{n-2}\cdots a_1a_0$ e $b = b_{n-1}b_{n-2}\cdots b_1b_0$ de $\mathbb{Z}_{2^n}$ procedemos da seguinte forma: escrevendo $a = a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + \cdots + a_12^1 + a_02^0$ e $b = b_{n-1}2^{n-1} + b_{n-2}2^{n-2} + \cdots + b_12^1 + b_02^0$ obtemos: $a.b = \left(a_{n-1}2^{n-1}+a_{n-2}2^{n-2}+\cdots+a_12^1+a_02^0\right)\left(b_{n-1}2^{n-1}+b_{n-2}2^{n-2}+\cdots+\right.$

$b_1 2^1 + b_0 2^0) = a_{n-1}.b_{n-1} 2^{2n-2} + \cdots + \Big(\sum_{s+r=n-1} a_r b_s \Big) 2^{n-1} + \cdots +$
$(a_1 b_0 + a_0 b_1) 2^1 + a_0 b_0 2^0$.

Como $c.2^r = 0$ em $\mathbb{Z}_{2^n}$ para $c \in \mathbb{Z}$ e $r \geq n$, vem que

$$a.b = \Big(\sum_{s+r=n-1} a_r b_s \Big) 2^{n-1} + \cdots + (a_1 b_0 + a_0 b_1) 2^1 + a_0 b_0 2^0.$$

Logo, podemos escrever $a.b$ como a seguinte n-upla de dígitos uns e zeros:

$$a.b = \Big(\sum_{s+r=n-1} a_r b_s \Big) \ldots (a_1 b_0 + a_0 b_1) a_0 b_0.$$

Exemplo O produto dos elementos $6 = 110$ e $5 = 101$ de $\mathbb{Z}_8 \equiv B^3$ é $(110).(101) = (1.2^2 + 1.2)(1.2^2 + 0.2 + 1.2^0)$ e, usando a propriedade distributiva, encontramos $(110).(101) = 1.2^4 + 1.2^3 + 1.2^2 + 1.2 = 11110_2$. Como $2^4 + 2^3 = 0$ em $\mathbb{Z}_8$, temos que $(110).(101) = 110$ em $\mathbb{Z}_8$.

O seguinte conceito será útil para efetuar de um modo bastante prático a subtração.

Definição 5.23 - *Complemento Binário*

Dado $a \in B = \{0, 1\}$, definimos $a' \in B$ por:

$$a' = 1 - a = \begin{cases} 0 & \text{se } a = 1 \\ 1 & \text{se } a = 0 \end{cases}$$

e dizemos que o elemento $a' \in B$ é o *complemento binário de* $a \in B$. Portanto, o complemento binário de $a \in B$ é o que falta a a para totalizar 1.

Mais geralmente, *o complemento binário de* $a = a_n a_{n-1} \cdots a_2 a_1 \in B^n$ é definido como sendo a n-upla $a' \in B^n$, dada por $a' = a'_n a'_{n-1} \cdots a'_2 a'_1$.

Por exemplo, $(10110)' = (1'0'1'1'0') = 01001 \in B^5$.

Subtração

Subtrair b de a com $a,\ b \in \frac{\mathbb{Z}}{2^n\mathbb{Z}} \equiv B^n$ é somar a com o oposto de b, isto é: $a - b = a + (-b)$. Como vimos anteriormente no anel $\mathbb{Z}_{2^n}$, o oposto de b é $2^n - b$, pois $b + (2^n - b) = 2^n = 0$ em $\mathbb{Z}_{2^n}$. Isto mostra que $-b$ tem a representação binária de $2^n - b$. Mas $2^n - b = (2^n - 1) - b + 1$, e como $2^n - 1 = (10\cdots00)_2 - (00\cdots01)_2$ ($n-1$ zeros), encontramos $2^n - 1 = 11\cdots1_2$ (n 1's). Assim, se b tem a representação $(b_n b_{n-1}\cdots b_2 b_1)_2$, temos que $[(2^n - 1) - b]$ é igual a

$$\begin{array}{cccccccc} & 1 & 1 & 1 & \cdots & 1 & 1 \\ - & b_n & b_{n-1} & b_{n-2} & \cdots & b_2 & b_1 \\ \hline & (b'_n) & (b'_{n-1}) & (b'_{n-2}) & \cdots & (b'_2) & (b'_1), \end{array}$$

que é igual a $b'_n b'_{n-1}\cdots b'_2 b'_1$. Mais geralmente, temos:

Proposição 5.24 *Dado $b = b_n b_{n-1}\cdots b_2 b_1 \in \mathbb{Z}_{2^n} \equiv B^n$, o oposto de b é dado por $b' + 1 = b'_n b'_{n-1}\cdots b'_2 b'_1 + 1$.*

Demonstração: Considere $b = b_n b_{n-1}\cdots b_2 b_1 \in \mathbb{Z}_{2^n}$. Então, $-b = 2^n - b = [(2^n - 1) - b] + 1 = (b'_n b'_{n-1}\cdots b'_2 b'_1)_2 + 1$. Por definição, $-b = b' + 1$. □

Exemplo 5.25 (i) - Calcule $-5 \in \mathbb{Z}_8$.

Solução: Temos que $n = 3$ e $5 = 101$. Então, pela proposição, vem que: $-5 = (101)' + 1 = 010 + 001 = 011$.

(ii) - Calcule 6-5 em $\mathbb{Z}_{16}$.

Solução: Temos, neste caso $n = 4$. Assim representaremos 6 e 5 por suas quádruplas: $6 = 0110$, $5 = 0101$, daí $6 - 5 = 6 + [-5] = 0110 + [(0101)' + 1] = 0110 + [(1010) + (0001)] = 0110 + 1011 = 10001 = 0001$. Observe que $(10000)_2 = 16 = 0$ em $\mathbb{Z}_{16}$.

Observação 5.26 Se calcularmos $a - b \in \mathbb{Z}_{2^n}$ usando o complemento binário, não precisaremos usar o processo de 'emprestar 1' reduzindo 2^i para uma posição abaixo ($(10)_2.2^{i-1}$), pois na subtração de $(2^n - 1) - b$ sempre teremos em cada posições os coeficientes de $2^n - 1$, que são todos 1 e portanto maiores ou iguais aos coeficientes de b. No caso da representação decimal, é como se

tomássemos sempre, de algum modo, o coeficiente 9, que é o maior dos dígitos decimais.

Por exemplo em $\mathbb{Z}_{100}$, efetuaremos 55-36, usando esta técnica adaptada. Observando que aqui $n = 2$, pois $100 = 10^2$ e os dígitos são todos os dez dígitos 0,1,2,...,9, temos que a representação dos números dados são os próprios. Calculemos -36 em $\mathbb{Z}_{100}$ usando o complemento binário: -36=100-36=[(100-1)-36]+1=[99-36]+1. Observe que em 99-36 não precisaremos completar nenhuma das casas, pois tanto 3 como 6 são menores que 9 (o maior dos dígitos). Pelo método comum, teríamos de completar a 1^a casa, pois $5 < 6$. Continuando, temos: -36=63+1 (=complemento decimal +1)=64. Daí, 55-36=55+64=119=19 em $\mathbb{Z}_{100}$.

Elementos regulares - Quando $n > 1$, 2^n não é primo e, portanto, nem todos os elementos de $\mathbb{Z}_{2^n}$ serão regulares para a multiplicação. Logo, a lei de cancelamento permanece válida apenas em casos restritos. Mais precisamente, vimos que:
$U_\bullet(\mathbb{Z}_{2^n}) = R_\bullet(\mathbb{Z}_{2^n}) = \{a \in \mathbb{Z}, 0 < a < 2^n, \text{ tal que } mdc(a, 2^n) = 1\}$. Então, $U_\bullet(\mathbb{Z}_{2^n}) = R_\bullet(\mathbb{Z}_{2^n}) = \{a \in \mathbb{Z},\ 0 < a < 2^n,\ a : \text{ímpar}\}$.

Exemplo 5.27 Em $B^4 \equiv \mathbb{Z}_{16}$, temos que $4.12=0$, ou seja, $(0100).(1100) = (110000) = (0000) \in B^4$. Também, $4.8 = 0$, pois $(0100).(1000) = (0000)$ em $\mathbb{Z}_{16}$, ou seja, $4.12 = 4.8$, mas $12 \neq 8$ em $\mathbb{Z}_{16}$.

O Dígito de Sinal

O anel B^n tem sido usado para a computação prática, apesar da presença de *divisores de zero* (um elemento não-nulo $b \in \mathbb{Z}_{2^n}$ é dito *divisor de zero* se existe um elemento não-nulo $a \in \mathbb{Z}_{2^n}$, tal que $a.b = 0$ em $\mathbb{Z}_{2^n}$). Por exemplo: 4 é divisor de zero em $\mathbb{Z}_8$, pois 4.2=0 em $\mathbb{Z}_8$). Um dos motivos que se usa o conjunto B^n com a identificação $B^n \equiv \mathbb{Z}_{2^n}$ é para introduzir o conceito de dígito de sinal.

A princípio, consideremos $\mathbb{Z}_{2^n} = \{0, 1, 2, \ldots, 2^n - 1\}$ com suas representações binárias. Podemos observar que toda a primeira metade destes números $0, 1, 2, \ldots, 2^{n-1} - 1$ têm dígito inicial zero na sua representação binária: $0 = 00\cdots0_2$, $1 = 00\ldots01_2, \ldots,$

$2^{n-1} - 1 = 011\ldots1_2$. Os outros representantes 2^{n-1}, $2^{n-1}+1$, $\ldots$, $2^n - 1$ de $\frac{\mathbb{Z}}{2\mathbb{Z}}$ têm, nas suas representações binárias, dígito inicial 1. Como cada um destes representantes é o oposto de um dos elementos da primeira metade de $\mathbb{Z}_{2^n}$, convencionaremos que em $\mathbb{Z}_{2^n}$ um elemento é dito *negativo* se ele tem dígito inicial 1 na sua representação binária.

Observe que $2^{n-1} = -2^{n-1}$, pois $2^{n-1} + 2^{n-1} = 2^n = 0$ em $\mathbb{Z}_{2^n}$, ou seja, 2^{n-1} é igual ao seu oposto. Então, para evitar qualquer ambiguidade que possa advir do fato de que $2^{n-1} = 100\cdots0_2$ é seu oposto, convencionaremos que ele *é negativo,* já que tem dígito inicial 1.

Para ficar mais claro, podemos fazer a seguinte representação geométrica com estes representantes de $\mathbb{Z}_{2^n}$: A princípio tomamos $\{0,\ 1,\ 2,\ \cdots,\ 2^{n-1},\ 2^{n-1}+1,\ \cdots,\ \cdots,\ 2^n-1\}$ como representantes de $\mathbb{Z}_{2^n}$ *com suas representações binárias.* Depois deslocamos este subconjunto de $\mathbb{Z}$ para a esquerda na reta real até ficarmos com o subconjunto de representantes:

$$\mathbb{Z}_{2^n} = \{-2^{n-1}, -(2^{n-1}-1), \cdots, -2, -1, 0, 1, 2, \cdots, 2^{n-1}-1\}.$$

Assim, $-1 = 2^n - 1 = 11\cdots11_2$, ou seja, -1 tem a representação binária de $2^n - 1$, $-2 = 2^n - 2 = 11\cdots10_2$, isto é, -2 tem a representação binária de $2^n - 2$, etc.

Exemplo 5.28 (i) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Logo, $n = 2$ e precisamos de 2 casas para a representação binária. $\mathbb{Z}_4 = \{-2, -1, 0, 1\}$ e a representação binária dos elementos são:

$$\begin{array}{rcrcl} -2 & = & 2 & = & 10_2 \\ -1 & = & 3 & = & 11_2 \\ & & 0 & = & 00_2 \\ & & 1 & = & 01_2 \end{array}$$

(ii) $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Logo, $n = 3$ e $\mathbb{Z}_8 \equiv B^3$.

Temos que $\mathbb{Z}_8 = \{-4, -3, -2, -1, 0, 1, 2, 3\}$ e as representações binárias são:

$$\begin{array}{lllll} -4 & = & 4 & = & 100_2 \\ -3 & = & 5 & = & 101_2 \\ -2 & = & 6 & = & 110_2 \\ -1 & = & 7 & = & 111_2 \end{array} \qquad \begin{array}{lll} 0 & = & 000_2 \\ 1 & = & 001_2 \\ 2 & = & 010_2 \\ 3 & = & 011_2 \end{array}$$

Observe o dígito de sinal 1 quando os representantes dos elementos de $\mathbb{Z}_{2^n}$ estão no intervalo $[2^{n-1},\ 2^n-1]$. Só que, neste caso, considera-se a representação binária, tomando-se os representantes com sinais negativos.

Exercícios

(1) Considere as operações $x \oplus y = x+y-1$ e $x \odot y = x+y-xy$ definidas sobre $\mathbb{Q}$ e verifique que $(\mathbb{Q}, \oplus, \odot)$ é um anel. Quais são os elementos neutros $0_{\mathbb{Q}}$ e $1_{\mathbb{Q}}$? Verifique que $a \odot b = 0_{\mathbb{Q}}$ se, e somente se, $a = 0_{\mathbb{Q}}$ ou $b = 0_{\mathbb{Q}}$. Determine $U_{\odot}(\mathbb{Q})$ e $R_{\odot}(\mathbb{Q})$.

(2) Seja $A = \{0_A, 1_A, a\}$ anel unitário. Mostre que só existe um par de tábuas (adição e multiplicação) para A. Pergunta: $1+1=2$? Por quê?

(3) - Faça as tabelas da adição e da multiplicação para os conjuntos $\mathbb{Z}_5$ e $\mathbb{Z}_6$.

(4) Resolver em $\mathbb{Z}_8 : \left\{ \begin{array}{l} \overline{5}x + \overline{2}y = \overline{3} \\ \overline{4}x + \overline{3}y = \overline{1}, \end{array} \right.$ em $\mathbb{Z}_6 : \left\{ \begin{array}{l} \overline{3}x + \overline{4}y = \overline{2} \\ \overline{4}x - \overline{2}y = \overline{0}. \end{array} \right.$

(5) Ache $x \in \mathbb{Z}_9$, tal que $\sqrt{\dfrac{\overline{11}}{\overline{5}}} + \overline{2}x = \overline{4}$.

(6) (a) Sendo $a^{-1}(mod\ m)$ o número $b \in \mathbb{Z},\ 1 \leq b < m$, tal que $ab \equiv 1(mod\ m)$, ache $7^{-1}(mod\ 11)$, $\frac{2}{24}(mod\ 15)$, $4^{-1}(mod\ 41)$, $2^{-1}(mod\ 101)$, $\frac{3}{24}(mod\ 19)$.

(b) Verifique se $\sqrt{\overline{7}} \in \mathbb{Z}_{16}$ e se $\sqrt{\overline{7}} \in \mathbb{Z}_{27}$.

(c) Resolver em $\mathbb{Z}_5$ e em $\mathbb{Z}_8$: $\overline{2}x^2 - \overline{15}x + \overline{5} = \overline{0}$.

(7) Seja $A = \mathbb{R} \setminus \{-1\}$ com a operação $x * y = x+y-xy$. Calcule $\sqrt{-8}$ e $\sqrt{4}$ se existirem.

(8) Determinar o conjunto dos elementos regulares e o conjunto dos elementos inversíveis de cada um dos seguintes anéis: **(a)** $\mathbb{Z}$ **(b)** $\mathbb{Q}$ **(c)** $\mathbb{Z} \times \mathbb{Z}$ **(d)** $\mathbb{Z}_3$ **(e)** $\mathbb{Z}_9$ **(f)** $\mathbb{Z}_{14}$ **(g)** $\mathbb{Z}_2 \times \mathbb{Z}_3$ **(h)** $\mathbb{Z}_{14}$ **(i)** $\mathbb{Z}_4 \times \mathbb{Z}_6$ **(j)** $(\mathbb{Q}, \oplus, \odot)$, onde $a \oplus b = a+b-1$ e $a \odot b = a+b-ab$.

(9) (a) Determine os elementos inversíveis dos anéis: $\mathbb{Z}_{14}$, $\mathbb{Z}_{15}$ e $\mathbb{Z}_{18}$.

(b) Resolver em **(i)** $\mathbb{Z}_{14}$ $\left\{ \begin{array}{rcl} \overline{5}x + \overline{3}y & = & \overline{3}, \\ \overline{2}x + \overline{11}y & = & \overline{11}. \end{array} \right.$

(ii) $\mathbb{Z}_{15}$ $\left\{ \begin{array}{rcl} \overline{7}x + \overline{9}y & = & \overline{5}, \\ \overline{5}x + \overline{12}y & = & \overline{4}. \end{array} \right.$ **(iii)** $\mathbb{Z}_{18}$ $\left\{ \begin{array}{rcl} \overline{5}x + \overline{2}y & = & \overline{1}, \\ x + \overline{11}y & = & \overline{7}. \end{array} \right.$

(10) (i) Resolver em $(\mathbb{Z}_2, +, .)$: $\overline{x}^2 + 2\overline{x} + \overline{1} = \overline{0}$, onde $2\overline{x} = \overline{x} + \overline{x}$.

(ii) Para $a \in \mathbb{Z}_2$, o que é $\sqrt{a} \in \mathbb{Z}_2$? Por que não posso aplicar o algoritmo $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ para resolver a equação acima?

(11) Seja $K = \{0, 1, a, b\}$ um anel, tal que K é comutativo com $1_K = 1$ e $U_\bullet(K) = \{1, a, b\}$. Construa as tábuas de adição e multiplicação deste anel.

(12) (i) Obtenha as duas soluções da equação: $\sqrt{\frac{\overline{12}}{\overline{3}}} + 3x = 7$ em $\mathbb{Z}_5$.

(ii) Calcule $\sqrt{\frac{\overline{13}}{\overline{7}}} + 2x^2 = 0$ em $\mathbb{Z}_9$.

(iii) Qual a representação ternária das soluções em **(ii)**?

(13) Explique o conceito de dígito de sinal e dê um exemplo.

(14) Usando complemento binário, quando for o caso, calcule em $B^5 \equiv \mathbb{Z}_{32}$ **(i)** 18, -18, -4, -7, **(ii)** $11011_2 + (-01110_2) + 11111_2$ **(iii)** $(-4) \cdot (-7)$ (na base 2).

(15) Faça a Aritmética Ternária Módulo 3^n, ou seja, desenvolva em $\mathbb{Z}_{3^n}$ a teoria de adição módulo 3, complemento ternário e subtração em $\mathbb{Z}_{3^n}$.

5.3 Anéis Booleanos

Já vimos que uma terna $(A, \oplus, .)$ (ou simplesmente A se as operações "$\oplus$" e "$\cdot$" estiverem claras no contexto) é um anel se $(A, \oplus)$ é um grupo comutativo e a operação "$\cdot$" é associativa e é distributiva em relação a operação "$\oplus$". Um anel $(A, \oplus, \cdot)$ é dito *unitário* se a operação "$\cdot$" admite elemento neutro, ou seja, se existe um elemento em A (que convém indicá-lo por 1_A), tal que, para todo $x \in A$, $x \cdot 1_A = 1_A \cdot x = x$.

Definição 5.29 Um anel $(A, \oplus, \cdot)$ é dito um *anel booleano* (ou *anel de Boole*) se $(A, \oplus, .)$ é um anel unitário e idempotente; isto é: $\exists 1_A$ e $\forall x \in A,\ x^2 = x$.

Exemplos 5.30 **(A) (i)** Seja $B = \{0, 1\}$ com adição e multiplicação definidas por

$+$	0	1
0	0	1
1	1	0

$\bullet$	0	1
0	0	0
1	0	1

É fácil verificar que $(B, +, .)$ é um anel booleano e fica como exercício. No entanto, observamos que o elemento neutro para a adição é $0_B = 0$ e $-0 = 0, \quad -1 = 1$. O elemento neutro para a multiplicação é $1_B = 1$ e $x^2 = x$ para $x = 0,\ 1$.

(ii) Seja $B^n = B \times B \times \cdots \times B$, com as operações assim definidas: $(a_1, a_2, \ldots, a_n) \oplus (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$ e $(a_1, a_2, \ldots, a_n) \bullet (b_1, b_2, \ldots, b_n) = (a_1.b_1, a_2.b_2, \ldots, a_n.b_n)$,
onde as operações de adição e multiplicação em cada coordenada são feitas em B, como definidas em (i).

Fica como exercício a verificação de que $(B^n, \oplus, \bullet)$ é um anel booleano. Em particular, se $0_B = 0$ e $1_B = 1$, então $0_{B^n} = (0, 0, \ldots, 0), \quad 1_{B^n} = (1, 1, \ldots, 1)$. Temos ainda o oposto de $a = (a_1, a_2, \ldots, a_n)$, denotado por $\ominus a$, como sendo
$(-a_1, -a_2, \ldots, -a_n)$.

(B) Seja E um conjunto não vazio qualquer e $A = \wp(E)$, com as operações $\oplus$ e $\cdot$ assim definidas: $x \oplus y = \big(x \cup y\big) \setminus \big(x \cap y\big)$ e $x.y = x \cap y$ para todos $x,\ y \in \wp(E)$, onde $\cup$ e $\cap$ são as operações de reunião e intersecção de subconjuntos. $(A, \oplus, .)$ é um anel de Boole.

(i) Já vimos que vale a propriedade associativa: $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ para todos $x,\ y,\ z \in A$. Assim, apenas a representaremos via diagrama de Venn.

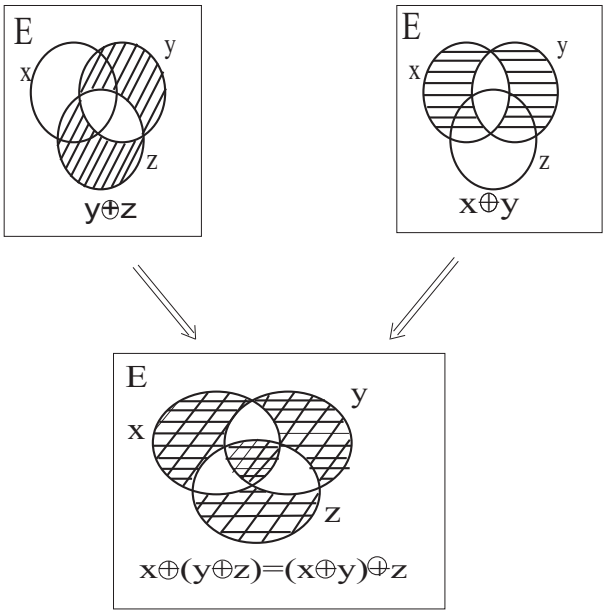


Figura 5.2: Associativa

(ii) $x \oplus y = x \cup y \setminus x \cap y = y \cup x \setminus y \cap x = y \oplus x$ (pois reunião e intersecção de subconjuntos são operações comutativas).
(iii) O elemento neutro de A para adição é $\emptyset$, pois para todo $x \in \wp(E), x \oplus e = (x \cup \emptyset) - (x \cap \emptyset) = x - \emptyset = x = \emptyset \oplus x$.
(iv) O oposto de $x \in A$ é o próprio x.

De fato, $x \oplus x = (x \cup x) - (x \cap x) = x - x = \emptyset$.

(v) Já sabemos que a operação de intersecção é associativa.
(vi) A propriedade distributiva: $x.(y \oplus z) = xy \oplus xz$ se resume aqui a $x \cap (y \cup z \setminus y \cap z) = \big((x \cap y) \cup (x \cap z)\big) \setminus x \cap y \cap z$, que pode ser provada usando diagramas de Venn (fica como exercício).
(vii) Para todo $x \in A$, $x^2 = x \cap x = x$. Logo, $(A, \oplus, .)$ é idempotente.
(viii) O elemento neutro para a operação de intersecção de subconjuntos é o elemento $1_A = E \in A$, pois $x \cap E = x$, $\forall x \in A$. Logo, A é unitário.

Proposição 5.31 *Todo anel booleano A é comutativo e $\ominus a = a$, para todo $a \in A$.*

Demonstração: Por hipótese, $a \oplus b = (a \oplus b)^2 = a^2 \oplus ab \oplus ba \oplus b^2$. Como A é idempotente, vem que $a \oplus b = a \oplus ab \oplus ba \oplus b$. Cancelando a e b e somando $\ominus ab$ em ambos os membros, obtemos: $\ominus ab = ba$. Fazendo $b = 1$, obtemos $a = \ominus a, \forall a \in A$; que é a 2^a afirmação da proposição. Daí $ab = (\ominus a)b = \ominus ab = ba$. □

Duas noções importantes em um anel booleano são:

Definição 5.32 Dado um anel booleano $(A, \oplus, \cdot)$, define-se *o complemento de* $a \in A$ por: $\overline{a} := a \oplus 1$, e para $a, b \in A$ define-se a *união* b e denota-se por $a + b$ o elemento $a + b := a \oplus b \oplus a.b$.

Quando $A = \wp(U)$, estes conceitos coincidem com os conceitos de complemento e reunião de subconjuntos no anel booleano $(A, \triangle, \cap)$. Veja Exercício (9)(f) do capítulo 3.

Dado um anel booleano A, as operações união e complemento exibem uma longa lista de propriedades familiares reunidas aqui, no seguinte teorema.

Teorema 5.33 *Em todo anel booleano* $(A, \oplus, \cdot)$, *e para todos* $a, b, c \in A$, *a operação binária "+" e a operação unária "—" têm as propriedades:*

(a) $0+0=0$, $0+1=1+0=1+1=1$	**(b)** $a + b = b + a$
(c) $a+(b+c)=(a+b)+c$	**(d)** $a \cdot (b+c)=a \cdot b+a \cdot c$
(e) $a+b \cdot c = (a+b)(a+c)$	**(f)** $a + a = a$
(g) $a + 0 = a$	**(h)** $a + 1 = 1$
(i) $a+\overline{a}=1, \quad a \cdot \overline{a}=0$	**(j)** $\overline{(a+b)}=\overline{a} \cdot \overline{b}$ e $\overline{a \cdot b}=\overline{a}+\overline{b}$
(k) $\overline{(\overline{a})} = a$	**(l)** $a \oplus b = a \cdot \overline{b} + \overline{a} \cdot b$

Demonstração: Faremos alguns ítens e os outros ficam como exercícios.
(a) $1+1 \stackrel{\text{def}}{=\!=} (1\oplus 1)\oplus 1\cdot 1 \stackrel{a=\ominus a}{=\!=\!=} 0\oplus 1 = 1$.
(b) $a+b \stackrel{\text{def}}{=\!=} a\oplus b\oplus a\cdot b \stackrel{\text{comut}}{=\!=\!=} b\oplus a\oplus b\cdot a = b+a$.
(d) $ab+ac \stackrel{\text{def}}{=\!=} ab\oplus ac\oplus ab\cdot ac = ab\oplus ac\oplus a^2bc$ pelas propriedades associativa do anel e comutativa, dada pela Proposição 5.31. Como $a^2 = a$, usando também a propriedade distributiva, temos: $ab + ac = a\cdot(b\oplus c\oplus bc) \stackrel{\text{def}}{=\!=} a(b+c)$.
(f) $a+a = a\oplus a\oplus a\cdot a \stackrel{\text{Prop.5.31}}{=\!=\!=\!=} a^2 = a$.
(j) $\overline{(a+b)} \stackrel{\text{def}}{=\!=} 1\oplus(a+b) \stackrel{\text{def}}{=\!=} 1\oplus(a\oplus b\oplus ab) = (1\oplus a)\oplus(1\oplus a)b = (1\oplus a)(1\oplus b) = \overline{a}\overline{b}$. □

5.4 Álgebras Booleanas

Definição 5.34 Um conjunto A, junto com duas operações binárias $+$ e $\cdot$, é uma *álgebra booleana* se, e somente se, verifica os seguintes axiomas:

(A.1) (Comutatividade). $\forall a, b \in A,\ a+b=b+a, \quad ab = ba$.

(A.2) (Existência de elementos neutros). $\exists 0_A,\ 1_A \in A$, tais que $a + 0_A = a$ e $a\cdot 1_A = a,\ \forall a \in A$. Em geral, denota-se 0_A e 1_A apenas por 0 e 1, respectivamente, se o anel A estiver claro no contexto.

(A.3) (Distributividade). Para todos $a, b, c \in A, \quad (a+b)c = ac+bc \quad$ e $\quad a+bc = (a+b)(a+c)$.

(A.4) (Existência do complemento). Para cada $a \in A,\ \exists b \in A$, tal que $a+b=1$ e $a\cdot b = 0$. O elemento b será denotado por $\overline{a}$.

Observação 5.35 (1) O conjunto de axiomas apresentados na definição anterior se deve a Huntington (1904). Entretanto, existem outros conjuntos de axiomas (equivalentes a estes) definidores de álgebra booleana, a saber: os axiomas devido a George Boole (1854).

(2) O conjunto de axiomas apresentado é independente, isto é, não existem axiomas que possam ser derivados dos demais. Também são consistentes, ou seja, não podemos derivar um absurdo destes

axiomas. Para exemplificar em que consiste um axioma ser dependente dos demais, temos que a comutatividade da adição é conseqüência dos demais axiomas em um anel unitário, pois: para todos $a, b \in A$, tem-se:

$(a+b)(1+1) = a(1+1) + b(1+1) = a+a+b+b.$

E por outro lado

$(a+b)(1+1) = (a+b)1 + (a+b)1 = a+b+a+b.$

Daí, cancelando a à esquerda e b à direita, obtemos: $a+b = b+a$. Assim, temos um exemplo de um conjunto de axiomas sobre um conjunto que não é independente.

(3) Em geral, exigimos que 0_A e 1_A sejam diferentes para que A seja diferente do anel nulo; $A = \{0\}$ (Exercício).

Exemplo 5.36 Sejam $U \neq \emptyset$ e $A = \wp(U)$. Então $(A, \cup, \cap)$ é álgebra booleana, onde $0 = \emptyset$ e $1 = U$, $\overline{a} = U \setminus a$ (Prove estas afirmações usando diagramas de Euler-Venn).

Definição 5.37 *Dual de uma Proposição*

Dada uma proposição p em uma álgebra booleana, a proposição *dual* de p é uma proposição q obtida de p, trocando $+$ por $\cdot$ e vice-versa e 1 por 0 e vice-versa, onde eles ocorrerem na proposição p.

Exemplo: $0+a = a$ é a dual de $1 \cdot a = a$. Claro que $1 \cdot a = a$ também é a dual de $0 + a = a$.

Teorema 5.38 Princípio da Dualidade.

O dual de qualquer teorema numa álgebra booleana também é um teorema. Em outras palavras: "Toda proposição ou identidade algébrica dual de outra proposição ou identidade algébrica verdadeira permanece verdadeira".

Além disso, se um teorema é consequência de "tais"e "tais" proposições, o dual se demonstra do mesmo modo, dualizando cada passo dado na demonstração. □

Exemplo 5.39 O dual de $a + ab = a$ é $a(a+b) = a$.

Para se "convencer" do teorema, observe a dualidade dos axiomas definidores de uma álgebra booleana.

Agora, daremos os principais teoremas de uma álgebra booleana. Cada proposição conterá uma proposição e sua dual com exceção de uma proposição que será sua própria dual. Claro que, provada uma proposição, sua dual também ficará provada devido ao princípio da Dualidade.

A título de ilustração da natureza da dualidade, na próxima proposição faremos as duas demonstrações. Deve-se observar que os passos em cada demonstração são duais dos passos da outra demonstração e, para cada passo, o mesmo postulado ou teorema é usado como justificativa.

Proposição 5.40 Idempotência

Para todo elemento a de uma álgebra booleana A, tem-se: $a + a = a \quad e \quad a \cdot a = a$.

Demonstração:

$$\begin{array}{rcll} a & = & a+0 & \text{A.2} \\ & = & a+a.\overline{a} & \text{A.4} \\ & = & (a+a)(a+\overline{a}) & \text{A.3} \\ & = & (a+a).1 & \text{A.4} \\ & = & a+a & \text{A.2} \end{array} \qquad \begin{array}{rcll} a & = & a.1 & \text{A.2} \\ & = & a(a+\overline{a}) & \text{A.4} \\ & = & a.a+a.\overline{a} & \text{A.3} \\ & = & a.a+0 & \text{A.4} \\ & = & a.a & \text{A.2} \end{array}$$

□

Proposição 5.41 Identidades

Para todo a pertencente a A, $\quad a + 1 = 1 \quad e \quad a \cdot 0 = 0$.

Demonstração:

$a + 1 \overset{\text{A.2}}{=\!=} (a+1).1 \overset{A.4}{=\!=} (a+1)(a+\overline{a}) \overset{\text{A.3}}{=\!=} a + 1.\overline{a} \overset{\text{A.2}}{=\!=} a + \overline{a} \overset{\text{A.4}}{=\!=} 1.$ □

Proposição 5.42 Absorção

Para todos $a, b \in A, \quad a + ab = a \quad e \quad a(a+b) = a$.

Demonstração:

$a + ab \overset{\text{A.2}}{=\!=} a \cdot 1 + ab \overset{A.3}{=\!=} a(1+b) \overset{\text{Prop.5.41}}{=\!=\!=} a \cdot 1 \overset{\text{A.3}}{=\!=} a.$ □

Proposição 5.43 *Em qualquer álgebra booleana A, cada uma das operações binárias "+" e "·" é associativa, isto é, para todos $a, b, c \in A$, tem-se:*

$$(a+b)+c = a+(b+c) \quad e \quad (ab)c = a(bc).$$

Demonstração: Usaremos um artifício antes:

(1) $a + a(bc) = a + (ab)c$, pois:

$$\begin{array}{rcll} a + a(bc) & = & a & \text{Prop.5.42} \\ & = & a(a+c) & \text{Prop.5.42} \\ & = & (a+ab)(a+c) & \text{Prop.5.42} \\ & = & a + (ab)c & \text{A.3} \end{array}$$

(2) $\overline{a} + a(bc) = \overline{a} + (ab)c$, pois:

$$\begin{array}{rcll} \overline{a} + a(bc) & = & (\overline{a}+a)(\overline{a}+bc) & \text{distr.} \\ & = & 1.(\overline{a}+bc) & \text{A.4} \\ & = & \overline{a}+bc & \text{A.2} \\ & = & (\overline{a}+b)(\overline{a}+c) & \text{distr.} \\ & = & [(\overline{a}+b).1](\overline{a}+c) & \text{A.2} \\ & = & [(\overline{a}+b)(a+\overline{a})](\overline{a}+c) & \text{A.4} \\ & = & [\overline{a}+(ab)](\overline{a}+c) & \text{distr.} \\ & = & \overline{a}+(ab)c & \text{distr.} \end{array}$$

Agora, multiplicando ambas as equações membro a membro, temos:

$$\begin{array}{rcll} [a+a(bc)].[\overline{a}+a(bc)] & = & [a+(ab)c].[\overline{a}+(ab)c] & \\ a.\overline{a}+a(bc) & = & a.\overline{a}+(ab)c & \text{distr.} \\ 0+a(bc) & = & 0+(ab)c & \text{A.4} \\ a(bc) & = & (ab)c & \text{A.2} \end{array}$$

□

Observação 5.44 Assim, não há ambiguidade ao se escrever abc, uma vez que $(ab)c = a(bc)$.

Proposição 5.45 *O elemento $\overline{a}$ associado ao elemento a em uma álgebra booleana A é único.*

Demonstração: Suponhamos que existem $b, c \in A$, tais que $a + b = 1$, $ab = 0$ e $a + c = 1$, $a.c = 0$. Então
$b = b.1 = b(a+c) = ba+bc = 0+bc = ac+bc = (a+b)c = 1.c = c$.

□

Corolário 5.46 *Para todo elemento a de uma álgebra booleana A, temos* $\overline{(\overline{a})} = a$.

Demonstração: Basta ver que: $\overline{a} + a = 1$ e $a \cdot \overline{a} = 0$. Logo, $\overline{(\overline{a})} = a$, por A.4. □

Corolário 5.47 *Em toda álgebra booleana* $\overline{0} = 1$ *e* $\overline{1} = 0$.

Demonstração: Segue das definições. Pela Proposição 5.45 há unicidade. □

Proposição 5.48 *Para todos elementos a, b de uma álgebra booleana A, tem-se:* $\overline{ab} = \overline{a} + \overline{b}$ *e* $\overline{a + b} = \overline{a} \cdot \overline{b}$

Demonstração: $ab + \overline{a} + \overline{b} \overset{\text{distr.}}{=\!=} (a + \overline{a} + \overline{b})(b + \overline{a} + \overline{b}) = (1 + \overline{b})(1 + \overline{a}) = 1 \cdot 1 = 1$ e $ab \cdot (\overline{a} + \overline{b}) \overset{\text{distr.}}{=\!=} ab \cdot \overline{a} + ab \cdot \overline{b} = a\overline{a} \cdot b + a \cdot b\overline{b} = 0 \cdot b + a \cdot 0 = 0 + 0 = 0$. Por definição, $\overline{ab} = \overline{a} + \overline{b}$ e, pelo Teorema 5.38, a proposição está provada. □

5.4.1 Ordens

O lema seguinte é importante para a definição de uma relação de ordem parcial sobre uma álgebra booleana.

Lema 5.49 *Em uma álgebra booleana, as proposições abaixo são equivalentes:*

(a) $ab = a$ **(b)** $a + b = b$ **(c)** $\overline{a} + b = 1$ **(d)** $a\overline{b} = 0$.

Demonstração: (a) $\Rightarrow$ (b) $a + b \overset{\text{(a)}}{=} ab + b \overset{\text{A.3}}{=} (a+1)b \overset{\text{Prop.5.41}}{=\!=} 1.b \overset{\text{A.2}}{=} b$.
(b) $\Rightarrow$ (c) $\overline{a} + b = \overline{a} + (a + b) = (\overline{a} + a) + b = 1 + b = 1$ (Justifique!).

(c) $\Rightarrow$ (d) $a\overline{b} = \overline{\overline{a\overline{b}}} = \overline{\overline{a} + \overline{\overline{b}}} = \overline{\overline{a} + b} \overset{\text{hip.}}{=} \overline{1} = 0$ (Justifique!).

(d) $\Rightarrow$ (a) $ab = ab + 0 \overset{\text{(d)}}{=} ab + a\overline{b} = a(b + \overline{b}) = a \cdot 1 = a$. Isto conclui a demonstração. □

Definição 5.50 Definimos a seguinte relação sobre uma álgebra booleana A : Para quaisquer dois elementos $a, b \in A$, $a\mathsf{R}b$ se a e b satisfazem uma das condições (e portanto todas condições) do Lema anterior.

Lema 5.51 *A relação* R *definida acima sobre uma álgebra booleana* A *é uma relação de ordem.*

Demonstração: Reflexiva. Segue-se do Lema 5.49(a) e da Proposição 5.40.

Anti-simétrica. Se $a\mathsf{R}b$ e $b\mathsf{R}a$ pelo Lema 5.49(b), $a + b = b$ e $b + a = a$. Pela comutatividade, temos $a = b$.

Transitiva. Se $a\mathsf{R}b$ e $b\mathsf{R}c$, então pelo Lema 5.49(a) temos: $ab = a$ e $bc = b$. Substituindo, em ac vem que: $ac = (ab)c = a(bc) = ab = a$. Logo, $a\mathsf{R}c$. □

Notação 5.52 : Sejam a, b pertencentes a uma álgebra booleana A. Se $a\mathsf{R}b$, denotaremos por $a \preceq b$ (que se lê:"*a precede b*". Além disso, se $a \neq b$, denotaremos este fato por $a \prec b$ ("*a precede estritamente b*").

Exemplos 5.53 (1) Considere a álgebra booleana $(\wp(U), \bigcup, \bigcap)$. Por definição e Lema 5.49(a), temos que $a \preceq b$ se, e somente se, $a \cap b = a$, ou seja, se, e somente se, $a \subseteq b$.

(2) Seja $A = (B^n, +, \bullet)$ com as operações assim definidas:

$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$,

$(a_1, a_2, \ldots, a_n) \bullet (b_1, b_2, \ldots, b_n) = (a_1.b_1, a_2.b_2, \ldots, a_n.b_n)$.

Então $a \preceq b$ se, e somente se, $a \bullet b = a$, ou seja, se, e somente se, $(a_1.b_1, \ldots, a_n.b_n) = (a_1, \ldots, a_n)$ com $a_i, b_i \in B = \{0, 1\}$. Como $a_i.b_i = 1$ se, e somente se, $a_i = b_i = 1$, vem que $a \preceq b \Longleftrightarrow a_i \leq b_i \in B$.

Para verificar esta condição, basta ver se a i-ésima coordenada de b é 1 quando a i-ésima coordenada de a é 1.

Teorema 5.54 *Para todos* $x,\ y,\ z$ *em uma álgebra booleana* A, *tem-se:*
(a) (i) $[x \preceq y \ \ e \ \ x \preceq z] \implies x \preceq yz$. **(ii)** $[x \preceq y,\ z \preceq y] \implies x + z \preceq y$.

(b) (i) $x \preceq y \implies x \preceq y + z, \quad \forall z \in A$. **(ii)** $y \preceq x \implies yz \preceq x,\ \forall z \in A$.

(c) $x \preceq y \iff \overline{y} \preceq \overline{x}$. **(d)** $0 \leq x \preceq 1,\ \forall x \in A$.

Demonstração: (a)(i) $x \cdot yz = xy \cdot z \overset{\text{hip.}}{=} xz \overset{\text{hip.}}{=} x$. Por definição e Lema 5.49(a), $x \preceq yz$.
(a)(ii) $(x+z)y = xy+zy \overset{\text{Lema5.49}}{=\!=} x+z$, o que implica que $x+z \preceq y$.
(b) Exercício.
(c) $x \preceq y \overset{\text{Lema5.49(c)}}{\iff} \overline{x} + y = 1 \iff [0 = \overline{1} = \overline{\overline{x} + y} = \overline{(\overline{x})}\overline{y} = \overline{y}\overline{(\overline{x})}] \overset{\text{Lema5.49(d)}}{\iff} \overline{y} \preceq \overline{x}$.
(d) Desde que $0 \cdot x = 0$ e $x.1 = x$, pelo Lema 5.49(a) temos que $0 \preceq x \preceq 1$. □

Corolário 5.55 *Para quaisquer* $x,\ y$ *em uma álgebra booleana* A, *existem* $\sup\{x, y\}$, $\inf\{x, y\}$ *e* $\sup\{x, y\} = x + y, \ \ \inf\{x, y\} = x \cdot y$. *Além disso, para todos* $x_1,\ x_2, \ldots, x_n \in A$ *(*$n \geq 1$*), temos que* $\sum_{i=1}^{n} x_i = \sup\{x_1, x_2, \ldots, x_n\}$ *e* $\prod_{i=1}^{n} x_i = \inf\{x_1, x_2, \ldots, x_n\}$.

Demonstração: Como $x \preceq x$ por (b)(ii), temos $x \preceq x + y$. Logo, $x + y$ é um limite superior de $\{x, y\}$. Por (a)(ii), segue-se que $x + y = \sup\{x, y\}$.
Do mesmo modo por (a)(i) e (b)(ii), prova-se que $xy = \inf\{x, y\}$. O resto segue-se por indução em n. □

Nota: Um conjunto parcialmente ordenado U, para o qual existem $\inf\{x, y\}$ e $\sup\{x, y\}$ para quaisquer $x,\ y \in U$, é dito uma *reticulado*. Assim, o Corolário anterior garante que toda álgebra booleana é uma reticulado.

O Teorema de Stone afirma que toda álgebra de Boole é isomorfa a uma álgebra de conjuntos $(\wp(U), \cup, \cap)$ para U conveniente.

Nossa intenção de agora em diante é provar este Teorema demonstrando que "toda álgebra de Boole é isomorfa a $(B^n, +, .)$ para algum $n \geq 1$, n natural". A versão original pode ser vista no exercício 10. O teorema será provado no caso de A ser atômica. Dizer que duas álgebras são isomorfas significa que existe uma bijeção entre elas que preserva as estruturas algébricas envolvidas, no caso: adição, multiplicação e complementação. Isto significa que a bijeção comuta com as operações das álgebras.

Definição 5.56 Um *átomo* em uma álgebra booleana A é um elemento $a \neq 0$, tal que, para todo $b \in A$, $0 \preceq b \preceq a$, então $b = 0$ ou $b = a$ (ou seja: $\forall b \in A \setminus \{0\}$, $ab = 0$, ou $ab = a$). Isto afirma que a é um átomo, se entre 0 e a não existe elemento.

Proposição 5.57 **(1)** *Se a é um átomo e $a \preceq x_1 + \cdots + x_n$, então $a \preceq x_i$ para algum i.*
(2) *Se a é um átomo, então, para todo $b \in A$, $a \preceq b$ ou (exclusivo) $a \preceq \overline{b}$.*

Demonstração: **(1)** Se $a \not\preceq x_i$, então $ax_i = \inf\{a, x_i\} = 0$, para todo $i = 1, 2, \ldots, n$. Daí $a = a(x_1 + \cdots + x_n) = ax_1 + \cdots + ax_n = 0 + \cdots + 0 = 0$, o que é absurdo.

(2) Se $a \not\preceq b$, então $ab = 0$, pois a é um átomo. Trocando b por $\overline{b}$ temos $a(\overline{\overline{b}}) = 0$. Por definição (item (d)) $a \preceq \overline{b}$. □

Exemplo 5.58 (1) Para qualquer $U \neq \emptyset$, os átomos de $(\wp(U), \bigcup, \bigcap)$ são os conjuntos unitários $\{x\} \subseteq U$;
(2) Os átomos em $(B^n, \bigcup, \bigcap)$ são as n-uplas $(x_1, x_2, \ldots, x_n) \in B^n$ com exatamente um dos x_i igual a "um".

Definição 5.59 Uma álgebra booleana A é dita *atômica* se, para todo elemento não nulo $b \in A$, existe um átomo $a \in A$ que precede b.

Proposição 5.60 *Toda álgebra booleana finita é atômica.*

Demonstração: Seja $b \neq 0$. Se b não é um átomo, existe b_1, $0 \prec b_1 \prec b$ e, portanto, $b_1 = bb_1$. Se b_1 não é um átomo, então existe b_2, $0 \prec b_2 \prec b_1 \prec b$. Daí $b_2 = b_2 b_1 = b_2 b_1 b$. Continuando, encontramos uma cadeia $0 \prec b_n \prec \cdots \prec b_1 \prec b_0 = b$, onde $n \geq 1$ e $b_k = b_k b_{k-1} \cdots b_1 b$, $k = 1, \ldots, n$. Como A é finita, esta cadeia estaciona em algum n e, neste caso, b_n será um átomo.□

Para o que segue, A é uma álgebra booleana atômica e $S = \{a_i, i \in I\}$ o conjunto dos átomos de A.

Proposição 5.61 *Para cada $x \in A$, seja $T_x \subseteq S$ o conjunto de átomos de A abaixo de x, isto é: $t \in T_x \iff t \in S$ e $t \preceq x$.*

Então, $x = \sum_{t \in T_x} t$ e nenhuma outra soma de átomos é igual a x.

Demonstração: Como x é um limite superior de T_x, pelo Corolário 5.55 segue-se que $\sup T_x = \sum_{t \in T_x} t \preceq x$. Se $supT_x \prec x$, então $x \not\preceq \sup T_x$ e pelo Lema 5.49(d) $x\overline{supT_x} \neq 0$. Como A é atômica, existe um átomo $a \preceq x.\overline{\sup T_x} = \inf\{x, \overline{\sup T_x}\}$. Assim, $a \preceq x$ e $a \preceq \overline{\sup T_x} \overset{\text{Pro5.57(2)}}{\iff} a \preceq x$ e $a \not\preceq \sup T_x$, ou seja, $a \in T_x$ e a não está incluído na soma $\sum_{t \in T_x} t$, o que é absurdo. Então, $x = \sup T_x = \sum_{t \in T_x} t$.

Se existe outra soma de átomos $x = \sum_{u \in U}$, $U \subseteq S$, então existe $t_0 \in T \setminus U$ ou $u_0 \in U \setminus T$. Daí $t_0 = t_0(\sum_{t \in T_x} t) = t_0 x = t_0(\sum_{u \in U} u) = \sum_{u \in U} t_0 u = 0 + \cdots + 0 = 0$ (pois 0 é o ínfimo de dois átomos distintos) ou $u_0 = u_0(\sum_{u \in U} u) = u_0 x = u_0(\sum_{t \in T_x} t) = \sum_{t \in T_x} u_0 t = 0 + \cdots + 0 = 0$. Em qualquer caso temos uma contradição. □

Corolário 5.62 *Sendo $S = \{a_i, i \in I\}$ o conjunto de todos os átomos de A, tem-se que, para todo $x \in A$, $x = \sum_{i \in I} \alpha_i a_i$, onde $\alpha_i \in \{0, 1\}$, $\alpha_i = 1$ se, e somente se, $a_i \preceq x$. Em particular, $\sum_{i \in I} a_i = 1$. Além disso, esta escritura como soma de átomos de A é única.*

Demonstração: Nada a demonstrar, tendo em vista a Proposição 5.61 e o Teorema 5.54(d). □

Exemplo 5.63 Seja $(A, +, \cdot) = (\wp(\mathbb{N}), \bigcup, \bigcap)$. Então o conjunto de átomos de A é $S = \{\{i\}, i \in \mathbb{N}\}$. Temos que $1_A = \sum_{i \in \mathbb{N}} \{i\} = \bigcup_{i \in \mathbb{N}} \{i\} = \mathbb{N}$.

Observe o caráter não finito de $\sum$.

Definição 5.64 Sejam $(A, \perp, \odot)$ e $(D, +, .)$ duas álgebras booleanas. Um isomorfismo de A em D é uma aplicação: $\varphi : A \longrightarrow D$ que satisfaz:

(i) φ é bijetora, (ii) $\varphi(x \perp y) = \varphi(x) + \varphi(y)$,

(iii) $\varphi(x \odot y) = \varphi(x).\varphi(y)$, (iv) $\varphi(\overline{x}) = \varphi(x)'$,

onde $\overline{x}$ e y' são os complementos de x e y em A e D, respectivamente.

Neste caso, dizemos que as álgebras A e D são isomorfas e escrevemos $A \simeq D$ ou $A \xrightarrow{\sim} D$.

Teorema 5.65 Teorema de Stone (Caso Finito).
Seja $(A, \perp, \odot)$ uma álgebra de Boole finita. Então A é isomorfa a $(B^n, +, \cdot)$, onde n é o número de átomos de A.

Demonstração: Como A é finita o conjunto S de átomos de A também é finito. Seja $S = \{a_1, \ldots, a_n\}$. Pelo Corolário 5.62 todo elemento x de A se escreve na forma $x = \alpha_1 a_1 \perp \cdots \perp \alpha_n a_n$. Definimos $\varphi : A \longrightarrow B^n$ por $\varphi(x) = (\alpha_1, \ldots, \alpha_n)$ e mostraremos que φ é um isomorfismo de álgebras.

Esta função é claramente sobrejetora e, devido ao Corolário 5.62, é também injetora. Observemos que $a_i^2 = a_i$ e $a_i \odot a_j = 0$ se $i \neq j$. Assim:
$\overline{x} = \alpha_1' a_1 \perp \cdots \perp \alpha_n' a_n$, onde $\alpha_i' = 1 + \alpha_i$ em B, e, se $y = \beta_1 a_1 \perp \cdots \perp \beta_n a_n$ é outro elemento de A, então:
$\varphi(x \perp y) = \varphi((\alpha_1 + \beta_1)a_1 \perp \cdots \perp (\alpha_n + \beta_n)a_n) \overset{\text{def.}}{=\!=}$
$(\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n) = (\alpha_1, \alpha_2, \ldots, \alpha_n) + (\beta_1, \beta_2, \ldots, \beta_n)$ em B^n. Logo, $\varphi(x \perp y) = \varphi(x) + \varphi(y)$.

Também:

$$\varphi(x \odot y) = \varphi\Big(\big(\sum_{i=1}^{n} \alpha_i a_i\big)\big(\sum_{j=1}^{n} \beta_j a_j\big)\Big) = \varphi\Big(\sum_{i,j=1}^{n} \alpha_i \beta_j (a_i \odot a_j)\Big) \overset{*}{=\!=}$$

$$\varphi\Big(\sum_{i=1}^{n} (\alpha_i.\beta_i) a_i\Big) = (\alpha_1.\beta_1, \ldots, \alpha_n.\beta_n) =$$

$(\alpha_1, \ldots, \alpha_n).(\beta_1, \ldots, \beta_n) = \varphi(x).\varphi(y)$,
onde (*) segue da observação acima. Finalmente

$\varphi(\overline{x}) = \varphi(\overline{\alpha_1 a_1 \perp \cdots \perp \alpha_n a_n}) = \varphi(\alpha_1' a_1 \perp \cdots \perp \alpha_n' a_n) =$
$= (\alpha_1', \ldots, \alpha_n') = (\alpha_1, \ldots, \alpha_n)' = \varphi(x)'$. Logo, φ é um isomorfismo

de álgebras, o que conclui o Teorema. □

Agora, o seguinte Corolário é de verificação simples.

Corolário 5.66 *Toda álgebra booleana finita tem* 2^n *elementos e, reciprocamente, para cada* $n \in \mathbb{N}$, *existe uma álgebra booleana com* 2^n *elementos, a saber:* $(B^n, +, \bullet)$. □

Exercícios

(1) (a) Verifique que os conceitos de união de elementos e complemento de elementos em um anel booleano coincidem com os conceitos de união de subconjuntos e complementar de subconjuntos quando o anel booleano é o anel $(\wp(U), \triangle, \cap)$ do exemplo 5.30(B).
(b) Faça as tabuadas do anel $(B, \oplus, \cdot)$, onde $B = \{0, 1\}$, e a tabuada de $(B, +)$. Este anel é booleano?
(2) Faça as tábuas das operações da álgebra booleana $(B, +, \cdot)$, onde $B = \{0, 1\}$.
(3) Use a Proposição 5.41 e prove que $0_A = 1_A$ se, e somente se, $A = \{0\}$, qualquer que seja a álgebra booleana A.
(4) Seja $(A, \oplus, \cdot)$ um anel booleano, defina $a + b = a \oplus b \oplus ab$. Mostre que $(A, +, \cdot)$ é uma álgebra booleana, onde $\overline{a} = 1 \oplus a$.
(5) Agora, faça a recíproca do exercício (4), ou seja, a partir de uma álgebra booleana $(A, +, \cdot)$, defina $a \oplus b = \overline{a}b + a\overline{b}$ e mostre que $(A, \oplus, \cdot)$ é um anel booleano.

Como consequência dos exercícios 4 e 5 tem-se que álgebras e anéis booleanos estão em correspondência 'um a um'. Você consegue provar isto?
(6) (a) Considere o conjunto dos divisores positivos de 30;
$D^+(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$, com as operações: $a + b = mmc(a, b)$ e $a \cdot b = mdc(a, b)$. Verifique que $(D^+(30), +, \cdot)$ é uma álgebra de Boole e, para $a, b \in D^+(30)$, $a \preceq b$ se, e somente se, $a|b$.
(b) Considere $n(\geq 1)$ primos distintos 2 a 2; $p_1, \ldots, p_n$ e $a = p_1 p_2 \cdots p_n$. Mostre que $D^+(a)$, com as operações de mmc e mdc, é uma álgebra booleana.
Sugestão Sejam: $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$, $c = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$, $d = p_1^{\delta_1} \cdots p_n^{\delta_n}$, onde $\beta_i, \gamma_i, \delta_i, \in B = \{0, 1\}$, $\forall i$. Para provar, por exemplo, que

$b + cd = (b + c)(b + d)$ basta mostrar que $mmc(b, mdc(c, d)) = mdc(mmc(b, c), mmc(b, d))$, o que é a mesma coisa que provar que $max\{\beta_i, min\{\gamma_i, \delta_i\}\} = min\{max\{\beta_i, \gamma_i\}, max\{\beta_i, \delta_i\}\} = (\beta_i + \gamma_i).(\beta_i + \delta_i)$, onde + e . são as operações booleanas da álgebra $B = \{0,\ 1\}$. Agora, estude o caso $\beta_i \leq \gamma_i \leq \delta_i$ e os outros 5 casos possíveis.

Prove que $\overline{b} = \dfrac{a}{b} = p_1^{\beta'_1} p_2^{\beta'_2} \cdots p_n^{\beta'_n}$, onde $\beta' = 0$ se $\beta = 1$, e $\beta' = 1$ se $\beta = 0$.

(7) **(a)** Mostre que não existe álgebra booleana com 3 elementos.
(b) Mostre que, se $(A, +, \cdot)$ é uma álgebra de Boole finita, então $|A| = 2.n$ para algum $n \geq 1$.
Sugestão: Mostre que, se existe $x \in A - \{0, 1, x_1, y_1, \ldots, x_n, y_n\}$, (onde $n \geq 0$ e $\overline{x_i} = y_i$), então $x \neq \overline{x}$ e $x, \overline{x} \notin \{0, 1, x_1, y_1, \ldots, x_n, y_n\}$.
(c) Como você prova que $|A| = 2^n$?

(8) Mostre que, se $x + y = 0$ (em uma álgebra booleana), então $x = y = 0$.

(9) Você é capaz de dar exemplos de álgebras booleanas não atômicas? Quais?

(10) Seja A uma álgebra booleana atômica, com $\{a_i, i \in I\}$ o conjunto de átomos de A. Prove que:

$(A, +, \cdot) \xrightarrow{\sim} (\wp(\{a_i, i \in I\}), \bigcup, \bigcap)$, mostrando que a aplicação:

$$\begin{array}{rccl} \varphi\colon & A & \longrightarrow & \wp(\{a_i, i \in I\}) \\ & x & \longrightarrow & \varphi(x) = \{a_i,\ \text{tal que}\ a_i \leq x\} \end{array}$$

satisfaz as condições da Definição 5.64.

Sugestão: Se $x \neq y \in A$, então $x\overline{y} \neq 0$ ou $y\overline{x} \neq 0$. Agora use o raciocínio da demonstração da Proposição 5.61 para provar que φ é injetora. Para a sobrejeção de φ, considere o Corolário 5.62.

(11) **(i)** Seja $B^\infty = \{(a_i)_{i \in \mathbb{N}} = (a_1, a_2, \ldots, a_n, \ldots);\quad a_i \in \{0, 1\}\}$.
Defina: $(a_i)_{i \in \mathbb{N}} \perp (b_i)_{i \in \mathbb{N}} = (a_i + b_i)_{i \in \mathbb{N}}$ e $(a_i)_{i \in \mathbb{N}} \odot (b_i)_{i \in \mathbb{N}} = (a_i.b_i)_{i \in \mathbb{N}}$.
Mostre que $(B^\infty, \perp, \odot)$ é uma álgebra booleana. Quais são os átomos de A?

(ii) Mostre que a e $\overline{a}$ são átomos em uma álgebra booleana A se, e somente se, $A = \{0, a, \overline{a}, 1\}$.

(12) Seja A uma álgebra booleana atômica. Mostre que:
(i) Se A é enumerável, então o conjunto de átomos de A é enumerável.
(ii) A recíproca é sempre falsa.
(iii) Conclua que não existe álgebra booleana atômica enumerável.
Sugestão: Teorema de Stone e Exercício (11).
(13) Fazer as tábuas de adição e multiplicação e o diagrama de Hasse das álgebras booleanas $(A_i, +, \cdot)$, $i = 1, 2$, onde **(i)** $A_1 = \{0, a, \overline{a}, 1\}$,
(ii) $A_2 = \{0, a, b, c, \overline{a}, \overline{b}, \overline{c}, 1\}$, onde a, b, c são átomos de A_2.
(iii) Seja $x \oplus y = \overline{x}y + x\overline{y}$. Faça as tábuas desta operação para $\oplus$ definida sobre A_1 e A_2.
(14) Seja A o conjunto de proposições sobre um conjunto não vazio S. Para p, $q \in A$, definimos $p\mathsf{R}q$ se, e somente se, p e q são logicamente equivalentes.

(i) Prove que R é uma relação de equivalência sobre A.

(ii) Seja $B = \frac{A}{\mathsf{R}}$ o conjunto quociente desta relação. Para $[p]$, $[q] \in B$, definimos $[p] \vee [q] = [p \vee q]$ e $[p] \wedge [q] = [p \wedge q]$. Mostre que $(B, \vee, \wedge)$ é uma álgebra booleana onde: $\overline{[p]} = [\neg p]$, $0_B = [F]$ (F uma contradição), $1 = [V]$ (V uma tautologia).

(iii) Seja E a álgebra booleana gerada por $[p]$ e $[q]$, $[p] \neq [q]$, fazendo uso das operações booleanas $\vee$, $\wedge$ e $\neg$. Mostre que $(E, \vee, \wedge)$ é uma álgebra booleana com $0_E = F$(contradição) e $1_E = V$(tautologia).

(iv) Mostre que os átomos de E são $[p] \wedge [q]$, $[p] \wedge \neg[q]$, $\neg[p] \wedge [q]$, $\neg[p] \wedge \neg[q]$ e mostre que E tem 16 elementos.

(v) Mostre que a ordem de E é caracterizada por: $[p] \leq [q]$ se, e somente se, $p \Longrightarrow q$. Construa o diagrama de Hasse de E.
(vi) Ache todos os elementos especiais de $E \setminus \{1\}$.

5.5 Álgebras das Funções Booleanas

Definição 5.67 Seja A uma álgebra booleana. A *álgebra das funções booleanas* n-árias sobre A é gerada pelas funções projeções $P_n^i : A^n \longrightarrow A$, definida por: $P_n^i(x_1, \ldots, x_n) = x_i$, e pelas funções constantes $h(x_1, \ldots, x_n) = a \in A$, fazendo uso das operações

booleanas: adição, multiplicação e complementação de funções. Em outras palavras, uma *função booleana* em n variáveis é uma função de A^n em A obtida recursivamente como sendo:

(i) as projeções P_n^i e as funções constantes h são funções booleanas,

(ii) Se f e g são funções booleanas, então $\overline{f}$, fg e $f+g$ definidas por $\overline{f}(X) = \overline{f(X)}$, $(fg)(X) = f(X)g(X)$ e $(f+g)(X) = f(X) + g(X)$, onde $X = (x_1, x_2, \ldots, x_n)$, são funções booleanas.

Devido às leis de DeMorgan ($\overline{xy} = \overline{x} + \overline{y}$ e $\overline{x+y} = \overline{x} \cdot \overline{y}$), à absorção e a outras propriedades de uma álgebra booleana, não há unicidade na expressão de uma função booleana. Por exemplo, a função booleana em duas variáveis $f(x_1, x_2) = \overline{x_1.x_2}$ também é dada por: $f(x_1, x_2) = \overline{x_1} + \overline{x_2}$. No entanto, existe uma forma padrão, ou canônica, (em realidade duas, devido ao princípio da dualidade) em que podemos expressar todas funções booleanas. No teorema a seguir, cada função booleana se expressa como somas de monômios $f(e)x_1^{e_1} \cdots x_n^{e_n}$, onde cada $x_i^{e_i}$ é x_i se $e_i = 1$, ou $\overline{x}_i$ se $e_i = 0$. Como $x_i^2 = x_i$ e $x_i + x_i = x_i$, não ocorrem potências naturais nem múltiplos naturais de x_i maiores que x_i em cada monômio das expressões do teorema a seguir. Antes de enunciá-lo, vejamos um exemplo.

Exemplo 5.68 (1) Sejam A uma álgebra booleana e $f : A \times A \longrightarrow A$ dada por $f(x, y) = \overline{x.y}$. Então $f(x, y)$ é uma função booleana, pois ela é gerada pelas projeções $P_2^1(x, y) = x$ e $P_2^2(x, y) = y$, fazendo uso de complementação: $f(x, y) = \overline{P_2^1(x, y).P_2^2(x, y)}$.

Alguns valores para $f(x, y)$, são:

$f(0,0) = \overline{0.0} = \overline{0} = 1$, $f(0,1) = \overline{0.1} = \overline{0} = 1$. $f(1,1) = \overline{1.1} = \overline{1} = 0$.

(2) Todas funções booleanas de uma variável se expressam do seguinte modo: $f(x) = f(0)\overline{x} + f(1)x$. Por exemplo, se $A = \{0, 1, a, \overline{a}\}$ e $g\colon A \longrightarrow A$ definida por $g(x) = a$ para todo $x \in A$. Então $g(x) = a \cdot 1 = a(x + \overline{x}) = ax + a\overline{x}$.

(3) Todas funções booleanas de duas variáveis se expressam do seguinte modo: $f(x,y) = f(0,0)\overline{x}\overline{y} + f(1,0)x\overline{y} + f(0,1)\overline{x}y + f(1,1)xy$. Por exemplo, se h é definida por $h(x,y) = x + y$, então $h(x,y) = x.1 + y.1 = x(y+\overline{y}) + y(x+\overline{x}) = x\overline{y} + \overline{x}y + xy$.

Veja que a função $f(x,y) = \overline{x.y}$ do exemplo **(1)** se escreve como $f(x,y) = \overline{x.y} = \overline{x} + \overline{y} = \overline{x}.1 + \overline{y}.1 = \overline{x}.(y+\overline{y}) + \overline{y}.(x+\overline{x}) = \overline{x}.\overline{y} + x\overline{y} + \overline{x}y$.

5.5.1 As Formas Canônicas

Teorema 5.69 *Seja A uma álgebra booleana. Então toda função booleana $f : A^n \longrightarrow A$ se expressa por:*

$$f(x_1,\ldots,x_n) = \sum_{e\in B^n} f(e_1,\ldots,e_n)x_1^{e_1}\cdots x_n^{e_n},$$

onde $e = (e_1,\ldots,e_n)$ e $x_i^{e_i} = x_i$, se $e_i = 1$, e $x_i^{e_i} = \overline{x}_i$, se $e_i = 0$.

De um modo compacto, podemos escrever: $f(x) = \sum_{e\in B^n} f(e)x^e$.

Demonstração: **(i)** $n = 1$

Neste caso, o teorema diz que $f(x) = f(0)\overline{x} + f(1)x$.

Comecemos com as funções geradoras.

(a) $f\colon A \longrightarrow A$, $f(x) = a \in A$, $\forall x \in A$. Então $f(0) = f(1) = a$ e $f(1)x + f(0)\overline{x} = ax + a\overline{x} = a(x+\overline{x}) = a\cdot 1 = a = f(x)$.

(b) $f\colon A \longrightarrow A$, $f(x) = x$, $\forall x \in A$. Então $f(0) = 0$ e $f(1) = 1$. Assim $f(0)\overline{x} + f(1)x = 0\overline{x} + 1\cdot x = x = f(x)$.

Suponhamos, agora, que f, $g\colon A \longrightarrow A$ possam ser expressas na forma canônica e seja $h(x) = \overline{f(x)}$. Mostremos que $h\colon A \longrightarrow A$ se expressa na forma canônica. Pelas leis de DeMorgan e propriedade distributiva, temos:

$h(x) = \overline{f(x)} = \overline{f(1)x + f(0)\overline{x}} = (\overline{f(1)x}).(\overline{f(0)\overline{x}}) = (\overline{f(1)}+\overline{x})(\overline{f(0)}+x) = \overline{f(1)}\cdot\overline{f(0)} + \overline{f(1)}x + \overline{f(0)}\overline{x} + \overline{x}x = \overline{f(1)}\cdot\overline{f(0)}.(x+\overline{x}) + \overline{f(1)}x + \overline{f(0)}\overline{x} = \overline{f(1)}.\overline{f(0)}x + \overline{f(1)}\cdot\overline{f(0)}\overline{x} + \overline{f(1)}x + \overline{f(0)}\overline{x} = \overline{f(1)}x(\overline{f(0)}+1) + \overline{f(0)}\overline{x}(\overline{f(1)}+1) = \overline{f(1)}x + \overline{f(0)}\overline{x} = h(1)x + h(0)\overline{x}$.

Se $j(x) = f(x)g(x)$, então $j(x) = (f(0)\overline{x} + f(1)x)(g(0)\overline{x} + g(1)x) = f(0)g(0)\overline{x}^2 + f(1)g(1)x^2 + (f(0)g(1)\overline{x}x + f(1)g(0)x\overline{x}) =$

$= j(0)\overline{x} + j(1)x + [f(0)g(1) + f(1)g(0)].0 = j(0)\overline{x} + j(1)x.$

Se $k(x) = f(x) + g(x)$, então
$k(x) = (f(0)\overline{x}+f(1)x)+(g(0)\overline{x}+g(1)x) = (f(0)+g(0))\overline{x}+(f(1)+g(1))x = k(0)\overline{x} + k(1)x.$

Isto prova que toda função booleana f de uma variável sobre A pode ser expressa na forma: $f(x) = f(0)\overline{x} + f(1)x.$

(ii) Suponhamos válido para toda função Booleana de $n-1$ variáveis sobre A, e seja $f : A^n \longrightarrow A$ uma função booleana sobre A. Se não ocorre x_n e $\overline{x}_n$ em f (isto é: f independe de x_n e de $\overline{x}_n$), então o resultado segue da hipótese de indução. Se f depende de x_n ou de $\overline{x}_n$, então podemos escrever $f(x) = f(x_1, \ldots, x_n) = x_n g(x_1, \ldots, x_{n-1}) + \overline{x}_n h(x_1, \ldots .x_{n-1})$, onde g, h: $A^{n-1} \longrightarrow A$ são funções booleanas. Por hipótese de indução, temos:

$$f(x) = x_n\Big(\sum_{u\in B^{n-1}} g(u)x_1^{u_1}x_2^{u_2}\cdots x_{n-1}^{u_{n-1}}\Big) +$$

$$+ \overline{x}_n\Big(\sum_{v\in B^{n-1}} h(v)x_1^{v_1}x_2^{v_2}\cdots x_{n-1}^{v_{n-1}}\Big) =$$

$$= \sum_{(u_1,\ldots,u_{n-1},1)\in B^n} g(u)x_1^{u_1}\cdots x_{n-1}^{u_{n-1}}x_n^1 +$$

$$\sum_{(v_1,\ldots,v_{n-1},0)\in B^n} h(v)x_1^{v_1}\cdots x_{n-1}^{v_{n-1}}x_n^0 =$$

$$= \sum_{(e_1,\ldots,e_n)\in B^n} f(e_1,\ldots,e_n)x_1^{e_1}\cdots x_n^{e_n},$$

pois $g(u) = f(u)$ e $h(v) = f(v)$, uma vez que g e h são restrições da função f. □

Observação: A expressão de f no Teorema 5.69 é dita *forma disjuntiva normal* e será vista com mais detalhe, adiante, quando também, trataremos da forma conjuntiva normal de f qualquer que seja a função $f : A^n \longrightarrow A$.

Exemplos 5.70 (1) Seja $A = \{0, 1, a, \overline{a}\}$ uma álgebra booleana. Construa a forma canônica de função $f : A^2 \longrightarrow A$ dada pela tabela:

x	y	$f(x,y)$
0	0	a
0	1	0
1	0	$\overline{a}$
1	1	1

Solução

Na forma canônica $f(x,y) = f(0,0)\overline{x}.\overline{y} + f(1,0)x\overline{y} + f(0,1)\overline{x}y + f(1,1)xy$. Substituindo os valores dados, obtemos: $f(x,y) = a\overline{x}.\overline{y} + \overline{a}x\overline{y} + xy$.

Observemos que, sendo dados os valores da função nos vértices (ou seja: nos pontos $(e_1, \ldots, e_n)$ de $B^n \subseteq A^n$), a função que se obtém é única. No entanto, se são dados valores que a função assume em pontos diferentes destes, podem haver várias funções ou, até mesmo, nenhuma função booleana que satisfaça aquelas condições dadas.

A técnica usada para se determinar tais funções, que assumem valores previamente dados em alguns pontos distintos dos vértices, é a técnica do 'coeficiente indeterminado', ou seja: resolve-se um sistema de m equações e n variáveis sobre a álgebra booleana.

Para a resolução normalmente se usam as propriedades da álgebra como complementação, idempotência, etc. Por exemplo, multiplicando cada equação por uma variável ou seu complemento, obtém-se outras equações geralmente mais simples. O seguinte exemplo ilustra esta técnica.

(2) Dê uma função booleana, de duas variáveis, definida em A^2, onde $A = \{0, a, \overline{a}, 1\}$, tal que

x	y	$f(x,y)$
0	a	a
1	1	1
$\overline{a}$	a	$\overline{a}$
a	1	a

Solução

A forma canônica de f é $f(x,y) = f(1,1)xy + f(1,0)x\overline{y} + f(0,1)\overline{x}y + f(0,0)\overline{x}.\overline{y}$. Substituindo os valores dados, obtemos as equações:

$a = f(0,a) = f(0,1)a + f(0,0)\overline{a}$ $(\star)$

$1 = f(1,1)$, e $\overline{a} = f(\overline{a},a) = f(1,0)\overline{a} + f(0,1)a$ $(\star\star)$

$a = f(0,1) = f(1,1)a + f(0,1)\overline{a}$ $(\star\star\star)$

Multiplicando $(\star)$ por a, obtemos: $a = f(0,1)a$, ou seja: $a = \min\{f(0,1), a\}$. Logo

$$f(0,1) = a \text{ ou } f(0,1) = 1, \qquad (I)$$

Veja o exercício (13)(i) da seção anterior.

Multiplicando a 2ª equação de $(\star\star)$ por a, obtemos: $0 = f(0,1)a$. Logo

$$f(0,1) = \overline{a} \text{ ou } f(0,1) = 0. \qquad (II)$$

De (I) e (II) temos uma contradição. Portanto tal função não existe.

Observação 5.71 Esta função não existe como função booleana; é claro que, como função de $A \times A \longrightarrow A$ qualquer, pode existir até mesmo várias funções que satisfazem as condições dadas. Por exemplo, definindo $f(x,y) = 0$ para todo $(x,y) \notin \{(0,a),(1,1),(\overline{a},a),(a,1)\}$.

Formas Disjuntiva e Conjuntiva Normais

Sabemos pelo Teorema de Stone que uma álgebra booleana finita tem 2^n elementos e é isomorfa a B^n, através da aplicação: $\varphi : A \longrightarrow B^n$, definida por $\varphi\big(\sum_{i=1}^{n} \alpha_i a_i\big) = (\alpha_1, \ldots, \alpha_n)$, onde $\{a_1, \ldots, a_n\}$ é o conjunto de átomos de A. Então, considerar funções

$f : A^m \longrightarrow A$ é equivalente a considerar funções
$f : B^{mn} \longrightarrow B^n$.

Uma função $f : B^{mn} \longrightarrow B^n$ é da forma
$f(x_1, \ldots, x_{mn}) = \big(f_1(x_1, \ldots, x_{mn}), f_2(x_1, \ldots, x_{mn}), \ldots, f_n(x_1, \ldots, x_{mn})\big)$. Agora, se f e g são funções de B^{mn} em B^n, as funções $f.g : B^{mn} \longrightarrow B^n$ e $f + g : B^{mn} \longrightarrow B^n$ definidas por $(f.g)(X) = f(X).g(X)$ e por $(f + g)(X) = f(X) + g(X)$, onde $X = (x_1, x_2, \ldots, x_{mn})$, são efetuadas coordenada a coordenada. Então, para estudar a álgebra das funções booleanas de A^m em A, essencialmente, basta estudar a álgebra das funções booleanas de B^k, $(k = mn)$ em B, que são as funções coordenadas típicas. Tendo, ainda, que B^k pode ser identificado com $\mathbb{Z}_{2^k}$ como álgebra de Boole, (não como o anel de restos módulo 2^k), quando se escreve todos os elementos de $\mathbb{Z}_{2^k} = \{\overline{0}, \overline{1}, \ldots, \overline{2^k - 1}\}$ na base dois, podemos considerar uma função de B^k em B como sendo uma função $f : \mathbb{Z}_{2^k} \longrightarrow B$ definida por $f(\overline{x}) = f(a_1, a_2, \ldots, a_n)$, onde $\overline{x} = (a_1 a_2 \cdots a_k)_2$.

Por exemplo, para $k = 4$, $f(\overline{30}) = f(\overline{14}) = f(1, 1, 1, 0)$, pois $30 \equiv 14(mod.16)$ e $14 = (1110)_2$.

Definição 5.72 As funções booleanas $p_e : B^n \longrightarrow B$ dadas por: $p_e(X) = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$, onde $X = (x_1, \ldots, x_n)$ e $e = (e_1 \cdots e_n)_2 \in \mathbb{Z}_{2^n}$, são chamadas de *funções minimais* ou *polinômios minimais*, e as funções booleanas $s_e(X) = \overline{p_e(X)} = x_1^{\overline{e}_1} + x_2^{\overline{e}_2} + \cdots + x_n^{\overline{e}_n}$, são chamadas de *funções maximais* ou *polinômios maximais* da álgebra booleana B^n. Isto faz sentido pois, em $B = \{0, 1\}$, tem-se que $p_e(X) \preceq p_{i,e_i}(X)$ e $p_{i,\overline{e}_i} \preceq s_e(X)$, onde $p_{i,j}(X) = x_i^j$ para $i = 1, \ldots, n \quad j = 0, 1$.

Adiante veremos que esses polinômios geram, em algum sentido, todas as funções booleanas de B^n em B.
Exemplo: Se $n = 5$, então $p_{11} = \overline{x}_1 x_2 \overline{x}_3 x_4 x_5$ e $s_{11} = x_1 + \overline{x}_2 + x_3 + \overline{x}_4 + \overline{x}_5$, pois $11 = (01011)_2$.

Exemplo 5.73 Para $n = 3$ temos as seguintes funções minimais e maximais sobre a álgebra B^3.

$\mathbb{Z}_8$	B^3		
i	$(e_1e_2e_3)$	p_i	s_i
0	000	$\overline{x}_1.\overline{x}_2.\overline{x}_3$	$x_1+x_2+x_3$
1	001	$\overline{x}_1.\overline{x}_2x_3$	$x_1+x_2+\overline{x}_3$
2	010	$\overline{x}_1.x_2.\overline{x}_3$	$x_1+\overline{x}_2+x_3$
3	011	$\overline{x}_1.x_2.x_3$	$x_1+\overline{x}_2+\overline{x}_3$
4	100	$x_1.\overline{x}_2.\overline{x}_3$	$\overline{x}_1+x_2+x_3$
5	101	$x_1.\overline{x}_2.x_3$	$\overline{x}_1+x_2+\overline{x}_3$
6	110	$x_1.x_2.\overline{x}_3$	$\overline{x}_1+\overline{x}_2+x_3$
7	111	$x_1.x_2.x_3$	$\overline{x}_1+\overline{x}_2+\overline{x}_3$

Lema 5.74 *Para todos* $e=(e_1e_2\cdots e_n)_2$, $j=(j_1j_2\cdots j_n)_2 \in \{0,1,\ldots,2^n-1\}$, *temos* $p_e(j)=\delta_{ej}$ e $s_e(j)=\overline{\delta}_{ej}$, *onde* $\delta_{ej}=1$ *se* $e=j$ *e* $\delta_{ej}=0$ *se* $e\neq j$.

Demonstração: Temos $p_e(X)=x_1^{e_1}\cdots x_n^{e_n}$. Então $p_e(j)=j_1^{e_1}j_2^{e_2}\cdots j_n^{e_n}=1$ se, e somente se, $j_i^{e_i}=1, \forall i$ se, e somente se, $j_i=e_i$ em $B=\{0,1\}$ se, e somente se, $e=(e_1e_2\cdots e_n)=(j_1j_2\cdots j_n)=j$. Agora, como $s_e(X)=\overline{p_e(X)}$, vem que $s_e(j)=\overline{p_e(j)}=\overline{\delta}_{ej}$ e o lema está concluído. □

O seguinte teorema dá um modelo padrão em que se expressam todas funções booleanas de B^n em B.

Teorema 5.75 *Todas funções booleanas* $f\colon B^n \longrightarrow B$ *podem ser representadas de modo único em cada uma das formas:*

$$f(X)=\sum_{e=0}^{2^n-1} f(e)p_e(X) \quad \Big(=\sum_{e\in B^n} f(e)p_e(X)\Big)$$

chamada de forma disjuntiva normal de f *e*

$$f(X)=\prod_{e=0}^{2^n-1}\Big(f(e)+s_e(X)\Big),$$

chamada de forma conjuntiva normal de f. □

De um modo grosseiro, podemos dizer que f é uma soma de produtos (de funções) e também é um produto de somas (de funções).

Abreviadamente, *f.d.n.* e *f.c.n.* significarão *forma disjuntiva normal* e *forma conjuntiva normal*, respectivamente.

Observemos que, como $f(e)$ é zero ou um, na f.d.n. de f só figuram as funções minimais $p_e(X)$, para as quais $f(e) = 1$. 'Dualmente' cada um dos fatores que aparecem na f.c.n. de f será suprimido se $f(e) = 1$. Isto porque o fator $f(e)+s_e(j) = 1+s_e(j) = sup\{1, s_e(j)\} = 1$ em $B = \{0, 1\}$. Antes de demonstrar o teorema, vamos à um exemplo.

Exemplo 5.76 Vamos achar a f.d.n. e a f.c.n. da função booleana $f : B^3 \longrightarrow B$ dada pela tabela:

$\mathbb{Z}_8$	B^3	
e	$e_1e_2e_3$	$f(e)$
0	000	0
1	001	1
2	010	1
3	011	0
4	100	0
5	101	0
6	110	0
7	111	1

A f.d.n. de f é dada por:

$$f(X) = f(0)p_0(X)+f(1)p_1(X)+f(2)p_2(X)+f(3)p_3(X)+$$

$$+f(4)p_4(X) + f(5)p_5(X) + f(6)p_6(X) + f(7)p_7(X)$$

que, pela observação acima, nos dá $f(X) = p_1(X)+p_2(X)+p_7(X)$. Pela tabela do exemplo anterior $f(X) = \overline{x}_1.\overline{x}_2x_3+\overline{x}_1x_2\overline{x}_3+x_1x_2x_3$.

A f.c.n. de f é dada por:

$f(X) = \big(f(0) + s_0(X)\big)\big(f(1) + s_1(X)\big)\big(f(2) + s_2(X)\big)\big(f(3) + s_3(X)\big)\big(f(4)+s_4(X)\big)\big(f(5)+s_5(X)\big)\big(f(6)+s_6(X)\big)\big(f(7)+s_7(X)\big)$. Novamente, pela observação acima, temos $f(X) = s_0(X) \cdot s_3(X) \cdot$

$s_4(X) \cdot s_5(X) \cdot s_6(X)$, para todo $X = (x_1, x_2, x_3)$ em B^3. Pela tabela do exemplo anterior, temos:
$f(X) = (x_1+x_2+x_3)(x_1+\overline{x}_2+\overline{x}_3)(\overline{x}_1+x_2+x_3)(\overline{x}_1+x_2+\overline{x}_3)(\overline{x}_1+\overline{x}_2+x_3)$, para todo $X = (x_1, x_2, x_3) \in B^3$.

Demonstração do Teorema
Pelo Lema 5.74, tem-se que, para todo $j \in B^n \equiv \{0, 1, 2, \ldots, 2^n - 1\}$:

$$\sum_{e=0}^{2^n-1} f(e)p_e(j) = \sum_{e=0}^{2^n-1} f(e)\delta_{ej} = f(j).$$

Logo, as funções $\sum_{e=0}^{2^n-1} f(e)p_e(X)$ e $f(X)$ definidas sobre B^n são iguais.
Do mesmo modo, para todo $j \in B^n \equiv \mathbb{Z}_{2^n}$, temos

$$\prod_{e=0}^{2^n-1} \big(f(e) + s_e(j)\big) = \prod_{e=0}^{2^n-1} \big(f(e) + \overline{\delta}_{ej}\big) =$$

$$= \big(f(0)+1\big)\big(f(1)+1\big)\ldots\big(f(j)+\overline{1}\big)\big(f(j+1)+1\big)\ldots\big(f(2^n-1)+1\big) =$$

$1.\ldots.1.f(j).1\ldots1 = f(j)$.
Como os valores da função $\prod_{e\in B^n}\big(f(e)+s_e(X)\big)$ coincidem com os valores de $f(X)$ em cada ponto $j \in B^n$, essas funções são iguais. Isto conclui o teorema. □

Observe que os índices i, de $p_i(X)$, e j, de $s_j(X)$, nas f.d.n. e f.c.n. de f, respectivamente, são complementares um do outro.

É possível fazer uma simplificação nas f.d.n. e f.c.n. de f do seguinte modo: em vez de escrevermos $f(X) = p_{i_1}(X) + p_{i_2}(X) + \cdots + p_{i_k}(X)$, na f.d.n. de f e $f(X) = s_{j_1}(X).s_{j_2}(X)\ldots s_{j_m}(X)$ na f.c.n. de f, escrevemos simplesmente:

$$f = \sum(i_1, i_2, \ldots, i_k) \quad \text{e} \quad f = \prod(j_1, j_2, \ldots, j_m),$$

ou seja, trocamos no somatório (produtório) os polinômios minimais (respectivamente maximais) por seus índices, já que há unicidade de expressão de uma função na forma canônica, tanto disjuntiva como conjuntiva. Para exemplificar, no exemplo anterior, temos: $f = \sum(1, 2, 7) = \prod(0, 3, 4, 5, 6)$.

Quando f é dada por uma tabela como no exemplo anterior, é fácil achar as formas disjuntiva e conjuntiva normais de f. Para calcular a f.d.n. de f, basta somar os polinômios minimais p_i's, onde $f(i) = 1$, e, para calcular a f.c.n. de f, multiplicam-se os polinômios maximais s_j's, onde $f(j) = 0$. Agora, se f é dada por uma expressão, podemos montar uma tabela apresentando $f(e)$ para $e \in B^n$ e daí proceder como no exemplo anterior. Outro modo é que, fazendo uso das leis de DeMorgan, complementação e a distributividade, podemos sempre achar as formas disjuntiva e conjuntiva normais de f.

Por exemplo, se $f : B^3 \longrightarrow B$ é dada por $f(x, y, z) = x\overline{z} + y$, então:
$f(x, y, z) = x.1.\overline{z} + 1.y.1 = x(y + \overline{y})\overline{z} + (x + \overline{x})y(z + \overline{z}) \overset{\text{distr.}}{=\!=} xy\overline{z} + x\overline{y}.\overline{z} + xyz + xy\overline{z} + \overline{x}yz + \overline{x}y\overline{z} = \sum(2, 3, 4, 6, 7)$.
Observe a simplificação feita $p_6(X) + p_6(X) = p_6(X)$.

Também $f(x, y, z) = x\overline{z} + y \overset{\text{distr.}}{=\!=} (x + y)(\overline{z} + y) = (x + y + 0)(0 + y + \overline{z}) = (x + y + z\overline{z})(x\overline{x} + y + \overline{z}) \overset{\text{distr.}}{=\!=} (x + y + z)(x + y + \overline{z})(x + y + \overline{z})(\overline{x} + y + \overline{z}) = \prod(0, 1, 5)$.
Observe aqui também a simplificação feita $s_1(x)^2 = s_1(x)$.

Estas são as f.d.n. e f.c.n. de f, respectivamente.

Assim, no caso da f.d.n. de f, cuja expressão de f é uma soma, onde cada parcela é um produto $x_{i_1}x_{i_2}\cdots x_{i_k}$, na falta de x_j e $\overline{x}_j$ na parcela acima, escrevemos esta parcela na forma $x_{i_1}x_{i_2}\cdots x_{i_k}(x_j + \overline{x}_j)$ (desde que $x_j + \overline{x}_j = 1$ em B) e aplicamos a lei distributiva obtendo $x_{i_1}x_{i_2}\cdots x_{i_k}x_j + x_{i_1}x_{i_2}\cdots x_{i_k}\overline{x}_j)$. Do mesmo modo, para a f.c.n. de f, na falta de x_j e $\overline{x}_j$ em cada fator $(x_{i_1} + \cdots + x_{i_k})$ do produtório, colocamos $(x_j\overline{x}_j + x_{i_1} + \cdots + x_{i_k})$ e aplicamos a lei distributiva obtendo $(x_j + x_{i_1} + \cdots + x_{i_k})(\overline{x}_j + x_{i_1} + \cdots + x_{i_k})$. Com isto, as variáveis x_j e $\overline{x}_j$, que não estavam presentes nesta parcela (fator), passam a estar presentes. Isto deve ser feito para cada variável que não esteja presente em cada uma das parcelas (fatores). Observe então que cada parcela na f.d.n. (ou fator na f.c.n.) de f produz duas parcelas (respectivamente dois fatores) com a variável x_j ou $\overline{x}_j$ acrescentadas. Com este processo, as funções minimais (maximais) aparecerão na expressão de f, resultando em

suas formas disjuntiva e conjuntiva normais.

Se usarmos apenas os índices $j \in \mathbb{Z}_{2^n} \equiv B^n$ incompletos, que corresponde ao produto $x_{i_1}x_{i_2}\ldots x_{i_k}$, podemos usar um procedimento sobre eles correspondente a esta técnica: Escreva f como uma soma, onde cada parcela é um produtos, tendo em vista a obtenção da f.d.n.. Cada uma destas parcela (que é um produto) é identificada com uma seqüência ordenada de 'zeros', 'uns' e traços, obedecendo a seguinte lei: se x_i ocorre no produto considerado, colocamos '1' na i-ésima posição da seqüência ordenada; se ocorre $\overline{x}_i$, colocamos 'zero' e, se não ocorrem x_i nem $\overline{x}_i$, colocamos um traço, sempre na i-ésima posição.
Depois, todos estes traços são substituídos por elementos de $B = \{0, 1\}$, de quantas forem as combinações possíveis, obtendo-se assim elementos $j \in B^n \equiv \mathbb{Z}_{2^n}$ e também o polinômio minimal correspondente. A soma de todos os $p_j(X)$ obtidos em todos os produtos é a f.d.n. de f.

Exemplo 5.77 Seja $f : B^4 \longrightarrow B, \quad f(x_1, x_2, x_3, x_4) = x_2\overline{x}_3.\overline{x}_4 + x_1x_2\overline{x}_3$. Então podemos fazer a seguinte tabela:

produtos	representação binária	polinômios minimais
$x_2.\overline{x}_3.\overline{x}_4$	- 1 0 0	0100=4, 1100=12
$x_1.x_2.\overline{x}_3$	1 1 0 -	1100=12, 1101=13

Observe os traços, na segunda coluna, onde não ocorrem as variáveis x_1 e $\overline{x}_1$ (primeira linha), e o traço onde não ocorrem as variáveis x_4 e $\overline{x}_4$ (segunda linha). Eles são substituídos por 0 e 1 obtendo, na terceira coluna, os expoentes dos polinômios minimais que ocorrerão na f.d.n. da função f. Assim, $f = \sum(4, 12, 13)$.

5.5.2 Álgebra das Funções Booleanas

Seja A uma álgebra booleana e denotemos por $A^n(F)$ o conjunto de todas funções booleanas $f : A^n \to A$. No início desta seção, definimos este conjunto como sendo gerado por todas funções constantes e projeções fazendo uso das operações booleanas de adição, multiplicação e complemetação. Logo, se $f,\ g \in A^n(F)$, então $\overline{f},\ f+g,\ f.g \in A^n(F)$, onde $\overline{f}(X) = \overline{f(X)},\ (f+g)(X) =$

$f(X)+g(X)$ e $(fg)(X) = f(X)g(X)$. Agora, demonstraremos que $A^n(F)$ com estas operações é, ele mesmo, uma álgebra booleana.

Proposição 5.78 *$(A^n(F), +, \cdot)$ é uma álgebra booleana.*

Demonstração: Para $f,\ g \in A^n(F)$, temos:
$(f + g)(X) = f(X) + g(X) = g(X) + f(X) = (g + f)(X)$ e
$(f.g)(X) = f(X).g(X) = g(X).f(X) = (g.f)(X)$.

Em ambos os casos, a primeira igualdade segue da definição, a segunda igualdade segue da propriedade comutativa em A e depois segue de definição novamente. Logo, $f + g = g + f$ e $f.g = g.f$ para todas funções $f, g \in A^n(F)$.

As funções $\Theta : A^n \to A$ e $I_A : A^n \to A$ dadas por $\Theta(X) = 0$ e $I_A(X) = 1$, para todo $X \in A^n$, são os elementos neutros para as operações de adição e multiplicação definidas sobre $A^n(F)$, respectivamente. Verifique!

Usando o fato de que A é uma álgebra booleana, tem-se:
$\big((f + g)h\big)(X) = (f + g)(X).h(X) = \big(f(X) + g(X)\big).h(X) = f(X).h(X) + g(X).h(X) = (f.h)(X) + (g.h)(X) = (f.h + g.h)(X)$.
Assim, $(f + g).h = f.h + g.h,\ \forall f, g, h \in A^n(F)$. Do mesmo modo, prova-se que: $f + gh = (f + g)(f + h),\ \forall f, g, h \in A^n(F)$.

Finalmente, $\forall f \in A^n(F),\ \forall X \in A^n$, temos: $(f + \overline{f})(X) = f(X) + \overline{f(X)} = 1 = I_A(X)$, e $(f\overline{f})(X) = f(X)\overline{f(X)} = 0 = \Theta(X)$. Logo, $f + \overline{f} = I_A$ e $f.\overline{f} = \Theta$. Isto conclui a proposição. □

Tendo em vista os exercícios (4) e (5) da seção anterior e definição 5.32, existe o anel de funções booleanas correspondente à álgebra de funções booleanas que será denotado por $(A^n(F), \oplus, \cdot)$, como é de praxe. Também é claro que o Teorema 5.33 é satisfeito para esse particular par de álgebra e anel booleanos.

Agora, enumeremos uma lista de propriedades satisfeitas pelo anel $(A^n(F), \oplus, .)$ e pela álgebra $(A^n(F), +, \cdot)$, correspondente (Seria bom que o leitor as provasse).

Propriedades

(a) $f \oplus g = g \oplus f$ **(b)** $f \oplus (g \oplus h) = (f \oplus g) \oplus h$
(c) $f(g \oplus h) = f.g \oplus f.h$ **(d)** $f \oplus \Theta = f$
(e) $f \oplus f = \Theta$ **(f)** $f \oplus g = f \oplus h \longleftrightarrow g = h$
(g) $f \oplus I_A = \overline{f}, \quad \overline{f} \oplus I_A = f$ **(h)** $f \oplus g = h \leftrightarrow f = g \ominus h = g \oplus h$
(i) $\overline{(f \oplus g)} = f \oplus \overline{g} = \overline{f} \oplus g$ **(j)** $f + g = f \oplus g \oplus f.g$
(k) $f + g = f \oplus g \leftrightarrow f.g = \Theta$
(l) $\sum_{i=1}^{n} f_i = \bigoplus_{i=1}^{n} f_i \Longleftrightarrow f_i.f_j = \Theta, \quad 1 \leq i < j \leq n.$

Definição 5.79 Dizemos que as funções f e g são *ortogonais* se $f.g = \Theta$, ou equivalentemente, $f + g = f \oplus g$.

Como os polinômios minimais p_i, p_j são ortogonais para $i \neq j$, a expressão de uma função booleana na forma disjuntiva normal (Teorema 5.69) tanto pode ser escrita como

$$f = \sum_{i=0}^{2^n-1} f(i)p_i \text{ como, } f = \oplus_{i=0}^{2^n-1} f(i)p_i,$$

pois $p_i p_j = \delta_{ij} p_i$. Em outras palavras, a expressão de f na f.d.n. sobre a álgebra booleana é a mesma expressão de f quando se passa para o anel booleano correspondente.

Mais geralmente, dada uma função booleana sobre a álgebra booleana usando as propriedades (j), (k) e (l) acima, que apresentam as relações entre $+$ e $\oplus$, podemos expressar f sobre o anel booleano correspondente. Basta, para isto, colocar f na f.d.n. e trocar a adição da álgebra booleana pela adição do anel booleano (pois as funções minimais são ortogonais), observando que $\overline{a} = 1 \oplus a$. Reciprocamente, se f é uma função booleana cuja expressão envolve as operações de um anel booleano, é possível expressar f sobre a álgebra booleana correspondente.

Por exemplo, se $f(x, y, z) = xy\overline{z} + \overline{x}yz + \overline{x}.\overline{y}z$ é a expressão de f sobre A, então como f está na f.d.n., temos que $f = xy\overline{z} \oplus \overline{x}yz \oplus \overline{x}.\overline{y}z = xy(1 \oplus z) \oplus (1 \oplus x)yz \oplus (1 \oplus x)(1 \oplus y)z$. Desenvolvendo e observando que $a \oplus a = 0$ no anel booleano, tem-se que $f(x, y, z) = z \oplus xy \oplus xz \oplus xyz$.

Ao todo existem 2^n produtos distintos envolvendo as variáveis $x_1, x_2, \ldots, x_n$, pois uma variável pode ocorrer ou não em um produto.

Definição 5.80 Sejam $l_0(X) = 1$ e $l_e(X),\ e \geq 1$ como sendo o produto das variáveis x_i obtido de $p_e(X)$ deletando todas as variáveis $\overline{x}_j,\ 1 \leq j \leq n$. Isto é, se $p_e(X) = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$, para obter $l_e(X)$, retiramos de $p_e(X)$ o fator $x_j^{e_j}$ se, e somente se, $e_j = 0$.

Exemplo: Para $n = 1$, temos:

$X = (x_1)$ e $p_0(X) = \overline{x}$, $p_1(X) = x$. Portanto, $l_0(X) = 1$, $l_1(X) = x$.

Para $n = 2$, temos:

$X = (x_1, x_2)$, $p_0(X) = \overline{x}_1\overline{x}_2$, $p_1(X) = \overline{x}_1 x_2$, $p_2(X) = x_1\overline{x}_2$, $p_3(X) = x_1 x_2$.

Portanto, $l_0(X) = 1,\ l_1(X) = x_2,\ l_2(X) = x_1,\ l_3(X) = x_1 x_2$.

Agora, podemos enunciar a *forma normal* de f que é uma *expressão canônica* de f sobre o anel booleano A.

Teorema 5.81 F o r m a N o r m a l

Toda função booleana $f : A^n \longrightarrow A$ *tem uma expressão típica*

$$f = \oplus_{i=0}^{2^n-1} g_i l_i \qquad \left(ou \quad f = \oplus_{e \in B^n} g_e l_e\right)$$

sobre o anel booleano $(A^n, \oplus, \cdot)$, *onde* $g_i \in A$.

Demonstração: Usando a álgebra booleana $(B^n, +, \cdot)$, escrevemos f na f.d.n. e, como os polinômios minimais são ortogonais, podemos escrever $f = \oplus_{i=0}^{2^n-1} f(i) p_i$. Agora, troquemos $\overline{x}_i$ por $1 \oplus x_i,\ i = 1, 2, \ldots, n$ (Ver definição 5.32 e os exercícios (4) e (5) da última seção) onde ele ocorrer e, usando as propriedades do anel booleano (como no exemplo anterior), obtém-se a expressão desejada de f.

A unicidade segue-se do fato que existem 2^n funções polinomiais $l_e(X)$ sobre A e, portanto, existem $|A|^{2^n}$ expressões distintas $\oplus_{e=0}^{2^n-1} g_e l_e$ sobre o anel A, ou seja, existem precisamente $|A|^{2^n}$ funções booleanas de n variáveis sobre o anel booleano A. No caso em que $A = B$, existem 2^{2^n} funções booleanas de n variáveis sobre A. □

Definição 5.82 *Expressão Par e Expressão Ímpar*

Dizemos que a função booleana f sobre o anel booleano tem *expressão ímpar*, se na expressão canônica de $f = \oplus_{e \in B^n} g_e l_e$, ocorrer $l_0 = 1$. Se não ocorrer $l_0 = 1$ na forma normal de f, dizemos que f tem *expressão par.*

Exemplo: Se a f.d.n. de f for $f(x, y) = \overline{x}.\overline{y}$, então a forma normal de f sobre o anel booleano correspondente é $f(x, y) = (1 \oplus x)(1 \oplus y) = 1 \oplus x \oplus y \oplus xy = l_0 \oplus l_2 \oplus l_1 \oplus l_3$. Logo $f(x, y)$ tem expressão ímpar.

O leitor poderá ver, no próximo item, como se constrói o circuito de uma função booleana. O circuito da função f dada acima é:

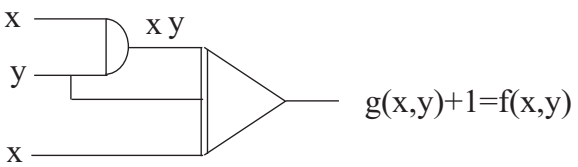


Figura 5.3: Expressão ímpar para f.

onde $g(x, y) = x \oplus y \oplus xy$.

5.5.3 Representação de Funções Booleanas por Circuitos

A álgebra booleana tem aplicações muito importantes dentro da teoria de Circuitos (eletrônicos, eletromecânicos, etc.) porque elas descrevem as leis básicas destes circuitos, que são chamados *circuitos booleanos.* Exemplos de tais circuitos são diodos, núcleos magnéticos, transistores, vários tipos de bulbos eletrônicos, chamados também de *circuitos lógicos.*

Embora os elementos de um circuito possam ser designados com uma variedade de características, concentraremos nossa atenção em três tipos de elementos: nas entradas (ou portas) **e**, **ou** e **ou-exclusivo**.

Elas correspondem, respectivamente, a uma máquina processadora das operações booleanas 'multiplicação', 'adição', e 'adição

exclusiva' (esta última é denotada por '$\oplus$' e corresponde à adição do anel booleano correspondente à álgebra booleana em questão, como visto anteriormente). Para exemplificar um pouco mais a operação 'ou-exclusivo', observe que na tabela de adição $\oplus$ do anel booleano $(B, \oplus, \cdot)$, $B = \{0, 1\}$, temos $a \oplus b = 1$ se, e somente se, a ou (*exclusivo*) b é 1, $\forall a,\ b \in B = \{0, 1\}$. Por outro lado, $a + b = 1$ se, e somente se, ou $a = 1$ ou $b = 1$ (Agora faça as tábuas e observe).

Assim, para entradas a e b, as saídas $a \cdot b$, $a + b$ e $a \oplus b$ são simbolizadas respectivamente por:

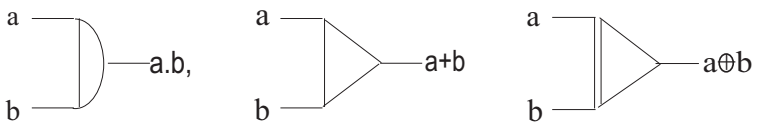


Figura 5.4: Portas lógicas

No campo da engenharia, estes símbolos são usados para ligações de canais em série e paralelo, respectivamente. Por exemplo, se desejamos enviar uma mensagem de uma fonte X a um destino Y, através dos canais A e B, e se denotamos 1 para mensagem recebida e 0 para mensagem não recebida, então $a.b$ e $a + b$ representam fielmente as ligações em série e paralelo dos canais A e B, respectivamente. Algum tipo de interpretação pode ser dada a $a \oplus b$, desde que se faça alguma dependência entre os canais a e b (Tente).

Representamos a máquina processadora da operação booleana complementação (ou negação) acrescentando um círculo cheio do seguinte modo:

Isto significa que, para entrada a, a máquina processa a informação e nos dá como saida $\overline{a}$.

Combinando a complementação e a multiplicação, temos os casos $\overline{a}.b$ e $\overline{a.b}$. As máquinas, tais que, para entradas a e b dão como saidas $\overline{a}.b$ e $\overline{a.b}$, respectivamente, são representadas por

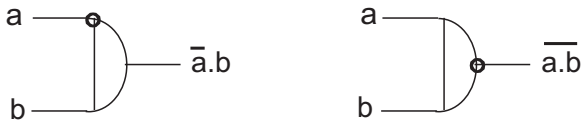


Figura 5.5: Produto e Negação do Produto.

e as máquinas, tais que, para entradas a, b nos dão como saídas $\overline{a} + b$ e $\overline{a + b}$ são representadas, respectivamente, por

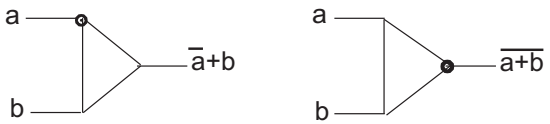


Figura 5.6: Soma e Negação da Soma.

Definição 5.83 Um *circuito booleano* é a realização de uma função booleana f em n variáveis $x_1, \ldots, x_n$ sobre a álgebra booleana A, ou seja, é um arranjo de sucessivas combinações em série (o que equivale à porta e) e em paralelo (o que equivale à porta ou) e complementações de n entradas x_1, $x_2, \ldots, x_n$, de modo que tenhamos saída $f(x_1, \ldots, x_n)$.

Portanto, toda função booleana em n variáveis sobre A dá origem a um circuito booleano com n entradas e, reciprocamente, para toda combinação de símbolos das portas "*e*"e "*ou*"e complementação sobre n entradas $x_1, x_2, \ldots, x_n$, existe uma função booleana em n variáveis sobre A associado a ele.

Exemplo 5.84 Os circuitos correspondentes à $f : A^3 \to A$, $f(x, y, z) = \overline{x}\overline{y} + \overline{x}z$ de $g : A^2 \to A$, $g(x, y) = xy + x\overline{y} + \overline{x}\ \overline{y}$ são, respectivamente:

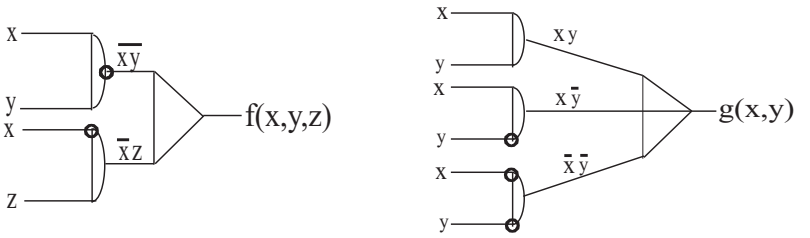


Figura 5.7: Circuitos das Funções f e g.

Definição 5.85 Sejam f, g funções booleanas em n variáveis sobre a álgebra booleana A. Dizemos que f e g são *funções equivalentes* se, a partir da expressão de uma das funções, obtém-se a outra, fazendo uso das operações booleanas. Também, definimos *circuitos equivalentes* como sendo circuitos com as mesmas entradas, cujas saídas são funções booleanas equivalentes.

Por exemplo, a função g do exemplo 5.84 e $h : A^2 \longrightarrow A$ dada por: $h(x, y) = x+\overline{y}$ são equivalentes, pois $g(x, y) = xy+x\overline{y}+\overline{x}\,\overline{y} = x(y+\overline{y})+\overline{x}\,\overline{y} = x.1+\overline{x}\,\overline{y} = x+\overline{x}\,\overline{y} = (x+\overline{x})(x+\overline{y}) = x+\overline{y} = h(x, y)$. Portanto, o circuito da função g do exemplo anterior é equivalente ao circuito

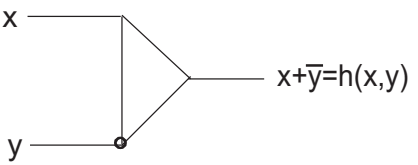


Figura 5.8: Circuito da Função h.

que é um circuito mais simples e mais econômico.

5.5.4 Simplificação e Mapas de Veitch-Karnaugh

Utilizando as propriedades de álgebra booleanas, podemos simplificar quaisquer funções booleanas, ou *expressões booleanas* em n variáveis, do mesmo modo que fizemos para simplificar proposições compostas. Por exemplo, a expressão booleana $P = XYZ +$

$\overline{X}Y\overline{Z} + X\overline{Y}\overline{Z}$ é uma expressão booleana nas variáveis X, Y e Z. Esta expressão pode ser vista como uma função de A^3 em A, onde A é uma álgebra booleana. No caso em que X, Y e Z são proposições, temos que P é a proposição composta $P = (X \wedge Y \wedge Z) \vee (\neg X \wedge Y \wedge \neg Z) \vee \big(X \wedge \neg(Y \wedge Z)\big)$.

Definição 5.86 Definimos uma *fórmula* (*booleana*) ou *expressão* (*booleana*), em n indeterminadas $0,\ 1, X_1,\ X_2, \ldots, X_n,$ como sendo qualquer polinômio nas variáveis $X_1, X_2, \ldots, X_n$ sobre $B = \{0, 1\}$ sujeito à restrição: $X_i^2 = X_i$ e $X_i + X_i = X_i, \forall i$. Em outras palavras, uma fórmula é obtida recursivamente como sendo:

(i) $0, 1, X_1, X_2, \ldots, X_n$ são fórmulas,

(ii) Se P e Q são fórmulas, então $\overline{P},\ PQ$ e $P+Q$ são fórmulas e

(iii) $X_i^2 = X_i, \quad X_i + X_i = X_i$.

Quando $X_1,\ X_2,\ X_3$ são, respectivamente, as proposições $p,\ q,$ e r sobre um conjunto não vazio S, temos que $P(p, q, r) = p \vee (q \wedge \neg r) \vee (p \wedge q \wedge r)$ é uma proposição composta sobre S.

Se atribuirmos, independentemente, os valores lógicos verdade ou falso ou, respectivamente, os valores 1 ou 0 às variáveis X_i em cada fórmula P, esta fórmula dá origem a uma única função booleana $f = f_P : B^n \to B$, onde $f(x_1, x_2, \ldots, x_n) \in B$ é o valor lógico (*zero* ou *um*) da fórmula P quando se substitui X_i pelo valor x_1. Obviamente, a expressão da função f associada à fórmula P definida acima não é única; por exemplo, se $P = \overline{X_1 + X_2}$, devido às leis de DeMorgan, temos que f e $g : B^2 \to B$ dadas por $f(x_1, x_2) = \overline{x_1 + x_2}$ e $g(x_1, x_2) = \overline{x}_1.\overline{x}_2$, são funções iguais e associadas à fórmula P.

Reciprocamente, cada função $f : B^n \longrightarrow B$ dá origem a uma fórmula booleana $P(X_1, X_2, \ldots, X_n)$, de modo que, se $f,\ g : B^n \longrightarrow B$ são funções iguais e $Q(X_1, X_2, \ldots, X_n)$ é uma fórmula associada à função g então P e Q são fórmulas equivalentes, ou seja, podemos obter uma da outra fazendo uso das propriedades da álgebra booleana.

Circuitos de fórmulas booleanas se faz do mesmo modo que se faz circuitos de funções booleanas. Por exemplo, o circuito da

fórmula $P = XY + \overline{X} + Y$ é

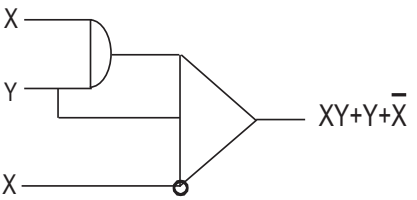


Figura 5.9: Circuito P

Dada uma fórmula booleana qualquer, usando as propriedades distributiva, associativa, leis de DeMorgan, etc. de uma álgebra booleana é fácil expressá-la como uma soma de produtos. Um caso particular é a sua forma disjuntiva normal. Consideremos uma fórmula em n variáveis $P(X_1, X_2, \ldots, X_n)$ e, como antes, denotemos $\overline{X}$ por X_i^0 e X_i por X_i^1. Pelo Teorema 5.75, segue-se que $X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$ (onde $a_i \in \{0, 1\}$) é uma parcela da forma disjuntiva normal de P se, e somente se, $f_P(a_1, a_2, \ldots, a_n) = 1$.

De fato, $P = \sum_{e \in B^n} f_P(e) X_1^{e_1} X_2^{e_2} \cdots X_n^{e_n}$. Logo,

$f_P(a_1, a_2, \ldots, a_n) = 1$ se, e somente se, $\sum_{e \in B^n} f_P(e) a_1^{e_1} a_2^{e_2} \cdots a_n^{e_n} = 1$,

ou seja, existe $e = (e_1, e_2, \ldots, e_n) \in B^n$, tal que $f_P(e) = a_1^{e_1} a_2^{e_2} \cdots a_n^{e_n} = 1$. Como $a_i^{e_1} = 1$ em B se, e somente se, $e_1 = a_i$ segue-se que $e = (a_1, a_2, \ldots, a_n)$.

Usando este fato, é fácil determinar a forma disjuntiva normal de uma fórmula P. Para isto, basta considerar a tabela de sua função associada f_P e adicionar os termos correspondente a n-upla $(a_1, a_2, \ldots, a_n)$, onde f_P tem o valor 1. Vejamos um exemplo.

Exemplo 5.87 Dê as funções associadas às fórmulas booleanas **(i)** $P = XY + \overline{X} + Y$, e **(ii)** $Q = X\overline{Z} + YZ + \overline{XZ}$ e use as funções associadas a elas para dar suas formas disjuntivas normais.

Solução: As funções associadas às fórmulas booleanas P e Q são, respectivamente: $f = f_P : B^2 \to B$ e $g = f_Q : B^3 \longrightarrow B$, dadas por: $f(x, y) = xy + \overline{x} + y$ e $g(x, y, z) = x\overline{z} + yz + \overline{xz}$, cujas tabelas são:

x	y	xy	$xy+y$	$\overline{x}$	$f(x,y)$
1	1	1	1	0	1
1	0	0	0	0	0
0	1	0	1	1	1
0	0	0	0	1	1

As parcelas que ocorrem na f.d.n. de P são aquelas do tipo $X^{a_1}Y^{a_2}$, onde $f(a_1,a_2)=1$. Assim, $P = X^1Y^1 + X^0Y^1 + X^0Y^0 = XY + \overline{X}Y + \overline{X}\,\overline{Y}$.

Segue a tabela da função g

x	y	z	xz	yz	$\overline{xz}+yz$	$\overline{z}$	$x\overline{z}$	$g(x,y,z)$
1	1	1	1	1	1	0	0	1
1	1	0	0	0	1	1	1	1
1	0	1	1	0	0	0	0	0
1	0	0	0	0	1	1	1	1
0	1	1	0	1	1	0	0	1
0	1	0	0	0	1	1	0	1
0	0	1	0	0	1	0	0	1
0	0	0	0	0	1	1	0	1

Pelas mesmas razões, as parcelas que ocorrem na f.d.n. de Q são aquelas do tipo $X^{a_1}Y^{a_2}Z^{a_3}$, onde $g(a_1,a_2,a_3)=1$. Assim, $Q = X^1Y^1Z^1 + X^1Y^1Z^0 + X^1Y^0Z^0 + X^0Y^1Z^1 + X^0Y^1Z^0 + X^0Y^0Z^1 + X^0Y^0Z^0$, ou seja,
$Q = XYZ + XY\overline{Z} + X\overline{Y}\,\overline{Z} + \overline{X}YZ + \overline{X}Y\overline{Z} + \overline{X}\,\overline{Y}Z + \overline{X}\,\overline{Y}\,\overline{Z}$.

Uma *simplificação* ou *minimização* de uma fórmula booleana é uma expressão booleana com o mínimo possível de polinômios minimais, no caso em que ela esteja escrita como somas de produtos (e não necessariamente na forma disjuntiva normal) e que seja equivalente à fórmula original. Isto significa que os termos redundantes da expressão original foram eliminados. Algebricamente, este processo pode ser feito usando as propriedades da álgebra booleana. Um método geométrico equivalente será explorado a seguir usando *mapas* ou *diagramas* de *Veitch-Karnaugh* (mapas V-K).

Devido às propriedades de uma álgebra booleana, não existe uma expressão mínima única para uma dada fórmula booleana. Por

exemplo, a lei de DeMorgan nos dá que $\overline{X}+\overline{Y}$ e $\overline{XY}$ são expressões mínimas, de alguma fórmula booleana, e são equivalentes.

Os mapas V-K são métodos geométricos que servem para minimizar uma expressão booleana que esteja escrita como somas de produtos. As leis de DeMorgan permitem tomar a expressão mínima de uma fórmula como somas de produtos, não necessariamente na forma disjuntiva normal. Isto implica que o circuito correspondente é mais econômico, pois usa o menor número possível de portas lógicas.

Mapas de Veitch-Karnaugh para 2 Variáveis

Temos quatro polinômios minimais nas variáveis X, Y, XY, $X\overline{Y}$, $\overline{X}Y, \overline{X}\ \overline{Y}$ descritos nas células que seguem. Estes polinômios estão associados às funções minimais xy, $x\overline{y}$, $\overline{x}y$ e à $\overline{x}.\ \overline{y}$, conforme a definição 5.72. Como cada polinômio minimal pode ou não ocorrer em uma dada fórmula booleana, então existem $2^4 = 16$ fórmulas booleanas em 2 variáveis. Logo, existem 16 funções $f : B \times B \longrightarrow B$; $(B = \{0, 1\})$ correspondentes.

Um mapa V-K para duas variáveis consiste de quatro células ou retângulos básicos que são os cruzamentos das regiões ou células correspondentes às literais X, $\overline{X}$, Y, $\overline{Y}$.

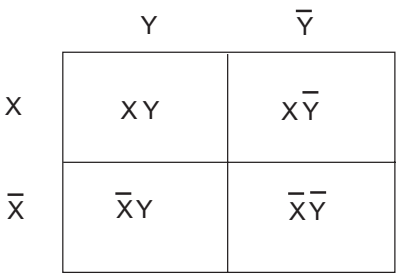


Figura 5.10: Mapas V-K para Duas Variáveis

Nestas células, coloca-se 1 se ela representa o polinômio minimal que está presente na fórmula P escrita como somas de produtos. *Células Adjacentes* são um par de células básicas cujos polinômios minimais diferem exatamente em uma literal (ou seja, tem

um lado do retângulo básico comum). Por exemplo, a célula que representa $\overline{X}Y$ é adjacente à célula que representa o polinômio minimal XY e também é adjacente à célula que representa o polinômio minimal $\overline{X}\ \overline{Y}$. Estas duas últimas células não são adjacentes, pois suas células não têm um lado comum, equivalentemente, não diferem apenas por uma literal. As literais X, Y, $\overline{X}$, $\overline{Y}$ são representadas por regiões de duas células adjacentes:

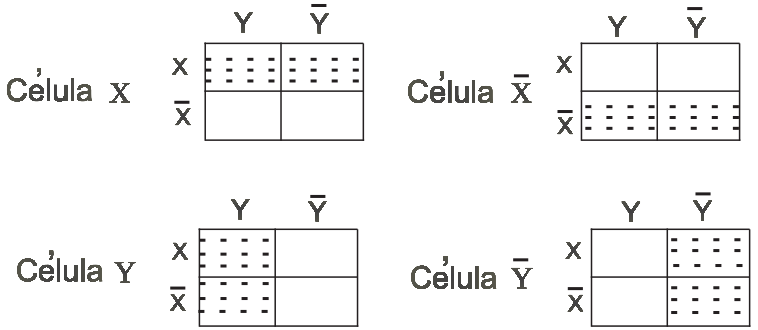


Figura 5.11: Células X's e Y's

Exemplos 5.88 **(1)** A literal X é igual a $XY + X\ \overline{Y}$, pois contém as regiões básicas de XY e $X\ \overline{Y}$. Algebricamente, $Y = XY + \overline{X}\ Y$, $\overline{X} = \overline{X}Y + \overline{X}\ \overline{Y}$ e $\overline{Y} = X\overline{Y} + \overline{X}\ \overline{Y}$.

(2) Vamos marcar nos mapas V-K as células básicas correspondentes às expressões: **(A)** $P(X,Y) = XY + \overline{X}Y$, **(B)** $Q(X,Y) = X\overline{Y} + \overline{X}Y$, e **(C)** $R(X,Y) = X\overline{Y} + \overline{X}Y + \overline{X}\ \overline{Y}$. A seguir, se for possível, simplifiquemos.

Solução:

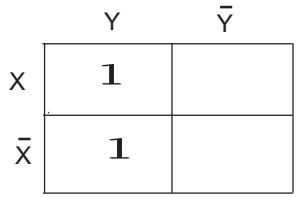


Figura 5.12: Exemplo A

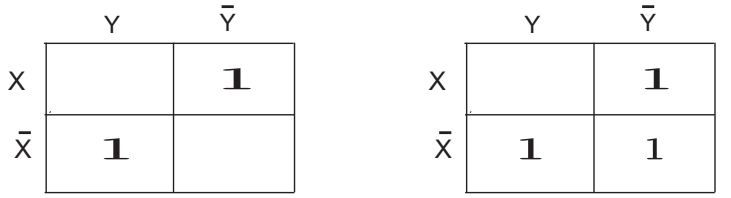


Figura 5.13: Exemplos B e C

(A) Temos que $P(X,Y) = Y$, pois no diagrama V-K para $P(X,Y)$, temos a célula Y totalmente marcada. Note, também, que a simplificação algébrica de P dá $Y : XY + \overline{X}Y = (X + \overline{X})Y = 1.Y$

(B) $Q(X,Y)$ não admite simplificação, pois no diagrama V-K não existem células adjacentes. Logo não existe nenhuma célula correspondente a uma literal.

(C) Como $R(X,Y)$ é composta de duas regiões, as regiões das literais $\overline{X}$ e $\overline{Y}$, devemos somar estas duas literais para obter: $R(X,Y) = \overline{X} + \overline{Y}$.

Algebricamente podemos obter a mesma simplificação. Usando a igualdade $\overline{X}\,\overline{Y} = \overline{X}\,\overline{Y} + \overline{X}\,\overline{Y}$, temos: $R(X,Y) = (X\overline{Y} + \overline{X}\,\overline{Y}) + (\overline{X}\,\overline{Y} + \overline{X}Y) = (X + \overline{X})\overline{Y} + \overline{X}(Y + \overline{Y}) = 1.\overline{Y} + \overline{X}.1 = \overline{X} + \overline{Y}$.

Notemos, também, que, se não duplicarmos $\overline{X}\,\overline{Y}$ em $R(X,Y)$, temos outra simplificação desta fórmula: $R(X,Y) = X\overline{Y} + \overline{X}(Y + \overline{Y}) = X\overline{Y} + \overline{X}$ e é preciso não esquecer de aplicar a propriedade distributiva para simplificar mais: $X\overline{Y} + \overline{X} = (X + \overline{X})(\overline{Y} + \overline{X}) = 1.(\overline{Y} + \overline{X}) = \overline{Y} + \overline{X}$. Assim, temos o circuito

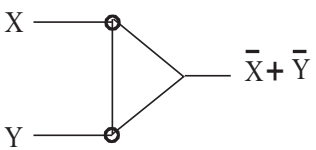


Figura 5.14:

que corresponde à simplificação de $R(X,Y)$ e é bem mais simples e econômico que o circuito correspondente a $R(X,Y)$.

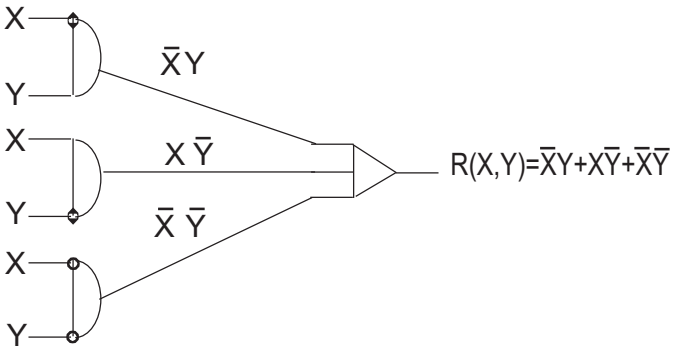


Figura 5.15:

Finalmente, observemos que, se dois polinômios minimais ocorrem em células adjacentes, eles podem ser combinados e, com isto, uma variável é eliminada da expressão. Por exemplo: $X\overline{Y} + XY = X(\overline{Y} + Y) = X.1 = X$. Além disso, se todas as células básicas foram marcadas é porque os quatro polinômios minimais ocorreram na expressão booleana. Logo, eles podem ser combinados resultando a expressão booleana 1. De fato, $XY + X\overline{Y} + \overline{X}Y + \overline{X}\ \overline{Y} = X(Y + \overline{Y}) + \overline{X}(Y + \overline{Y}) = X.1 + \overline{X}.1 = X + \overline{X} = 1$.

Mapas de Veitch-Karnaugh para 3 Variáveis

Os mapas de V-K para 3 variáveis são retângulos divididos em 8 células básicas de modo que a região de uma das literais X, Y, Z e $\overline{X}, \overline{Y}, \overline{Z}$ é metade da região total. Além disso, a região da literal X não "cruza"a região de seu complemento $\overline{X}$, mas cruza com todas as outras regiões variáveis Y, $\overline{Y}$, Z e $\overline{Z}$. O mesmo deve ocorrer com $\overline{X}$.

Agora, considerando as regiões das variáveis Y e $\overline{Y}$, temos que cada uma delas ocupam a metade da região total do retângulo e não se cruzam, mas cruzam com todas as outras regiões das variáveis $X, \overline{X}$, Z e $\overline{Z}$. As mesmas considerações valem para as variáveis Z e $\overline{Z}$. Veja figura.

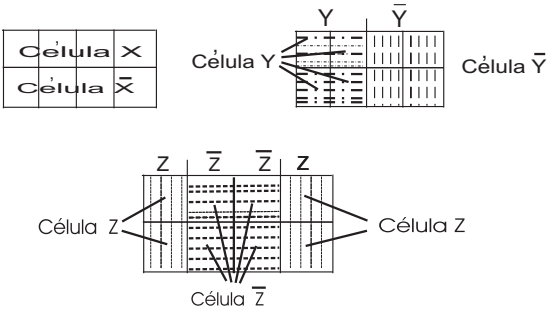


Figura 5.16: Células

Células adjacentes são aquelas que representam polinômios minimais que diferem por uma literal. Um modo de fazer o mapa com estas exigências, é considerar o cilindro, onde os segmentos $\overline{AB}$ e $\overline{A'B'}$ do mapa que segue devem ser colados.

Veja na próxima figura que as regiões correspondentes a XYZ e a $X\overline{Y}Z$ são adjacentes, pois os termos diferem pelas literais Y e $\overline{Y}$. O mesmo ocorre com as regiões correspondentes a $\overline{X}YZ$ e $\overline{X}\ \overline{Y}Z$. Isto justifica porque devemos colar os segmentos $\overline{AB}$ com $\overline{A'B'}$. Veja figura

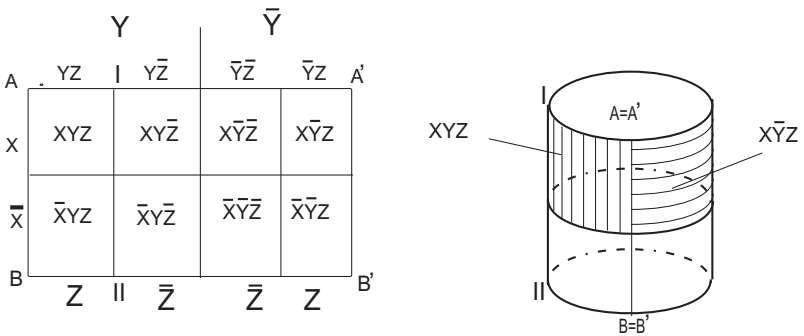


Figura 5.17: Cilindro

Outro modo de visualizar este mapa, é atentar para as regiões das literais X, $\overline{X}$, Y, $\overline{Y}$, Z e $\overline{Z}$ que correspondem a uma região de quatro células adjacentes. Assim, temos essas seis regiões, como mostra a figura 5.16.

Se, numa fórmula booleana, ocorrem polinômios minimais com células adjacentes, a única literal distinta destas células adjacentes é eliminada na soma. Por exemplo, $\overline{X}YZ + \overline{X}\ \overline{Y}Z = \overline{X}Z$, cuja região corresponde à intersecção das regiões das literais $\overline{X}$ e Z.

Para visualizar melhor os blocos das células adjacentes que representam os polinômios minimais de uma fórmula booleana, que podem ser combinados e simplificados, é costume circular estes blocos, pois estes correspondem a uma boa simplificação. Note, como já vimos anteriormente, que um polinômio minimal pode ser usado mais de uma vez se for necessário. No caso de $R(X, Y)$, o polinômio minimal $\overline{X}\ \overline{Y}$ foi usado duas vezes.

Exemplo. Use mapas V-K para minimizar as expressões

(a) $P = P(X, Y, Z) = XY\overline{Z} + X\overline{Y}\ \overline{Z} + \overline{X}\ \overline{Y}\ \overline{Z} + \overline{X}YZ$,

(b) $Q = Q(X, Y, Z) = X\overline{Y}Z + X\overline{Y}\ \overline{Z} + \overline{X}YZ + \overline{X}\ \overline{Y}Z + \overline{X}\ \overline{Y}\ \overline{Z}$ e

(c) $R = R(X, Y, Z) = XYZ + XY\overline{Z} + X\overline{Y}Z + X\overline{Y}\ \overline{Z} + \overline{X}YZ + \overline{X}\ \overline{Y}Z + \overline{X}\ \overline{Y}\ \overline{Z}$.

Solução:

(a) No mapa V-K para P, note as células $X\overline{Z}$, $\overline{Y}\ \overline{Z}$ e $\overline{X}YZ$ envolvidas com elipses que devem ser somadas.

(b) No mapa V-K para Q, ocorre uma região de quatro células básicas adjacentes referente a $\overline{Y}$, e temos duas células adjacentes referentes à região $\overline{X}Z$, pois $\overline{X}Z = \overline{X}\ \overline{Y}Z + \overline{X}YZ$. Veja os mapas a seguir.

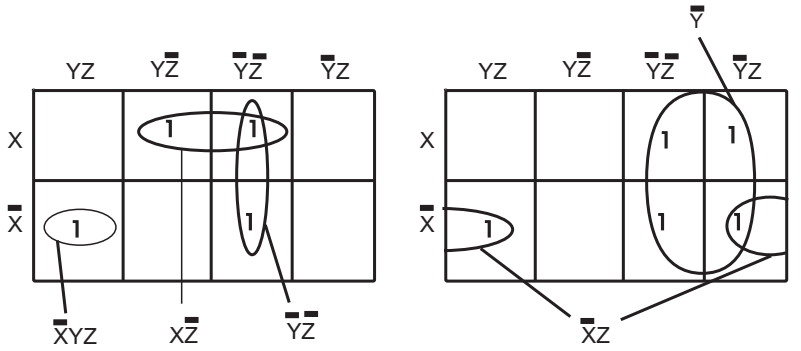


Figura 5.18: Mapa V-K para P e Q

(c) No mapa V-K para R, temos três blocos de quatro retângulos básicos correspondentes às regiões de X, $\overline{Y}$, e Z. Esta última denotada no mapa V-K por asteriscos. Logo, $R \equiv X + \overline{Y} + Z$. Veja o mapa a seguir.

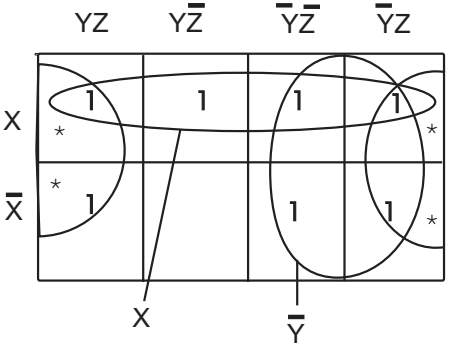


Figura 5.19: Mapa V-K para R

Note que os blocos de células adjacentes dentro de blocos de quatro células não precisam ser considerados.

Os diagramas de V-K também servem para simplificar expressões de funções, e o tratamento é o mesmo que aquele feito para fórmulas booleanas. Por exemplo, consideremos a função $f : B^3 \to B$ dada pelo diagrama

a	b	c	$f(a,b,c)$
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	0

Como $f(1,1,1)=1$, o termo abc deve ocorrer na forma disjuntiva normal de f. Como $f(1,0,1)=1$, o termo $a\overline{b}c$ deve ocorrer na f.d.n. de f, pois, quando $a=\overline{b}=c=1$, então $(a,b,c)=(1,0,1)$ e $a\overline{b}c=1.1.1=1$. De modo análogo, os termos $a\overline{b}\overline{c}$ devem ocorrer na f.d.n. de f, pois, quando $a=\overline{b}=\overline{c}=1$, então $f(a,b,c)=f(1,0,0)=1$ e $a\overline{b}\overline{c}=1.1.1=1$. Enfim, a forma disjuntiva normal de f é a soma dos polinômios minimais, onde f tem o valor 1, ou seja: $f(a,b,c)=abc+a\overline{b}c+a\overline{b}\overline{c}+\overline{a}bc+\overline{a}\overline{b}c$ e a fórmula booleana correspondente a f é $F(X,Y,Z)=XYZ+X\overline{Y}Z+X\,\overline{Y}\,\overline{Z}+\overline{X}YZ+\overline{X}\,\overline{Y}\,Z$.

Teorema 5.89 *Seja $F(X_1,X_2,\ldots,X_n)$ uma fórmula booleana associada à função booleana $f:B^n\to B$. Então a forma disjuntiva normal F é dada por*

$$F(X_1,X_2,\ldots,X_n)=\sum_{(a_1,\ldots,a_n)\in B^n} f(a_1,a_2,\ldots,a_n).X_1^{a_1}X_2^{a_2}\cdots X_n^{a_n},$$

onde $f(a_1,a_2,\ldots,a_n)=1$.

Mapas de Veitch-Karnaugh para 4 Variáveis

O processo para obter os mapas V-K para quatro variáveis é o mesmo processo anterior. Por exemplo, as regiões de A e $\overline{A}$ tem cada uma delas a metade da região total e suas regiões não se cruzam, mas cruzam com todas as outras regiões das outras células. Assim por diante.

Eles têm a configuração que segue, onde só foram indicadas as células básicas da diagonal.

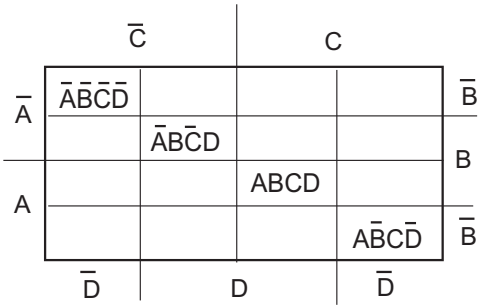


Figura 5.20: Mapa V-K para 4 Variáveis

Cada uma das dezesseis células corresponde a um polinômio minimal e é a interseção de quatro regiões A ou $\overline{A}$, B ou $\overline{B}$, C ou $\overline{C}$ e D ou $\overline{D}$.

O processo de simplificação é o mesmo que o anterior, de modo que, agora, o agrupamento principal é uma *oitava* que corresponde a uma das literais A, $\overline{A}$, B, $\overline{B}$, $C, \overline{C}$, D ou $\overline{D}$. Depois, seguem as quadras, cuja simplificação elimina duas variáveis dos polinômios minimais envolvidos. Depois, seguem os pares de células adjacentes, cuja simplificação elimina uma variável do polinômio minimal correspondente.

Os polinômios minimais já usados em alguns pares, quadras ou oitavas podem ser repetidos para formar outras combinações de pares, quadras ou oitavas.

Novamente, deve-se identificar os segmentos $\overline{PQ}$ com $\overline{P'Q'}$ (nesta ordem), pois as quatro células da região $\overline{C}\ \overline{D}$ são adjacentes as quatro células da região $\overline{D}C$: por exemplo, $\overline{A}B\overline{C}\ \overline{D}$ e $\overline{A}BC\overline{D}$ são polinômios minimais de células adjacentes. Além disso, os segmentos $\overline{PP'}$ e $\overline{QQ'}$ devem ser identificados (nesta ordem), pois as células correspondentes, por exemplo, aos polinômios minimais $\overline{A}\ \overline{B}CD$ e $A\overline{B}CD$, que estão de lados opostos, são adjacentes.

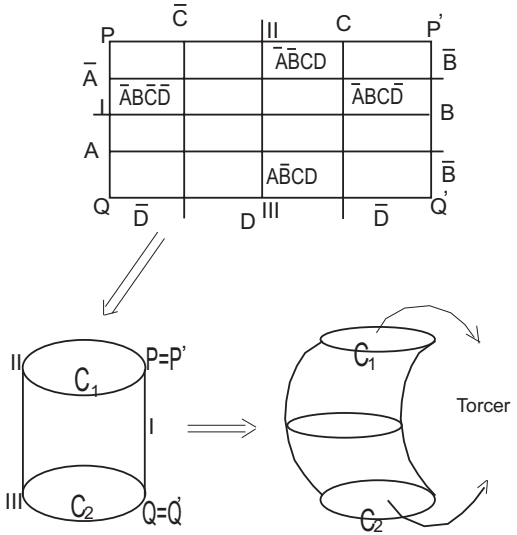


Figura 5.21: Cilindro Torcido

Com isto, identificando as curvas $C1$ e $C2$ preservando a orientação, obtém-se uma figura dita *Toro* de genus 1 (o pneu).

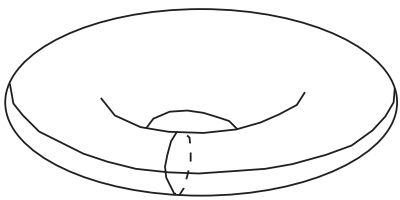


Figura 5.22: Toro de Genus 1.

Exemplo. Dada a função $f : B^4 \to B$ do diagrama que segue, dê uma fórmula booleana associada a esta função. Use mapas V-K, simplifique a fórmula e dê uma expressão para a função como soma de produtos, mais simples possível.

a	b	c	d	$f(a,b,c,d)$
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	1
0	1	0	0	0
0	1	0	1	1
0	1	1	0	0
0	1	1	1	1
1	0	0	0	1
1	0	0	1	1
1	0	1	0	0
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	0
1	1	1	1	1

Solução: Sabendo-se que o polinômio minimal $A^a B^b C^c D^d$, onde $f(a,b,c,d) = 1$, ocorre na f.d.n. da fórmula booleana $F(A,B,C,D)$ associada à função f, temos que $F = \overline{A}\ \overline{B}\ \overline{C}\ D + \overline{A}\ \overline{B}\ C\ \overline{D} + \overline{A}\ \overline{B}\ C\ D + \overline{A}\ B\ \overline{C}\ D + \overline{A}\ B\ C\ D + A\ \overline{B}\ \overline{C}\ \overline{D} + A\ \overline{B}\ \overline{C}\ D + A\ \overline{B}\ C\ D + A\ B\ \overline{C}\ \overline{D} + A\ B\ \overline{C}\ D + A\ B\ C\ D$.

Todos estes polinômios minimais estão identificados no mapa V-K que segue.

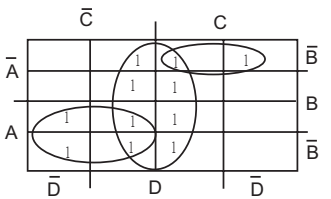


Figura 5.23:

Podemos notar que temos a região D totalmente preenchida (uma oitava). As quadras e duplas desta região não precisam ser consideradas (Por quê?). Temos a quadra circulada no mapa que

dá a região A intersecção $\overline{C}$. Logo, é $A\overline{C}$, e a dupla circulada no mapa é a inteseção das regiões $\overline{A}$, $\overline{B}$ e C. Logo, é $\overline{A}\ \overline{B}\ C$. Somando os resultados, temos: $F = \overline{A}\ \overline{B}\ C + A\overline{C} + D$ e também $f(a,b,c,d) = \overline{a}\ \overline{b}\ c + a\overline{c} + d$.

Finalmente, também usam-se os mapas de V-K para simplificar expressões com mais de 4 variáveis, e o processo vai se complicando mais. Isto pode ser visto em livros sobre Circuitos Lógico, quanto a nós, paremos por aqui.

Exercícios

(1) Construa todas funções booleanas binárias sobre $A = \{0, a, \overline{a}, 1\}$ que satisfazem as condições dada na tabela:

x	y	$f(x,y)$
0	a	a
1	1	$\overline{a}$
$\overline{a}$	a	0
a	1	0

(2) Sendo $s_e(X) = x_1^{\overline{e}_1} + \cdots + x_n^{\overline{e}_n}$, demonstre que $s_e(j) = \overline{\delta}_{ij}$ por dualidade da demonstração do Lema 5.74, ou seja: demonstre que $[(s_e(j) = 0) \Longleftrightarrow (j_r = \overline{e}_r \text{ para } r = 1, 2, \ldots, n)]$.

(3) Descreva o processo dual do processo realizado na prova do Teorema 5.75 e do Exemplo 5.77 para determinar os índices dos polinômios maximais de f.

(4) Determine a função booleana realizada por cada um dos circuitos:

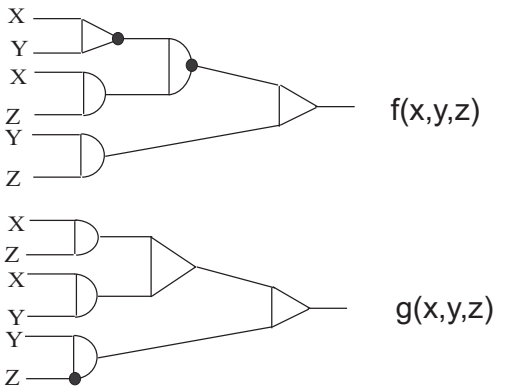


Figura 5.24: Exercício 4.

(5) Determine um circuito equivalente e mais simples (se possível) para cada circuito do exercício anterior.

(6) Dadas $g(x) = [(x_1.\overline{x}_2)(x_1 + x_2)] + [\overline{x_1.\overline{x}_2}.(\overline{x_1 + x_2})]$ sobre a álgebra booleana $(B^2, +, .)$ e $f(x) = \overline{x}_1 + \overline{\overline{x}_2 + x_3}$ sobre a álgebra booleana $(B^3, +, .)$,

(i) Dê as formas conjuntiva e disjuntiva normais e as formas normais de g e f.

(ii) Construa os circuitos de todas as formas canônicas de g e de f;

(7) Repita o exercício anterior para a função $h(x_1, x_2, x_3, x_4) = x_1 + x_2\overline{x}_3 + x_3\overline{x}_4$ definida sobre B^4.

(8) **(i)** Calcule todas as $16 = 2^{2^2}$ funções booleanas de B^2 em B;

(ii) Mostre que existem precisamente 2^{2^n} funções booleanas de n variáveis sobre $B = \{0, 1\}$.

(9) Quais as funções booleanas associadas aos circuitos abaixo:

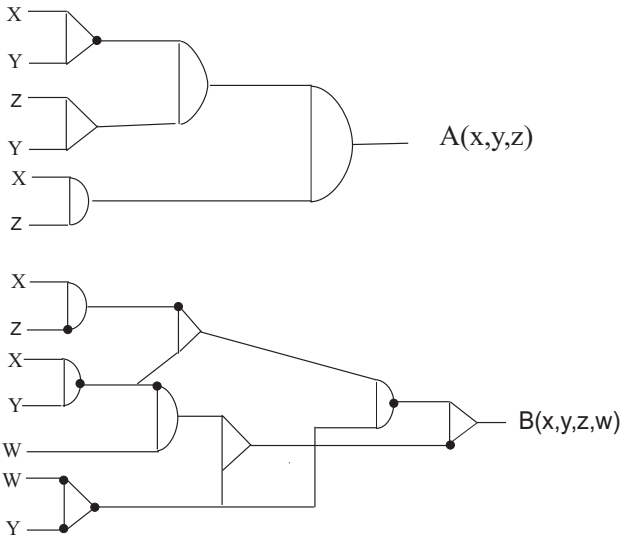


Figura 5.25: .

(10) Escreva a função $f(x) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3$, sobre a álgebra booleana $(B^3(F), +, \cdot)$. Observação: $a \oplus b = a\overline{b} + \overline{a}b$.

(11) Ache as f.c.n. e f.d.n. de

(i) $f(x) = \overline{x_1x_2x_3x_4} \oplus x_1x_2 \oplus x_3x_4$ e

(ii) $f(x, y, z) = x\overline{z} + y$.

(12) Obtenha a representação normal de

(i) $f(x) = \prod(0, 1, 5, 6)$, onde $x = (x_1, x_2, x_3)$ e

(ii) $g(x) = x_1\overline{x}_2 + x_2\overline{x}_3 + \overline{x}_1x_3$.

(13) Determine todos os valores de (x_1, x_2, x_3, x_4) que satisfaçam

(i) $\begin{cases} (x_1x_2 + \overline{x}_3)\overline{x}_4 = 1 \\ (\overline{x_1 + x_4} + x_2)x_3 = 0 \end{cases}$ e **(ii)** $\begin{cases} (x_1x_2 + \overline{x}_3)\overline{x}_4 = 1 \\ (x_2x_4 + \overline{x}_1.x_3)x_4 = 0. \end{cases}$

(14) Obtenha circuitos mais econômicos de cada item do exercício 6.

(15) Construa um circuito correspondente à função $f(x_1, x_2, x_3) = x_1\overline{x}_2 + x_2(\overline{x}_1 + x_3)$.

(16) Considere a álgebra booleana $A = \{0, a, \overline{a}, b, \overline{b}, c, \overline{c}, 1\}$

(a) Faça o diagrama de Hasse para A.

(b) Quantos átomos A possui? Quais?

(c) Determine $a+b,\ a+c,\ b+c$.

(d) Calcule uma função (se existir alguma) $f : A^2 \to A$ que satisfaça $f(1,1) = \overline{a},\quad f(1,c) = \overline{c},\quad f(0,0) = a,\quad f(a,\overline{b}) = c$.

(17) Há cinco livros em uma estante $v,\ w,\ x,\ y$ e z. Você deve selecionar alguns livros de modo a satisfazer todas as condições a seguir:

(i) Selecionar v ou w ou ambos;

(ii) Selecionar x ou z, mas não ambos;

(iii) Selecionar v e z juntos ou nenhum dos dois;

(iv) Se selecionar y, também deve selecionar z;

(v) Se selecionar w, também deve selecionar v e y.

Pede-se:

(a) Coloque esta situação como uma expressão usando os símbolos lógicos,

(b) Simplifique a expressão obtida,

(c) A partir de (b), dê um outro conjunto (menor em número) de condições equivalentes às 5 condições dadas.

(19) Considere as variáveis x_1, x_2, x_3. Faça o diagrama de Hasse correspondente ao conjunto $\{0, 1, x_1 + x_2 + x_3, x_1, x_2, x_3, x_1x_2x_3, x_1x_2, x_2 + x_3, x_1x_3, x_1 + x_2, x_2x_3, x_1 + x_3\}$.

Capítulo 6

NOÇÕES DE COMPUTABILIDADE

6.1 Enumerabilidade e Cardinalidade

É natural indagar se dois conjuntos têm ou não o mesmo número de elementos. Para conjuntos finitos, a resposta pode ser obtida contando os elementos de cada conjunto. Já no caso infinito, a resposta vai depender de como se define que dois conjuntos têm o mesmo número de elementos. Antigamente se pensava que todos os conjuntos infinitos tinham o mesmo número de elementos. A seguinte definição, que é a mais natural, e que revolucionou a teoria dos conjuntos, é devida ao matemático alemão Georg Cantor (1845-1918).

Definição 6.1 Dois conjuntos A e B são ditos *equivalentes* ou *equipotentes* (mesma potência) e denota-se por $A \sim B$, se existe uma função bijetora de A em B. Neste caso, também se diz que A e B têm o mesmo *número cardinal*, ou a mesma *cardinalidade*. A cardinalidade de A é denotada por $|A|$, ou por $\sharp(A)$. A cardinalidade dos números naturais é denotada por *Aleph Zero*. Em símbolos $|\mathbb{N}| = \aleph_0$.

Exemplo 6.2 (a) $\{0,\ 1,\ 5\} \sim \{a,\ b,\ *\}$, pois $f(0) = b,\ f(1) = a$, e $f(5) = *$ é uma bijeção entre os dois conjuntos dados, e $|\{0, 1, 5\}| = 3 = |\{a,\ b,\ *\}|$.

(b) $\mathbb{N}^* = \{1, 2, 3, 4, \ldots\} \sim P = \{0, 2, 4, \ldots\}$, pois $f(x) = 2(x - 1)$ é uma bijeção de $\mathbb{N}^*$ em P. Logo $\sharp(P) = \aleph_0$

(c) $A = \{0, 1\}$ não é equipotente a $B = \{0, 2, 6\}$, pois não existe função bijetora de A em B.

(d) $0,\ 1,\ 5,\ 34,\ 80, \aleph_0$ são números cardinais.

Lema 6.3 A relação de equipotência definida acima, sobre as partes de um conjunto universo U, é de equivalência.

Demonstração: Basta ver que para $A,\ B$ e $C \subset U,\ id_A \colon A \to A$ é uma função bijetora e, se $f \colon A \to B,\ \ g \colon B \to C$ são funções bijetoras, então $f^{-1} \colon B \to A$ e $g \circ f \colon A \to C$ são bijetoras. □

6.1.1 Aleph Zero e Conjuntos Contáveis

Definição 6.4 Seja $I_n = \{1, 2, \ldots, n\},\ n > 0$. Um conjunto A é dito *finito* se ele é vazio ou existe uma função bijetora $f : I_n \to A$, para algum $n > 0$ em $\mathbb{N}$. Denotando $f(i)$ por a_i, tem-se que $A = \{a_1, a_2, \ldots, a_n\}$. Caso contrário, A é dito *infinito*.

Definição 6.5 Um conjunto A é dito *enumerável* se A é equipotente a $\mathbb{N}$, ou seja, se existe uma função bijetora $f : \mathbb{N} \to A;\ f(i) = a_i$. Neste caso, a função f é dita uma *enumeração* para A.

Um conjunto é dito *contável* se ele é finito ou enumerável.

Exemplo 6.6 (1) $\mathbb{N}$ é enumerável, pois a função identidade de $\mathbb{N}$, $Id_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$, $Id_{\mathbb{N}}(i) = i$, enumera $\mathbb{N}$.

(2) $P = \{0, 2, 4, \ldots\} \sim \mathbb{N}$ é enumerável, pois $f : \mathbb{N} \to P$, dada por $f(i) = 2i$, é uma bijeção.

(3) O conjunto dos números inteiros $\mathbb{Z}$ é enumerável, pois:

$$f : \mathbb{N} \to \mathbb{Z},\ \text{dada por}\ f(n) = \begin{cases} \frac{n}{2}, & \text{se } n: \text{ é par} \\ -\frac{n+1}{2}, & \text{se } n: \text{ é ímpar} \end{cases}$$

é bijetora. (Prove!).

(4) $A = \{0, 1, 1/2, 1/3, \ldots\}$ é enumerável, pois: $f : \mathbb{N} \to A$ dada por: $f(0) = 0$, e $f(i) = 1/i\ ,\ i \neq 0$, é uma função bijetora.

(5) Se A é enumerável, então $A \times \{b\} = \{(a, b);\ a \in A\}$ é enumerável. De fato, por hipótese existe $\varphi : \mathbb{N} \to A$: bijetora. Daí $f : \mathbb{N} \to A \times \{b\},\ f(n) = (\varphi(n), b)$ é uma enumeração de $A \times \{b\}$.

(6) $0, 1, 2, 4, 3, 5, 6, 8, 10, 7, 9, 11, 12, 14, 16, 18, \ldots$ é uma enumeração de $\mathbb{N}$, pois há uma lei de formação para esta reenumeração dos números naturais: em ordem crescente vamos colocando o primeiro número natural par, depois o primeiro número natural ímpar, segue-se os dois próximos pares e os dois próximos ímpares, depois três números pares e três números ímpares, assim por diante, sempre em ordem crescente. Com esta lei de formação, sabemos que posição ocupa qualquer número natural n dado. Por exemplo o número 7 ocupa a décima posição. Agora, a seqüência $0, 2, 4, 6, 8, \ldots, 1, 3, 5, 7, 9, \ldots$ de todos os números naturais não é uma enumeração de $\mathbb{N}$, pois 1 aparece na posição "infinita".

Teorema 6.7 Todo conjunto infinito A contém um subconjunto enumerável.

Demonstração: Tome $f : \wp(A) - \emptyset \to A$ uma função escolha (veja cap.4 §4.6 (B)) e considere a seqüência $a_1 = f(A)$, $a_2 = f(A \setminus \{a_1\}), \ldots, a_n = f(A \setminus \{a_1, \ldots, a_{n-1}\})$. Como A é infinito, o conjunto $A \setminus \{a_1, \ldots, a_n\}$ não é vazio, para qualquer $n \in \mathbb{N}$. Por construção de f, tem-se que $a_i \neq a_j$, para $i \neq j$. Assim $D = \{a_1, a_2, \ldots, a_n, \ldots\}$ é enumerável. □

Teorema 6.8 Todo subconjunto de um conjunto enumerável ou contável é contável.

Demonstração: Seja A enumerável, $A = \{a_1, a_2, \ldots, a_n, \ldots\}$ e $B \subseteq A$. Se B é finito, então B é contável. Se B não é finito, seja a_{n_1} o primeiro elemento da enumeração acima que aparece em B. Seja a_{n_2} o primeiro elemento da enumeração de A, que aparece em $B \setminus \{a_{n_1}\}$. Continuando com este procedimento, obteremos uma seqüência $a_{n_1}, a_{n_2}, \ldots$ contida em A e que acaba por dar uma enumeração de B. No caso de A ser finito, obrigatoriamente B é finito. Logo contável. □

Exemplo 6.9 O conjunto dos números primos naturais é enumerável, pois este conjunto é infinito e $\mathbb{N}$ é enumerável.

Proposição 6.10 Um conjunto A é infinito se, e somente se, existe um subconjunto próprio de A equipotente a A.

Demonstração: ($\Longrightarrow$) Se A é infinito, pelo Teorema 6.7 existe um subconjunto de A enumerável, digamos $S = \{a_1, a_2, a_3, \ldots\}$.

Tome $B = A - \{a_1\}$, e $f : A \to B$, $f(x) = \begin{cases} x, & \text{se } x \in A \setminus S \\ a_{i+1}, & \text{se } x = a_i \in S. \end{cases}$

A função f é bijetora.

($\Longleftarrow$) Reciprocamente, se existe uma função bijetora $f : A \to B$, onde B é uma parte própria de A, então pelo Princípio da Casa do Pombo A é infinito. □

Teorema 6.11 Sejam $\{A_i\}_{i \in I}$, $I \subseteq \mathbb{N}^*$ uma família contável de conjuntos dois a dois disjuntos e contáveis. Então $A = \bigcup_{i \in I} A_i$ é contável.

Demonstração: Tal ordenação (se A é finito) ou enumeração (caso contrário) de A pode ser obtida por um passeio de Cantor. Para isto, seja $A_i = \{a_{i1}, a_{i2}, a_{i3}, \ldots\}$ uma enumeração de A_i se A_i é infinito, e uma ordenação, caso A_i é finito. Considere o passeio de Cantor sobre a matriz

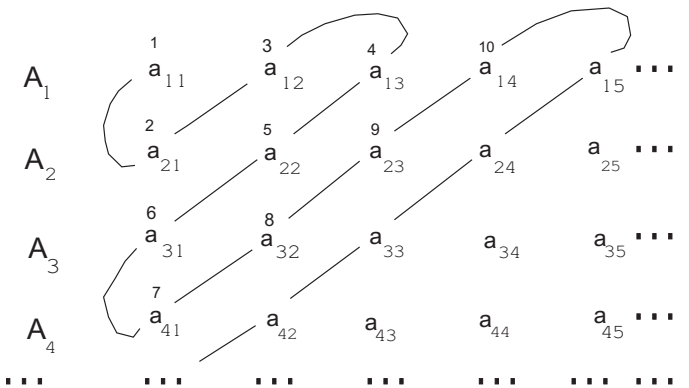


Figura 6.1: Passeio de Cantor.

Assim temos a ordenação ou enumeração de A : $a_{11}, a_{21}, a_{12}, a_{13}, a_{22}, a_{31}, \ldots$ □

Corolário 6.12 $\mathbb{N} \times \mathbb{N}$ é enumerável.

Demonstração: Tome as famílias $A_i = \{(i, n),\ n \in \mathbb{N}\}$ no Teorema anterior. □

Corolário 6.13 O conjunto de todas as seqüências finitas de um conjunto A contável não vazio é enumerável.

Demonstração: Note que o conjunto de todas seqüências finitas sobre A é infinito, mesmo que A seja finito. Se $A = \{a\}$, então o conjunto citado é $\{a, aa, aaa, \ldots\}$. Logo, se A não é unitário, mas é finito, podemos ordenar seus elementos e, se A é infinito, podemos enumerar seus elementos. Então podemos descrever $A = \{a_1, a_2, a_3, \ldots\}$.

Para enumerar ou ordenar $A \times A$, tome as famílias $A_i = \{(a_i, a_n), a_n \in A\}$ no Teorema acima. Um passeio de Cantor enumera ou ordena (não de modo único) $S = A \times A$, do seguinte modo:

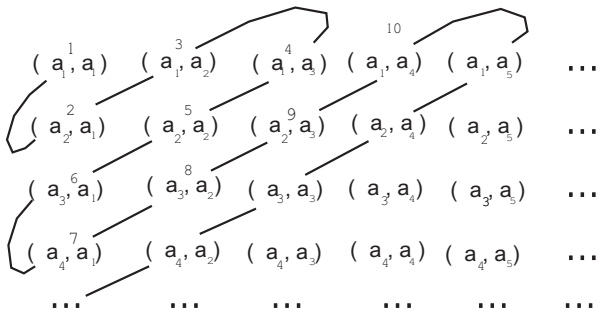


Figura 6.2: Segundo Passeio de Cantor.

E com isto temos a enumeração de todas as seqüências finitas de comprimento dois: (a_1, a_1), (a_2, a_1), (a_1, a_2), (a_1, a_3), (a_2, a_2), (a_3, a_1), (a_4, a_1), $(a_3, a_2), \ldots$

Para enumerar (ou ordenar) as seqüências finitas de comprimento três, ou seja, os elementos de $A \times A \times A = A \times S$, faça $B_i = \{(a_i, s_j),\ s_j \in S\}$ no Teorema anterior. Isto é possível, pois, S já está enumerado pelo passeio de Cantor anterior. Assim:

$$
\begin{array}{lccccc}
B_1: & (a_1,a_1,a_1) & (a_1,a_2,a_1) & (a_1,a_1,a_2) & (a_1,a_1,a_3) & \cdots \\
B_2: & (a_2,a_1,a_1) & (a_2,a_2,a_1) & (a_2,a_1,a_2) & (a_2,a_1,a_3) & \cdots \\
B_3: & (a_3,a_1,a_1) & (a_3,a_2,a_1) & (a_3,a_1,a_2) & (a_3,a_1,a_3) & \cdots \\
B_4: & (a_4,a_1,a_1) & (a_4,a_2,a_1) & (a_4,a_1,a_2) & (a_4,a_1,a_3) & \cdots \\
\bullet & \bullet & \bullet & \bullet & \bullet & \cdots
\end{array}
$$

Agora um passeio de Cantor sobre esta tabela enumera $A \times A \times A$, ou seja, as seqüências de comprimento 3.

Prosseguindo assim, enumeramos o conjunto das seqüências de qualquer comprimento fixado. Daí, um passeio de Cantor sobre a tabela

$$
\begin{array}{rccccc}
A: & a_1 & a_2 & a_3 & a_4 & \cdots \\
A\times A: & (a_1,a_1) & (a_2,a_1) & (a_1,a_2) & (a_1,a_3) & \cdots \\
A\times A\times A: & (a_1,a_1,a_1) & (a_2,a_1,a_1) & (a_1,a_2,a_1) & (a_1,a_1,a_2) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

obtém-se a conclusão desejada. □

Como conseqüência deste Corolário, temos que o conjunto das seqüências finitas de um conjunto enumerável é enumerável; mas um fato surpreendente do conceito de enumeração é que o dual desta proposição é falsa, ou seja,

Proposição 6.14 O conjunto das seqüências enumeráveis (ou infinitas) de elementos de um conjunto finito L (com pelo menos 2 elementos) não é enumerável.

O método da prova desta proposição, chamado método diagonal de Cantor está na raiz de muitos paradoxos e tem papel central em todo o conhecimento matemático: o argumento do método diagonal prova que existem funções que não são computáveis, que existem conjuntos recursivamente enumeráveis que não são recursivos e, finalmente, alcança o seu apogeu no teorema de Gödel acerca da incompletude da aritmética. Este método será aplicado em computabilidade de funções, a seguir.

Para a demonstração da proposição, vamos mostrar que o conjunto das seqüências enumeráveis de entradas 0 e 1, isto é, em $L = \{0, 1\}$, não é enumerável (note que não há perda de generalidade, pois, se $L = \{a_1, a_2, \ldots, a_n\}$, sempre podemos codificar $a_1, a_2, a_3, \ldots, a_n$ por distintas seqüências de 0's e 1's (veja exercício) e, desta forma, o conjunto das seqüências em L pode ser associado a um subconjunto das seqüências em $\{0, 1\}$. Por outro lado, podemos identificar as seqüências em $\{0, 1\}$ com as seqüências em, digamos, $a_1 \equiv 0$ e $a_2 \equiv 1$. O que acabamos de provar é que os conjuntos de seqüências enumeráveis com componentes em um conjunto finito, com pelo menos 2 elementos, têm a mesma cardinalidade). Agora, suponhamos que S, o conjunto das seqüências em $\{0, 1\}$, fosse enumerável, isto é, $S = \{A_1,\ A_2, \cdots\}$. Para visualizar, suponhamos, por exemplo, que

$$
\begin{array}{rcl}
A_1 & = & \mathbf{1}1001000010101011110001010101010110101 \cdots \\
A_2 & = & 1\mathbf{0}1010101010111100011101010101000010000 \cdots \\
A_3 & = & 00\mathbf{0}1110101010100000110001011111000010 1 \cdots \\
A_4 & = & 110\mathbf{1}1100011001011100001111111110111100 \cdots \\
\vdots & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \cdots \\
A_n & = & 11001100001100111100.\ldots\ldots\mathbf{1}.\ldots\ldots \cdots
\end{array}
$$

Fixada esta enumeração (ou outra qualquer), tomamos a seqüência 'dual' da seqüência diagonal; $0110\cdots0\cdots$; que não aparece na lista acima, pois difere da n-ésima seqüência listada na n-ésima posição. Em geral, se a_{ii} é o i-ésimo elemento de A_i, tome a seqüência $(1 - a_{11})(1 - a_{22})\cdots(1 - a_{ii})\cdots$ Ela não pertence a S. Logo, S não é uma enumeração. □

Proposição 6.15 O conjunto $\mathbb{Q}$ dos números racionais é enumerável.

Demonstração: Sejam $\mathbb{Q}^+ = \{\frac{a}{b},\ a > 0,\ b > 0,\ a,\ b \in \mathbb{N}$ e $mdc(a,b)=1\}$ e $\mathbb{Q}^- = \{-x,\ x \in \mathbb{Q}^+\}$. Então $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$. Pelo Corolário 6.12 enumeramos $\mathbb{N} \times \mathbb{N}$. Se identificarmos $\frac{a}{b} \in \mathbb{Q}^+$ com $(a,b) \in \mathbb{N} \times \mathbb{N}$, temos uma bijeção de $\mathbb{Q}^+$ em um subconjunto infinito T de $\mathbb{N} \times \mathbb{N}$. Como subconjunto infinito de conjunto enumerável é enumerável (Teorema 6.8), temos que T, e portanto $\mathbb{Q}^+$, são enumeráveis. Seja $f : \mathbb{N} \to \mathbb{Q}^+$ uma enumeração de $\mathbb{Q}^+$. Então:

$$\mathbb{N} \xrightarrow{f} \mathbb{Q}^+ \xrightarrow{g} \mathbb{Q}^-,$$

enumera $\mathbb{Q}^-$, onde a função g é dada por: $g(x) = -x$. Pelo Teorema 6.11, $\mathbb{Q}$ é enumerável. □

Nota. Com isto, temos que os seguintes conjuntos têm cardinalidade $\aleph_0$: conjunto dos números inteiros pares, $\mathbb{N} \times \mathbb{N}$, o conjunto dos números racionais $\mathbb{Q}$ e o conjunto dos números inteiros $\mathbb{Z}$.

Corolário 6.16 O conjunto P de todos os polinômios $p(x) = a_0 + a_1x + \cdots + a_nx^n$ com coeficientes inteiros é enumerável.

Demonstração: Para cada $(k,m) \in \mathbb{N} \times \mathbb{N}$, seja $P(k,m) = \{$polinômios de grau m e $|a_0| + \cdots + |a_m| = k\}$. Como $P(k,m)$ é finito, por definição $P(k,m)$ é contável. Assim

$$P = \bigcup_{(k,m)\in\mathbb{N}\times\mathbb{N}} P(k,m)$$

é contável e infinito. Logo P é enumerável, pelo Teorema 6.11. □

6.1.2 O Contínuo e Outros Números Cardinais

A Proposição 6.14 mostra que nem todos os conjuntos são contáveis. Agora, veremos outros exemplos de conjuntos que não são contáveis.

Proposição 6.17 O intervalo real $[0,1]$ não é contável.

Demonstração: Considere todas as seqüências infinitas em $[0,1]$ formadas de 0's e 1's. Pela Proposição 6.14, este subconjunto não é contável. Pelo Teorema 6.8, $[0,1]$ não pode ser contável. □

Definição 6.18 Diz-se que um conjunto A apresenta a *potência do contínuo* e denota-se por $|A| = \mathbf{c}$, se A equipotente a $[0,1]$.

Exemplo 6.19 **1.** O intervalo real $]0,1[:= \{x \in \mathbb{R} : 0 < x < 1\}$ apresenta a potência do contínuo.

Vamos construir uma função bijetora de $[0,1]$ em $]0,1[$. Sejam $B = \{0, 1, 1/2, 1/3, \ldots\}$, $C = \{1/2, 1/3, 1/4, \ldots\}$ e consideremos $\varphi : B \to C$ dada por: $\varphi(0) = \frac{1}{2}$ e $\varphi(\frac{1}{n}) = \frac{1}{n+2}$, $n \geq 1$. Como $\varphi : B \to C$ é bijetora, tem-se $B \sim C$. Agora, $[0,1] \setminus B =]0,1[\setminus C$ e, portanto, a função $f(x) = \begin{cases} \varphi(x), & x \in B \\ x, & x \in [0,1] \setminus B, \end{cases}$ dá uma bijeção entre $[0,1]$ e $]0,1[$.

2. Sejam $a, b \in \mathbb{R}, a < b$ e $A =]a,b[$. Então A apresenta a potência do contínuo, pois: $f :]0,1[\to A$, dada por: $f(x) = a + (b-a)x$, é bijetora. Prove!

Em particular, $|]-1,1[| = \mathbf{c}$.

3. Vamos mostrar, agora, que $\mathbb{R}$ apresenta a hipótese do contínuo.

Como $g(x) = \dfrac{x}{1-|x|}$ dá uma bijeção de $]-1,1[$ em $\mathbb{R}$, pois admite inversa $g^{-1}(x) = \dfrac{x}{1+|x|}$ (verifique), temos que $g \circ f :]0,1[\to \mathbb{R}$ dada por $g \circ f(x) = \dfrac{2x-1}{1-|2x-1|}$ dá uma bijeção entre $]0,1[$ e $\mathbb{R}$. Logo $|\mathbb{R}| = \mathbf{c}$.

Observação 6.20 Observe então que $\mathbb{R}$ ou qualquer intervalo real não é contável.

Corolário 6.21 O conjunto dos números irracionais I_r não é contável.

Demonstração: Basta ver que $\mathbb{R} = \mathbb{Q} \cup I_r$. Como $\mathbb{Q}$ é contável, se I_r fosse contável pelo Teorema 6.11, viria que $\mathbb{R}$ seria contável. □

Até agora conhecemos os seguintes números cardinais: os números cardinais finitos, $\aleph_0$ e $\mathbf{c}$. O Teorema de G. Cantor, a seguir, mostra que existe uma infinidade de outros números cardinais.

Definição 6.22 Dados cardinais $\alpha,\ \beta$ sejam $A,\ B$ conjuntos de cardinalidade $\alpha,\ \beta$, respectivamente.

Dizemos que *alfa é menor ou igual a beta* e denotemos por $\alpha \leq \beta$ se existe uma função injetora $f : A \to B$. Se, além disso, $A \not\sim B$, dizemos que α *é estritamente menor que* β e denotemos por $\alpha < \beta$. Se $\alpha \leq \beta$ e $\beta \leq \alpha$, dizemos que α e β *são iguais.*

Por exemplo, $\aleph_0 < \mathbf{c}$, pois: $\varphi : \mathbb{N} \to \mathbb{R}$ dada por: $\varphi(x) = x$ é injetora e $\mathbb{N}$ não é equipotente a $\mathbb{R}$, pois $\mathbb{N}$ é enumerável e $\mathbb{R}$ não é enumerável.

Teorema 6.23 *G. Cantor.*

Para todo conjunto A tem-se que a cardinalidade de A é estritamente menor que a cardinalidade do conjunto das partes de A, ou seja, $|A| < |\wp(A)|$.

Demonstração: $f : A \to \wp(A)$ dada por: $f(a) = \{a\}$ é injetora e não é sobrejetora, pois $\emptyset \notin Imf$. Logo $|A| \leq |\wp(A)|$.

Seja $g : A \to \wp(A)$ uma função qualquer. Considere o subconjunto S de A, definido por $S = \{x \in A : x \notin g(x)\}$. Se g fosse sobrejetora, existiria $y \in A$, tal que $g(y) = S$. Por construção, temos: $y \in S \iff y \notin g(y) = S$, absurdo. Portanto não pode haver sobrejeção de A em $\wp(A)$. E então $|A| < |2^A|$. □

Nota: O Teorema 6.23 nos dá a seguinte cadeia de desigualdade de números cardinais infinitos

$$\aleph_0 < \mathbf{c}\ < |\wp(\mathbb{R})| < |\wp\big(\wp(\mathbb{R})\big)| < \cdots$$

Isto mostra que temos uma infinidade de números cardinais infinitos. Ainda pelo teorema de Cantor, temos $\aleph_0 < |\wp(\mathbb{N})|$. Também vimos que $\aleph_0 < \mathbf{c}$. O próximo teorema mostra a relação de $|\wp(\mathbb{N})|$ e $\mathbf{c}$.

Teorema 6.24 A cardinalidade do conjunto das partes de $\mathbb{N}$ é igual à cardinalidade de $\mathbb{R}$, ou seja, $|\wp(\mathbb{N})| = \mathbf{c}$.

Demonstração: Seja $f : \mathbb{R} \to \wp(\mathbb{Q})$ definida por: $f(a) = \{x \in \mathbb{Q} :\ x < a\}$. Mostremos que f é injetora.

Seja $a < b,\ a,\ b \in \mathbb{R}$. Como $\mathbb{Q}$ é denso em $\mathbb{R}$, isto é, $\forall a,\ b \in \mathbb{R}$ se $a < b$, então existe $x \in \mathbb{Q}$, tal que $a < x < b$. De fato, como $0 < b - a$, existe $n \in \mathbb{N}$, tal que $0 < \frac{1}{n} < a - b$. Daí existe $j \in \mathbb{N}$, tal que $a < j.\frac{1}{n} < b$. Com isto, mostramos que $j/n \in f(b)$ e $j/n \notin f(a)$, ou seja, $f(a) \neq f(b)$. Logo, f é injetora e, por definição, $|\mathbb{R}| \leq |\wp(\mathbb{N})|$.

Para a recíproca, usaremos o fato de que $F : \wp(A) \to B^A,\ B = \{0,1\}$, dada por: $F(S) = c_S$, é bijetora, onde c_S é a função característica de S, (veja o exercício 4 do cap.4 §4.6(c)). Desta bijeção temos que $|\wp(A)| = |B^A|$. Agora, seja $G : B^{\mathbb{N}} \to [0,1]$ dada por: $G(c_S) = 0, c_S(0)c_S(1)c_S(2)\cdots$ um decimal infinito composto de 0's e 1's. Se $c_{S_1},\ c_{S_2} \in B^{\mathbb{N}}$ e $c_{S_1} \neq c_{S_2}$, então $c_{S_1}(i) \neq c_{S_2}(i)$ para algum $i \in \mathbb{N}$. Logo $G(c_{S_1})$ e $G(c_2 S)$ são distintos, pois diferem pelo menos na i-ésima posição, ou seja, G é uma função injetora. Assim, por definição, $|B^{\mathbb{N}}| \leq |[0,1]| = \mathbf{c}$. Daí $|\wp(\mathbb{N})| \leq \mathbf{c}$ devido à bijeção F dada acima. Concluímos que $|\wp(\mathbb{N})| = \mathbf{c}$. □

Hipótese do contínuo

Existe número cardinal entre $\aleph_0$ e $\mathbf{c}$? Originalmente Cantor apoiou a conjectura que é conhecida como *hipótese do Contínuo*: "não existe número cardinal β tal que $\aleph_0 < \beta < |\wp(\mathbb{N})| = \mathbf{c}$". Mas, em 1963, demonstrou-se que a hipótese do contínuo é independente dos axiomas da teoria dos conjuntos, aproximadamente do mesmo modo em que o Quinto Postulado de Euclides, sobre linhas paralelas, é independente dos outros axiomas da geometria.

Exercícios

(1) Mostre que A é contável se, e somente se, existe uma sobrejeção $\varphi : \mathbb{N} \to A$.

(2) Mostre que: **(a)** $\mathbb{N} \sim (\mathbb{N} \setminus I_k)$, **(b)** $A \sim (A \setminus B)$, onde A é um conjunto infinito e B é um subconjunto finito de A.
(c) Com base em (a) e (b) justifique: Em um hotel com infinitos quartos, todos eles ocupados, ainda há vagas para mais n pessoas.

(3) **(a)** - Sejam $\varphi : \mathbb{N} \longrightarrow \mathbb{N}^*$ e $\psi : \mathbb{N}^* \longrightarrow \mathbb{N} \times \mathbb{N}$ dadas por $\varphi(a) = a + 1$, e $\psi(b) = (s,t)$, onde $b = 2^s(2t+1)$. Mostre que $\psi \circ \varphi$

enumera $\mathbb{N} \times \mathbb{N}$.

(b) - A partir de (a), dê uma outra prova de que $\mathbb{Q}$ é enumerável.

(4) Codifique toda seqüência não nula do intervalo real $[0, 1]$ como uma seqüência infinita de 0's e 1's.
Obs.: Uma codificação de elementos de $A \neq \emptyset$ por elementos de $D \neq \emptyset$ é uma função injetora $f : A \to D$ e, neste caso, dizemos que $a \in A$ fica codificado por $f(a) \in D$.

Use que toda seqüência não nula do intervalo real $[0, 1]$ pode ser escrita como uma seqüência infinita da forma: $0, a_1a_2a_3a_4 \ldots$, onde $a_i \in \{0, 1, \ldots, 9\}$. Por exemplo: $0,5 = 0,499999999999 \ldots$.

Seja $S = \{x_1,\ x_2\}$ para os exercícios **(5), (6), (7)**.

(5) Seja A o conjunto das seqüências finitas sobre S. Dê uma enumeração para A.

(6) Mostre que toda seqüência de elementos de S pode ser codificada como uma seqüência de elementos de $\{0, 1\}$.

Sugestão: Codifique x_i com uma seqüência de 'zeros' e 'uns'.

(7) Use o exercício (6), se necessário, e prove que o conjunto de todas seqüências de elementos de S e o conjunto de todas seqüências formadas de zeros e uns têm a mesma cardinalidade. Qual a sua cardinalidade?

(8) Sejam $f : A \to \mathbb{R}$ injetora e A não contável. Qual a cardinalidade de A? (Observe a Hipótese do Contínuo para dar a resposta).

(9) Mostre que, se $|A| = |D|$, então $|\wp(A)| = |\wp(D)|$.

(10) Prove que os conjuntos $E = [-1,\ 1)$ e $F = (3,\ 6]$ são equipotentes e dê a aplicação inversa.

6.2 Algoritmos e Máquinas de Turing

A noção de algoritmos sempre foi muito comum ao matemático ou àqueles que têm alguma familiaridade mesmo com a matemática elementar. Hoje em dia, com o advento da computação, da informatização e da globalização, o conceito de algoritmo extrapola as fronteiras da matemática e é um conceito entendido e falado quase que por todos usuários dos modernos meios de comunicação informatizados. Mas o que vem a ser um algoritmo?
Os processos de adição, multiplicação, divisão, subtração de números inteiros e o procedimento para extração de raiz quadrada são exemplos de algoritmos.

É conhecido, da escola de ensino médio que um processo para calcular as raízes da equação de segundo grau $ax^2+bx+c=0$ (com coeficientes $a,\ b,\ c$ reais), é fazer x igual a $(-b\pm\sqrt{b^2-4ac})(2a)^{-1}$, se $b^2-4ac\geq 0$. Agora, se a_i são reais, para $i=1,\ 2,\cdots,n$; um algoritmo que produza as raízes de $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$, utilizando as operações de adição, multiplicação, subtração, divisão e raízes m-ésimas, não existe para $n\geq 5$. Um problema clássico da matemática antiga era a de conseguir um procedimento que permitisse trisseccionar um ângulo qualquer usando um compasso e uma régua não demarcada. Pode-se mostrar, também, que tal procedimento não existe. Contudo, com o uso de várias réguas, ou apenas uma régua demarcada, mais um compasso é possível trisseccionar um ângulo.

Percebe-se, então, que um dado algoritmo é relativo aos métodos que se pretende utilizar, e aí podemos entender um algoritmo como sendo um "procedimento geral"composto de instruções específicas a serem seguidas fielmente por um agente executor. Isto requer, entre outras coisas, que as instruções sejam claras e completamente não ambiguas, de preferência utilizando um texto ou um formalismo finito. Um algoritmo pode apresentar problemas. Mesmo com instruções claras e não ambiguas, um algoritmo pode não parar. Por exemplo, o algoritmo para extração de raízes quadradas não pára se o número cuja raiz se procura não seja um quadrado perfeito. Saber se um dado algoritmo, com uma certa entrada de dados, pára ou não pára é conhecido como *problema da parada*.

Adiante será visto que não existe um algoritmo que decide o problema da parada. Para que um resultado a respeito de algoritmo seja possível, devemos ter uma noção precisa, formal, do que seja um algoritmo. Uma formalização usual na teoria matemática dos algoritmos é considerar algoritmos como sendo procedimentos que transformam palavras, em um alfabeto finito, em outras palavras. Mais formalmente temos:

Definição 6.25 Um *alfabeto* β é um conjunto de pelo menos 2 símbolos, um símbolo para denotar o branco e, pelo menos, mais um símbolo.

Uma *palavra* sobre este alfabeto é uma seqüência finita de símbolos. Denotando por β^* o conjunto das palavras sobre β, *os algoritmos* são funções de β^* em β^*.

Este é o enfoque básico que se usa nas linguagens de programação de computadores.

Gödelização.

Embora na prática um alfabeto possa conter vários elementos, podemos sempre associar palavras w sobre um alfabeto β com números naturais $G(w)$ de tal maneira que um número natural esteja associado com, no máximo, uma palavra em β^*. A uma tal associação chamamos de Gödelização e chamamos $G(w)$ de número de Gödel de w (com respeito a G).

Desde que $\mathbb{N}$ pode ser pensado como a classe das palavras $|$, $||$, $|||, \ldots$, ou seja, palavras sobre o alfabeto $\{0, |\}$ (0 para simbolizar o branco) resulta que, 'via Gödelização', não há nenhuma perda de generalidade se considerarmos apenas algoritmos sobre $\mathbb{N}$, ou sobre β^*, onde β é um alfabeto de apenas dois símbolos.

Definição 6.26 Dado um alfabeto β, uma Gödelização de β^* é uma função G de β^* em $\mathbb{N}$ que obedece as seguintes condições:

(1) $G : \beta^* \to \mathbb{N}$ é injetora.

(2) Existe um algoritmo tal que, para cada $w \in \beta^*$, $G(w)$ pode ser computado em um número finito de passos.

(3) $Im(G) = G(\beta^*)$ é bem determinada, ou seja, dado $n \in \mathbb{N}$ é possível decidir em um número finito de passos se n pertence ou não pertence a $Im(G)$.

(4) Se $n \in Im(G)$, existe um algoritmo para se determinar a pré-imagem w de n (isto é: $n = G^{-1}(w)$) em um número finito de passos.

Neste caso, dizemos que $G(w)$ é o *número de Gödel de* w.

Exemplo

Seja β o nosso alfabeto: $\beta = \{a, b, c, \ldots, z\}$. Então β^* contém propriamente todas as palavras da língua portuguesa; por exemplo, *abback* pertence a β^*, pois é uma seqüência finita de letras. A cada palavra de comprimento n, digamos $x_1x_2\cdots x_n$, considere os n primeiros números primos: $2, 3, 5, \ldots, p_n$ e defina

$$G(x_1x_2\cdots x_n) = 2^{d_1}3^{d_2}\cdots p_n^{d_n},$$

onde $d_i = j$ se x_i é a j-ésima letra do alfabeto.

Assim, $G(aba) = 2^1 3^2 5^1 = 90$, $G(dacaba) = 2^4.3^1.5^3.7^1.11^2.13^1 = 66.066$.

Por outro lado, $330 = 2.3.5.11$ não é número de Gödel de nenhuma palavra, pois a decomposição de 330 envolve quatro primos distintos, mas não os quatro primeiros primos: falta o primo 7. O número $420 = 2^2.3.5.7$ é o número de Gödel de 'baaa'.

Observe que a função G satisfaz as 4 condições exigidas acima, pois usa-se o teorema fundamental da aritmética e $n = p_1^{\alpha_1}\ldots p_n^{\alpha_n}$ é um número de Gödel de alguma palavra se, e somente se, p_i é o i-ésimo primo e, neste caso, $w = (\alpha_1-$ésima letra α_2-ésima letra $\cdots$ α_n-ésima letra) do alfabeto.

Através desse processo de aritmetização, podemos reduzir problemas sobre algoritmos a problemas sobre algoritmos numéricos. Isto é basicamente o propósito do estudo das funções recursivas que iniciaremos adiante. Começaremos com a noção de computabilidade segundo *Turing* e mostraremos que o *Problema da Parada* é insolúvel via Tese de Church.

6.2.1 Noções de Máquinas de Turing

Como objeto uma *máquina de Turing* consiste, essencialmente, de uma fita e um dispositivo chamado *cabeça de leitura e impressão* que será denotado (l/i). A fita é dividida e composta de células (quadrados) não sobrepostos e é potencialmente infinita à esquerda e à direita, no sentido de que se pode acrescentar células à direita ou à esquerda, quantas forem necessárias. A computação acontece com a cabeça l/i fazendo impressões de símbolos nos quadrados (células). Estes quadrados estão em branco com exceção de um número finito deles. Se um dos quadrados não está em branco, o símbolo 1 está impresso nele. Portanto, o alfabeto para a máquina de Turing é $\{0,\ 1\}$, onde o símbolo 0 significa o branco. Note que, como podemos usar notação unária para representar números, isto não causa restrição sobre o que podemos computar.

Assumimos que em cada estágio da computação, a máquina está em um dos seguintes estados internos: $q_1,\ q_2, \ldots, q_m$, onde m é fixo para cada máquina. Durante a computação, a cabeça l/i corre sobre a fita e eventualmente pára sobre um quadrado. Quando ela está sobre um quadrado, reconhece (lê) o símbolo 0 ou 1 que está neste quadrado e, de acordo com o símbolo lido e o estado interno, executa uma das seguintes operações:

(1) *Apaga* o símbolo 0 ou 1 escrito nele, ... Notação: 0.
(2) *Imprimi* o símbolo 1, ... Notação: 1.
(3) *Move* um espaço imediatamente à esquerda . . . . . E.
(4) *Move* um espaço imediatamente à direita . . . . . D.

Logo a cabeça l/i também apaga e move. A operação (1) pode ser escrita também por *Imprima* o "zero". A operação (2) significa que a célula em que a cabeça l/i está ficará com um símbolo 1 imprimido nela, mesmo se antes já tinha este símbolo, ou o 0 escrito nele. Em outras palavras, esta operação apaga esta célula e escreve 1 nela.

Uma instrução para a máquina de Turing é uma *quádrupla*

$$(q_i, S, Op, q_j)$$

onde q_i é o estado presente da máquina, $S \in \{0, 1\}$ é o símbolo lido, $Op \in \{0, 1, D, E\}$ é uma das quatro operações acima a ser realizada

e q_j é o novo estado da máquina. Notemos que são aceitas as quádruplas $(q_i, 0, 0, q_j)$ e $(q_i, 1, 1, q_j)$, o que significa que a máquina apenas muda de estado.

Portanto, a menos que a máquina pare, ela irá executar uma das instruções e irá para um certo estado. Fisicamente, a cabeça l/i apaga o símbolo na célula sobre o qual está e escreve outro (talvez o mesmo), ou ainda, vai para a célula imediatamente à esquerda ou à direita, além disso, vai para outro estado (eventualmente o mesmo), dependendo apenas do estado anterior e do símbolo que leu, a menos do estado inicial da máquina. Em outras palavras, estado + símbolo lido determinam o ato e o novo estado.

Algumas *convenções* sobre as máquinas de Turing são:

(1) A máquina de Turing (MT) começa a computação no estado q_1 (dito estado inicial).

(2) A máquina pára quando não há instrução possível a executar.

(3) Instruções ambíguas não serão permitidas, ou seja, desde que o estado e símbolo lido determina a operação a realizar e o novo estado da máquina, temos que duas quádruplas com as duas primeiras entradas iguais terão as duas outras entradas também iguais, ou seja: Se (q_i, S, Op, q_j) e (q_i, S, Op', q_k) são quádruplas de um mesmo programa de uma máquina de Turing, então $Op' = Op$ e $k = j$. Por simplicidade também escreveremos uma quádrupla na forma $q_i\ S\ Op\ q_j$, evitando as vírgulas e parênteses. Com isto, definimos

Um *programa* (em geral, em vez de programa, dizemos uma *máquina de Turing*, identificando os programas às máquinas) para uma máquina de Turing (MT) será uma seqüência de *quádruplas* (q_i, S, Op, q_j) sujeitas às convenções anteriores.

Finalmente, um conjunto constituído do conteúdo da fita, do quadrado que está sendo lido e o estado da máquina é dito uma *configuração* da máquina.

Exemplo 6.27 (A) Escreva três 1's consecutivos (isto é: sem inserção de zeros entre eles) numa fita totalmente em branco de uma MT.

Solução: Um programa é:

(1) $q_1 01 q_1$ (1') $q_1 1 D q_2$ (2) $q_2 01 q_2$
(2') $q_2 1 D q_3$
(3) $q_3 01 q_3$ (3') $q_3 1 D q_4$

Como a fita está em branco, por convenção a máquina começa a computação pela 1^a instrução. Depois de realizar a 1^a instrução, a cabeça l/i fica sobre o 1 que acabou de escrever e a máquina no estado q_1; logo realizará a instrução (1'). Realizando esta instrução, a cabeça l/i fica sobre o 'zero' à esquerda do 1, e a máquina no estado q_2. Logo, realizará a instrução (2) e depois a instrução (2'), (3) e (3'). Observe que a máquina pára no estado q_4, pois neste estado não são dadas instruções. Daí ficamos com a seguinte configuração final na fita

$$\cdots\cdots 000111\mathbf{0}_{q_4}000\cdots\cdots ,$$

como foi pedido, onde $\mathbf{0}_{q_4}$ significa que a cabeça l/i está sobre este símbolo no estado q_4.

Observação: Note que as instruções (1), (2) e (3) servem para escrever três 1's enquanto as instruções (1'), (2') e (3') servem para retirar a cabeça l/i de cima do 1 escrito. Generalizando, temos:

(B) Dê um programa para escrever n 1's consecutivos ($n \geq 2$) em uma fita em branco, mas agora faça a cabeça l/i retornar no 1 mais a esquerda do seqüência de 1's.

Solução: Um programa é:

(1) $q_1 01 q_1$ (1') $q_1 1 D q_2$
(2) $q_2 01 q_2$ (2') $q_2 1 D q_3$
... ...
(n) $q_n 01 q_{n+1}$ (n') $q_{n+1} 1 E q_{n+1}$
(n+1) $q_{n+1} 0 D q_{n+2}$.

Note que a instrução (n), assim como a instrução (3) do exercício (A), escreve o último símbolo 1 mas neste caso muda de estado e, (n') que corresponde a instrução (3') do exercício (A) em vez de só tirar a cabeça l/i de cima do último 1 impresso, não só faz isto, mas já começa a voltar a cabeça l/i para o primeiro 1 impresso. Ela busca o primeiro zero depois da seqüência de 1's

e a instrução (n+1) a coloca sobre o primeiro 1 impresso. Este programa usou $n+2$ estados e $2n+1$ instruções.

Exemplo 6.28 Escreva uma MT que quando iniciada com a cabeça l/i no 1 mais à esquerda de uma seqüência de n 1's ($n > 0$) de uma fita que só contém este bloco de un's, apaga este 1 e duplica o restante do bloco de un's (se existir bloco restante) e pára com a cabeça l/i no 1 mais a esquerda do bloco (se existir).

Uma solução é:

(1) $q_1 1 0 q_1$	(1′) $q_1 0 D q_2$	(7) $q_7 1 D q_7$	(7′) $q_7 0 E q_8$
(2) $q_2 1 E q_3$	(2′) $q_2 0 D q_{13}$	(8) $q_8 1 0 q_8$	(8′) $q_8 0 E q_9$
(3) $q_3 0 E q_4$	(3′) $q_3 1 E q_4$	(9) $q_9 1 E q_{10}$	(9′) $q_9 0 E q_{12}$
(4) $q_4 0 1 q_4$	(4′) $q_4 1 E q_5$	(10) $q_{10} 0 E q_{11}$	(10′) $q_{10} 1 E q_{10}$
(5) $q_5 0 1 q_5$	(5′) $q_5 1 D q_6$	(11) $q_{11} 1 E q_{11}$	(11′) $q_{11} 0 1 q_4$
(6) $q_6 0 D q_7$	(6′) $q_6 1 D q_6$	(12) $q_{12} 1 E q_{12}$	(12′) $q_{12} 0 D q_{13}$

A primeira instrução apaga o primeiro 1 do bloco de n un's e ficamos um bloco de $n-1$ un's. A instrução (1') leva a cabeça l/i para a direita para ver se há mais 1 (isto é, para ver se $n = 1$ ou não). Caso $n = 1$, a instrução (2') pára a máquina e temos o caso desejado. Se $n > 1$, obrigatoriamente a máquina vai para a instrução (2). Daí por diante, a cada 1 reconhecido e apagado no bloco de $n-1$ un's restante, a máquina copia dois 'uns' à esquerda do bloco, em quadrados adjacentes e consecutivos, do seguinte modo:

(a) Observando que $n > 1$ (instrução (2)), a máquina pula o primeiro zero à esquerda do bloco de $n-1$ un's (instruções (2) e (3)) e escreve dois 1 em quadrados adjacentes e consecutivos (instruções (4), (4'), (5')).

(b) Depois volta no último 1 à direita do bloco de un's restante (instruções (5'), (6), (6'), (7), (7')) e o apaga (instrução (8)).

(c) Caso tenha mais 'uns' não apagados do bloco original de n–1 un's que restou, a cabeça l/i vai para a esquerda pulando este bloco (instruções (9) e (10')) e pula o zero que separa este bloco (que está sendo apagado) do bloco que está sendo criado (instrução (10)). Pula este novo bloco (instrução (11)) e acrescenta à esquerda dele dois novos 1's em quadrados adjacentes e consecutivos (instruções

(11'), (4') e (5)). Agora a instrução (4') leva a máquina a uma rotina, a menos que não tenha mais 'uns' no bloco que restou. Neste caso, foi apagado o último 1 do bloco de $n-1$ un's, (instrução (8)) e forçosamente a máquina seguiu o caminho (8)→ (8')→ (9') → (12)→ (12') e pára com a cabeça l/i sobre o 1 mais a esquerda do bloco impresso.

Agora, vamos começar a pensar em MT que calcula funções. Para isto vamos precisar de algumas convenções. Para representar o número natural $n \geq 1$ utilizaremos a cadeia de n 1's: ..00111..100.. sem inserção de zeros entre eles. Esta cadeia é denotada por 1^n. A fita está em uma *configuração padrão* se está em branco ou contém somente uma cadeia da forma 1^n. Observe que para cada número natural $n \in \mathbb{N},\ n > 0$, é possível imprimir este número numa fita em branco usando esta convenção; basta fazer um programa semelhante ao programa do exemplo 6.27 (B), usando $n+2$ estados. Mais ainda, dados $m,\ n$ naturais e maiores do que zero, é possível escrever 1^m01^n numa fita em branco; basta concatenar dois programas, um programa que imprima 1^m com outro programa que imprima 1^n, veja exercício.

Definição 6.29 Dizemos que uma máquina de Turing T *representa* uma (*calcula* a) função $f : A \to \mathbb{N},\ A \subseteq \mathbb{N}$ não vazio, se

(a) com entrada 1^{n+1} a máquina inicia a computação (pela primeira instrução no estado inicial q_1) examinando o 1 mais a esquerda do bloco.

(b) Se $f(n) = m$, então T pára e a fita está em branco, se $m = 0$, ou pára no 1 mais à esquerda do bloco 1^m da fita que só tem esta seqüência, se $m \neq 0$.

(c) Se $n \notin Dom(f)$, então T não pára, ou pára fora do 1 mais à esquerda de qualquer configuração padrão.

Note que usamos 1^{n+1} para representar a entrada n e 1^m para representar a saída m. Com isto, diferimos a entrada zero da fita em branco, no início da computação e é possível satisfazer a condição (a) da definição, qualquer que seja $n \in \mathbb{N}$.

Exemplo 6.30 Dê um programa para uma máquina de Turing que representa a função $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n + 1$.

Solução: Acabamos de ver que existe um programa que imprime 1^{n+1} na fita em branco. Logo, consideraremos que entramos com o número n, ou seja, a fita contém 1^{n+1} somente. Feito isto, considerando que a cabeça l/i está sobre o 1 mais à esquerda do bloco 1^{n+1}, um programa para $f : \mathbb{N} \to \mathbb{N}$ é o seguinte:

$$(1) \quad q_1 11 q_2.$$

Por exemplo, vamos calcular $f(2)$ pelo programa dado. Ao mesmo tempo, daremos as configurações da máquina em cada etapa da computação. Para sabermos em que célula está a cabeça l/i, convencionaremos que ela está na célula em que está o número em negrito. Assim

$$\begin{array}{ll} \cdots 000\mathbf{1}11000\cdots & (q_1 11 q_2) \\ \cdots 000\mathbf{1}11000\cdots & \text{no estado } q_2 \end{array}$$

e a máquina pára com a cabeça l/i sobre o primeiro 1 à esquerda do bloco 1^3, pois no estado q_2 não é dado instrução. Como, por convenção, no final da computação 1^3, representa o número natural 3, temos, novamente por convenção, que $f(2) = 3$.

Verifique, agora, que $f(3) = 4$, por esta máquina de Turing.

Exemplo 6.31 Dê uma máquina (ou seja, um programa) que represente a função constante $f : \mathbb{N} \to \mathbb{N},\ f(n) = 1$, para todo $n \in \mathbb{N}$.

Solução: Tendo entrado com 1^{n+1}, por convenção a computação começa com a cabeça l/i sobre o 1 mais à esquerda do bloco 1^{n+1}. Um programa é:

$$(1) \quad q_1 10 q_2 \qquad (1') \quad q_1 01 q_3 \qquad (2) \quad q_2 0 D q_1.$$

Por exemplo, verificaremos que, pelo programa, $f(1) = 1$. Por convenção, iniciamos a computação com a fita contendo somente o bloco 1^2. Novamente o número em negrito significará que a cabeça l/i está sobre ele. Logo, a máquina começa a computação pela instrução 1, estando no estado q_1. A configuração da fita, juntamente com a próxima instrução, é:

$\cdots\cdots 0\ 0\ 0\ \mathbf{1}\ 1\ 0\ 0\ 0\cdots\cdots$	$(q_1 1 0 q_2)$
$\cdots\cdots 0\ 0\ 0\ \mathbf{0}\ 1\ 0\ 0\ 0\cdots\cdots$	$(q_2 0 D q_1)$
$\cdots\cdots 0\ 0\ 0\ 0\ \mathbf{1}\ 0\ 0\ 0\cdots\cdots$	$(q_1 1 0 q_2)$
$\cdots\cdots 0\ 0\ 0\ 0\ \mathbf{0}\ 0\ 0\ 0\cdots\cdots$	$(q_2 0 D q_1)$
$\cdots\cdots 0\ 0\ 0\ 0\ 0\ \mathbf{0}\ 0\ 0\cdots\cdots$	$(q_1 0 1 q_3)$
$\cdots\cdots 0\ 0\ 0\ 0\ 0\ \mathbf{1}\ 0\ 0\cdots\cdots$	(no estado q_3)

Por convenção, temos a saída 1. Logo $f(1) = 1$.

Agora, calcule $f(2)$, $f(3)$ e convença-se de que as instruções (1) e (2) servem para apagar todo o bloco, enquanto que (1') dá a conclusão para $f(n) = 1$.

Exemplo 6.32 Dê a MT que calcula a função $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 2n$.

Solução: Uma máquina de Turing que calcula $f(n)$, para cada $n \in \mathbb{N}$ é dada no exemplo 6.28.

Definição 6.33 Uma *função parcial* de números naturais, $f : \mathbb{N}^n \to \mathbb{N}$, é uma função $f : A \to \mathbb{N}$ onde A é um subconjunto não vazio de $\mathbb{N}^n$. Portanto, uma função parcial $f : \mathbb{N}^n \to \mathbb{N}$ não precisa estar definida em todo $\mathbb{N}^n$, ou seja, é uma relação $f \subseteq \mathbb{N}^n \times \mathbb{N}$, tal que $Dom(f) \neq \emptyset$ e, para cada $x \in Domf$, existe um único $y \in \mathbb{N}$, tal que $(x, y) \in f$. Logo, toda função $f : \mathbb{N}^n \to \mathbb{N}$ é uma função parcial.

Todas as funções tratadas daqui para a frente, a menos que se diga o contrário, serão funções parciais. Tais funções também podem ser representadas em máquinas de Turing. Formalmente, temos

Definição 6.34 Uma função parcial $f : \mathbb{N}^n \to \mathbb{N}$ é dita ser *Turing-Computável* (ou *computável por uma* MT) se existe uma máquina de Turing T que calcula $f(a_1, a_2, \ldots, a_n)$ do seguinte modo:

(1) A fita contém somente $1^{a_1+1}01^{a_2+1}0\cdots01^{a_n+1}$ no início da computação.

(2) A máquina inicia a computação pela primeira instrução no estado inicial q_1, examinando o 1 mais à esquerda do bloco mais à esquerda.

(3) Se $(a_1, \ldots, a_n) \in Dom(f)$, então T pára e a fita está em branco e, neste caso, $f(a_1, a_2, \ldots, a_n)$ é zero, ou, então, T pára no 1 mais à esquerda de alguma configuração padrão e, neste caso, $f(a_1, a_2, \ldots, a_n)$ é o número de 1's naquele bloco.
Se $(a_1, a_2, \ldots, a_n) \notin Dom\ f$, então T não pára ou pára fora do 1 mais à esquerda de alguma configuração padrão e, neste caso, $f(a_1, a_2, \ldots, a_n)$ não está definido.

Exemplo A. A função $f : \mathbb{N}^n \to \mathbb{N}$ dada por: $f(a_1, a_2, \ldots, a_n) = 1$ é Turing-Computável.

Solução: De fato, uma MT que calcula $f(a_1, a_2, \ldots, a_n)$ é dada por:
(1) $q_1 10 q_2$ (1') $q_1 0 D q_3$ (2) $q_2 0 D q_1$ (3) $q_3 10 q_2$ 3') $q_3 01 q_4$.
Por exemplo, se $f : \mathbb{N}^3 \to \mathbb{N}$, $(n = 3)$, então, para verificar que $f(2, 1, 0) = 1$, temos que, por convenção, a configuração inicial é

$$\cdots 0\ 0\ 0\ \mathbf{1}\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0 \cdots\cdots \qquad (q_1 10 q_2)$$

com a cabeça l/i sobre o 1 em negrito, por convenção.

Assim, temos a configuração toda:

0 **1**110110100	$(q_1 10 q_2)$
0 **0**110110100	$(q_2 0 D q_1)$
00 **1**10110100	$(q_1 10 q_2)$
00 **0**10110100	$(q_2 0 D q_1)$
000 **1**0110100	$(q_1 10 q_2)$
000 **0**0110100	$(q_2 0 D q_1)$
0000 **0**110100	$(q_1 0 D q_3)$
00000 **1**10100	$(q_3 10 q_2)$
00000 **0**10100	$(q_2 0 D q_1)$
000000 **1**0100	$(q_1 10 q_2)$
000000 **0**0100	$(q_2 0 D q_1)$
0000000 **0**100	$(q_1 0 D q_3)$
00000000 **1**00	$(q_3 10 q_2)$
00000000 **0**00	$(q_2 0 D q_1)$
000000000 **0**0	$(q_1 0 D q_3)$
0000000000 **0**	$(q_3 01 q_4)$
0000000000 **1**	

Portanto a configuração final da fita é $\ldots 00100 \ldots$ e temos como saída o número 1.

Note que as instruções (1) e (2) apagam qualquer entrada 1^{x+1}, enquanto (1') serve para pular o branco que separava os blocos 1^{x+1} e 1^{y+1}. Daí vem a instrução (3), que apagará um símbolo 1 do 2^o bloco e voltará à rotina dada pelas instruções (1) e (2), apagando 1^{y+1} totalmente. Quando não houver mais blocos para apagar, estamos na instrução (1') e ela reconhece isto indo para a instrução (3'). Daí, ela pára sobre o 1.

Exemplo B. Mostre que a função adição $f : \mathbb{N}^2 \to \mathbb{N}$, dada por $f(x, y) = x + y$ é Turing-Computável.

Solução: Como iniciamos com a seqüência $1^{x+1}01^{y+1}$ na fita, um modo é pôr 1 no espaço em branco entre os dois blocos, apagar os três 1's, da esquerda para a direita e avançar um espaço à direita. Observe que, se x e y são zeros, então a fita final estará em branco. O programa é:

(1) - $q_1 1 D q_1$ (busca o branco entre 1^{x+1} e 1^{y+1})
(2) - $q_1 01 q_2$ (troca o 0 por 1)
(3) - $q_2 1 E q_2$
(4) - $q_2 0 D q_3$ (3 e 4 buscam o 1 mais à esquerda)
(5) - $q_3 10 q_4$ (apaga o 1 mais à esquerda)
(6) - $q_4 0 D q_5$ (avança à direita)
(7) - $q_5 10 q_6$ (apaga o 2^o 1 mais à esquerda)
(8) - $q_6 0 D q_7$ (avança à direita).
(9) - $q_7 10 q_8$ (apaga o 3^o 1 mais à esquerda)
(10)- $q_8 0 D q_9$ (avança à direita e pára).

Exemplo C. A função multiplicação $m(x, y) = x.y$ é Turing-Computável.

Solução: Uma idéia da MT que computa esta função é a seguinte:

Como temos que somar $y + y + \ldots + y$ x vezes, uma solução é usar o bloco 1^{x+1} como um contador para controlar o número de repetições das operações.

Para começar, a máquina apaga o 1 mais à esquerda do bloco 1^{x+1}, se não restou nada neste bloco, ela apaga o resto e pára (porque neste caso $x = 0$). Se restou mais 1's no bloco 1^x, ela

apaga o 1 mais à direita do bloco 1^{y+1}. Se não restou nada, ela apaga tudo na fita e pára (porque neste caso $y = 0$). Se o bloco 1^y restante é não-vazio, a máquina move o bloco 1^y exatamente y casas para a direita. Aí a máquina fica com a seguinte configuração:

$$\ldots 001^x 00 \ldots 001^y 00 \ldots$$

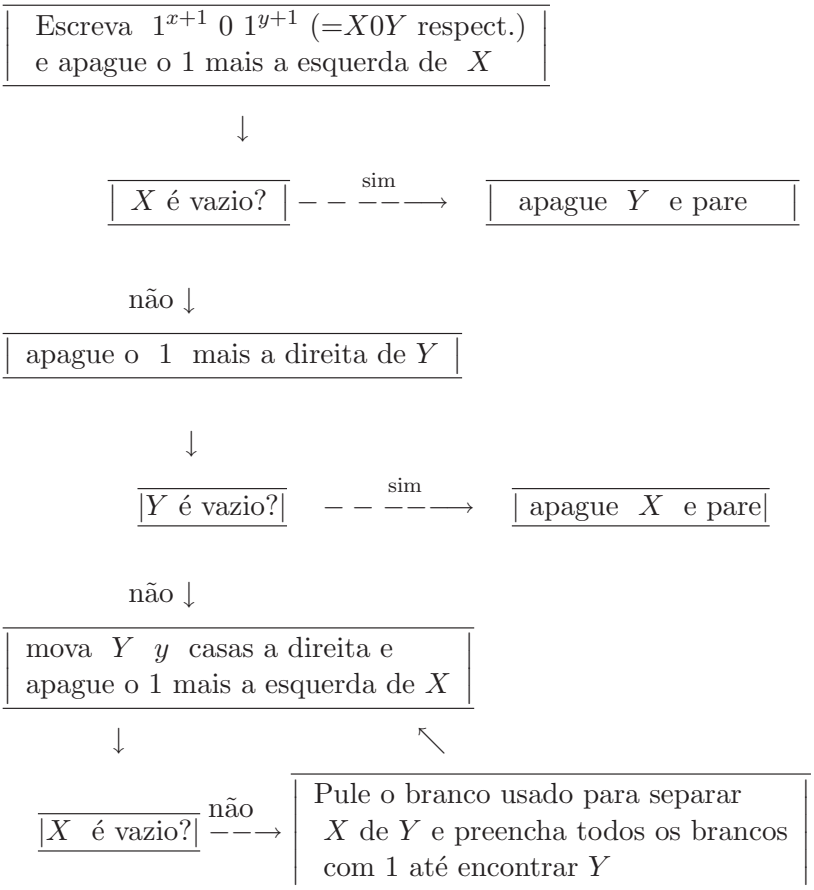
com exatamente $y + 1$ zeros entre os blocos 1^x e 1^y.

Daqui para a frente, a máquina entra numa "rotina"usando o seguinte processo:

A máquina apaga o 1 mais à esquerda do bloco 1^x (ficando com 1^{x-1}). Se 1^{x-1} for vazio, ela pára examinando o 1 mais à esquerda do bloco 1^y (pois neste caso $x = 1$). Se o bloco 1^{x-1} restante é não-vazio, ela pula o 1º zero entre os blocos 1^{x-1} e 1^y, logo à direita de 1^{x-1}, e preenche os brancos com 1 até encontrar um 1. Até aqui temos a configuração $1^{x-1}01^{2y}$. Daí ela move o bloco 1^{2y} y casas para a direita e repete o processo.

Denotando os blocos 1^{x+1} e 1^{y+1} e suas alterações, durante a computação, por bloco X e bloco Y, respectivamente, a máquina pode ser representada pelo seguinte diagrama:

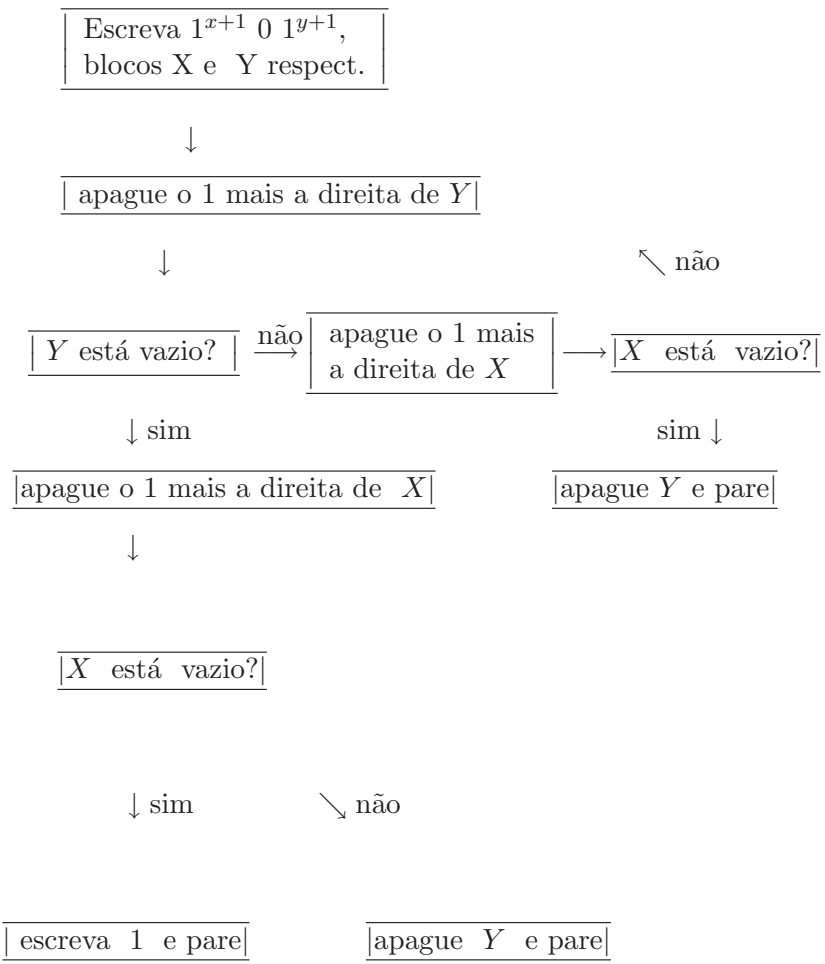
Diagrama corrido para $f(x, y) = x.y$



Um progama para esta função pode ser visto nas páginas 114-116 da referência [1].

Como último exemplo, daremos um diagrama corrido para um programa para a função característica da igualdade entre dois números. Esta função deve ter saída 1, se duas entradas x e y são iguais e 0, caso contrário. A idéia é apagar, em cada passo, um par de 1's, um 1 de cada um dos blocos 1^{x+1} e 1^{y+1} e escrever '1' se os blocos terminarem ao mesmo tempo e '0', caso contrário. Como não se sabe qual bloco termina primeiro, o problema fica mais complicado.

O diagrama é o seguinte:



Na lista de exercícios foi proposto que você apresente um programa para esta função.

Agora, vamos apenas dizer, resumidamente, como podemos compor funções parciais em uma máquina de Turing. A composição de funções parciais será mais explorada quando tratarmos de funções computáveis por uma Máquina de Registro Ilimitado. Os processos são análogos.

Se g é uma função de uma variável e f uma função de n variáveis, aplicamos primeiro f à X e depois aplicamos g à $f(X)$. A máquina que representa a função parcial composta $g \circ f$, dado que T_f e T_g representam f e g respectivamente, é a máquina $T_{g\circ f}$ obtida justapondo T_f a uma *simulação* de T_g, digamos $T_{g'}$, do seguinte modo:

(a) Se $f(m) = r$, sejam (k) $q_l\ S\ Op\ q_t$ a última instrução que pára a MT T_f na configuração padrão e, Q_i os estados de T_g. Seja S o conjunto de instruções: (k+1) $q_t 1 E q t+1$, (k+1) $q_t 0 E q_{t+1}$, (k+2) $q_{t+1} 01 q_{t+2}$. Agora, reenumere os estados de T_g por $Q_i = q_{i+1+t}$. Daí a seqüência $T_g \bigcup S \bigcup T'_g$ é o programa de $T_{g\circ f}$, a menos de pequenos rearranjos que temos que fazer para incluir o caso de

(b) $T_{g\circ f}$ não parar, ou parar fora de configuração padrão com entrada $1^{m_1+1}0\cdots 01^{m_n+1}$, se $f(m_1, m_2, \ldots, m_n)$ não está definida.

A composição de funções parciais de várias variáveis é representada similarmente. Por exemplo, se

$$f(x_1, \ldots, x_m) = h(g_1(x_1, \ldots, x_{n_1}), \ldots, g_m(x_1, \ldots, x_{n_s})),$$

a representação de T_f é obtida por simulações convenientes de $T_{g_1}, T_{g_2}, \ldots, T_{g_m}$ com T_h.

Exemplo 6.35 Sejam $f : \mathbb{N}^2 \to \mathbb{N},\ f(x, y) = x + y$ e $g : \mathbb{N} \to \mathbb{N},\ g(x) = x + 2$.

Um programa para f é dado no Exemplo B, e um programa para g é dado por:

(1) $q_1 1 E q_2$ (2) $q_2 01 q_3$.

Portanto, um programa para $g \circ f$ $\big((g \circ f)(x, y) = x + y + 2\big)$ é dado por:

(1) $q_1 1 D q_1$ (2) $q_1 01 q_2$ (3) $q_2 1 E q_2$ (4) $q_2 0 D q_3$ (5) $q_3 10 q_4$ (6) $q_4 0 D q_5$ (7) $q_5 10 q_6$ (8) $q_6 0 D q_7$ (9) $q_7 10 q_8$ (10) $q_8 0 D q_9$ (11) $q_9 1 E q_9$

(12) $q_9 01 q_{10}$, (13) $q_{10} 1 E q_{11}$, (14) $q_{11} 01 q_{12}$

ou seja, os estados q_1, q_2 e q_3 do programa que calcula $g(x)$ passam a ser os estados q_{10}, q_{11} e q_{12} do programa que calcula $(g \circ f)(x, y)$. As primeiras instruções correspondem ao programa para calcular $f(x, y)$. A décima instrução de $f(x, y)$ parava a máquina no estado q_9 buscando o 1 mais à esquerda do bloco, enquanto aqui continuamos. Mas, antes de entrar diretamente com as instruções da máquina T_g, (que simula g) como sendo as instruções (11) e (12), mudamos as instruções q_1 e q_2 para q_{10} e q_{11}, de modo que as instruções (1) e (2) de g passam a ser as instruções (13) e (14) de $f \circ g$. É necessária esta correção antes de simular T_g, pois para calcular $g(f(n))$ devemos entrar com $1^{f(n)+1}$ na fita em branco enquanto a saída $f(n)$ é $1^{f(n)}$, por convenção. Por isso usamos as instruções (11) e (12) para fazer esta correção antes de simular T_g em $T_{g'}$. Isto é possível, pois a cabeça l/i estava sobre o 1 mais à esquerda da configuração padrão $1^{f(x,y)}$ e $Dom(f)$ é $\mathbb{N}^2$.

Finalmente, daremos uma enumeração das máquinas de Turing para mostrar, via *Tese de Church*, que existem funções parciais que não são computáveis por nenhum processo. Além disso, mostrar que o Problema da Parada para Máquinas de Turing é indecidível.

Teorema 6.36 *TESE DE CHURCH*

Toda função parcial $f : \mathbb{N}^n \to \mathbb{N}$ que é computável, segundo algum processo, é Turing-Computável. □

Comentário. Note que não há como provar que a tese de Church é verdadeira, pois não há como dar uma boa formalização de processo intuitivo em uma teoria. No entanto há meios matemáticos de provar que ela está errada; basta exibir uma função parcial computável por algum processo que não seja Turing Computável. Apesar de inúmeras tentativas nesta direção, todas têm resultado em fracassos. Por esta e outras fortes evidências, acredita-se que a tese de Church é válida. A tese de Church é interessante porque (estando certa) diz que a Turing-computabilidade, apesar de simples, capta perfeitamente a noção (semântica) que temos do termo 'computabilidade de funções parciais'.

Teorema 6.37 O conjunto das funções parciais (ou das funções) de $\mathbb{N}$ em $\mathbb{N}$ não é enumerável.

Demonstração: A demonstração pode ser feita pelo método diagonal de Cantor, do seguinte modo: Suponhamos que temos uma enumeração de todas as funções de $\mathbb{N}$ em $\mathbb{N}$, e seja $f_1, f_2, f_3, \ldots, f_n, \ldots$ tal enumeração. Construa a função $g : \mathbb{N} \to \mathbb{N}$, tal que $g(1) \neq f_1(1),\ g(2) \neq f_2(2), \ldots, g(n) \neq f_n(n), \ldots$. Desta forma, g é uma função de $\mathbb{N}$ em $\mathbb{N}$ e, como $g(n) \neq f_n(n)$, então $g \neq f_n,\ \forall n \in \mathbb{N}$. Logo g não foi listada, absurdo. Portanto, o conjunto de todas as funções de $\mathbb{N} \to \mathbb{N}$ não é enumerável. Como este conjunto é um subconjunto de todas as funções parciais de $\mathbb{N} \to \mathbb{N}$, pelo Teorema 6.8 segue-se a conclusão. □

Agora, se provarmos que as máquinas de Turing são enumeráveis podemos enunciar, via Tese de Church, o seguinte

Corolário 6.38 Existem funções (parciais ou não) de $\mathbb{N}$ em $\mathbb{N}$ que não são computáveis, isto é: não são computáveis por qualquer critério. □

6.2.2 Enumeração das Máquinas de Turing

Para enumerar as máquinas de Turing, observemos que o alfabeto sobre o qual se definem os programas para elas é $\{0, 1, D, E, q_1, q_2, \ldots, q_n, \ldots\}$: um conjunto infinito, mas enumerável. Uma máquina de Turing nada mais é do que uma *palavra finita* neste alfabeto enumerável.

Pelo Corolário 6.13, o conjunto das palavras é enumerável. Como nem todas as palavras sobre este conjunto é uma máquina de Turing, vem que o conjunto de todas as máquinas de Turing é um subconjunto próprio e infinito deste conjunto enumerável. Portanto, é também enumerável, pelo Teorema 6.8.

Para demonstrar que o problema da parada é indecidível em máquinas de Turing precisaremos exibir uma enumeração das máquinas de Turing que representam funções parciais unárias, isto é: funções parciais de $\mathbb{N}$ em $\mathbb{N}$. Para isto precisamos dizer que tipos de palavras são máquinas de Turing. Uma enumeração para as

máquinas de Turing que representam funções parciais unárias é a seguinte: *especificamos cada máquina concatenando suas quádruplas numa única palavra*, começando com a quádrupla cujo primeiro símbolo é o estado inicial da máquina. Depois segue a quádrupla cujo primeiro símbolo é o segundo estado da máquina, e assim por diante. Com isto as quádruplas serão concatenadas em uma única palavra do seguinte modo:

$$1^{\underline{a}} \text{ instrução } 2^{\underline{a}} \text{ instrução } 3^{\underline{a}} \text{ instrução } \ldots \ n^{\underline{a}} \text{ instrução.}$$

Por exemplo a máquina que descreve a função parcial $f : \mathbb{N} \to \mathbb{N}$, definida por $f(a) = 1$, dada no Exemplo 6.31 é:

$$q_1 01 q_3 q_1 10 q_2 q_2 0 D q_1,$$

que é a concatenação das instruções 1', 1 e 2, nesta ordem.

Notemos que, como existem duas quádruplas com instruções q_1, é preciso escolher qual delas vêm primeiro. Neste caso, o segundo símbolo da quádrupla (zero ou um) decide a ordem, e a ordem aqui é "$q_i 0 \cdots$ *precede* $q_i 1 \cdots$". De um modo preciso, o critério **Cr**, para que uma palavra represente uma máquina de Turing, é o seguinte:

Cr.1 - O comprimento da palavra é múltiplo de 4.

Cr.2 - Nas posições 1, 4, 5, 8, 9, 12,..., $4n, 4n+1, \ldots$, ocorrem apenas os símbolos q_i;

Cr.3 - Nas posições 2, 6, 10, 14,..., $4n+2, \ldots$, ocorrem apenas os símbolos 0 ou 1.

Cr.4 - Nas posições 3, 7, 11,..., $4n+3, \ldots$, ocorrem os símbolos D, E, 0 e 1, apenas.

Cr.5 - Nenhum par da forma $q_i 0$ ou $q_i 1$ ocorre mais de uma vez nas palavras, para cada $i \geq 1$.

Desde que fixamos os símbolos que aparecem nas posições $4n$, $4n+1$, $4n+2$, $4n+3$, este critério caracteriza todas as palavras que são máquinas de Turing. O critério 5 serve para impedir o aparecimento de máquinas com instruções contraditórias e também para impedir repetições desnecessárias de quádruplas.

As palavras com apenas 4 símbolos que satisfazem o critério **Cr** serão consideradas como um *Novo Alfabeto*. Para enumerá-lo, usando o passeio de Cantor, enumeramos os índices i e j em q_iXYq_j

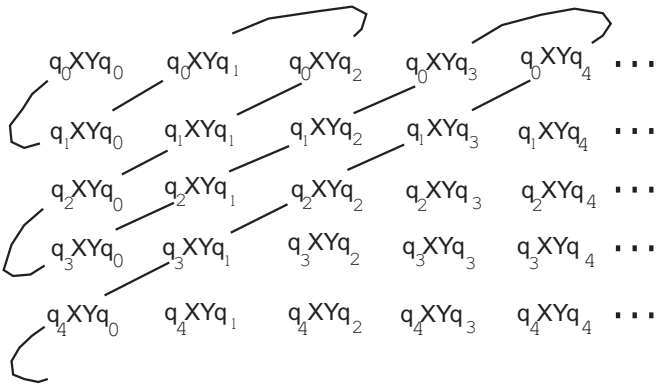


Figura 6.3: Passeio de Cantor para índices (i,j).

e, para cada par de índices (i, j) em q_iXYq_j, prevalece a ordem:

$$q_i00q_j,\ q_i01q_j,\ q_i0Dq_j,\ q_i0Eq_j,\ q_i10q_j,\ q_i11q_j,\ q_i1Dq_j,\ q_i1Eq_j$$

Deste modo, o novo alfabeto tem a enumeração:

$Z_0 = q_000q_0,\ Z_1 = q_001q_0, \ldots,\ Z_7 = q_01Eq_0,\ Z_8 = q_100q_0, \ldots,$ $Z_{15} = q_11Eq_0, Z_{16} = q_000q_1, \ldots,\ Z_{23} = q_01Eq_1,\ Z_{24} = q_000q_2,$ $\ldots,\ Z_{31} = q_01Eq_2,\ Z_{32} = q_100q_1, \ldots.$

Para enumerar as palavras de comprimento 2, isto é, 2 quádruplas, façamos um passeio de Cantor sobre a matriz

$$
\begin{array}{ccccccc}
Z_0Z_0 & Z_0Z_1 & Z_0Z_2 & Z_0Z_3 & Z_0Z_4 & Z_0Z_5 & Z_0Z_6 \\
Z_1Z_0 & Z_1Z_1 & Z_1Z_2 & Z_1Z_3 & Z_1Z_4 & Z_1Z_5 & Z_1Z_6 \\
Z_2Z_0 & Z_2Z_1 & Z_2Z_2 & Z_2Z_3 & Z_2Z_4 & Z_2Z_5 & Z_2Z_6 \\
Z_3Z_0 & Z_3Z_1 & Z_3Z_2 & Z_3Z_3 & Z_3Z_4 & Z_3Z_5 & Z_3Z_6 \\
Z_4Z_0 & Z_4Z_1 & Z_4Z_2 & Z_4Z_3 & Z_4Z_4 & Z_4Z_5 & Z_4Z_6 \\
Z_5Z_0 & Z_5Z_1 & Z_5Z_2 & Z_5Z_3 & Z_5Z_4 & Z_5Z_5 & Z_5Z_6, \\
Z_6Z_0 & Z_6Z_1 & Z_6Z_2 & Z_6Z_3 & Z_6Z_4 & Z_6Z_5 & Z_6Z_6,
\end{array}
$$

como foi feito no Teorema 6.11 ou Corolário 6.13. Assim temos a enumeração:
$Z_0Z_0,\ Z_1Z_0,\ Z_0Z_1,\ Z_0Z_2,\ Z_1Z_1,\ Z_2Z_0,\ Z_3Z_0,\ Z_2Z_1,\ Z_1Z_2,\ Z_0Z_3,\ Z_0Z_4, \ldots$

Desta enumeração eliminamos as palavras Z_iZ_i, que correspondem às máquinas de Turing com a única instrução Z_i, $i = 1, 2, \ldots$, já enumerada anteriormente. Palavras do tipo Z_iZ_j e Z_jZ_i, $i \neq j$ são contadas apenas uma vez, pois correspondem a mesma máquina. Finalmente eliminamos palavras que não satisfazem o critério **Cr.5**, por exemplo, $Z_0Z_1 = q_000q_0q_001q_0$ e $Z_1Z_4 = q_001q_0q_00Eq_0$. O que restar dá uma enumeração das máquinas de Turing com duas instruções (duas palavras). De fato, este subconjunto é um conjunto infinito de um conjunto enumerável (Teorema 6.8). Assim temos uma enumeração das palavras de comprimento 2:
$N_0 = Z_0Z_4 = q_000q_0q_010q_0,\ N_1 = Z_5Z_0 = Z_0Z_5 = q_000q_0q_011q_0,$
$N_2 = Z_4Z_1 = Z_1Z_4 = q_001q_0q_010q_0,\ N_3 = Z_0Z_6 = q_000q_0q_01Dq_0,$
$N_4 = Z_1Z_5 = q_001q_0q_011q_0, N_5 = Z_2Z_4 = q_00Dq_0q_010q_0,\ N_6 = Z_7Z_0 = Z_0Z_7 = q_000q_0q_01Eq_0,\ N_7 = Z_6Z_1 = Z_1Z_6 = q_001q_0q_01Dq_0,\ N_8 = Z_2Z_5 = q_00Dq_0q_011q_0$, etc.

Usando as máquinas de Turing de 1 palavra e a enumeração N_i das máquinas de Turing de 2 palavras, façamos uma tabela

como na demonstração do Corolário 6.13. Um passeio de Cantor sobre ela nos dá uma enumeração destas palavras de comprimento 3. Usando o processo anterior para eliminar as palavras que não correspondem às máquinas de Turing com 3 instruções, obtemos uma enumeração das máquinas de Turing de 3 instruções:
$P_0 = Z_8N_0 = Z_8Z_0Z_4 = Z_0Z_4Z_8 = q_000q_0q_010q_0q_100q_0$, $P_1 = Z_9N_0 = Z_0Z_4Z_9 = q_000q_0q_010q_0q_101q_0$, $P_2 = Z_8N_1 = Z_0Z_5Z_8 = q_000q_0q_011q_0q_100q_0, \ldots$

Com o mesmo processo, enumeramos máquinas de Turing de comprimento n ($n > 3$) qualquer. Finalmente colocamos todas elas numa matriz, onde a primeira linha são as máquinas de Turing de uma instrução, a segunda linha são as máquinas de Turing de duas instruções, e assim sucessivamente,

$$
\begin{array}{cccccccccc}
Z_0 & & Z_1 & \rightarrow & Z_2 & & Z_3 & \rightarrow & Z_4 & Z_5 \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
N_0 & & N_1 & & N_2 & & N_3 & & N_4 & N_5 \\
& \swarrow & & \nearrow & & \swarrow & & & & \\
P_0 & & P_1 & & P_2 & & P_3 & & P_4 & P_5 \\
\downarrow & \nearrow & & & & & & & & \\
\ldots & & \ldots & & \ldots & & \ldots & & \ldots & \ldots
\end{array}
$$

Finalmente, um passeio de Cantor sobre ela nos dá as primeiras máquinas de Turing:
$M_0 = Z_0 = q_000q_0$, $M_1 = N_0 = q_000q_0q_010q_0$, $M_2 = Z_1 = q_001q_0$, $M_3 = Z_2 = q_00Dq_0$, $M_4 = N_1 = q_000q_0q_011q_0$, $M_5 = P_0 = q_000q_0q_010q_0q_100q_0, \ldots$

Assim temos uma enumeração efetiva das máquinas de Turing e, portanto, vale o Corolário anterior.

Para mostrar que o problema da parada é indecidível em máquinas de Turing, temos que ir mais adiante. Para isto, seja f_n a função

parcial que corresponde a M_n e considere

$$d : \mathbb{N} \to \mathbb{N}, \quad d(n) = \begin{cases} 1, & \text{se } f_n(n) \text{ é indefinida,} \\ f_n(n) + 1, & \text{se } f_n(n) \text{ é definida.} \end{cases}$$

Então a função d não está na lista. De fato, se $d = f_m$ para algum m, então $d(m) = f_m(m)$. Mas, por definição da função d, temos: $f_m(m) = 1$ se $f_m(m)$ é indefinida, e $f_m(m) = f_m(m) + 1$ se $f_m(m)$ é definida, absurdo. Como d não está na lista, d não é Turing-Computável.

No entanto, embora d não seja Turing-Computável, é 'possível' calcular seus valores. Lembrando que na definição de Turing-Computável a máquina começa a computação no 1 mais à esquerda do bloco mais à esquerda, temos:
M_0 representa $f_0(n) = n+1$; $f_1(n)$ é indefinida, pois M_1 não pára; $f_2(n) = f_3(n) = n+1$ e $f_4(n)$ e $f_5(n)$ também são indefinidas, pois M_4 e M_5 não param, etc. Assim temos $d(0) = f_0(0)+1 = 2$, $d(1) = 1$, $d(2) = f_2(2) + 1 = 4$, $d(3) = f_3(3) + 1 = 5$, $d(4) = d(5) = 1$, etc.

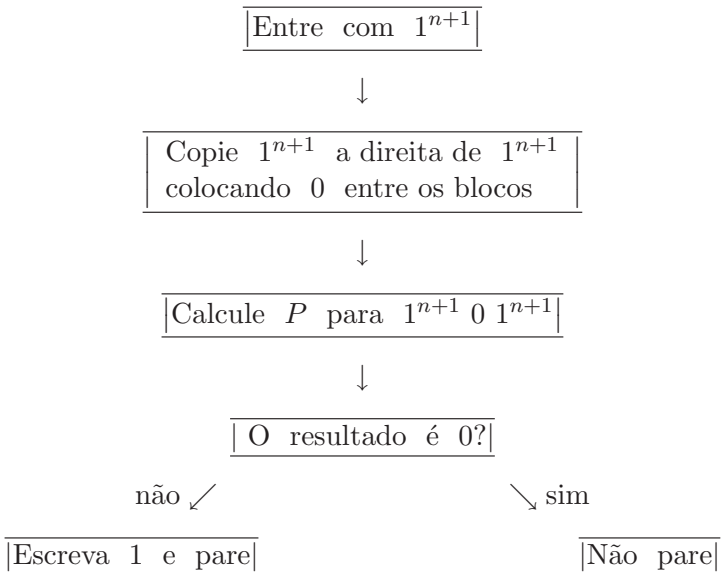
Como é possível que d não seja computável, se estamos computando seus valores? Na verdade, para funções parciais definidas, ou para funções parciais que são indefinidas mas param, é fácil calcular o valor de $d(n)$ se temos tempo suficiente. O problema são aquelas funções parciais que não param. Em alguns casos, como nas máquinas M_1, M_4 e M_5, é fácil decidir que não param, mas nas máquinas complexas pode ser difícil e muitas vezes o é.
CONCLUSÃO: *Aceitando a Tese de Church, não existe um método efetivo que decida se uma dada função parcial Turing-Computável pára ou não, para uma dada entrada*, ou seja: *A Tese de Church implica que o problema da Parada é indecidível por máquinas de Turing.*

Observação 6.39 É possível dar uma outra prova, sem fazer apelo à Tese de Church, de que o Problema da Parada é indecidível por máquina de Turing. Suponha que exista uma função parcial Turing-Computável $P(m, n)$, que decida se a máquina M_m pára

ou não pára com entrada n :

$$P(m,n) = \begin{cases} 0, & \text{se } M_m \text{ pára com entrada } n, \\ 1, & \text{caso contrário.} \end{cases}$$

$P : \mathbb{N}^2 \to \mathbb{N}$ não está na lista $M_0,\ M_1,\ M_2, \ldots$, pois é uma função parcial de 2 variáveis. No entanto, a função parcial definida pelo seguinte diagrama é, obviamente, Turing-Computável se $P(m,n)$ o for:



O diagrama define uma função parcial de uma variável que é Computável segundo Turing e, portanto, está na nossa lista, digamos que é representada por M_s. Por construção, M_s pára com entrada n se, e somente se, M_s não pára com entrada n (para todo n). Em particular, M_s pára com entrada s se, e somente se, M_s não pára com entrada s, absurdo.

Desse modo, quer a Tese de Church seja verdadeira ou não, as máquinas de Turing não são capazes de resolver seu próprio problema de parada.

Exercícios

(1) Defina: Alfabeto, Palavras sobre um alfabeto, Algoritmos e dê exemplos diferentes dos algoritmos vistos até aqui.

(2) Defina Gödelização e dê exemplos de Gödelização diferentes dos vistos até aqui. Qual o número de Gödel do seu primeiro nome?

(3)(i) Para um dado $n \in \mathbb{N},\ n > 0$ faça uma máquina de Turing que escreva 1^n numa fita em branco.

(ii) Dados $m,\ n \in \mathbb{N}$, ambos não nulos, escreva 1^m01^n numa fita em branco.

(4)(i) Faça programas que computem, por máquinas de Turing, as funções totais: $f : \mathbb{N}^3 \to \mathbb{N}$ e $g : \mathbb{N} \to \mathbb{N}$, dadas por: $f(x, y, z) = x + z$, e $g(x) = \begin{cases} 1 & \text{se } x = 0, \\ 0 & \text{se } x \neq 0. \end{cases}$

(ii) Faça um programa para $g \circ f$ fazendo uma simulação dos programas obtidos para f e g em (i).

(5) Responda sim ou não, fazendo um breve comentário que justifique a resposta:

(i) O conjunto das funções totais de $\mathbb{N}$ em $\mathbb{N}$ é enumerável.

(ii) O conjunto de todas as Máquinas de Turing é enumerável.

(iii) Existe uma função $f : \mathbb{N} \to \mathbb{N}$ que não é computável por nenhum critério, mas é impossível exibi-la.

(6) Dê uma outra enumeração das máquinas de Turing.

(7) Faça um breve comentário sobre: "O problema da parada é indecidível via máquinas de Turing".

(8) Faça programas que computem, por máquinas de Turing, as funções parciais $f : \mathbb{N} \to \mathbb{N}$ dada por

$f(x) = \begin{cases} 1, & x : \text{ par} \\ \text{indefinida}, & x : \text{ ímpar}, \end{cases}$ e $h : \mathbb{N} \to \mathbb{N}$ dada por

$h(x) = \begin{cases} \frac{x}{2}, & x : \text{ par} \\ \text{indefinida}, & x : \text{ímpar}. \end{cases}$

(9) Mostre que a função característica da igualdade, $c : \mathbb{N}^2 \to \{0, 1\}$, definida por $c(m, n) = \begin{cases} 1, & \text{se } m = n \\ 0, & \text{se } m \neq n. \end{cases}$ é Turing-

Computável.

(10) (a) Prove que a projeção na primeira coordenada $P_2^1 : \mathbb{N}^2 \to \mathbb{N}$, definida por $P_2^1(m, n) = m$ é Turing-Computável.

(b) Como você prova que a i-ésima projeção $P_k^i : \mathbb{N}^k \to \mathbb{N}$, definida por $P_k^i(n_1, \ldots, n_i, \ldots, n_k) = n_i$, $k \geq i \geq 1$ é Turing-Computável?

6.3 Funções computáveis

Nas secções subsequentes descreveremos um outro caminho para tornar precisa a idéia de funções computáveis, formalizando o conceito que se teve a princípio de um computador, suas leis de fundamentação para a teoria matemática de computabilidade e funções computáveis.

Já vimos que algoritmos muitas vezes estão ligados ao desenvolvimento de programas para executar operações matemáticas. Por exemplo, se queremos resolver:

(a) Dado n, ache o n-ésimo número primo.

(b) Dado um polinômio, ache sua derivada.

(c) Dados $a, b \in \mathbb{Z}$, ache $mdc(a, b)$, ou

(d) Dados $a, b \in \mathbb{Z}$, decida quando a é múltiplo de b.

Para todos esses problemas, podemos desenvolver algoritmos tais que, para determinadas entradas, eles nos dão como respostas saídas desejáveis. No caso (a), as entradas são números naturais e saídas números naturais primos, no caso (b), as entradas e saídas são polinômios, no caso (c), as entradas são pares de números inteiros e as saídas são números naturais e, finalmente, no caso (d), as entradas são números naturais e as saídas são 0 ou 1(se convencionarmos 0 para falso e 1 para verdadeiro).

A idéia informal de algoritmo, como sendo uma lista com um número finito de instruções não ambíguas, cada instrução executável de modo que tenhamos uma resposta em um número finito de passos, será associada à noção de função computável. Nossas definições são dadas baseadas nas noções em que foram construídos os computadores mais simples. Mas não é por isso que algoritmos

ou procedimentos executados por computadores modernos, não são exemplos de procedimentos efetivos; basta ter em mente a Tese de Church. Qualquer computador, moderno ou não, é limitado no sentido de quantidade de números que pode receber como entradas e a quantidade de espaço de trabalho; por exemplo, um dos fatores limitantes é o tempo, outro é o espaço físico. Um programa para nossa máquina será finito e requererá que a computação seja completada em apenas um número finito de passos. Entradas e saídas serão sempre números ou seqüências finitas de números naturais. Mas isto não é restritivo no sentido de não computar funções em outros domínios, pois sempre podemos codificar e decodificar objetos por números naturais, como temos visto no processo de Gödelização, por exemplo.

Máquina de Registro Ilimitado - MRI

Uma das primeiras idealizações de um computador trazida à manifestação é chamada de *MÁQUINA DE REGISTRO ILIMITADO (=MRI)*, que é uma ligeira variação da máquina concebida primeiro por Shepherdson e Sturgis (1963).

Uma MRI tem um número ilimitado de registros denotados por $R_1, R_2, \ldots$. Cada R_i, em qualquer momento, contém algum número natural que denotaremos por r_i. Podemos representa-la por

$$\overline{|r_1|r_2|r_3|r_4|\cdots|r_i|\cdots|}$$

onde cada registro R_i contém o número natural r_i. Cada número r_i do registro R_i pode ser alterado pela MRI, em resposta a uma dada instrução. Essas instruções correspondem a operações numéricas implementadas na máquina.

Definição 6.40 Um *Programa* para uma MRI é uma lista finita de instruções dos tipos das descritas abaixo:
(a) *Instrução Zero*: Para cada $n = 1, 2, 3, \ldots$ existe a instrução zero $Z(n)$. A resposta da MRI à instrução $Z(n)$ é alterar o conteúdo do registro R_n para o número natural 'Zero', deixando os outros registros inalterados.

Notação: $Z(n)$ ou $0 \to R_n$, ou ainda $r_n := 0$ (que significa: r_n foi alterado para 'zero').

(b) *Instrução Sucessor*: Para cada $n = 1, 2, 3, \ldots$ existe a instrução sucessor denotada por $S(n)$. A MRI dá como resposta à instrução $S(n)$ o número natural $r_n + 1$, no registro R_n, deixando os outros registros inalterados. Isto é, a MRI acrescenta 1 ao conteúdo do registro R_n e deixa os outros registros inalterados.

Notação: $S(n)$ ou $r_n + 1 \to R_n$ ou $r_n := r_n + 1$ (que significa: r_n foi alterado para $r_n + 1$.

(c) *Instrução Transferência*: Para cada par (m, n), $m = 1, 2, 3, \ldots$ e $n = 1, 2, 3, \ldots$, existe a instrução transferência, denotada por $T(m, n)$. A resposta da MRI a esta instrução é trocar r_n por r_m no registro R_n, deixando os outros registros inalterados.

Notação: $T(m, n)$ ou $r_m \to R_n$ ou $r_n := r_m$ (que significa: troque r_n por r_m, ou transfira r_m para o registro R_n).

(d) *Instrução Salto*: Na operação de um algoritmo informal pode ter um estágio quando um curso alternativo de ação é descrito, dependendo do progresso das operações em estágios anteriores. Em outras situações pode ser necessário repetir uma dada rotina várias vezes. Na MRI é possível realizar tal procedimento fazendo uso das instruções salto, saltando para trás ou para frente na lista de instruções. Por exemplo, se uma determinada instrução $I_k, k \neq 10$, da lista do programa, é "*Se* $r_2 = r_6$ *vai para a* $10^{\underline{a}}$ *instrução da lista do programa, em outro caso vai para a próxima instrução* (I_{k+1}) *da lista do programa*". Esta instrução será denotada por $J(2, 6, 10)$. Geralmente, para cada $m = 1, 2, \ldots$, $n = 1, 2, \ldots$ e $q = 1, 2, \ldots$ existe a instrução salto $J(n, m, q)$, desde que esta instrução não seja a instrução I_q. A resposta da MRI para a instrução $J(m, n, q)$ é como segue: Suponhamos que esta instrução é encontrada no programa. Os conteúdos dos registros R_n e R_m são comparados e

— se $r_m = r_n$, a MRI pula para q-ésima instrução do programa para executá-la,

— se $r_m \neq r_n$, a MRI passa à próxima instrução da lista para executá-la.

Se a instrução salto é impossível é porque o programa tem menos de q instruções e, neste caso, a MRI pára.

As instruções Zero, Sucessor e Transferência são ditas *instruções aritméticas.*

A Computação e a Parada de uma MRI

Por convenção, a computação inicia com uma dada *configuração inicial* $a_1, a_2, a_3, \ldots$, nos registros $R_1, R_2, R_3, \ldots$, onde a_i são números naturais. Uma *configuração inicial* é uma seqüência quase nula de números naturais $(a_1, a_2, \ldots, a_n, 0, 0, \ldots)$. Isto significa que os registros estão todos vazios, exceto um número finito deles.

Suponhamos que um programa para uma MRI consista de s instruções denotadas por $I_1, I_2, \ldots, I_s$. A máquina começa a computação executando as instruções em ordem, isto é, começa executando I_1, depois I_2, e assim por diante, a menos que seja encontrada uma instrução salto $I_k : J(n, m, q)$. Neste caso a MRI executa a instrução $J(n, m, q)$, como descrita anteriormente, ou seja, passa a instruçãoI_q, caso $n = m$, ou passa à instrução I_{k+1}, caso $n \neq m$..

A princípio a MRI executa as instruções enquanto for possível, e a MRI *pára* quando, e apenas quando, não existe uma próxima instrução a ser executada. Isto pode ser descrito do seguinte modo: Se a MRI computa um programa com as instruções $I_1, I_2, \ldots, I_s$ e, tem executado a instrução I_k e a próxima instrução da lista a ser executada é I_v, então a MRI pára:

(i) Se $k = s$ e I_s é uma instrução aritmética (isto é: a MRI executa a última instrução da lista e não há mais instrução a ser executada, pois I_s não é uma instrução salto para trás),

(ii) Se $I_k = J(m, n, v)$, $r_m = r_n$ e $v > s$ (isto é: I_k pede para a MRI executar uma instrução que não existe no programa),

(iii) Se $I_k = J(m, n, v)$, $r_m \neq r_n$ e $k = s$ (neste caso a MRI deve ir à próxima instrução do programa I_{s+1}, que não existe).

Em qualquer destes casos dizemos que a computação pára depois da instrução I_k, e a configuração final é a seqüência $r_1, r_2, \ldots$ nos registros depois desta etapa.

Vamos identificar um programa para uma MRI com a própria MRI. Como exemplo, considere o seguinte programa

$I_1 : J(1,2,6)$ $\quad$ $I_4 : J(1,2,6)$
$I_2 : S(2)$ $\quad$ $I_5 : J(1,1,2)$
$I_3 : S(3)$ $\quad$ $I_6 : T(3,1)$.

Se considerarmos a computação dada por esta MRI sobre a configuração inicial

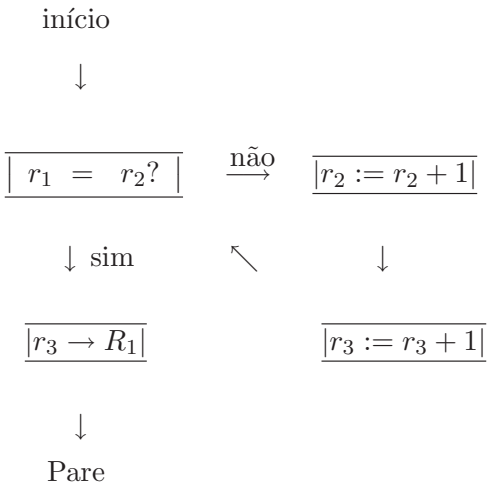
$$\overline{|8|6|2|0|\cdots}$$

podemos representar todo estágio da computação que ocorre dentro da máquina, exibindo a configuração e a próxima instrução a ser executada pela MRI em cada etapa da computação.

Configuração					Próxima instrução
8	6	2	0	$\cdots$	I_1
8	6	2	0	$\cdots$	I_2 (pois $r_1 \neq r_2$)
8	7	2	0	$\cdots$	I_3
8	7	3	0	$\cdots$	I_4
8	7	3	0	$\cdots$	I_5 (pois $r_1 \neq r_2$)
8	7	3	0	$\cdots$	I_2 (pois $r_1 = r_1$)
8	8	3	0	$\cdots$	I_3
8	8	4	0	$\cdots$	I_4
8	8	4	0	$\cdots$	I_6 (pois $r_1 = r_2$)
4	8	4	0	$\cdots$	

Observe que a máquina pára nesta última configuração porque I_6 é uma instrução aritmética e não há uma próxima instrução. Portanto, para a entrada $8, 6, 2, 0, \ldots$ temos como saída a seqüência $4, 8, 4, 0 \ldots$.

Um *diagrama corrido* ou simplesmente um *diagrama* descreve informalmente muito bem as etapas de um programa e tem o mérito de dar globalmente uma visualização de como ocorre a computação. Por exemplo, o diagrama do programa anterior é



Note a convenção, dada no diagrama, para a instrução salto $J(m, n, k)$: normalmente aparece a interrogação $r_m = r_n$? Aí, existem 2 caminhos alternativos a seguir, dependendo dos conteúdos r_m e r_n dos registros R_m e R_n, respectivamente. Note, também, o salto para trás forçado pela resposta 'não' à 2^a questão: $r_1 = r_2$? Ele é obtido pela 5^a instrução $J(1, 1, 2)$, que é um salto incondicional, pois sempre temos $r_1 = r_1$, e esta instrução força a volta à instrução I_2, quando ela é encontrada.

Quando escrevemos um programa para executar um dado algoritmo, muitas vezes é melhor escrever o diagrama como um passo intermediário, decorre daí, que a translação de um diagrama em um programa é usualmente rotineira.

Pode existir computação que nunca pára: por exemplo, nenhuma computação do programa P_1 dado pelas instruções

$$I_1 : S(1) \ \text{ e } \ I_2 : J(1, 1, 1)$$

sobre qualquer configuração inicial pára. De fato, a instrução salto dada pela instrução I_2 invariavelmente causa, nesta máquina, um retorno para a instrução I_1.

Existem programas mais sofisticados em que a computação nunca pára. Mas, na execução de um programa, isto sempre é causado, essencialmente, por um tipo de rotina na lista de instruções, gerada por uma ou mais instruções salto.

A questão de decidir quando uma particular computação eventualmente pára ou não pára é um pouco complicada, como já temos visto quando tratamos de máquinas de Turing.

6.3.1 Funções MRI Computáveis

Para cada seqüência quase nula $(a_1, a_2, \ldots)$ de números naturais existe $n \in \mathbb{N}$ que depende da seqüência tal que $a_m = 0$, se $m > n$. Se P é um programa para uma MRI denotemos por $P(a_1, a_2, \ldots, a_n)$ a execução do programa P pela MRI sobre a configuração inicial $(a_1, a_2, \ldots, a_n, 0 \ldots)$.

Definição 6.41 Dizemos que $P(a_1, \ldots, a_n)$ ou $P(a_1, a_2, \ldots, a_n, 0 \ldots)$ *converge* se, com a configuração inicial $(a_1, a_2, \ldots, a_n, 0, \ldots)$ a MRI pára; e dizemos que *converge para* $b \in \mathbb{N}$ se, além disso, no final da computação, b é o elemento do registro R_1, isto é, $r_1 = b$. Se $P(a_1, \ldots, a_n)$ não pára dizemos que $P(a_1, \ldots, a_n)$ *diverge.*

Sejam $f : \mathbb{N}^n \to \mathbb{N}$ uma função parcial e P um programa para uma MRI. Dizemos que P *computa* f (ou *computa* $f(x)$) por uma MRI se para toda n-upla $(a_1, \ldots, a_n) \in Dom(f)$ temos que $P(a_1, \ldots, a_n)$ converge para $b = f(a_1, \ldots, a_n)$. Se $(a_1, \ldots, a_n) \notin Dom(f)$, então $P(a_1, \ldots, a_n)$ diverge.

Uma função parcial $f : \mathbb{N}^n \to \mathbb{N}$ é dita MRI *computável* se existe um programa P que computa $f(x)$ em uma MRI.

Denotemos por C_n *a classe das funções parciais* $f : \mathbb{N}^n \to \mathbb{N}$ que são MRI computáveis.

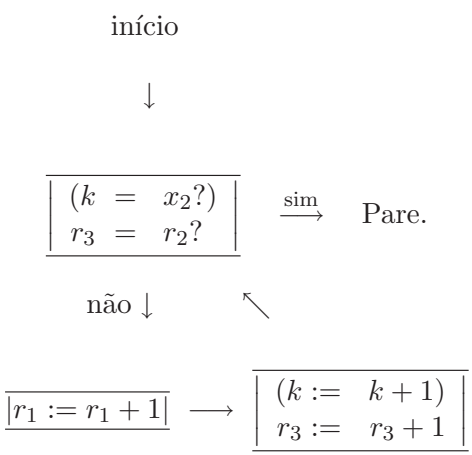
Exemplo 6.42 (a) Seja $f : \mathbb{N}^2 \to \mathbb{N}$ definida por $f(x_1, x_2) = x_1 + x_2$.

Um programa que computa f pode ser obtido somando 1 à x_1, x_2 vezes, usando a instrução sucessor. A configuração inicial é $x_1, x_2, 0, \ldots$. Nosso programa adiciona 1 à r_1 (no registro R_1), usando R_3 como um contador que marca o número de 1's acrescidos a r_1.

Uma configuração típica será: $x_1 + k, x_2, k, 0, \ldots$ A parada deve ser imposta quando $x_2 = k$, pois aí temos $x_1 + x_2$ em R_1. Um programa é dado por:

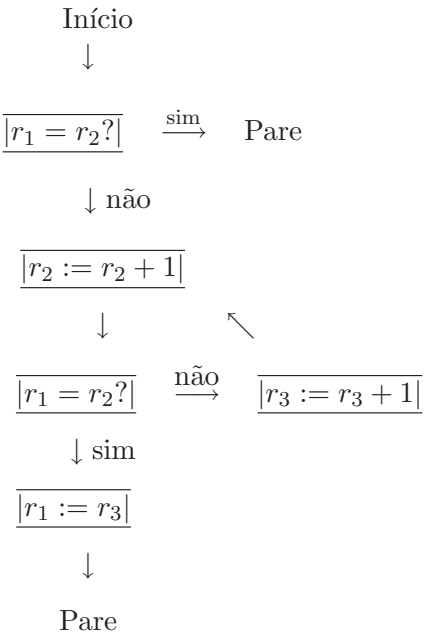
$$I_1 : J(2,3,5) \qquad I_2 : S(1) \qquad I_3 : S(3) \qquad I_4 : \ J(1,1,1),$$

cujo diagrama é:



(b) Seja $f : \mathbb{N} \to \mathbb{N}$ definida por $f(x) = x \overset{\bullet}{-} 1$, onde $x \overset{\bullet}{-} 1 := \begin{cases} x - 1, & \text{se } x > 0, \\ 0, & \text{se } x = 0. \end{cases}$

Um diagrama é o seguinte



Como $f(x)$ é uma função de uma variável a configuração inicial é: $x, 0, \ldots$ e o programa do diagrama anterior é como segue: Primeiro verificamos se $x = 0$ $(r_1 = r_2)$. Se for, paramos; se não, usamos os registros R_2 e R_3 como contadores com $r_2 = k + 1$ e $r_3 = k$, $k = 0, 1, 2, \ldots$ e entramos na seguinte rotina: verificar se $x = k + 1$ $(r_1 = r_2)$. Se for, o resultado final é k, isto é, $T(3, 1)$, se não, acrescentamos 1 aos registros R_2 e R_3 e repete-se o processo. Portanto, depois de k etapas na computação, a configuração típica é: $x, k + 1, k, 0 \ldots$ e o programa é:

$I_1 : J(1, 2, 7)$, $I_2 : S(2)$, $I_3 : J(1, 2, 6)$, $I_4 : S(3)$, $I_5 : J(1, 1, 2)$, $I_6 : T(3, 1)$.

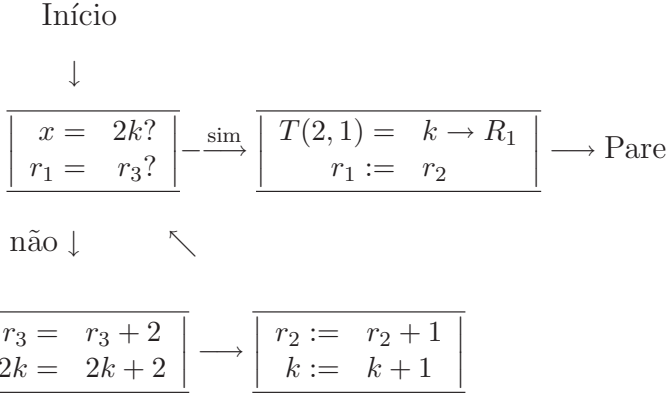
(c) $f(x) = \begin{cases} \frac{1}{2}x, & \text{se } x \text{ é par} \\ \text{indefinida}, & \text{se } x\text{: ímpar} \end{cases}$

Neste exemplo, temos que o domínio de f é o conjunto dos números pares, e devemos fazer um programa que não pára se a entrada é ímpar.

Utilizemos dois registros como contadores contendo k e $2k$, $k = 0, 1, \ldots$ para verificarmos se $x = 2k$. Se $x = 2k$, a resposta

é k, se não, adicionamos 1 a k e 2 a $2k$. Claramente, se $x = 2n+1$, o procedimento não pára.

Uma configuração típica é: $x, k, 2k, 0, \ldots,$ e o diagrama é o seguinte



A partir deste diagrama, fazemos o seguinte programa para esta função parcial:

$I_1 : J(1,3,6),\ I_2 : S(3),\ I_3 : S(3),\ I_4 : S(2),\ I_5 : J(1,1,1),\ I_6 : T(2,1)$.

Logo, $f(x)$ é MRI computável.

Observação. Não existe um único programa que computa por uma MRI uma dada função parcial. Basta ver que, uma vez obtido um programa P que computa uma função f, podemos construir outro programa P' adicionando a P instruções sem efeito, ou seja, instruções que não alteram mais o conteúdo do registro R_1, e P' pára em uma dada n-uplas se, e somente se, P pára nesta n-upla, e ambos os programas divergem nas mesmas n-uplas. No entanto, a recíproca é verdadeira: Dado um programa P para uma MRI, se existir alguma função parcial $f : \mathbb{N}^n \to \mathbb{N}$, tal que P computa $f(x)$, então ela é única. Assim,

Notação 6.43 Seja P um programa para uma MRI, tal que $P(a_1, \ldots, a_n)$ converge pelo menos em uma n-upla $(a_1, \ldots, a_n)$.

Denotemos por f_P^n a única função parcial de $\mathbb{N}^n$ em $\mathbb{N}$ que é computável por P.

De fato, a função parcial $g : \mathbb{N}^n \to \mathbb{N}$, definida por $g(x_1, \ldots, x_n) = b$ se, e somente se, $P(x_1, \ldots, x_n)$ converge para b, é a única função parcial de $\mathbb{N}^n$ em $\mathbb{N}$ que pode ser computado pelo programa P em uma MRI.

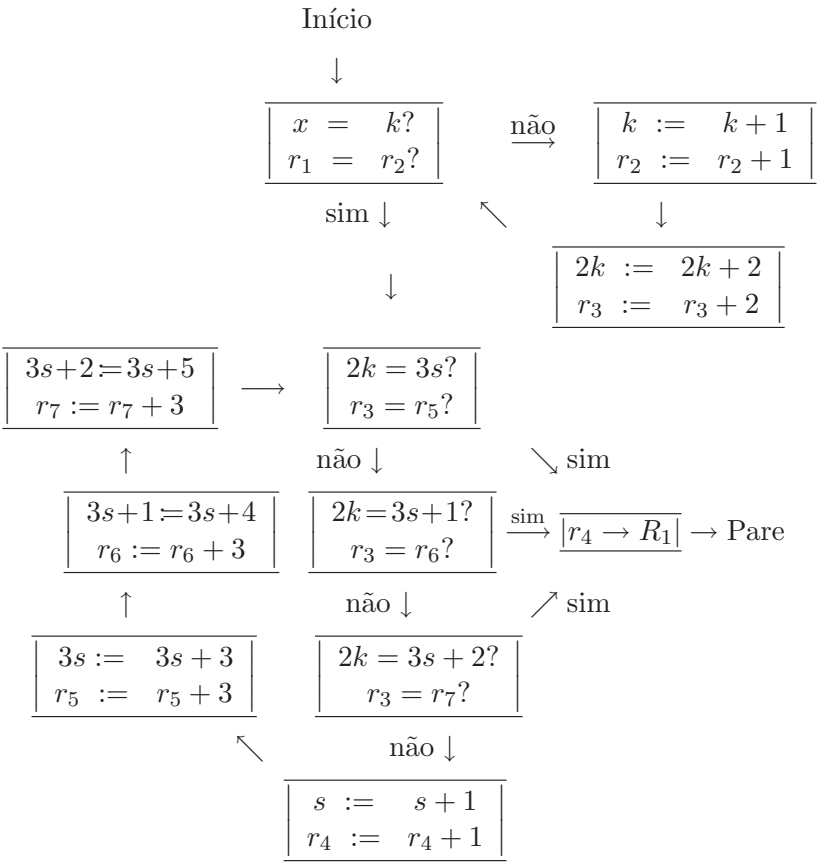
Por exemplo, dado o programa $P = \ I_1 : \ S(1)$, então, para qualquer número de variáveis n, $P(x_1, x_2, \ldots, x_n)$ dá como resultado $x_1 + 1$ em R_1, sobre qualquer entrada $(x_1, x_2, \ldots, x_n, 0, \ldots)$. Logo, $f_P^n(x_1, \ldots, x_n) = x_1 + 1$ é a única função parcial de $\mathbb{N}^n$ em $\mathbb{N}$ computável por P.

Finalmente, façamos um programa que compute por uma MRI a seguinte função parcial: $f(x) = \left[\frac{2x}{3}\right]$, onde $[q]$ significa o maior número inteiro contido no número racional q.

Solução: Um programa pode ser feito do seguinte modo: Usamos dois registros, digamos R_2 e R_3 como contadores com $r_2 = k$ e $r_3 = 2k$, e perguntamos quando $x = k$ $(x = r_2)$ para $k = 0, 1 \ldots$. Se $x \neq k$, usamos $S(2)$ e duas vezes $S(3)$ para fazer $r_2 = k + 1$ e $r_3 = 2k + 2$. Repete-se o processo perguntando se $x = r_2$, até obter $x = r_2 = k$. Com isto, $r_3 = 2k = 2x$ e resta programar o maior inteiro contido em $\frac{2k}{3}$ para obter $f(x)$.

Para esta segunda etapa do programa, usamos quatro registros, digamos R_4, R_5, R_6 e R_7 como contadores, onde $r_4 = s$, $r_5 = 3s$, $r_6 = 3s + 1$ e $r_7 = 3s + 2$, e perguntamos quando $2k$ é igual a $3s$, $3s + 1$ e $3s + 2$ para $s = 0, 1 \ldots$ (pois $\left[\frac{r_5}{3}\right] = \left[\frac{r_6}{3}\right] = \left[\frac{r_7}{3}\right] = r_4 = s$). Quando isto ocorrer, colocamos como resposta $s = r_4$ em R_1. A configuração inicial é $x, 0, 0, \ldots$, pois f é uma função parcial de uma variável, e uma configuração típica de um determinado estágio da computação é $x, k, 2k, s, 3s, 3s+1, 3s+2, 0, 0, \ldots$. Como os valores iniciais para k e s são zero, as três primeiras instruções do programa a seguir servem para deixar a configuração inicial na forma $x, 0, 0, 0, 0, 1, 2, 0 \ldots$ (uma configuração inicial típica).

O diagrama é:



O programa que computa $f(x)$ feito sobre o diagrama acima é:

$I_1 : S(6)$	$I_7 : S(3)$	$I_{13} : S(5)$	$I_{19} : S(7)$
$I_2 : S(7)$	$I_8 : J(1,1,4)$	$I_{14} : S(5)$	$I_{20} : S(7)$
$I_3 : S(7)$	$I_9 : J(3,5,23)$	$I_{15} : S(5)$	$I_{21} : S(7)$
$I_4 : J(1,2,9)$	$I_{10} : J(3,6,23)$	$I_{16} : S(6)$	$I_{22} : J(3,3,9)$
$I_5 : S(2)$	$I_{11} : J(3,7,23)$	$I_{17} : S(6)$	$I_{23} : T(4,1)$
$I_6 : S(3)$	$I_{12} : S(4)$	$I_{18} : S(6)$	

Para finalizar esta seção, vamos tratar de *predicado decidível* e *computabilidade sobre outros conjuntos.*

No capítulo 1, vimos que um predicado n-ário de números naturais, é uma sentença aberta sobre o conjunto dos números naturais contendo n variáveis. A *função característica* do predicado M, denotada por $c_M(x)$, onde $x = (x_1, x_2, \ldots, x_n)$, é definida por:

$$c_M(x) = \begin{cases} 1, & \text{se } M(x) \text{ é verdadeira,} \\ 0, & \text{se } M(x) \text{ é falso.} \end{cases}$$

Por exemplo, se $M(x, y)$ é o predicado "x divide y", então $c_M(x, y) = 1$, se x divide y, e $c_M(x, y) = 0$, no outro caso.

Definição 6.44 *Predicado Decidível*

Um predicado n-ário de números naturais $M(x)$, (onde $x = (x_1, x_2, \ldots, x_n)$) será dito *decidível* se sua função característica $c_M : \mathbb{N}^n \to \mathbb{N}$ for MRI computável. Caso contrário, o predicado será dito *indecidível.*

Um subconjunto A de $\mathbb{N}^n$ será dito *decidível* se sua função característica for MRI computável.

Exemplo 6.45 (a) - O predicado $M(x)$: "$x = 0$"é decidível, pois sua função característica

$$c_M(x) = \begin{cases} 1, & \text{se } x = 0 \\ 0, & \text{se } x \neq 0 \end{cases}$$

é MRI computável. De fato, o seguinte programa computa $c_M(x)$.

$$I_1 : J(1, 2, 3), \quad I_2 : J(1, 1, 4), \quad I_3 : S(2), \quad I_4 : T(2, 1).$$

(b) - O predicado $M(x_1, x_2)$: "$x_1 \neq x_2$"sobre $\mathbb{N} \times \mathbb{N}$ é decidível. Para verificar esta afirmação, faça o exercício (1)(c) no final deste capítulo.

Observação 6.46 Existem predicados, como *x é multiplo de y*, que, apesar de simples, quaisquer programas para as suas funções características são extremamente complicados e extensos. Adiante, neste capítulo, desenvolveremos algumas técnicas de computabilidade que nos permitirão dizer que algumas funções parciais mais complexas são computáveis, sem ter a necessidade de exibir qualquer programa que as compute por uma MRI.

Agora, faremos um breve comentário sobre a computabilidade em outros conjuntos, numéricos ou não, mas enumeráveis. Apesar de uma MRI trabalhar apenas com números naturais, isto não significa que estamos restritos apenas a este campo númerico, pois sempre podemos codificar objetos por números.

Definição 6.47 Um *código* de um conjunto de objetos D é uma função $\alpha : D \to \mathbb{N}$ injetiva. Dizemos que o objeto d está *codificado* pelo número natural $\alpha(d)$.

Um exemplo de codificação é o processo de Gödelizacão que vimos em seções anteriores.

Agora suponhamos que $f(x)$ é uma função parcial de D em D, $D \neq \emptyset$. Dizemos que $f^* = \alpha \circ f \circ \alpha^{-1} : \mathbb{N} \to \mathbb{N}$ *codifica a função parcial* f. Dizemos, também, que a função parcial $f : D \to D$ é MRI *computável* se $f^* : \mathbb{N} \to \mathbb{N}$ é MRI computável. Tendo em vista estes conceitos, podemos estudar computabilidade sobre qualquer domínio enumerável.

Exemplo 6.48 Considere a função $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x - 1$. Esta função é MRI computável sobre $\mathbb{Z}$. De fato, a função $\alpha(n) = \begin{cases} 2n, & \text{se } n \geq 0 \\ -2n-1, & \text{se } n < 0 \end{cases}$ codifica números inteiros. Sua inversa é dada por $\alpha^{-1}(m) = \begin{cases} \frac{1}{2}m, & \text{se } m \text{ é par,} \\ -\frac{1}{2}(m+1), & \text{se } m \text{ é ímpar.} \end{cases}$ Logo, $f^* = \alpha \circ f \circ \alpha^{-1} : \mathbb{N} \to \mathbb{N}$ é uma função dada por

$$f^*(x) = \begin{cases} 1, & \text{se } x = 0 \ \ (\text{i.e.} \ \ x = \alpha(0)), \\ x-2, & \text{se } x > 0 \text{ e } x \text{ é par} \ \ (\text{i.e. } x = \alpha(n), n > 0), \\ x+2, & \text{se } \ x \ \text{ é ímpar} \ \ (\text{i.e. } x = \alpha(n), n < 0). \end{cases}$$

Agora é rotina escrever um programa para f^*. Assim podemos concluir que $f : \mathbb{Z} \to \mathbb{Z}$ é MRI computável. Veja exercício (3)(b) no final deste capítulo.

6.3.2 Gerando Funções Computáveis

Neste parágrafo veremos vários métodos de combinar funções parciais MRI computáveis para obter outras funções parciais MRI computáveis. Isto possibilita-nos mostrar bem rapidamente que uma

determinada função parcial MRI computável é MRI computável, sem a necessidade de escrever um programa que a compute, programa este que pode ser bastante trabalhoso e tedioso.

Primeiro verificaremos que algumas funções parciais particularmente simples são MRI computáveis. Essas funções parciais serão chamadas de *funções básicas*. São as funções *Zero* $\Theta : \mathbb{N}^n \to \mathbb{N}$, *Sucessor* $S : \mathbb{N} \to \mathbb{N}$ e *Projeção* $P_n^i : \mathbb{N}^n \to \mathbb{N}$, definidas, respectivamente, por $\Theta(x) = 0, \forall x \in \mathbb{N}^n$, $S(x) = x + 1, \forall x \in \mathbb{N}$ e $P_n^i(x) = x_i, \forall x = (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$. Depois, usando técnicas que serão desenvolvidas nas seções posteriores, mostraremos que funções parciais mais complexas, geradas a partir destas, são MRI computáveis.

Lema 6.49 As funções básicas Θ, S, P_n^i são MRI computáveis.

Demonstração: Essas funções parciais correspondem às instruções aritméticas dadas a uma máquina MRI, cujos programas são, respectivamente: Programa $Z(1)$, Programa $S(1)$ e Programa $T(i, 1)$. □

União de Programas

Adiante necessitaremos de escrever programas que incorporem outros programas como sub-programas ou como rotinas de um programa maior. Segue uma técnica para fazer isto.

Suponhamos que temos os programas P e Q e desejamos escrever um programa com a seguinte característica: Primeiro queremos a ação de P e depois a ação de Q. A intuição diz que primeiro devemos colocar, neste novo programa, as instruções de P seguidas das instruções de Q e, portanto, existem dois pontos a considerar:

(A) Suponhamos que $P : I_1, I_2, \ldots, I_s$. Como a computação sobre P é completada quando a próxima instrução é I_v com $v > s$, devemos exigir que a computação, no novo programa composto, tenha I_v como sendo a 1^a instrução de Q, ou seja, $v = s + 1$ com $I_{s+i} = I'_i$, onde $Q : I'_1, I'_2, \ldots, I'_t$. Assim, para a construção do novo programa, somos obrigados a considerar programas P que invariavelmente param porque a próxima instrução, depois do programa P, deve ser I_{s+1}. Dizemos que tais programas estão na *forma*

canônica. Claro que somente instruções saltos podem fazer com que um programa não pare na forma canônica. Então diremos que um programa $P = I_1,\ I_2, \ldots, I_s$, está na *forma canônica* se, para toda instrução salto $J(m, n, q)$ de P, temos que $q \leq s + 1$. Os programas do exemplo 6.45(a) e do exercício (2) estão na forma canônica. A forma canônica não é restritiva, como mostra o lema a seguir.

Lema 6.50 Para todo programa P que pára, existe um programa P^* na forma canônica, tal que a computação em P e em P^* é a mesma, exceto possivelmente no modo dos programas pararem. Em particular, para todos $a_1, \ldots, a_n, b \in \mathbb{N}$, tem-se que $P(a_1, a_2, \ldots, a_n)$ converge para b se, e somente se, $P^*(a_1, \ldots, a_n)$ converge para b e, portanto, $f^n_P = f^n_{P^*}$ para todo $n > 0$.

Demonstração: Se P está na forma canônica, tome P^* igual a P. Caso contrário, sejam $I_1,\ I_2, \ldots, I_s$ as instruções do programa P. Então, para obter P^* de P, basta mudar as instruções salto que param para as instruções salto que param na instrução I_{s+1}. Assim, podemos escrever $P^* : I^*_1,\ I^*_2, \ldots, I^*_s$, onde $I_k = I^*_k$, se I_k é uma instrução aritmética, e, se I_k é uma instrução salto, digamos, $I_k = J(m, n, q),\ q > s + 1$, então $I^*_k = J(m, n, s + 1)$. Daí P^* satisfaz as condições desejadas. □

O outro ponto a considerar quando unimos P e Q é
(B) relativo às 'instruções salto' de Q. Se a instrução $J(i, j, r)$ ocorre no programa Q, significa que temos um salto para a r-ésima instrução de Q, que na união de P e Q será agora $s + r$. Portanto, para adequá-la à união de P e Q, devemos corrigir para $J(i, j, s+r)$. Com estas modificações temos:

Definição 6.51 *União ou Concatenação de Programas.*

Sejam P e Q programas de comprimento s e t respectivamente, ambos na forma canônica. A *união* ou *concatenação* dos programas P e Q denotados por PQ é o programa:

$$I_1,\ I_2, \ldots, I_s,\ I^*_{s+1}, \ldots, I^*_{s+t},$$

onde $P :\ I_1,\ I_2, \ldots, I_s$ e $I^*_{s+1}, \ldots, I^*_{s+t}$ são as instruções $I_1,\ I_2, \ldots,$ I_t de Q, respectivamente, onde as instruções salto $J(m, n, q)$ do programa Q são substituídas por $J(m, n, s + q)$.

Com esta definição, é claro que o efeito do programa PQ é o desejado, isto é, toda computação sobre PQ corresponde à computação inicial P seguida da computação Q, cuja configuração inicial de Q é a configuração final da computação de P.

Suponhamos, agora, que desejamos compor programas Q e P tendo P como sub-rotina. Para escrever este novo programa Q', é preciso achar um registro que fica inalterado pelo programa P. O seguinte procedimento busca este registro.

Como temos um número finito de instruções em P, existe um menor número u, tal que nenhum dos registros R_v, $v > u$, são mencionados no programa P, ou seja, se $Z(n)$ ou $S(n)$ ou $T(m,n)$ ou $J(m,n,p)$ é uma instrução de P, então $n \leq u$ e $m \leq u$. Portanto, o conteúdo de R_v é inalterado na computação dada por P e não influencia os valores $r_1, r_2, \ldots, r_u$. Assim, quando escrevemos o programa Q', o registro R_v para $v > u$ pode ser usado, por exemplo, para guardar informações, sem ser afetado por qualquer computação da sub-rotina P.

Denotemos o número u por $\rho(P)$. Para $v > u$, os registros R_v que foram usados são chamados de *arquivos* ou *arquivos de memória*.

Finalmente, se P é um programa na forma canônica que computa a função $f(x_1, x_2, \ldots, x_n)$ e P é usado como rotina de um programa maior, as entradas $x_1, x_2, \ldots, x_n$ usadas para calcular $f(x_1, x_2, \ldots, x_n)$ convém ser guardadas nos registros $R_{\rho(P)+1}, \ldots, R_{\rho(P)+n}$, em vez dos registros $R_1, \ldots, R_n$, como o programa P simples requer, além disso, a saída $f(x_1, x_2, \ldots, x_n)$ computada pela rotina P convém ser guardada no registro $R_{\rho(P)+n+1}$, em vez de R_1, como foi convencionado. Esses cuidados devem ser considerados, pois, além de os registros $R_1, \ldots, R_{\rho(P)}$ poderem conter todo tipo de informações não desejadas, os valores x_i, $i = 1, \ldots, n$ e $f(x_1, \ldots, x_n)$ podem ser usados, caso necessário, em qualquer momento da computação, já que sabemos onde buscá-los. Todos esses conceitos serão usados no teorema seguinte.

Substituição

Dá-se o nome de *substituição* ao processo de obter novas funções

parciais substituindo funções parciais em outras funções parciais, ou seja, fazendo uso da composição de funções parciais. O próximo teorema mostra que, quando este processo é usado sobre funções parciais MRI computáveis, obtém-se funções parciais MRI computáveis. Então podemos dizer que a classe de todas as funções parciais MRI computáveis (denotada por C') é fechada para a operação de substituição.

Notemos que se $f(y_1, \ldots, y_k)$ e $g_1(x), \ldots, g_k(x)$ são funções parciais, então $h(x) = f(g_1(x), \ldots, g_k(x))$ está definida se, e somente se, $g_1(x), g_2(x), \ldots, g_k(x)$ estão definidas e $(g_1(x), \ldots, g_k(x))$ pertence ao domínio de f. Em particular, se f e $g_1, \ldots, g_k$ são funções, então h é uma função.

Teorema 6.52 Suponhamos que $f(y_1, y_2, \ldots, y_k)$ e $g_1(x), \ldots, g_k(x)$ são funções parciais MRI computáveis, onde $x = (x_1, \ldots, x_n)$. Então, $h(x)$ obtida por substituição e definida por $h(x) := f\big(g_1(x), \ldots, g_k(x)\big)$ também é MRI computável.

Demonstração: Por hipótese e Lema 6.50 existem programas na forma canônica F, G_1, $\ldots$, G_k que computam f, g_1, $\ldots$, g_k, respectivamente. Seja $\rho = \max\{\rho(F), \rho(G_1), \ldots, \rho(G_k)\}$. Façamos um programa H, contendo uma ligeira modificação desses programas como subprogramas, e que computa h do seguinte modo: Entre com a configuração (inicial) $x_1, x_2, \ldots, x_n, 0, \ldots$ usando a instrução sucessor. Esta etapa, em geral, é evitada em qualquer programa e, em geral, começamos o programa já supondo a configuração inicial na máquina. Considerando isto, iniciamos com
(1) Transfira x_i do arquivo R_i para o arquivo $R_{\rho+i}$, $i = 1, 2, \ldots, n$, usando a instrução Transferência.
(2) Aplique G_1^* em $x = (x_1, \ldots, x_n)$. Isto dá $g_1(x)$ em R_1.
(3) Coloque $g_1(x)$ no arquivo $R_{\rho+n+1}$ usando a instrução Transferência.
(4) Apague $R_1, \ldots, R_\rho$ usando a instrução zero.
(5) Transfira x_i de $R_{\rho+i}$ para R_i usando a instrução Transferência.
(6) Aplique G_2^* em x, obtendo $g_2(x)$ em R_1.
(7) Usando a instrução Transferência, coloque $g_2(x)$ no arquivo $R_{\rho+n+2}$.

(8) Repetindo o raciocínio para todos os outros programas G_i, obteremos $g_1(x)$, $g_2(x), \ldots, g_k(x)$ nos arquivos $R_{\rho+n+1}$, $R_{\rho+n+2}$, $\ldots, R_{\rho+n+k}$, respectivamente.

(9) Agora apagamos novamente os registros $R_1, \ldots, R_\rho$ e transferimos os conteúdos $g_1(x), \ldots, g_k(x)$ dos arquivos $R_{\rho+n+1}, \ldots$, $R_{\rho+n+k}$ para os registros $R_1, \ldots, R_k$.

(10) Aplique F^* e pare.

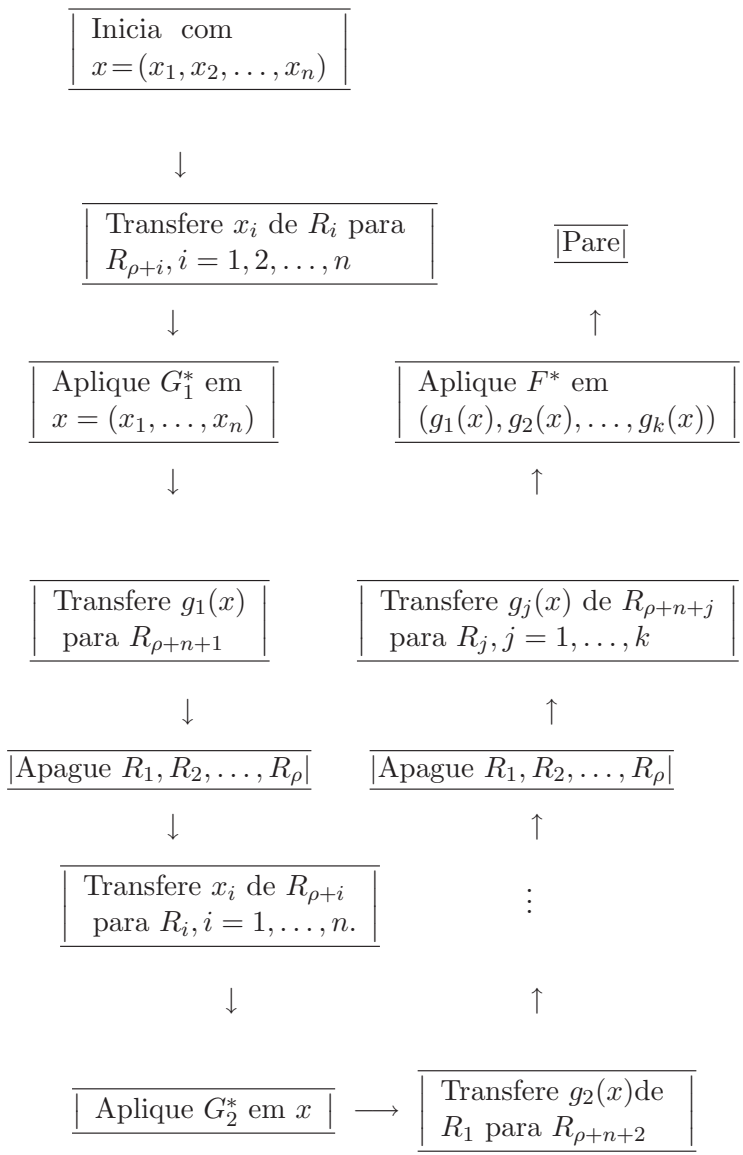
Quando aplicarmos F^* na k-upla $(g_1(x), \ldots, g_k(x))$ obteremos $f(g_1(x), \ldots, g_k(x))$, pois F está na forma canônica e obrigatoriamente a máquina vai parar com $f(g_1(x), \ldots, g_k(x))$ em R_1. Uma configuração típica quando estamos aplicando G_r^* (é o programa G_r como subprograma de H), $1 < r < k$ é

R_1	R_2	$\cdots$	R_n	$\cdots$	R_ρ	$\cdots$
s_1	s_2	$\cdots$	s_n	$\cdots$	s_ρ	$\cdots$

$R_{\rho+n}$	$R_{\rho+n+1}$	$\cdots$	$R_{\rho+n+r-1}$
x_n	$g_1(x)$	$\cdots$	$g_{r-1}(x)$

$R_{\rho+n+r}$	$\cdots$
0	$\cdots$

Como foi descrito nos passos anteriores, o diagrama para o programa H é:



Tendo em vista este diagrama, a construção do programa H é um trabalho bastante simples. Claramente, a computação $H(x)$ pára se, e somente se, cada computação $G_i(x)$ $(1 \leq i \leq k)$ e $F\big(g_1(x), \ldots, g_k(x)\big)$ param. □

Exemplo 6.53 Sejam $f(x_1, x_2) = x_1 + x_2$, $g_1(x_1, x_2) = x_2$ e $g_2(x_1, x_2) = \begin{cases} 1, & \text{se } x_1 = x_2, \\ 0, & \text{se } x_1 \neq x_2. \end{cases}$ Então

$$f\big(g_1(x_1, x_2), g_2(x_1, x_2)\big) = \begin{cases} x_2 + 1, & \text{se } x_1 = x_2, \\ x_2 & \text{se } x_1 \neq x_2. \end{cases}$$

Temos os programas: $F = I_1 : J(2,3,5),\ I_2 : S(1),\ I_3 : S(3),\ I_4 : J(1,1,1)$, $G_1 = I_1 : T(2,1)$ e $G_2 = I_1 : J(1,2,4),\ I_2 : T(3,1),\ I_3 : J(1,1,6),\ I_4 : S(3),\ I_5 : J(1,1,2)$.

Estes programas estão na forma canônica e $k = n = 2$. As constantes $\rho(F) = 3,\ \rho(G_1) = 2$ e $\rho(G_2) = 3$ nos dão $\rho = \max\{3, 2\} = 3$. Logo, o programa H é dado por:

$I_1 : T(1,4)$	$I_7 : Z(3)$	$I_{13} : S(3)$	$I_{19} : T(6,1)$
$I_2 : T(2,5)$	$I_8 : T(4,1)$	$I_{14} : J(1,1,11)$	$I_{20} : T(7,2)$
$I_3 : T(2,1)$	$I_9 : T(5,2)$	$I_{15} : T(1,7)$	$I_{21} : J(2,3,25)$
$I_4 : T(1,6)$	$I_{10} : J(1,2,13)$	$I_{16} : Z(1)$	$I_{22} : S(1)$
$I_5 : Z(1)$	$I_{11} : T(3,1)$	$I_{17} : Z(2)$	$I_{23} : S(3)$
$I_6 : Z(2)$	$I_{12} : J(1,1,15)$	$I_{18} : Z(3)$	$I_{24} : J(1,1,21)$

Observe que $G_1^* = I_3,\ G_2^* = I_{10}, \ldots, I_{14}$ e $F^* = I_{21}, \ldots, I_{24}$. Assim, para construir um programa para a composição $f(g_1(x), g_2(x), \ldots, g_k(x))$, não basta, simplesmente, concatenar os programas de $g_1(x), g_2(x), \ldots, g_k(x)$ e de $f(y_1, \ldots, y_k)$. Além disso, é preciso ajustar estes programas adequadamente.

A partir de funções parciais dadas, podemos obter novas funções parciais permutanto ou identificando variáveis, ou ainda, adicionando uma ou várias variáveis 'mudas' nas funções parciais. Mais formalmente, se $f(x, y)$ é dada, então:

$g(y, x) := f(x, y)$ (é uma permutação)

$h(x) := f(x, x)$ (é uma identificação)

$j(x, y, z) := f(y, z)$ (é uma adição de uma variável muda)

O teorema a seguir é um corolário do Teorema anterior e mostra que essas funções parciais, bem como combinações delas, transformam funções parciais MRI computáveis em funções parciais MRI computáveis.

Teorema 6.54 Suponhamos que $f(y_1, \ldots, y_k)$ é uma função parcial MRI computável e $x_{i_1}, \ldots, x_{i_k}$ é uma seqüência de k variáveis das variáveis $x_1, \ldots, x_n$ (possivelmente com repetições). Então a função parcial h definida por: $h(x_1, \ldots, x_n) := f(x_{i_1}, \ldots, x_{i_k})$ é MRI computável.

Demonstração: Escrevendo $x = (x_1, \ldots, x_n)$, temos que $h(x)$ é definida por $h(x) := f\big(p_n^{i_1}(x), \ldots, p_n^{i_k}(x)\big)$, que é MRI computável devido ao Lema 6.49 e ao Teorema 6.52. □

6.3.3 Funções Recursivas Primitivas

Apesar de que a definição mais convincente de procedimentos mecânicos seja dada pelo conceito de máquinas abstratas de Turing, o conceito equivalente de funções recursivas aparece primeiro, historicamente, mais ou menos com a culminação das definições recursivas simples de adição e multiplicação. Isto porque a noção de recursão é uma sofisticação da noção de indução aplicada às definições, onde se tenta tirar o máximo de proveito das propriedades de ordem dos naturais. Por isso as funções recursivas estão mais próximas dos ábacos que conhecemos para operar com inteiros (por exemplo, adição, multiplicação etc.).

A recursão é um método de definição de funções parciais, especificando cada um de seus valores em termos de outros valores previamente definidos e, possivelmente, usando outras funções parciais já dadas. Para ser mais preciso,

Definição 6.55 Sejam $f(x)$ e $g(x, y, z)$ (onde $x = (x_1, \ldots, x_n)$) funções parciais não necessariamente MRI computáveis. A função parcial $h(x, y)$ definida por:

(i) $h(x, 0) := f(x)$

(ii) $h(x, y + 1) := g\big(x, y, h(x, y)\big)$

é dita ser definida por *recursão das funções parciais* $f(x)$ e $g(x, y, z)$ e as equações (i) e (ii) são ditas *equações de recursão.*

À primeira vista surge uma pequena dúvida quanto ao modo como é definida, e até parece não ser uma definição válida, porque na 2ª linha fica $h(x, y)$ definida em termos dela mesma. Ocorre que a variável y aparece como uma testemunha de quantas vezes

é aplicada a função parcial $h(x, y)$ e este fato afastará qualquer dúvida. Por exemplo, suponhamos que queremos calcular $h(x, 3)$. Como $y = 3$ é não nulo, é preciso usar a equação (ii) com $3 = y+1$. A equação em (ii) mostra que precisaremos de $h(x, 2)$, que, por sua vez, precisará de $h(x, 1)$, que precisará de $h(x, 0)$. Agora usamos (i). Isto mostra a não ambigüidade da definição, e os valores de $h(x, y)$ para $y > 0$ são obtidos de $h(x, y')$ com $y' < y$, previamente calculados.

A função parcial $h(x, y)$ definida por recursão de $f(x)$ e $g(x, y, z)$ será função apenas quando $f(x)$ e $g(x, y, z)$ são funções; e o domínio de $h(x, y)$ satisfaz:

$(x, 0) \in Dom(h)$ se, e somente se, $x \in Dom(f)$,

$(x, y + 1) \in Dom(h)$ se, e somente se, $(x, y) \in Dom(h)$ e $\big(x, y, h(x, y)\big) \in Dom(g)$.

Observação 6.56 Quando a variável x não for envolvida, as equações de recursão (i) e (ii) se resumem a:

(i') $h(0) = a$ e

(ii') $h(y + 1) = g\big(y, h(y)\big)$

e, neste caso, dizemos que a função parcial $h(y)$ é obtida por *recursão simples* de $g(y, z)$.

As funções parciais $h(x, y)$ ou $h(y)$ são obtidas de modo único pelas equações de recursão, fato este que não provaremos aqui.

Exemplo 6.57 (a) Adição de números naturais definida por

$x + 0 = x$,

$x + (y + 1) = (x + y) + 1$.

Assim a adição (ou seja, a função $h(x, y) = x + y$) é definida por recursão das funções: $f(x) = x$ e $g(x, y, z) = z + 1$. Por exemplo, $h(x, 0) = f(x) = x$, $h(x, 1) = g(x, 0, h(x, 0)) = h(x, 0) + 1 = x + 1$ etc.

(b) A função $y!$ definida por:

$0! = 1$ e

$(y + 1)! = (y + 1)y!$

é definida por recursão simples da função $g(y, z) = (y+1)z$. Basta por:

(i') $h(0) = 1$ e **(ii')** $h(y + 1) = g\big(y, h(y)\big) = (y + 1)h(y)$.

O teorema seguinte mostra que a classe das funções parciais MRI computável é fechada para a recursão, ou seja:

Teorema 6.58 Sejam $f(x)$ e $g(x, y, z)$ funções parciais MRI computáveis, onde $x = (x_1, \ldots, x_n)$. Então a função parcial $h(x, y)$ obtida de $f(x)$ e $g(x, y, z)$ por recursão é MRI computável.

Demonstração: Veja o Teorema 4.4 do livro de N. Cutland, da referência. □

Funções Recursivas Primitivas

No contexto geral de recursão existem vários tipos de recursões a serem consideradas. A definição de recursão que demos anteriormente gera uma classe de funções parciais chamadas *Funções Recursivas Primitivas*. A noção que segue dá um outro enfoque formal à noção de computabilidade.

Definição 6.59 *F.R.P.*

A classe das *funções recursivas primitivas* é a menor classe de funções parciais que contém as funções básicas Zero: $Z(x) = 0, \forall x$, Sucessor: $S(x) = x + 1$, $\forall x$, Projeções: $P_n^i(x_1, x_2, \ldots, x_n) = x_i$, e é fechada para as operações de composição e recursão, onde "menor" é entendido como intersecção de conjuntos e "fechada para" significa que sempre que se aplica as operações de composição ou recursão aos elementos do conjunto, o objeto resultante também está no conjunto.

Observe, então, que a classe das F.R.P. é obtida como o resultado de sucessivas aplicações das operações de recursão e composição em quaisquer outras funções parciais, assim obtidas a partir das funções básicas. A classe das F.R.P. é uma subclasse da classe das funções parciais MRI computáveis devido aos Lema 6.49, Teorema 6.52 e Teorema 6.58.

Agora, usaremos os Teoremas 6.52 (composição) e 6.58 (recursão) para computar uma coleção de funções recursivas primitivas. Claro que a coleção total de F.R.P. é infinita e, portanto, a nossa lista, que será finita, vai depender da escolha das funções parciais $f(x)$ e $g(x, y, z)$ nas equações de recursão e também das

funções parciais $f(y)$ e $g_1(x), \ldots, g_k(x)$ do Teorema 6.52, previamente escolhidas.

Usaremos repetidamente o fato de que, devido ao Teorema 6.58, as funções parciais $f(x)$ e $g(x, y, z)$ não necessitam ser funções definidas em todas as variáveis para que a função parcial $h(x, y)$ seja uma F.R.P. Finalmente, queremos observar que, se o leitor voltar atrás, verificará que todas as funções parciais vistas até aqui são F.R.P. e também todos os resultados vistos: Teoremas, Lemas etc., continuam válidos se trocarmos MRI computável por F.R.P. A lista a seguir ajuda nesta verificação.

Exemplo 6.60 As seguintes funções parciais são recursivas primitivas (e, portanto, são MRI computáveis).

(a) $+(x, y) = x + y$.

Demonstração: Basta ver que a função parcial $g(x, y, z) = z+1$ do exemplo 6.57(a) é composição das funções básicas: Sucessor e $p_3(x, y, z)$.

(b) $.(x, y) = xy$.

Demonstração: Exercício (5) da lista no final do capítulo.

(c) $\wedge(x, y) = x^y$.

Demonstração: A função parcial x^y é dada por:

$$x^y = \begin{cases} 1, & \text{se } y=0, \\ x^{y-1}.x, & \text{se } y>0. \end{cases}$$

Logo, usando (b) e recursão para $g(x, y, z) = xz$ e $f(x) = 1$, temos que x^y pertence a classe das F.R.P.. De fato, f é recursiva primitiva e

$$g(x_1, x_2, x_3) = .\Big(P_3^1\big(x_1, x_2, \wedge(x, y-1)\big), P_3^3\big(x_1, x_2, \wedge(x, y-1)\big)\Big).$$

(d) $x \stackrel{\bullet}{-} 1 = \begin{cases} 0, & \text{se } x = 0. \\ x - 1, & \text{se } x \geq 1. \end{cases}$

Demonstração: É definida por recursão simples para $h(0)=0$ e $g(y, z)=y$.

(e) Subtração Limitada $x \stackrel{\bullet}{-} y = \begin{cases} x - y, & \text{se } x \geq y, \\ 0, & \text{se } x < y. \end{cases}$

Demonstração: É definida por recursão e (d) usando $f(x) = x$ e $g(x, y, z) = z \stackrel{\bullet}{-} 1$.

(f) *Função sinal* (do inglês Signal) $sg(x) = \begin{cases} 1, & \text{se } x \neq 0, \\ 0, & \text{se } x = 0. \end{cases}$

Demonstração: $sg(0) = 0$ e $sg(x+1) = 1$ por recursão simples, onde $h(0) = 0$ e $g(y,z) = 1$.

(g) *Função Teste do Zero* $\overline{sg}(x) = \begin{cases} 1, & \text{se } x = 0, \\ 0, & \text{se } x \neq 0. \end{cases}$

Demonstração: $\overline{sg}(x) = 1 \stackrel{\bullet}{-} sg(x)$.

Por substituição, $f(g(x)) = 1 \stackrel{\bullet}{-} sg(x)$, onde $f(x) = 1 \stackrel{\bullet}{-} x$ e $g(x) = sg(x)$; ou ainda $h(y+1) = g\big(y, h(y)\big)$, onde $g(x,y) = xy$.

(h) $|x - y|$.

Demonstração: $|x-y| = (x \stackrel{\bullet}{-} y) + (y \stackrel{\bullet}{-} x)$, por substituição, (a) e (e).

(i) $x!$

Demonstração: Exemplo 6.57(b).

(j) $min\{x,\ y\}$.

Demonstração: $min\{x,y\} = x \stackrel{\bullet}{-} (x \stackrel{\bullet}{-} y)$.

Sejam $g_1(x,y) = x$ (projeção), $f(x,y) = g_2(x,y) := x \stackrel{\bullet}{-} y$. Então, por substituição, $min\{x,y\} = f\big(g_1(x,y), g_2(x,y)\big)$.

(k) $max\{x,\ y\}$.

Demonstração: $max\{x,\ y\} = x + (y \stackrel{\bullet}{-} x)$, por substituição, usando (a) e (e).

(l) $r(x,\ y)$ =resto da divisão de y por x.

Convencionaremos $r(0,y) = y$ para obtermos uma função.

Demonstração: $r(x,0) = 0$ e

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

Então, $r(x,0) = 0$ e $r(x,y+1) = \big(r(x,y)+1\big) sg\big(|x - (r(x,y)+1)|\big)$, que pode ser obtida por recursão de $g(x,y,z) = \big(z+1\big) sg\big(|x - (z+1)|\big)$. Como $g(x,y,z)$ é recursiva primitiva, por aplicações de várias substituições, usando os exercícios anteriores e $r(x,y+1) = g(x,y,r(x,y))$, temos que $r(x,y)$ é recursiva primitiva.

(m) $q(x,y)$ =quociente da divisão de y por x.

Definimos $q(0,y)=0$. Então, $q(x,y)$ é definida por:

$$q(x,y+1)=\begin{cases} q(x,y)+1, & \text{se } r(x,y)+1=x,\\ q(x,y), & \text{se } r(x,y)+1\neq x.\end{cases}$$

Assim, $q(x,y)$ é definida por $h(x,0)=0$ e $h(x,y+1)=g(x,y,h(x,y))$, onde $g(x,y,z)=z+\overline{sg}\big(|x-(r(x,y)+1)|\big)$.

(n) $div(x,y)=\begin{cases}1, & \text{se } x|y,\\ 0, & \text{se } x\nmid y\end{cases}$

e definimos $0|0$ e $0\nmid y$ se $y\neq 0$.

Este exemplo mostra que o predicado "x divide y" (ou "y é múltiplo de x") é decidível.

Demonstração: Basta ver que $div(x,y)=\overline{sg}\big(r(x,y)\big)$. Assim, a função $div(x,y)$ é primitiva recursiva (MRI computável) por substituição.

(o) Ímpar$(x)=\begin{cases}1, & \text{se } x \text{ é ímpar},\\ 0, & \text{se } x \text{ é par}.\end{cases}$

Demonstração: Esta função é definida por recursão simples, onde $h(0)=0$ e $g(x,y)=\overline{sg}(y)$, daí $h(y+1)=g\big(y,h(y)\big)=\overline{sg}\big(h(y)\big)$.

Assim, o conjunto dos números naturais ímpares é decidível (ver definição 6.44).

(p) *Função Maior Inteiro da Metade*

$$\left[\tfrac{n}{2}\right]=\begin{cases}\frac{n}{2}, & \text{se } n \text{ é par},\\ \frac{n-1}{2}, & \text{se } n \text{ é ímpar}.\end{cases}$$

Demonstração: Definimos $\left[\frac{n}{2}\right]$ por recursão simples, definindo a função h por: $h(0):=0$ e $h(y+1):=g\big(y,h(y)\big)$, onde $g(x,y)=y+$ *ímpar*(x). Note que $g(x,y)=p_2(x,y)+$ *ímpar*$(p_1(x,y))$, que, pelos Teoremas e resultados anteriores obtidos, é recursiva primitiva.

Corolário 6.61 *Definição por casos*

Suponhamos que $f_1(x), \ldots, f_k(x)$ são funções parciais recursivas primitivas (ou MRI computáveis) e $M_1(x), \ldots, M_k(x)$ predicados decidíveis, tais que, para cada x, exatamente um dos predicados $M_1(x), \ldots, M_k(x)$ vale. Então é recursiva primitiva (MRI computável) a função parcial

$$f(x) = \begin{cases} f_1(x), & \text{se } M_1(x)\text{vale,} \\ f_2(x), & \text{se } M_2(x)\text{vale,} \\ \ldots & \ldots \\ f_k(x), & \text{se } M_k(x)\text{vale .} \end{cases}$$

Demonstração: Basta escrever $f(x)$ na forma $f(x) = \sum_{i=1}^{k} c_{M_i}(x) f_i(x)$, onde $c_{M_i}(x)$ é a função característica do predicado M_i. Daí, por substituição, usando adição e multiplicação, $f(x)$ é recursiva primitiva (MRI computável). □

Corolário 6.62 *Álgebra da Decibilidade*

Suponhamos que P e Q são predicados decidíveis. Então, os seguintes predicados também são decidíveis: **(a)** $\sim P$, **(b)** $P \wedge Q$, **(c)** $P \vee Q$.

Demonstração: As funções características destes predicados são respectivamente **(a)** $c_{\sim P}(x) = 1 \stackrel{\bullet}{-} c_P(x)$, **(b)** $c_{P \wedge Q}(x) = c_P(x).c_Q(x)$ ou $c_{P \wedge Q}(x) = min\{c_P(x),\ c_Q(x)\}$ e **(c)** $c_{P \vee Q}(x) = max\{c_P(x),\ c_Q(x)\} = sg\big(c_P(x) + c_Q(x)\big)$, que são funções parciais MRI computáveis. □

A recursão pode ser usada para construir funções recursivas primitivas (ou MRI computáveis) a partir de outras funções recursivas primitivas (resp. MRI computáveis). Um exemplo importante do uso de recursão é dado na seguinte situação:

Teorema 6.63 Suponhamos que $f(x, y)$ seja uma função qualquer, que é também função recursiva primitiva (MRI computável), e $x = (x_1, \ldots, x_n)$. Então, as funções de x e y, *soma limitada* $\sum_{z<y} f(x, z)$ e *produto limitado* $\prod_{z<y} f(x, z)$, definidas pelas equações de recursão a seguir, também são funções recursivas primitiva (resp. MRI computáveis)

$$\begin{cases} \sum_{z<0} f(x,z) & := & 0, \\ \sum_{z<y+1} f(x,z) & := & \sum_{z<y} f(x,z) + f(x,y), \end{cases}$$

e

$$\begin{cases} \prod_{z<0} f(x,z) & := & 1 \\ \prod_{z<y+1} f(x,z) & := & \left(\prod_{z<y} f(x,z)\right).f(x,y) \end{cases}$$

Demonstração: Basta ver que a recursão preserva a classe das funções recursivas primitivas (resp. MRI computáveis). □

É fácil ver que, se o limite em z na soma e produtos limitados é dado por qualquer função, que é função recursiva primitiva (resp. MRI computável), então o resultado é ainda computável, como segue.

Corolário 6.64 Suponhamos que as funções $f(x,z)$ e $K(x,w)$ são funções recursivas primitivas (MRI computáveis), então as funções de x de w : $\sum_{z<K(x,w)} f(x,z)$ e $\prod_{z<K(x,w)} f(x,z)$ também são funções recursivas primitivas (MRI computáveis).

Demonstração: Basta substituir y por $K(x,w)$ na soma e produtos limitados. □

6.3.4 Minimização Limitada e Codificação Por Primos

Uma outra técnica usada para a construção de funções recursivas ou MRI computáveis (pois preserva estas classes) é a *minimização limitada.* Fazendo uso desta nova técnica, daremos outra coleção particular de funções recursivas primitivas (MRI computáveis) e de predicados decidíveis. Aproveitando as funções parciais dadas, daremos a codificação por primos, cujo interesse é que esta codificação permite guardar muitas informações num único número.

Na definição que segue, a expressão: "$min\ z < y, (\cdots)$" significa "*o menor natural z menor que y tal que* $\cdots$".

Definição 6.65 *Minimização Limitada.* Dada uma função parcial $f(x,z)$, onde $x=(x_1,\ldots,x_n)$, definimos uma nova função parcial denotada por $g(x,y)=min\ z<y,(f(x,z)=0)$ e definida por

$$g(x,y):=\begin{cases} min\{z\in\mathbb{N},\ z<y\}, & \text{tal que } f(x,z)=0, \text{ se } \exists\ z,\\ y, & \text{se não existe } z.\end{cases}$$

Se $f(z)$ é função parcial apenas da variável z, então g é definida só em termos da variável y.

O operador "$min\ z<y$"é chamado de *operador de minimização limitada.*

Teorema 6.66 Suponhamos que $f(x,y)$ é uma função. Se $f(x,y)$ é recursiva primitiva (ou MRI computável), então a função $min\ z<y,\ \big(f(x,z)=0\big)$ é recursiva primitiva (MRI computável).

Demonstração: Considere a função $h(x,v)=\prod_{u<v} sg\big(f(x,u)\big)$, que é recursiva primitiva (MRI computável) pelo Corolário 6.64. Dados $x,\ y$, seja $z_0=minz<y,\ \big(f(x,z)=0\big)$. Então é fácil ver que,

se $v<z_0$, então $h(x,v)=1$;

Se $z_0\leq v<y$, então $h(x,v)=0$.

Assim

z_0 é o número de v's menores que y $(v<y)$, tal que $h(x,v)=1$, que é igual a $\sum_{v<y}h(x,v)$, ou seja:

$$min\ z<y,\ \big(f(x,z)=0\big)=\sum_{v<y}\big(\prod_{u\leq v} sg\big(f(x,u)\big)\big),$$

que é recursiva primitiva (resp. MRI computável) pelo Teorema 6.63. □

Como nas soma e produto limitados, o limite na minimização limitada pode ser dado por qualquer função recursiva primitiva (ou MRI computável) $K(x,w)$, pois, basta substituir y por $K(x,w)$, temos o seguinte corolário.

Corolário 6.67 Sejam $f(x,z)$ e $K(x,w)$ funções. Se $f(x,z)$ e $K(x,w)$ recursivas primitivas (MRI computáveis), então $min\ z < K(x,w),\ \big(f(x,z)=0\big)$ também é recursiva primitiva (resp. MRI computável). □

Temos ainda as seguintes aplicações envolvendo a minimização limitada.

Corolário 6.68 Suponhamos que $R(x,y)$ é um predicado decidível. Então

(a) A função parcial $f(x,y) = min\ z < y,\ \big(R(x,z)\big)$ é recursiva primitiva (resp. MRI computável).

(b) Os seguintes predicados são decidíveis.

(i) $M_1(x,y) \equiv \forall z < y\big(R(x,z)\big)$

(ii) $M_2(x,y) \equiv \exists z < y\big(R(x,z)\big)$.

Demonstração: **(a)** $f(x,y) = min\ z < y,\ \big(\overline{sg}(c_R(x,z)) = 0\big)$.

(b)(i) $c_{M_1}(x,y) = \prod_{z<y} c_R(x,z)$

(ii) $M_2(x,y) = \sim \big(\forall z < y,\ (\sim R(x,z))\big)$, é decidível pelo ítem **(i)** anterior e Corolário 6.62**(a)**. □

Agora, usaremos a minimização limitada em alguns casos e daremos outra coleção de funções recursivas primitivas ou MRI computáveis.

Teorema 6.69 As seguintes funções parciais são primitivas recursivas (MRI computáveis).

(a) $D(x) = $n^o de divisores de x (convencionamos que $D(0) = 1$),

(b) $Pr(x) = \begin{cases} 1, & \text{se } x \text{ é primo,} \\ 0, & \text{se } x \text{ não é primo.} \end{cases}$ (Isto é: o predicado "x é primo" é decidível.

(c) $p_m = m$-ésimo número primo (com a convenção $p_0 = 0$, $p_1 = 2$, $p_2 = 3$, etc).

(d) $[x]_y = \begin{cases} \text{o expoente de } p_y \text{ na decomposição em fatores primos de } x, \text{ para } x > 0 \text{ e } y > 0, \\ 0, \quad \text{se } x = 0 \text{ ou } y = 0. \end{cases}$

Demonstração: **(a)** $D(x) = \sum_{y \le x} div(y,x)$, onde div é a função dada no exemplo 6.60**(n)**, que é recursiva primitiva (MRI

computável). Logo, pelo Teorema 6.63 segue o afirmado. Outro método é usar que $div(y,x) = c_=(y,x) + c_=(2y,x) + \cdots + c_=(xy,x)$ para $x \geq 1$, onde $c_=(z,t)$ é a função característica da igualdade "$z = t$".

(b) $Pr(x) = \begin{cases} 1, & \text{se } D(x) = 2 \text{ (isto é } x > 1 \text{ e os únicos} \\ & \text{divisores positivos de } x \text{ são 1 e } x. \\ 0, & \text{em outro caso.} \end{cases}$

Então $Pr(x) = \overline{sg}(|D(x) - 2|)$.

(c) Pelo Teorema de Euclides (veja exercício (10)), sabemos que, dado um número primo ímpar p, existe um primo q, $p < q < p! + 1$. Então podemos definir a função p_m, que dá o m-ésimo número primo por:

$\begin{cases} p_0 = 0,\ p_1 = 2,\ p_2 = 3 \\ p_{m+1} = minz < (p_m! + 1),\ (z > p_m \text{ e } z\text{: primo}),\ \text{se } m \geq 2. \end{cases}$

O exercício (1)(d) mostra que o predicado "$z > y$"é decidível. Logo pelo Corolário 6.62 o predicado "$z > y$ e z : primo" é decidível. Como p_m é definida por recursão, segue-se do Corolário 6.68 que esta função é recursiva primitiva (resp. MRI computável).

(d) Temos que $[x]_y$ é dada por $min\ z < x,\ (p_y^{z+1} \nmid x)$, que é recursiva primitiva (resp. MRI computável), pois o predicado '$p_y^{z+1} \nmid b$' é decidível. □

Exemplo 6.70 Calculemos $[100]_y$ para todo y. Como $100 = 2^2.5^2$, temos que $[100]_0 = 0$, $[100]_1 = 2$ (expoente de $p_1 = 2$), $[100]_2 = 0$, $[100]_3 = 2$ e $[100]_y = 0$ para todo número y maior que 3.

Para a decodificação de uma seqüência, precisaremos da função (comprimento) que informa quantos primos em seqüência podemos encontrar na decomposição de $x > 1$ ($x \in \mathbb{N}$) a partir de $p_1 = 2$ (historicamente, esta função é denotada por lh, "length").

$lh(x) = min\ z < x,\ ([x]_z = 0)$.

Por exemplo, $lh(6) = lh(2.3) = lh(p_1.p_2) = 2$,

$lh(21) = lh(3.7) = lh(p_2.p_4) = 0$,

$lh(123) = lh(2.3^2.7) = lh(p_1.p_2^2.p_4) = 2$.

E agora podemos codificar uma seqüência finita qualquer de números naturais $b = (a_1, a_2, \ldots, a_n)$ pelo número $x = p_1^{a_1+1} p_2^{a_2+1} \cdots p_n^{a_n+1}$.

Observe que os p_i's estão em seqüência (do mesmo modo como fizemos no processo de Gödelização), de modo que $lh(x) = n$ e, portanto, corresponde ao 'tamanho' da n-upla. Para que isto ocorra, é suficiente somar 1 a todo expoente a_i de p_i, pois queremos codificar toda seqüência de comprimento n, inclusive seqüências contendo zeros. Assim, a codificação não fica ambígua para zero. Por exemplo, $b = (1, 0, 2)$ é codificado por $x = 2^2.3.5^3 = p_1^2.p_2.p_3^3$, e não por $y = 2.3^0.5^2 = p_1.p_3^2$, onde os primos não aparecem em seqüência, ou seja, $lh(y) = 1$ e não 3, como de fato é. Por este processo de codificação, o número a_j da posição j, na seqüência b, fica codificado por $p_j^{a_j+1}$. Observe que este processo mostra que o processo de Gödelização é recursivo primitivo. Além disso, como cada seqüência de comprimento n (n finito) tem uma codificação que é um número natural, temos aí uma aplicação injetora das seqüência finitas de números naturais em $\mathbb{N}$.

Para podermos decodificar qualquer número a_j da seqüência b, devemos definir

$(x)_j = [x]_j \dot{-} 1$.

Finalmente, para decodificar uma seqüência b codificada em um número x, observe inicialmente que esta função que codifica seqüências por números naturais é injetora, mas não é sobrejetora. Logo, dado um número x, precisamos saber se ele está na imagem (denotemo-la por S) desta função, ou seja, precisamos saber se x codifica alguma seqüência b de números naturais. Com a convenção de que um número x só codifica alguma seqüência até $lh(x)$, o que faremos, na prática, é tomar uma decomposição de x e, se ocorrer um primo p_j, ver se falta nesta decomposição algum primo p_i, com $i < j$. Se não faltar p_i para j, o maior dos índices, então x codifica alguma seqüência, caso contrário, x não codifica nenhuma seqüência. Este procedimento é recursivo primitivo e é descrito na função característica de S.

$$cod(x) = \begin{cases} 1, & \text{se } x \text{ não tem fatores primos maiores que } p_{lh(x)}, \\ 0, & \text{caso contrário.} \end{cases}$$

Usando o fato de que: $lh(x) < x$ (veja exercício), então $cod(x)$ é

dado por $cod(x) = \overline{sg}\big(min\ n\ (lh(x) < n \leq x : p_n|x\big)$, que é uma função recursiva primitiva por resultados anteriores.

Exemplo 6.71 **(a)** Para $x = 10 = 2.5$, temos que $lh(x) = 1$, pois falta o primo $p_2 = 3$. Logo, 10 não codifica nenhuma seqüência, ou seja, $cod(10) = 0$. Por outro lado, $min\ n\ \big(lh(10) < n \leq 10 : p_n|10\big) = 3$ e $\overline{sg}(3) = 0$.
(b) O número $30 = 2.3.5$ codifica a seqüência $b = (0, 0, 0)$ e $lh(30) = 3$.

Como não existe $n > 3$, tal que $p_n|30$, temos que
$\overline{sg}\big(min\ n(3 < n \leq 30) : p_n|30\big) = \overline{sg}(0) = 1 = cod(30)$.

(c) Se x é tal que $cod(x) = 1$, então x pode ser decodificado por

$$Decod(x) = \big((x)_1, (x)_2, \ldots, (x)_{lh(x)}\big) = b,$$

onde $(x)_i = [x]_i \overset{\bullet}{-} 1 = a_i$.

Por exemplo, $360 = 2^3.3^2.5$ satisfaz $cod(360) = 1$. Daí $Decod(360) = \big((360)_1, (360)_2, (360)_3\big) = (2, 1, 0)$.

Observação 6.72 A noção da codificação por primos pode ser usada para reduzir a classe das funções recursivas primitivas de várias variáveis à classe de funções recursivas primitivas de uma variável. Daí ser possível enumerar efetivamente as funções recursivas primitivas.

6.3.5 A Função de Ackermann e a Complexidade das F.R.P.

Para fechar o capítulo de Computabilidade, trataremos um pouco da *complexidade das F.R.P.* e da *função de Ackermann*.

Um pouco de experiência com as F.R.P. faz suspeitar de que podemos considerar vários níveis de complexidade entre as funções recursivas. Por exemplo

- complexidade da definição: quantas recursões são usadas, por exemplo.

- complexidade de cálculo: por exemplo, somar é mais simples que multiplicar, que é mais simples que exponenciar, que é

mais simples que fazer $(x^{\cdot^{\cdot^{\cdot^{x}}}})$ (y vezes). Teceremos apenas alguns comentários sobre o assunto.

Existem pelo menos dois bons conceitos de hierarquia de F.R.P., os conceitos segundo Grzegorczyk e Ritchie. O que eles fazem é precisar esta noção do ponto de vista matemático. Em termos simples, a idéia é buscar uma função que nos dê uma visão geral de todas as funções recursivas primitivas de uma só vez. Um exemplo intuitivo de tal função é a função que diagonaliza todas as F.R.P.; outro é a exponenciação iterada que diagonaliza as funções elementares (outra classe de funções). A idéia de Grzegorczyk foi construir, por recursão, uma classe de funções $\Theta_i,\ i = 1, 2, \ldots$ parecidas com a função de Ackermann $\psi(m, n)$, que crescem mais rapidamente que as funções $\psi(m, n)$, e, depois, usá-las para dividir a classe das F.R.P. em subclasses $\varepsilon^1,\ \varepsilon^2, \ldots, \varepsilon^n, \ldots$, onde a classe das F.R.P é igual à reunião de todas as classes ε^i. Por definição, a subclasse ε^i é a menor subclasse das funções recursivas primitivas que contém as funções: $Z(x),\ S(x),\ p^i_n(x)$ e Θ^i e é fechada para a composição e minimização limitada. Além disso, uma função $f \in \varepsilon^i$ se existe $g \in \varepsilon^i$ já definida, tal que $f(x, y) \leq g(x, y)$.

A Hierarquia de Ritchie lida com classes de funções parciais computáveis (por algum método) previsíveis e busca seqüências de funções parciais computáveis para a qual uma previsão na complexidade do cálculo possa ser feito de um modo razoavelmente simples.

A função de Ackermann é definida do seguinte modo:

$$\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \qquad \begin{cases} \psi(0, y) = y + 1, \\ \psi(x + 1, 0) = \psi(x, 1), \\ \psi(x + 1, y + 1) = \psi\big(x, \psi(x + 1, y)\big). \end{cases}$$

A pergunta é: Por que $\psi(x, y)$ é computável? (não necessáriamente no sentido MRI). Apesar de que ψ parece provir de uma definição recursiva, como temos visto, na verdade ela envolve recursão em duas variáveis. No entanto, ψ é, de fato, uma função, pois as equações são definidas de modo não ambíguo. Antes de demonstrar este fato, façamos um comentário sobre as equações. A primeira equação é clara, enquanto que, nas duas últimas equações,

observe que $\psi(x,y)$ com $x > 0$ é definido em termos de valores $\psi(x_1,y_1)$ com $x_1 < x$ ou $x_1 = x$ e $y_1 < y$. Assim, se considerarmos a tabela

$$\begin{array}{cccccc}
(0,0) & (0,1) & (0,2) & \cdots & (0,y) & \cdots \\
(1,0) & (1,1) & (1,2) & \cdots & (1,y) & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
(x,0) & (x,1) & (x,2) & \cdots & (x,y) & \cdots \\
(x+1,0) & (x+1,1) & (x+1,2) & \cdots & (x+1,y) & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots,
\end{array}$$

para obter $\psi(x,y)$, com $x > 0$, a definição de ψ nos faz proceder da seguinte maneira: Considerando a linha $x+1$ e coluna $x+1$ de (x,y), precisaremos de alguns valores $\psi(a,b)$ com (a,b), ou em linhas acima da linha de (x,y), eventualmente numa coluna mais distante da primeira coluna, ou (a,b) na mesma linha de (x,y), mas em uma coluna mais próxima da primeira. Isto ocorre para cada valor $\psi(x,y)$ que se deseja calcular. Assim, obrigatoriamente, atingiremos a primeira linha ou a primeira coluna. No caso de alcançar a 1ª coluna (equação 2), ela nos leva à linha imediatamente superior, se houver, de entrada x (1^a coordenada) e nos faz usar a equação 3, para $y = 0$. Na equação 3, usaremos a 1^a coluna, e mais tarde o resultado obtido, e a linha acima $x-1$, se houver. Desta forma, vamos subindo nas linhas da matriz anterior, formada de elementos de $\mathbb{N}\times\mathbb{N}$, até atingir a 1ª linha formada de elementos da forma $(0,y)$, $\quad y \in \mathbb{N}$; e não precisamos nos preocupar com y, pois é dado o valor $\psi(0,y)$. Por exemplo, para calcular $\psi(2,1)$, temos:

$\psi(2,1) = \psi\big(1,\psi(2,0)\big)$ e precisamos de $\psi(2,0)$,
$\psi(2,0) = \psi(1,1)$ e precisamos de $\psi(1,1)$,
$\psi(1,1) = \psi\big(0,\psi(1,0)\big)$ e precisamos de $\psi(1,0)$,
$\psi(1,0) = \psi(0,1)$ e $\psi(0,1) = 2$.

Daí $\psi(1,1) = \psi(0,2) = 3$ e, portanto, $\psi(2,1) = \psi(1,3)$. Mas $\psi(1,3) =$
$\psi\big(0,\psi(1,2)\big)$, e precisamos de $\psi(1,2)$,

$\psi(1,2) = \psi\big(0, \psi(1,1)\big)$ e, como $\psi(1,1) = 3$, vem que $\psi(1,2) = \psi(0,3) = 4$.

Assim, $\psi(1,2) = \psi(1,3) = \psi(0,4) = 5$.

Observe, na tabela, como foi a seqüência de passos para calcular $\psi(2,1)$.

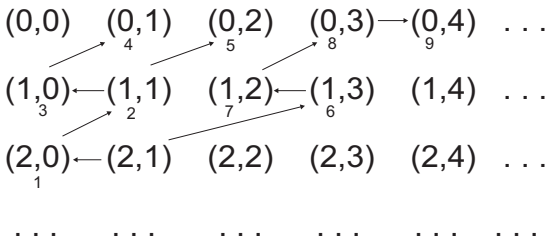


Figura 6.4: seqüência de passos para calcular $\psi(2,1)$.

Agora, provemos que $\psi(x,y)$ está bem definida em $\mathbb{N} \times \mathbb{N}$, por indução dupla nas variáveis x e y. Comecemos por indução na variável x.

(a) $x = 0$. Por definição, $\psi(0,y) = y+1$ para todo $y \in \mathbb{N}$. Logo, $\psi(0,y)$ está bem definida.

(b) Agora, suponhamos, como hipótese de indução na primeira variável, que $\psi(z,y)$ esteja bem definida para todo $z \leq x$ e qualquer $y \in \mathbb{N}$ e provemos que $\psi(x+1,y)$ está bem definida, para qualquer $y \in \mathbb{N}$.

Agora usaremos indução na segunda variável.

(i) $y = 0$. Por definição, $\psi(x+1,0) = \psi(x,1)$. Por hipótese de indução, na primeira variável vem que $\psi(x+1,0)$ está bem definido.

(ii) Suponhamos, como hipótese de indução na segunda variável, que $\psi(x+1,t)$ está bem definida, para todo $t \leq y$, e demonstremos que $\psi(x+1,y+1)$ está bem definido.

Por definição, $\psi(x+1,y+1) = \psi(x,\psi(x+1,y))$. Pela hipótese de indução na segunda variável, $\psi(x+1,y)$ é um número bem definido. Portanto, pela hipótese de indução na primeira variável, $\psi(x+1,y+1) = \psi(x,\psi(x+1,y))$ é um número bem definido. Logo, $\psi(x,y)$ está bem definida em todo $(x,y) \in \mathbb{N} \times \mathbb{N}$. Isto conclui a demonstração.

A função de Ackermann não é recursiva primitiva. A demonstração desta afirmação segue-se de 2 fatos:

(I) A classe das F.R.P. é enumerável. Isto pode ser demonstrado codificando todas F.R.P. de um número qualquer de variáveis à F.R.P. de apenas uma variável, usando a codificação por primos, que temos visto anteriormente. Daí enumerar as funções recursivas primitivas de uma variável.

(II) A função $\psi(x, y)$ domina todas funções unárias recursivas primitivas (isto é, se g é recursiva primitiva de uma variável, então existe m tal que $g(x) < \psi(m, x),\ \forall x \in \mathbb{N}$).

A demonstração dos fatos (I) e (II) podem ser encontrados no livro de R. Peter referência [6]. Agora podemos enunciar

Proposição 6.73 $\psi(x, y)$ não é recursiva primitiva.

Demonstração: Se $\psi(x, y)$ fosse recursiva primitiva, então $f(x) = \psi(x, x)$ também seria pelo Teorema 6.52. Pelo fato **(II)** existiria $m \in \mathbb{N}$, tal que $f(x) < \psi(m, x)$, para todo $x \in \mathbb{N}$. Em particular, teríamos $\psi(m, m) = f(m) < \psi(m, m)$, o que é absurdo. □

Apesar de $\psi(x, y)$ não pertencer à classe das funções recursivas, primitivas ela pertence a uma outra classe mais ampla de funções recursivas chamadas de *Funções Recursivas Parciais*. Esta classe é gerada (do mesmo modo que as F.R.P) pelas funções básicas: Sucessor, Zero, Projeções e é fechada para as operações de composição e recursão mas, neste caso, acrescenta o Operador μ; veja o livro de W. Carnielli citado na biliografia. Prova-se que esta classe é a mesma classe das funções Turing computáveis.

Exercícios

(1) Faça um programa para cada uma das funções parciais abaixo, para que elas sejam MRI computáveis.

(a) $f(x) = \begin{cases} 0, & \text{se } x = 0, \\ 1, & \text{se } x \neq 0. \end{cases}$ **(b)** $f(x) = 5$.

(c) $f(x,y) = \begin{cases} 0, & \text{se } x = y, \\ 1, & \text{se } x \neq y. \end{cases}$ **(d)** $f(x,y) = \begin{cases} 0, & \text{se } x \leq y, \\ 1, & \text{se } x > y. \end{cases}$

(e) $f(x) = \begin{cases} \frac{1}{3}x, & \text{se } x = 3q, \\ 0, & \text{em outros casos.} \end{cases}$

(2) Determine uma função parcial de duas variáveis que seja MRI computável pelo programa P: $I_1 = J(1,2,6),\ I_2 = S(2),$
$I_3 = S(3),\ I_4 = J(1,2,6),\ I_5 = J(1,1,2),\ I_6 = T(3,1).$

(3) (a) - Mostre que a função parcial $f : \mathbb{Z} \to \mathbb{Z}\ f(x) = 2x$ é MRI computável.

(b) - Mostre que a codificação $f^* : \mathbb{N} \to \mathbb{N}$, dada no exemplo 6.48, é MRI computável, exibindo um programa para f^*.

(c) Mostre que o predicado '$x \geq 0$' é decidível sobre $\mathbb{Z}$.

(4) (a) - Sem escrever qualquer programa, mostre que as funções parciais abaixo são MRI computáveis.
(i) função constante $f(x) = m, \forall x$. **(ii)** a função $g(x) = mx, \forall x$.
(b) Suponha que $f(x,y)$ é MRI computável, e $m \in \mathbb{N}$. Mostre que $h(x) := f(x,m)$ é MRI computável.
(c) Suponhamos que $g(x)$ é uma função de $\mathbb{N}$ em $\mathbb{N}$ MRI computável. Mostre que o predicado $M(x,y)$: "$g(x) = y$"é decidível.

(5) Mostre que a função $\bullet : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por:

$$x.y = \begin{cases} 0, & \text{se } y = 0, \\ (x.(y-1)) + x, & \text{se } y > 0, \end{cases}$$ é definida por recursão.

(6) (i) Mostre que o predicado '$x < y$' é decidível.

(ii) Use **(i)** e Corolário 6.62 para mostrar que o predicado de igualdade de números (isto é: '$x = y$´) é decidível.

(7) Faça um programa para cada uma das funções parciais abaixo para que sejam MRI computáveis:

(i) $f : \mathbb{N} \to \mathbb{N} \mid\ f(x) = 3x$. Dê $P(0),\ P(1),\ P(2)$.

(ii) $f : \mathbb{N} \to \mathbb{N} \mid\ f(x) = [\frac{x}{2}]$ (maior inteiro da metade). Dê $P(0),\ P(1),\ P(5)$.

(iii) $f : \mathbb{N} \to \mathbb{N} \mid\ f(x) = 5$. **(iv)** $f : \mathbb{N} \to \mathbb{N} \mid\ f(x) = x - 2$.

(8) Dê uma enumeração para as MRI.

(9) Mostre que os predicados M_1 : '$x \neq y$' e M_2 : '$x > 3$' $(x \in \mathbb{N})$ são decidíveis sobre $\mathbb{N}$. Dê suas funções características, os diagramas corridos, seus programas P_1 e P_2 e verifique se $P_1(2,2)$ e $P_1(2,3)$ convergem. Verifique se $P_2(2)$ e $P_2(4)$ convergem.

(10) *Teorema de Euclides.* Mostre que, para todo primo ímpar

p, existe um primo q, tal que $p < q < (p! + 1)$. Sugestão: Use o Teorema fundamental da aritmética e raciocine por contradição.

(11) Calcule $\psi(2, 3)$, destacando a seqüência de pares $(x, y) \in \mathbb{N}\times\mathbb{N}$ usados, fazendo uma seqüência numa tabela de elementos de $\mathbb{N}\times\mathbb{N}$.

(12) Mostre que as seguintes funções parciais são recursivas primitivas:

(a) $g(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$, onde $a_0,\ a_1, \ldots, a_n \in \mathbb{N}$.

(b) $[\sqrt{x}]$ (maior inteiro da raiz quadrada). **(c)** $mmc(x, y)$ e $mdc(x, y)$.

(d) $f(x)$ =número de divisores primos de x.

(e) A função ϕ de Euler, definida por: $\phi(x)$ =número de inteiros positivos entre 0 e x que são primos com x.

(f) A função parcial definida por: $f(0) = f(1) = 1$ e $f(n + 1) = f(n - 1) + f(n)$, para todos $n \geq 1$. Sugestão: Mostre que $g(x) = 2^{f(x)}3^{f(x+1)}$ é recursiva primitiva e depois use o Teorema 6.69**(d)**.

(13) Prove que a função de Ackermann $\psi(m, n)$ pode ser calculada para $m = 1, 2, 3$ por: **a.** $\psi(1, n) = n + 2$,

b. $\psi(2, n)=2n+3$ e **c.** $\begin{cases} \psi(3, n + 1) &= 2\psi(3, n) + 3, \\ \psi(3, 0) &= 5. \end{cases}$

(14) Mostre que $\psi(m, n) > n$ por indução dupla.

Sugestão: Primeiro, por indução sobre m, mostre que $\psi(0, n) > n$ para todo n. Depois, suponha que $\psi(m, n) > n$ para todo n e prove que $\psi(m + 1, n) > n$ para todo n (neste caso, use indução sobre n).

(15) Mostre que $\psi(m, n + 1) > \psi(m, n)$.
Sugestão: Pode ser feito por indução simples em m, usando o exercício 14.

(16) Mostre que $\psi(m + 1, n) \geq \psi(m, n + 1)$.

Sugestão: Mostre que $\psi(1, 0) = \psi(0, 1)$. Assuma verdadeiro para $m = 0$ e $k \leq n$ e prove que $\psi(1, n+1) \geq \psi(0, n+1)$. Até aqui você mostrou que o resultado vale para $m = 0$ e todo n. Deverá mostrar, em seguida, que vale para $m + 1$ e todo n. Para isto **(a)** Note que $\psi(m + 1, 0) = \psi(m, 1)$ (logo, vale para $n = 0$ em $m + 1$).

(b) Supondo $\psi(m+1,n) \geq \psi(m,n+1)$, mostre que $\psi(m+1,n+1) \geq \psi(m,n+1)$ usando os exercícios 15 e 16.

(17) Mostre que $lh(x) < x$, para todo $x > 1$.

RESPOSTAS DE ALGUNS EXERCÍCIOS

RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 1 §2 (a):
Para a negação basta colocar "Não é verdade"ou "É falso que" no início de cada uma das proposições.
RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 1 §2 (b):
Os valores verdades das proposições $p \wedge q$ são: (a) V, (b) F, (c) F, (d) V.
RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 1 §2 (c):
(1) São proposições (a) e (d). (2)(d) É falso que as ciências matemáticas são fáceis. ou é falso que 2 é menor que 3. (3)(a) $p \underline{\vee} q$, (b) $p \wedge q$, (c) $(p \wedge q) \underline{\vee} (\neg p \wedge \neg q)$, (d) $\neg p \wedge \neg q$. (4) Basta colocar "é falso que"ou "não é verdade que"no início de cada proposição. (5)(a) F, (b) V, (c) F, (d) F, (e) V, (f) F, (g) V, (h) F, (i) V. (6) São tautologias as proposições dos ítens: (a), (b), (f), (g), (h).
RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 1 §3.
(1) Basta ver que cada membro de $\equiv$ tem as mesmas tabelas-verdade.
(2) Verifique que as proposições $(p \to q) \to r$ e $p \to (q \to r)$ não tem as mesmas tabelas-verdade. (3) Semelhante ao exercício (1). (4) Ok.
(5) Usando o Teorema 1.13, ou fazendo uso das tabelas-verdade podemos ver que (i) e (iii) são tautologias, enquanto que (ii) é logicamente equivalente a $\neg q \wedge (p \longleftrightarrow r)$. (6)(a) implica, (b) não implica, (c) implica.
(9)(i) Basta fazer as tabelas de $\neg(p \wedge q)$ e $\neg(p \vee q)$, respectivamente.
(ii) $p|q$ é falsa, apenas quando p e q forem, ambas, verdadeiras; enquanto que $p \downarrow q$ é verdadeira, apenas quando p e q forem, ambas falsas.

RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 1 §4 e §5.

(1)(a) Pode-se usar quaisquer quantificadores, (b) $\exists x \in \mathbb{N}, \exists y \in \mathbb{N} \mid x + y = 8$. (c) Idêntica ao ítem (a).

(2)(a) $\exists x : \big(P(x) \vee Q(x)\big) \wedge \neg S(x)$, (b) $\exists x : P(x) \wedge \neg S(x)$, (c) $\forall x : \neg A(x) \vee \neg B(x)$, (d) $\forall x : \neg A(x) \longleftrightarrow C(x)$.

(3)(a) $mdc(2,3) \neq 3$ e $mmc(2,3) = 6, V$, (b) $\frac{3}{5} = \frac{6}{10}$ e $5.6 \neq 3.10$, F, (c) $\frac{1}{2} \leq \frac{2}{3}$ e $2.2 < 1.3, F$, (d) Todo número inteiro é primo, F.

(4)(i) Joana, Sílvia ou Maria é irmã de João e André, (ii) Joana, Sílvia ou Maria é irmã de João ou André, (iii) Joana, Sílvia e Maria são irmãs de João e André.

(5)(a) Verdadeira, $\{(1,1),(1,2),(1,3),(2,1),(2,2),(3,1)\}$, (b) Verdadeira $x = 1$, (c) Falso e a negação é: "$\exists x, \exists y : x^2 + y^2 \geq 12$"cujo conjunto solução é: $\{(2,3),(3,2),(3,3)\}$, (d) Verdadeira, $\{(1,1,2),(1,1,3),(1,2,2),(1,2,3),(2,1,2),(2,1,3),$
$(1,3,3),(3,1,3),(2,2,3),(2,3,3),(3,2,3)\}$, (e) Falso, a negação é: $\forall x, \forall y, \exists z \mid x^2 + y^2 \geq 2z^2$, cuja solução é $z = 1$ (pois $\forall x, \forall y \in A : x^2 + y^2 \geq 12$.).

(6)(a) $\sim P(x,y,z)$: "$\forall x, y \in A, \exists z \in A : x + 2y + 3z < 12$"(para $z = 1$ temos que $x + 2y + 3 < 12$, $\forall x, y \in A$), é falso (veja que para $x = y = 3$, não existe $z \in A$ tal que $3 + 3.3 + 3z < 12$).

(7)(i) Sejam P o conjunto de todas as pessoas, $M(y,x)$: "y é mãe de x". "$\forall x \in P,\ \exists y \in P \mid [M(y,x) \wedge \big(\forall z \in P,\ z \neq y \longrightarrow \neg M(z,x)\big)]$" ou "$\forall x \in P, \exists! y \in P \mid M(y,x)$". (ii) "$\forall x \in \mathbb{R}, x \neq 0,\ \exists y \in \mathbb{R} \mid x.y = 1$". (iii) $\forall \epsilon > 0,\ \exists \delta > 0 \mid \forall x \in \mathbb{R},\ x \neq a, |x - a| \longrightarrow |f(x) - L| < \epsilon$".

(8) Demonstre por contra-recíproca:"a: par $\Longrightarrow a^2$: par"e também por contradição: "a^2 : ímpar e a : par".

(9) (a) Se $a = 3$ então $a^2 = 4$, F, (b) Se $a^2 \neq 4$ então $a \neq 3$, F (c) $a \neq 3$ ou $a^2 = 4$, F (d) $a = 3$ e $a^2 \neq 4$, V. Isto confirma o Teorema 1.20.

RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 1.

(1) São proposições os ítens (a) F, (b) V, (d) F, (e) V, (g) V.
(2) (i) "Hoje não é terça-feira", (ii) "Existe poluição em São Paulo", (iii) "O verão no Rio de Janeiro não é quente e ensolarado"ou "O verão no Rio de Janeiro não é quente ou não é ensolarado".
(3) Alguns ítens: (e) "Se os votos não foram contados então a eleição não está decidida", (h) "Os votos não foram contados ou, a eleição não está decidida e os votos foram contados".
(4) (a) $p \wedge \neg\, q$, (b) $q \wedge \neg r$, (c) $p \wedge \neg\, q \wedge r$, (d) $p \longrightarrow (q \wedge r)$, (e) $[p \longrightarrow (q \wedge r)] \wedge \neg[(q \wedge r) \longrightarrow p]$, (f) $p \longrightarrow q$.
(5)(a) F, (b) V, (c) V, (d) V, (e) V, (f) V, (g) V, (h) F.
(6) Ambos os ítens são ou exclusivo.
(7) Negação: "Hoje choveu e amanhã não vai fazer frio", Contrarecíproca: "Se amanhã não fazer frio então hoje não choveu".
(9)(i) $min\{0,8;\ 0,4\} = 0,4$, (ii) $min\{1-0,8; 1-0,4\} = 0,2$, (iii) $0,8$, (iv) $0,6$.
(10) Não, pois não admite valor lógico ou falso ou verdadeiro.
(11) (a) Note que se uma das proposições esta certa então todas as outras estão erradas. Só a proposição de número 99 "exatamente 99 proposições desta lista são falsas"é a verdadeira. (b) Seja $P(n)$: "Pelo menos n proposições desta lista são falsas". Note que $P(n)$: verdadeira $\Longrightarrow P(s)$: verdadeira, $\forall s \leq n$. Logo $P(51),\ P(52), \ldots, P(100)$ são falsas e $P(1),\ P(2), \ldots, P(50)$ são verdadeiras.
(12) São tautologias (a), (b), (c), (e), (f), (g). (13) (i) $P = p \wedge q \wedge \neg r$, (ii) $Q = (p \wedge q \wedge \neg r) \vee (p \wedge \neg\, q \wedge r) \vee (\neg p \wedge q \wedge r)$. Esta é a forma disjuntiva normal de Q.
(17) (i) "Tem estudante que passa mais de cinco horas por semana em classe", (ii) "Todo (ou Cada) estudante passa mais de cinco horas por semana em classe", (iii) "Tem estudante que não passa mais de cinco horas por semana em classe", (iv) "Todo estudante não passa mais de cinco horas por semana em classe".
(18) (a) "Qualquer pessoa que é motorista é atenciosa"ou simplesmente "Todo motorista é atencioso", (b) "Todas as pessoas são motoristas e atenciosas" (e não motoristas atenciosos), (c) "Exis-

tem pessoas que se são motoristas, são atenciosas", (d) "Existem pessoas que são motoristas e são atenciosas".

(19) Seja U o conjunto universo, constituido de todos os alunos de sua classe. (a) $\exists x \in U \mid C(x) \wedge D(x) \wedge F(x)$, (b) $\forall x \in U,\ C(x) \wedge D(x) \wedge F(x)$, (c) $\exists x \in U \mid C(x) \wedge D(x) \wedge \neg F(x)$, (d) $\nexists x \in U \mid C(x) \wedge D(x) \wedge F(x)$, (e) $\forall x \in U,\ C(x) \vee D(x) \vee F(x)$.

(20) Sejam $P(x)$: "x é perfeito" e H o conjunto de todas as pessoas, $A(x)$: "x é meu amigo". (a) "$\nexists x \in H,\ P(x)$", ou equivalentemente "$\forall x \in H, \sim P(x)$": todos são imperfeitos, (b) $\sim [\forall x \in H :\ P(x)]$, (c) $\forall x \in H,\ \big(A(x) \rightarrow P(x)\big)$, (d) $\exists x,\ \big(A(x) \wedge P(x)\big)$, (e) $\forall x \in H,\ \big(A(x) \wedge P(x)$ ou $\big(\forall x \in H,\ A(x)\big) \wedge \big(\forall x \in H,\ P(x)\big)$, (f) $\neg\big(\forall x \in H,\ A(x)\big) \vee \big(\exists x \in H,\ P(x)\big)$ ou $[\exists x \in H, \neg A(x)] \vee [\exists x \in H :\ P(x)]$.

(21) (i) (a) V, (b) V, (c) F, (d) F, (e) V, (f) F. (ii) (a) V, (b) V, (c) F, (d) V, (e) F, (f) V, (g) F.

(22) (a) V, (b) V, (c) V, (d) V.

(23) (a) $P(-1) \vee P(0) \vee P(1) \vee P(2)$, (b) $P(-1) \wedge P(0) \wedge P(1) \wedge P(2)$, (c) $\neg P(-1) \vee \neg P(0) \vee \neg P(1) \vee \neg P(2)$, (d) $\neg P(-1) \wedge \neg P(0) \wedge \neg P(1) \wedge \neg P(2)$, (e) $\neg[P(-1) \vee P(0) \vee P(1) \vee P(2)]$, (f) $\neg[P(-1) \wedge P(0) \wedge P(1) \wedge P(2)]$.

(24) Sejam $p,\ q$ proposições, $T(p)$: "p é uma tautologia", $C(p)$: "p é uma contradição". (a) $\exists p,\ T(p)$, (b) $\forall p,\ \big(C(p) \rightarrow T(\neg p)\big)$, (c) $\exists p,\ q,\ \big(\neg T(p) \wedge \neg C(p) \wedge \neg T(q) \wedge \neg C(q) \wedge T(p \vee q)\big)$, (d) $\forall p,\ q,\ \big(T(p) \wedge T(q) \longrightarrow T(p \wedge q)\big)$.

(25) (a) "Se existe impressora com defeito e ativa então tem impressão que foi perdida", (b) "Se todas as impressoras estão ativas então alguma impressora tem uma longa fila", (c) "Se existe uma impressora que tem uma longa fila e perdeu impressões então existe impressora com defeito", (d) "Se todas impressoras estão ativas e todas tem uma longa fila então alguma impressão foi (será) perdida".

(26) Nem sempre tem o mesmo valor verdade, por exemplo, tome $U = \mathbb{Z},\ P(x)$: "$x \geq 0$" e $Q(x)$: "$x^2 \geq 1$".

(27) Pelas regras de inferência para proposições quantificadas temos: $\forall x, \big(P(x) \wedge Q(x)\big) \Longleftrightarrow P(c) \wedge Q(c),\ c$: arbitrário $\Longleftrightarrow P(c),\ c$: arbitrário e $Q(c),\ c$: arbitrário $\Longleftrightarrow$ "$\forall x\ P(x) \wedge \forall x\ Q(x)$".

(28) Semelhante ao anterior.

(29) Se A é verdadeiro, ou seja, A é uma tautologia T, então (a) $(\forall x P(x)) \wedge T \equiv \forall x P(x) \equiv \forall x\big(P(x) \wedge T\big)$ e (b) $\big(\exists x P(x)\big) \wedge T \equiv \exists x P(x) \equiv \exists x\big(P(x) \wedge T\big)$. Raciocínio análogo se A é uma contradição.
(30) Sejam $U = \mathbb{R}$, $P(x)$: "$x < 0$", $Q(x)$: "$x \geq 0$". Então (i) $\big(\forall x, x < 0\big) \vee (\forall x,\ x \geq 0)$ é falsa, enquanto que $\forall x\ (x < 0 \vee x \geq 0)$ é verdadeira, (ii) $\big(\exists x,\ x < 0\big) \wedge \big(\exists x,\ x \geq 0\big)$ é verdadeira, enquanto que $\exists\big(x < 0 \wedge x \geq 0\big)$ é falsa.
(31) (b) "Para todos números reais $x,\ y$ se x e y são positivos então o produto, xy, também é positivo.
(32) (a) "Algum aluno desta classe tem enviado uma mensagem por e-mail para um outro aluno desta classe". (b) "Algum aluno desta classe tem enviado uma mensagem por e-mail à todos os alunos desta classe". (c) "Todos os alunos desta classe tem enviados mensagens por e-mail à todos os alunos desta classe". (d) "Todos os alunos desta classe tem enviados mensagens por e-mail a um aluno da classe". (e) "Todos os alunos desta classe tem recebido uma mensagem por e-mail de algum aluno".
(33) (a) $\forall x, y \in \mathbb{Z},\ x \leq 0,\ y \leq 0 \longrightarrow x + y \leq 0$, (b) $\exists x,\ y \in \mathbb{Z},\ x \geq 0, y \geq 0 \mid x - y < 0$, (c) $\forall x,\ y \in \mathbb{Z},\ x^2 + y^2 \geq (x + y)^2$, (d) $\forall x \in \mathbb{Z}, x \geq 0 \longrightarrow (\exists a, b, c, d \in \mathbb{Z} \mid x = a^2 + b^2 + c^2 + d^2)$.
(34) (I) (a) V, (b) V, (c) V, (d) V, (e) V, (f) F, (g) F, (h) F,
(II) (a) V, (b) V, (c) F, (d) V, (e) F.
(35) (i) $l \in \mathbb{R}$ é um limite superior de S se $l \geq x,\ \forall x \in S$; (ii) $s \in \mathbb{R}$ é o supremo de S se $s \geq x,\ \forall x \in S$, e $\forall l \in \mathbb{R} \mid l \geq x,\ \forall x \in S \Longrightarrow l \geq s$.
(36) $\lim_{n\to\infty} a_n = L$ quando "$\forall \epsilon > 0,\ \exists n_0 \in \mathbb{N} \mid \forall n \geq n_0 \Longrightarrow |a_n - L| < \epsilon$".
(37) Tem-se que $\log_2 3 = \frac{a}{b} \in \mathbb{Q}$ se, e somente se, $2^a = 3^b$, com $a > 0,\ b > 0$. Absurdo, pois 2^a é par e 3^b é ímpar.
(38) (a) É válido, por Modus Ponens, (b) Válido, por Modus Ponens, (c) Válido, por Modus Tollens, (d) Não é válido, é uma falácia por negação da hipótese.
(39) O ítem (b) é válido.
(44) (i) claro, pois $x \leq y$ ou $y \leq x$. (ii) Divida em casos, por exemplo, façamos o caso $y \leq z \leq x$. Temos $min\{x, min\{y, z\}\} = min\{x, y\} = y$. Por outro lado $min\{min\{x, y\}, z\} = min\{y, z\} =$

y. Logo vale a igualdade.
(45) $n = 10k+l,\ 0 \leq l \leq 9$. Daí $n^2 = 10s+l^2$ e $n^4 = 10r+l^4$. Logo o último dígito de n^2 e n^4 são, respectivamente, o último dígito de l^2 e l^4.
(46) Note que n tem que ser par.
(47) (i) Tome 100 números consecutivos entre $10001 = (100)^2+1$ e $10200 = (101)^2-1$. A prova é construtiva. (ii) Se $2.(10)^{500}+15 = x^2$ e $2.(10)^{500}+16 = y^2$, então $y^2 = x^2+1$ e podemos tomar $y > x > 0$. Segue que $y \geq x+1$ e portanto $y^2 \geq (x+1)^2$. Da equação $y^2 = x^2+1$ temos um absurdo. Prova não construtiva.
(48) (a) É válido, (b) É válido, (c) Não é válido, (faça uma análise por casos, considerando a proposição "Matemática não é fácil"verdadeira e depois considerando ela é falsa, (d) É válido, (e) Não é válido.

RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 2:
(6) Seja a_n o n-ésimo termo da seqüência dada. Então (a) $a_0 = 1,\ a_n = 2.a_{n-1},\ n \geq 1$. (b) Pelo Exercício (4) $a_0 = 0$ e $a_n = a_{n-1} + (2n-1),\ n \geq 1$, onde $a_j = j^2$. (c) $a_0 = a_1 = 1$ e $a_{n+1} = a_n + a_{n-1},\ n \geq 1$.
(7) $E(0) = 1$ e $E(i+1) = \frac{n-i}{i+1}E(i),\ 0 \leq i < n$.
(9) (A) Por divisões sucessivas para o cálculo do mdc (página 65), encontramos: (a) $mdc(14;\ 7684) = 2 = (549).(14) + (-1).(7684)$.
(b) $mdc(4118; 7684) = 68 = (-50).(4148) + (27).(7684)$.
(c) $mdc(180; 252) = 36 = (3).(180) + (-2).(252)$.
(d) $mdc(1144; -351) = 13 = (4).(1144) + (13).(-351)$.
(e) $mdc(8024; 412) = 4 = (-21).(8024) + (409).(412)$.
(B) $mdc(6, 10, 14) = 2 = (2).(6) + (-1).(10) + 0.(14)$.
(10) (i) Segue a proposição 2.7. (ii) Use o item (i).
(11)(ii) Devido a proposição 2.7, ou exercício (10)(i).
(13) Temos $a=48.b,\ b > 1$. Logo $b=3, 5, 7$ e $a=144,\ 240,\ 336$.
(14) (d) Sejam $d_1 = mdc(ba, bc)$ e $d_2 = mdc(a, c)$. Como $d_2|a$ e $d_2|c$ temos que $bd_2|ba$ e $bd_2|bc$. Pela definição 2.10 ítem (3) temos que $bd_2|d_1$.

Reciprocamente, como $b|ba$ e $b|bc$, pelo item (3) da definição

2.10 temos que $b|d_1$. Seja $d_1 = bz,\ z \in \mathbb{Z}$. Como $ba = d_1x,\ bc = d_1y,\ x,\ y \in \mathbb{Z}$, substituindo temos: $ba = bzx,\ bc = bzy$. Logo $(b \neq 0)\ \ a = zx,\ c = zy$, ou então, $z|a$ e $z|c$. Por definição $z|d_2$. Isto implica que $bz|bd_2$, isto é, $d_1|bd_2$. Como d_1 e bd_2 são positivos vem que $d_1 = bd_2$.

(g) Pelo Teorema Fundamental da Aritmética $l = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, p_i distintos dois a dois, $1 \leq i \leq r,\ r \geq 1$. Como p_i^2 é fator de ab e $mdc(a,b) = 1$, cada p_i^2 é fator de a ou (exclusivo) b.

(16) Todo número natural n se escreve como $n = a_s10^s + a_{s-1}10^{s-1} + \cdots + a_110 + a_0$. Como $a_r10^r \equiv (-1)^r a_r(mod.11),\ r = 0, 1, \ldots$ temos que $n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^s a_s(mod.11)$. Portanto $11|n$ se, e somente se, $11|a_0 - a_1 + a_2 - \cdots + (-1)^s a_s$. Também temos que $9|n \iff 9|a_0 + a_1 + \cdots + a_s$ e $5|n \iff 5|a_0$.

(17) (i) $abcabc = a10^5 + b10^4 + c10^3 + a10^2 + b10 + c \equiv a(-9) + 3b - c + 9a - 3b + c(mod.13) \equiv 0(mod.13)$. Logo 13 divide $abcabc$. Raciocínio análogo para 11 e 7. (ii) Por (i) encontramos $310310 = 2.5.7.11.13.31$. (iii) É primo pois 997 não é divisível por nenhum primo menor que $\sqrt{997}$.

(18) (i) resto 4, (ii) resto 6, (iii) 07. Note que de $7^{10} \equiv 1(mod.11)$, temos que $7^{10q+r} = (7^{10})^q.7^r \equiv 7^r(mod.11)$. Então coloque a potência (de 7), 7^{1321} na forma $10q + r$, fazendo congruência dela módulo 10.

(19) Por exemplo, $f(x) = 5x + 1(mod.26)$. Então $f^{-1}(x) = 21x + 5(mod.26)$, (pois $5.21 \equiv 1(mod.26)$). "A terra é azul" é levada por f na seqüência "*f wzmmf z wabi*".

(20)

+	0	1
0	0	1
1	1	10

e

$$\begin{array}{cccccc} & & {\scriptstyle 10} & {\scriptstyle 10} & {\scriptstyle 1} & \\ & {\scriptstyle 1} & & & 1 & 1 \\ & & 1 & 1 & 1 & 1 \\ & 1 & 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 \end{array}$$

(22) (i) 21113_4 (ii) 202031_4 (iii) $-(2132_4 - 223_4) = -1303_4$ (iv) Quociente 12_4 e resta 312_4 (v) Quociente 33_4 e resta 3_4 (vi) Quociente 11_4 e resta 10_4.

(23) (i) 1001101101_2 (ii) 212000_3 (iii) 1545_7 (iv) 515_{11}.

(24) $12011_3 = 139$.

(25) Semelhante ao exercício (23).

(26) Os dígitos da base 4 são 0,1,2 e 3; logo em 1532_4 o 5 não pode

aparecer.

(27) $9,421875 = 9 + 0,421875$. Temos $9 = 1001_2$ e $0,421875 = 0,011011_2$, Logo $9,421875 = 1001,011011_2$.

(28) (a) (i) $0,8125 = 0,1101_2$ (ii) $\frac{3}{4} = 0,75 = 0,11_2$ (iii) $0,6875 = 0,1011_2$ (iv) $\frac{5}{8} = 0,625 = 0,101_2$ (v) $0,7 = 0,1\overline{0110}_2$ (vi) Pelo item (iv) $0,625 = \frac{5}{8}$. Logo $24,625 = 24 + \frac{5}{8} = 11000,101_2$. (vii) $29 = 11101_2$ e $0,1875 = 0,0011_2$. Logo $29,1875 = 11101,0011_2$ (viii) $0,22\cdots = 0,\overline{001110}$, (Veja exemplo 2.26(A)(iii).

(b) (i) $0,1101_2 = \frac{1}{2}+\frac{1}{4}+\frac{1}{16} = 0,8125$ (ii) $0,111_2 = \frac{1}{2}+\frac{1}{4}+\frac{1}{8} = 0,875$ (iii) $0,101101_2 = \frac{1}{2} + \frac{1}{8} + \frac{1}{16} + \frac{1}{64} = 0,703125$.

(29) (i) De $1+r+r^2+\cdots+r^n+\cdots = \dfrac{1}{1-r}$, para $0 < r < 1$, temos $2^{-3}+2^{-7}+2^{-11}+\cdots = 2^{-3}\big(1+2^{-4}+2^{-8}+\cdots\big) = 2^{-3}.\dfrac{1}{1-2^{-4}} = \dfrac{2}{15}$, e $2^{-4}+2^{-8}+2^{-12}+\cdots = \dfrac{1}{15}$. Logo a resposta é $\frac{1}{2}+\frac{2}{15}+\frac{1}{15} = \frac{7}{10}$.

(30) (a) Proposição 2.23 (b) $a = 6D_{16} = \big((110)(1101)\big) = 1101101_2$, $b = 3A_{16} = 111010_2$, $a - b = 6D_{16} - 3A_{16} = 33_{16}$ (c) $x + y = 7C_{16} + A2_{16} = 11E_{16}$, e $x - y = 7C_{16} - A2_{16} = -(A2_{16} - 7C_{16}) = -26_{16}$, e pela proposição 2.23, $x + y = \big((0001)(0001)(1110)\big) = 100011110_2$.

$x - y = -26_{16} = -\big((0010)(0110)\big) = -100110_2$.

(31)(i) Fazendo o processo inverso da Proposição 2.23, para a base octal, junte os números da seqüência em blocos de 3 dígitos ordenados à partir da vírgula e passe cada bloco para a base dez: $(101111,01)_2 = \big((101)(111),(010)\big)_2 = 57,2_8$ e $(111010,1001)_2 = \big((111)(010),(100)(100)\big)_2 = 72,44_8$. Na base hexadecimal temos: $(101111,01)_2 = \big((0010)(1111),(0100)\big)_2 = 2F,4_{16}$ e $(111010,1001)_2 = \big((0011)(1010),(1001)\big) = 3A,9_{16}$.

(ii) Use a Proposição 2.23 para obter:
$A85E,16_{16} = 1010100001011110,0001011_2$. Para reduzir para a base octal não podemos usar a Prop. 2.23, (Por que?). Passe para a base decimal e depois para a base octal para obter: $A85E_{16} = 124136,054_8$. E
$761F,98_{16} = 73037,46_8 = 111011000011111,10011_2$.

(32) Façamos as tabuadas da base octal (mais curtas).

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	10
2	2	3	4	5	6	7	10	11
3	3	4	5	6	7	10	11	12
4	4	5	6	7	10	11	12	13
5	5	6	7	10	11	12	13	14
6	6	7	10	11	12	13	14	15
7	7	10	11	12	13	14	15	16

•	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	10	12	14	16
3	0	3	6	11	14	17	22	25
4	0	4	10	14	20	24	30	34
5	0	5	12	17	24	31	36	43
6	0	6	14	22	30	36	44	52
7	0	7	16	25	34	43	52	61

(33)(i) Quociente $1C8_{16}$ e resto 139_{16}. (ii) $2142_8.34_8 = 75270_8$.
(iii) $230702_8 \div 12520_8 = 16,261\cdots_8$.
(34) Os procedimentos são os mesmos da Prop. 2.23.

RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 3.
(1) São falsos os ítens: (a), (b), (d), (e), (g), (h), (i), (j), (m), (o), (p). Os outros são verdadeiros.
(2) (a) $\in$ (b) $\subseteq$ (c) $\subseteq$ (d) $\subseteq$.
(3) São falsos os ítens (a) $1 \notin B$, (b) $1 \notin C$, (c) $3 \notin C$, (d) $5 \notin B$ e são verdadeiros os ítens: (e) $\forall x, x \in C \Longrightarrow x \in C$, (f) $\forall x, x \in \emptyset \Longrightarrow x \in B$.
(4) (a) Y, (b) $\{4\}$, (c) $\emptyset$, (d) $\{4,5,6,7,8\}$, (e) X, (f) $\{4,5\}$, (g) $\{1,2,3,4,5,6,8\}$.
(5) (a) A, (b) $\{4\}$, (c) $\{4,6,10,12\}$, (d) $\{3,11\}$, (e) $\{1,4\}$, (f) $\{3,9,10,11\}$, (g) $\{5,6,7\}$, (h) $\{0,2,4,\ldots,2n,\ldots\}$, (i) $\{5,6,7,8\}$.

(8) (a) Falso, tome $A = \{1\}$, $B = \{1,2\}$ e $C = \{1,2,3\}$; (b) Falso, tome $A = \{1,2\}$, $B = \{1,3\}$ e $C = \{1,4\}$; (c) Falso, tome $A = \{1,2,3,5\}$, $B = \{1,2,4\}$ e $C = \{1,4,5\}$; (d) Ok.

(9) Use também diagrama de Venn.

(11) (a) $\mathbb{R}\backslash\{-1\}$, (b) $\{x \in \mathbb{R} : -1 < x \leq 1\}$, (c) $\{x \in \mathbb{R} : x < -1\}$, (d) $\{-1\}$.

(12) (i) $\{(-3,2), (\frac{1}{3}, \frac{1}{3})\}$, (ii) $A \setminus \{(-3,2), (\frac{1}{3}, \frac{1}{3})\}$.

(15) (i) falso, (ii) $A = \{a\}$, $B = \{b\}$. Então $\{(a,b)\}$ pertence a $\wp(A \times B)$ e não pertence a $\wp(A) \times \wp(B)$.

(16) $\wp(A) = \{\emptyset, \{a\}, \{b\}, \{\{a,b\}\}, \{a,b\}, \{a,\{a,b\}\}, \{b,\{a,b\}\}, A\}$.

(17) $\{0,3,5,7\} \times \{0,3,5,7\}$.

(18) (i) $\{1,2\}$, (ii) $\{1,2,6\}$, (iii) $\emptyset$, (iv) $A\backslash B = \{1,3,5\}$, $B - A = \{6,8,10\}$, (v) $A - B = \{x \in \mathbb{N} \mid x \text{ é par}\}$, $B - A = \emptyset$.

(20) (a) Um retângulo limitado pelas retas $x = 1$, $x = 4$, $y = -2$ e $y = 3$.

(21)(a) $\{(a,2),(a,3),(a,4),(b,2),(b,3),(b,4)\}$ (b) $\{(a,3),(b,3)\}$, (c) $\{(a,2),(b,2)\}$, (d) $\{(a,2),(a,3),(a,4),(b,2),(b,3),(b,4)\}$, (e) $\{(a,2),(a,4),(b,2),(b,4)\}$.

(23) Use indução quando for o caso.

(24) (a) B unitário ou A vazio, (b) $n(A).n(B)+n(A \bigcap B) = n(A)+n(B)$.

(25) (a) 190, (b) 810, (c) 245.

(26) $\bigcup_{i \in \mathbb{R}} A_i = \mathbb{R}^2 - \{(0,y), y \in \mathbb{R}\}$ e $\bigcap_{i \in \mathbb{R}} A_i = \{(0,0)\}$.

(27) (i) (a) $\{1,2,3,\{1,2,3\}\}$, (b) $\{\emptyset\}$, (c) $\{\emptyset,\{\emptyset\}\}$, (d) $\Big\{\emptyset, \{\emptyset\}, \big\{\emptyset,\{\emptyset\}\big\}\Big\}$; (ii) $n+1$.

(28) Do exercício (4): (a) y = 11100000, (b) 00010000, (c) 00000000, (d) 00011111, (e) 11111000, (f) 00011000, (g) 11111101;

Do exercício (5) (a) 111111111, (b) 001000000, (c) 001101010, (d) 010000100, (f) 010011100.

(30) Sejam $a = a_1a_2\cdots a_n$, $b = b_1b_2\cdots b_n$ as seqüências de bits associadas aos conjuntos A e B, respectivamente. Então as seqüências de bits associadas aos conjuntos $A - B = A \bigcap B^c$ e $A \triangle B$ são, respectivamente: $a \wedge \overline{b}$ e $(a \vee b) \wedge (\overline{a \wedge b})$.

RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 4 §1.

(1) (a) reflexiva, anti-simétrica e transitiva (b) reflexiva, simétrica e transitiva (c) simétrica (d) simétrica (e) simétrica (f) simétrica (g) reflexiva, anti-simétrica e transitiva (h) reflexiva, anti-simétrica e transitiva.

(3) só a propriedade reflexiva

(7) A relação não é reflexiva, pois $a_{44} = 0$; não é simétrica pois a matriz não é simétrica; não é anti-simétrica pois $a_{12} = a_{21} = 1$; não é transitiva pois $a_{23} = a_{34} = 1$ e $a_{24} = 0$.

(8) $\mathsf{R} = \{(a,b),(b,a)\}$, $\mathsf{S} = \{(b,c),(c,b)\}$ definidas sobre $\{a,b,c\}$. Então R e S são simétricas mas $\mathsf{R} \circ \mathsf{S} = \{(c,a)\}$ não é simétrica.

(9) É preciso que, para cada $a \in A$ exista $b \in A$ tal que $(a,b) \in \mathsf{R}$. $\mathsf{R} = \{(a,a),(b,b),(a,b),(b,a)\}$, definida sobre $\{a,b,c\}$, é simétrica, transitiva, mas não é reflexiva.

(12) Se $\mathsf{R} = \{(a,a),(b,b),(c,c),(a,b),(b,c)\}$ definida sobre $\{a,b,$ $c,\}$, então $\mathsf{R} \circ \mathsf{R}^{-1}$ não é transitiva.

(13)(b) Antigo (c) $\mathsf{R} = \{(a,b),(b,a)\}$, $\mathsf{S} = \{(b,c),(c,b)\}$ definidas sobre $\{a,b,c\}$.

(15) $2^{m.n}$.

(16) Existem 2^{n^2-n} relações reflexivas, $2^{(n+1).n.2^{-1}}$ relações simétricas e $3^{n(n-1).2^{-1}}.2^n$ relações anti-simétricas.

(17) $\mathsf{S} \circ \mathsf{R} = \{(2,3),(3,2),(4,1)\}$, $I_B \circ \mathsf{R} = \{(2,4),(3,3),(4,2)\} = \mathsf{R} \circ I_A$,
$\mathsf{R} \circ \mathsf{S} = \{(3,4),(4,3)\}$.

$$M_{\mathsf{R}} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad M_{\mathsf{S}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$M_{\mathsf{S}\circ\mathsf{R}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad M_{\mathsf{R}\circ\mathsf{S}\circ\mathsf{R}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

(18) $\mathsf{S} \circ \mathsf{R} = \{(1,0),(2,1)\}$, $\mathsf{R} \circ \mathsf{S} = \{(2,0),(2,1),(3,2)\}$, $\mathsf{R} \circ \mathsf{S} \circ \mathsf{R} = \{(1,0),(1,1),(2,2)\}$ e $\mathsf{R}^3 = \{(0,0),(0,1),(0,2),(0,3),$ $(1,2),(2,1),(2,3)\}$.

(20) $\mathsf{D} = \{(2,3),(2,4),(4,3)\} \subseteq \{1,2,4\} \times \{3,4\}$ e D com a menor

cardinalidade possível é univocamente determinado.

(21) Mostre por indução que $\mathsf{R}^r = \{(i,j) \in \mathbb{Z}^2 \mid j = i + r\}$.

(23)(a) $\mathsf{S} \cup \mathsf{R} = \{(1,1),(1,2),(1,4),(2,1),(2,2),(2,3),(2,4),(3,1),(3,3),(4,2),(4,3),(4,4)\}$.

(b) $\mathsf{R} \cap \mathsf{S} = \{(1,2),(1,4),(2,1),(3,3)\}$ (c) $\mathsf{T}^c = \{(2,2),(3,3),(3,4),(4,2),(4,3)\}$

(d) $\mathsf{R} \cup \mathsf{T}^c = \{(1,2),(1,4),(2,1),(2,2),(2,3),(2,4),(3,1),(3,3),(3,4),(4,2),(4,3)\}$

(e) $(\mathsf{R} \cup \mathsf{S}) \cap \mathsf{T} = \{(1,1),(1,2),(1,4),(2,1),(2,3),(2,4),(3,1),(4,4)\}$

(f) $\mathsf{R} \cup \mathsf{S}^c = \{(1,2),(1,3),(1,4),(2,1),(2,3),(2,4),(3,1),(3,2),(3,3),(3,4),(4,1),(4,3)\}$

(g) $\left(\mathsf{R} \cup (\mathsf{S} \cap \mathsf{T}^c\right)^c = \{(1,1),(1,3),(3,2),(3,4),(4,1),(4,4)\}$

(h) $(\mathsf{S} \cup \mathsf{T}) \cap (\mathsf{R} \cup \mathsf{T}^c) = \{(1,2),(1,4),(2,1),(2,2),(2,3),(2,4),(3,1),(3,3),(4,2)\}$; e

$$M_{\mathsf{S}\cup\mathsf{R}} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \qquad M_{\mathsf{R}\cap\mathsf{S}} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M_{\mathsf{T}^c} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad M_{\mathsf{R}\cup\mathsf{T}^c} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

$$M_{(\mathsf{R}\cup\mathsf{S})\cap\mathsf{T}} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M_{\mathsf{R}\cup\mathsf{S}^c} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$M_{\left(\mathsf{R}\cup(\mathsf{S}\cap\mathsf{T}^c\right)^c} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad \text{e finalmente}$$

$$M_{(\mathsf{S}\cup\mathsf{T})\cap(\mathsf{R}\cup\mathsf{T}^c)} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 4 §2.

(1)(a) $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ (b) {Pares, Ímpares} (c) $\{\overline{0}, \overline{1}, \ldots, \overline{9}\}$ (d) $\{\overline{0}, \overline{1}, \ldots, \overline{11}\}$.

(4) Se R e S são as relações definidas sobre $\{a, b, c, d, e\}$ e $\{r, s, t, x, y, z\}$, respectivamente, então $\Pi_{\mathsf{R}} = \{\{a, c\}, \{b, e\}, \{d\}\}$ e $\Pi_{\mathsf{R}} = \{\{r, t\}, \{s, x, y\}, \{z\}\}$.

(6) $\Pi_{\mathsf{R}} = \{\overline{(1,1)}, \overline{(1,2)}, \overline{(1,3)}, \overline{(1,4)}, \overline{(2,4)}, \overline{(3,4)}\}$ onde $\overline{(a,b)} = \{(r,s) \in A \text{ tal que a soma } r+s \text{ dá } a+b\}$,
$\Pi_{\mathsf{S}} = \{\overline{(1,1)}, \overline{(1,2)}, \overline{(1,3)}, \overline{(1,4)}\}$.

(7) $\Pi_1 = \{\{a\}, \{b\}, \{c\}, \{d\}\}$, $\Pi_2 = \{\{a, b\}, \{c, d\}\}$, $\Pi_3 = \{\{a, c\}, \{b, d\}\}$, $\Pi_4 = \{\{a, d\}, \{b, c\}\}$, $\Pi_5 = \{\{a\}, \{b, c, d\}\}$, $\Pi_6 = \{\{b\}, \{a, c, d\}\}$, $\Pi_7 = \{\{c\}, \{a, b, d\}\}$, $\Pi_8 = \{\{a, b, c\}, \{d\}\}$, $\Pi_9 = \{\{a\}, \{b\}, \{c, d\}\}$, $\Pi_{10} = \{\{a\}, \{c\}, \{b, d\}\}$, $\Pi_{11} = \{\{a\}, \{d\}, \{b, c\}\}$, $\Pi_{12} = \{\{b\}, \{c\}, \{a, d\}\}$, $\Pi_{13} = \{\{b\}, \{d\}, \{a, c\}\}$, $\Pi_{14} = \{\{c\}, \{d\}, \{a, b\}\}$, $\Pi_{15} = \{\{a, b, c, d\}\}$.

(8) Vamos dar uma fórmula recorrente: Seja P_n é o número de partições de um conjunto com n elementos, digamos $\{a_1, a_2, \ldots, a_n\}$. Tome outro elemento a_{n+1} e considere um bloco do conjunto $\{a_1, a_2, \ldots, a_n, a_{n+1}\}$ contendo a_{n+1}. Supõe que ele contém k elementos adicionais (todos de $\{a_1, a_2, \ldots, a_n\}$). Esses elementos podem ser escolhidos de $\binom{n}{k}$ maneiras diferentes. Os $n-k$ elementos restantes podem ser particionados em P_{n-k} blocos. Como k pode ser qualquer número de 0 até n, a regra *soma de produtos* nos dá a fórmula recursiva: $P_{n+1} = \sum_{k=0}^{n} \binom{n}{k} P_{n-k} = \sum_{k=0}^{n} \binom{n}{k} P_k$.

Temos $P_3 = 5$, $P_4 = 15$ e $P_5 = 52$ que pode ser verificado pela fórmula ou diretamente, por cálculo.

(9) $\mathsf{R} = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,1), (3,4), (4,3)\}$.

(10) Só (b).

(11) Só a representação à esquerda é de uma relação de equivalência.

(12) A classe de equivalência de um elemento a é constituído de todos os elementos que você pode chegar até ele por um caminho de setas partindo de a, sem saltos.

(13) (b) $\overline{0} = \{0\}$, $\overline{a} = \{a.2^m,\ m \in \mathbb{Z}\},\ a \neq 0$.

(14) Se R é uma relação de equivalência; sejam $a, b, c \in A$ tais que $a\mathsf{R}b$ e $b\mathsf{R}c$. Então $a\mathsf{R}c$ (pela transitiva) e, pela simetria, $c\mathsf{R}a$. Logo R é circular. Suponha agora que R é reflexiva e circular. Se $a\mathsf{R}b$ temos $a\mathsf{R}b$ e $b\mathsf{R}b$. Por hipótese (neste caso $b = c$), $b\mathsf{R}a$. Logo R é simétrica. Além disso, se $a\mathsf{R}b$ e $b\mathsf{R}c$ então $c\mathsf{R}a$ pela circular. Como R é simétrica $a\mathsf{R}c$. Logo R é também transitiva. Portanto, de equivalência.

(16) Se $\Pi_{\mathsf{R}} = \{\overline{a}_1, \ldots, \overline{a}_r\}$, $\Pi_{\mathsf{S}} = \{\overline{b}_1, \ldots, \overline{b}_s\}$ então $\bigcup_{i,j} (\overline{a}_i \cap \overline{b}_j) = A$, $1 \leq i \leq r$, $1 \leq j \leq s$. Temos no máximo rs intersecções $\overline{a}_i \cap \overline{b}_j$ distintas.

(17) Para $\alpha \circ \beta = \beta \circ \alpha$ tome $\beta = \alpha$. Para $\alpha \circ \beta \neq \beta \circ \alpha$, tome $\alpha = \{(a,a),(a,b),(b,a),(b,b),(c,c)\}$ e $\beta = \{(a,a),(b,b),(b,c),(c,b),(c,c)\}$ definidas sobre $\{a, b, c\}$.

(18) Posto quatro e classes de equivalências distintas:$\overline{0}, \overline{1}, \overline{2}, \overline{4}$.

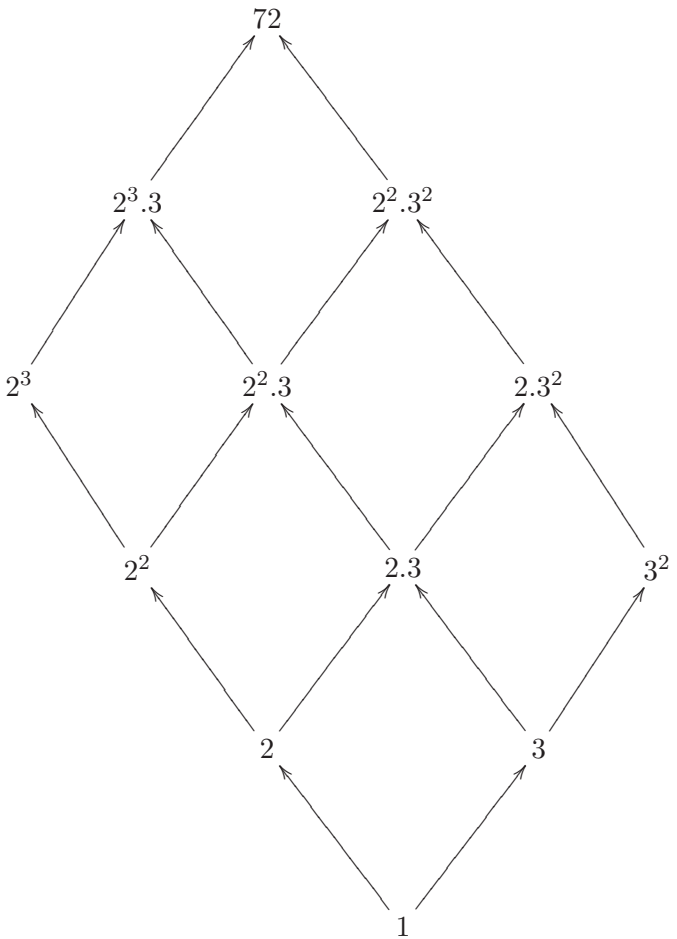
RESPOSTAS DOS EXERCÍCIOS DO CAPÍTULO 4 §3.

(2)(i) 2 e 3 são incomparáveis, $\{2, 4, 8, 32\}$ é uma cadeia. (ii) Os limites superiores de A são todos os números naturais da forma $6q$, $q \in \mathbb{N}$, $\max A = \sup A = 6$ e 6 é o único elemento maximal; 1 é o único limite inferior. Logo $1 = \inf A$, não existe $\min A$, 2 e 3 são elementos minimais.

(3)(i) não é linear, pois $(0,1)$ e $(1,0)$ são incomparáveis. (ii) É totalmente ordenado, pois $(0,0) \preceq_2 (0,1) \preceq_2 (1,0) \preceq (1,1)$. (iii) as definições são exatamente as mesmas para (a, b) e $(c, d) \in E \times E$.

(7)(i) segue do exercício (5), (ii) $(1,2)$, $(2,1)$ são incomparáveis. Logo não é total. (iii) a ordem inversa é $(a, b) \succeq (c, d) \iff a$ é múltiplo de c e $b \geq d$. (iv) Ambos são elementos maximais e minimais, limites inferiores $(1,0)$, $(1,1)$, e $\inf A = (1,1)$, não existe $\min A$. Limites superiores são da forma $(2s, b)$, com $s \in \mathbb{N}$ e $b \geq 2$; $\sup A = (2,2)$, não existe $\max A$.

(10)



(a) a natureza do diagrama de Hasse do conjunto $D^+(p_1^{k_1}.p_2^{k_2})$ é análogo ao caso acima, ou seja, no nível zero coloca-se o número $1 = p_1^0.p_2^0$, no primeiro nível coloca-se os elementos incomparáveis p_1 e p_2, no segundo nível coloca-se os elementos incomparáveis $p_1^2,\ p_1.p_2$ e p_2^2 (se $k_1 > 1$ e $k_2 > 1$). Em geral, no nível s coloca-se todos os possíveis elementos $p_1^a.p_2^b$, com $a + b = s,\ 0 \leq a \leq k_1,\ 0 \leq b \leq k_2$, com uma seta de $p_1^a.p_2^b$ à $p_1^{a+1}.p_2^b$ (caso este divide $p_1^{k_1}.p_2^{k_2}$) e outra seta de $p_1^a.p_2^b$ à $p_1^a.p_2^{b+1}$ (caso este divide $p_1^{k_1}.p_2^{k_2}$).

(11) Prove que a intersecção de duas ordens é uma ordem. A re-

união de duas ordens não é uma ordem, pois se R é uma ordem sobre A, diferente da ordem trivial Δ_A então $\mathsf{R} \cup \mathsf{R}^{-1}$ nunca é ordem, pois existem $a \neq b$ com (a,b) e $(b,a) \in \mathsf{R} \cup \mathsf{R}^{-1}$.
(13) Se R é relação de ordem, seja $(a,b) \in \mathsf{R} \cap \mathsf{R}^{-1}$. Então $(a,b) \in \mathsf{R}$ e $(a,b) \in \mathsf{R}^{-1}$, ou seja, $(a,b) \in \mathsf{R}$ e $(b,a) \in \mathsf{R}$. Como R é de ordem $b = a$. Logo $\mathsf{R} \cap \mathsf{R}^{-1} \subseteq I_E$. Como R e R^{-1} são relações de ordem $I_E \subseteq \mathsf{R} \cap \mathsf{R}^{-1}$. Façamos agora $\mathsf{R} \circ \mathsf{R} = \mathsf{R}$. Seja $(x,z) \in \mathsf{R} \circ R$. Então existe y tal que (x,y) e $(y,z) \in \mathsf{R}$. Como R é transitiva $(x,z) \in \mathsf{R}$. Logo $\mathsf{R} \circ \mathsf{R} \subseteq \mathsf{R}$. Seja $(x,y) \in \mathsf{R}$. Como $(y,y) \in \mathsf{R}$ temos que $(x,y) \in \mathsf{R} \circ \mathsf{R}$ e por isso $\mathsf{R} \subseteq \mathsf{R} \circ \mathsf{R}$. Logo $\mathsf{R} \circ \mathsf{R} = \mathsf{R}$.

Reciprocamente se $\mathsf{R} \cap \mathsf{R}^{-1} = I_E$ e $\mathsf{R} \circ \mathsf{R} = \mathsf{R}$, então $I_E \subseteq \mathsf{R}$. Logo R é reflexiva. Sejam $x, y \in E$ tais que (x,y) e $(y,x) \in \mathsf{R}$. Então $(x,y) \in \mathsf{R}$ e $(x,y) \in \mathsf{R}^{-1}$, ou $(x,y) \in \mathsf{R} \cap \mathsf{R}^{-1} = I_E$. Logo $x = y$ e portanto R é anti-simétrica. Finalmente, sejam $(x,y),\ (y,z) \in \mathsf{R}$. Logo $(x,z) \in \mathsf{R} \circ \mathsf{R} = \mathsf{R}$ e R é, então, transitiva. Portanto R é relação de ordem.
(14) A ordem $\preceq_1$ é total, pois dados $x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n)$ em X^n. Se $x \neq y$ então, existe $i,\ 1 \leq i \leq n$ tal que $x_i \neq y_i$ (em X). Tome i_0 o menor dos índices i tal que $x_i \neq y_i$. Como $\preceq$ é total temos: $x_{i_0} \prec y_{i_0}$ ou $y_{i_0} \prec x_{i_0}$. Daí $x \preceq y$ ou $y \preceq x$.
(15) Denotando por R_i a relação sobre o conjunto $\{a,b,c,d,e\}$ cuja matriz é $M_i,\ i = 1,\ 2,\ 3,\ 4$ somente R_1 e R_3 são relações de ordens.
(16) Para R_1 os pares de elementos $a,\ c$ e $b,\ c$ são incomparáveis; e para R_3 os elementos $b,\ c$ são incomparáveis.

ALGUNS PARADOXOS EM MATEMÁTICA

Já vimos que na lógica clássica só há duas ocorrências como valores lógicos: falso ou verdadeiro. Não há uma terceira ocorrência como valor lógico, como acontece em outras teorias lógicas. Agora vamos apresentar vários paradoxos em matemática, a maioria deles baseados no problema da diagonal de uma teoria.

A diagonalização de uma sentença é uma sentença de caráter mais ou menos universal, que pode ser colocada dentro de algumas teorias. Para defini-la, é preciso um pouco mais de teoria sobre lógica e sugerimos ao leitor que busque em livros sobre o assunto. O problema das sentenças diagonais é que, apesar de ser uma sentença clara e bem colocada dentro da teoria, ela deveria ser uma proposição. Mas não o é, pois é uma sentença que não é verdadeira e nem é falsa, como veremos em vários exemplos a seguir. Por isto se diz que existem teorias (sobre $\mathbb{Q}$, por exemplo) que são incompletas, pois existem proposições na teoria que nem são verdadeiras, nem são falsas. Para dar uma idéia melhor da diagonal, suponhamos um conjunto de proposições, que possui um subconjunto A de proposições, que tem a propriedade de refletir as demais. Assim, cada proposição neste conjunto é simétrica, em relação a A, a uma outra proposição distinta dela, sendo que cada proposição de A tem a propriedade de ser simétrica em relação a si mesma. Em resumo, o subconjunto A é como se fosse um espelho. Cada proposição (objeto) é uma afirmação sobre seu simétrico (imagem) e vice-versa. Portanto, se p é uma proposição de A, então p faz uma afirmação sobre si mesmo.

Os ítens de (A), (B), (D), (E), (H), (I), (J), (M) se referem ao problema da diagonal. Pergunta: Existem outros ítens que se

referem a este problema?

(**A**) Epimenedes de Creta disse: "Todos os Cretenses são mentirosos"; o que, de outra maneira, ele disse: "Eu estou mentindo".

Se a sentença "Eu estou mentindo" for verdadeira, então ele está mentindo ao dizer "Eu estou mentindo". Logo, a sentença é falsa: Contradição. Se a sentença "Eu estou mentindo"é falsa, então ela é verdadeira.

A análise é complicada, porque esta sentença está na diagonal da teoria. Esta sentença é a sentença: "Meu simétrico está mentindo". Ocorre que a pessoa e seu simétrico são os mesmos, pois estão na diagonal.

O próximo paradoxo é uma outra versão e parece ser mais simples de ver.

(B) Em uma folha de papel em branco escreva a sentença p: "A sentença do outro lado é falsa", e, no verso, escreva a sentença q: "A sentença do outro lado é falsa". Verifique que p é verdadeiro se, e somente se, q é falso. Como p e q são iguais, temos uma contradição!

(C) Novamente numa folha de papel em branco escreva a mesma sentença p: "A sentença do outro lado é falsa" e, no verso, escreva a sentença r: "A sentença do verso é verdadeira". Verifique que p e r não podem assumir nenhum valor lógico.

(D) Paradoxo de Berry

Suponha que podemos associar sentenças a cada número natural, compostas de qualquer combinação de letras, símbolos tipográficos e símbolo branco (para separar palavras). É claro que temos apenas um número finito de números naturais enumerados, usando, por exemplo, até 70 símbolos (pois o alfabeto é finito). Listemos estes números.

Agora "o menor número natural não listado usando menos de setenta símbolos" denota um número natural bem definido. Mas a sentença tem 69 símbolos e, portanto, o menor número natural não listado usando até 70 símbolos é enumerado usando 69 símbolos.

(E) Paradoxo de Greeling

Uma palavra é dita ser autológica se seu significado se aplica a ela mesma e dita ser heterológica caso contrário. Por exemplo:

Palavra é uma palavra autológica; *polissílaba, english, português* são palavras autológicas. As palavras *monossílaba, inglês, green* são palavras heterológicas. Pergunta: A palavra "heterológica" é heterológica?

Se ela for, então seu significado não se aplica a ela mesma, e então ela é autológica. Se, caso contrário, ela é autológica, então ela deve ser heterológica.

(F) Paradoxo da Prova Inesperada.

Um professor diz aos alunos que na próxima semana vai haver uma prova surpresa, em algum dia da semana. Os alunos, sabendo que o professor nunca mente, começam a raciocinar: A prova não pode ser realizada na sexta-feira (último dia da semana), senão não será prova surpresa.

Então para ser prova surpresa deve ser realizada até quinta-feira: Riscam sexta-feira. Ficando quinta-feira para o último dia para a prova surpresa, esta também não pode ser realizada quinta-feira porque, sendo o último dia, não seria surpresa, também riscam quinta-feira. Então fica quarta-feira para o último da prova surpresa. Mas, do mesmo modo, eles concluem que não pode ser quarta-feira, nem terça-feira e, portanto, segunda-feira também não pode. Levaram este argumento para o professor e, como este não mente, teve que cancelar a prova surpresa.

(G) Paradoxo de Hempel.

O filósofo Carl G. Hempel propôs em 1937 o seguinte paradoxo, conhecido como *paradoxo da confirmação.*

Supõe que um ornitologista deseja investigar a seguinte hipótese: "Todos os corvos são pretos". A confirmação para esta hipótese consiste em examinar a maior quantidade possível de corvos e, se ele achar pelo menos um corvo que não é preto, a hipótese é falsa. Por outro lado, quanto mais corvos pretos ele achar, torna mais provável a hipótese.

Consideremos as propriedades $C(x)$: "x é corvo" e $P(x)$: "x é preto". Nossa hipótese "Para todo x, se x é corvo, então x é preto"se escreve, em símbolos, do seguinte modo:

$$\forall X,\ C(x) \to P(x).$$

Por contra-recíproca, a hipótese é logicamente equivalente a: $\forall x, \sim P(x) \to \sim C(x)$. Como $\sim C(x) \to \sim C(x)$ e estas duas condi-

cionais implicam em $\sim C(x)$, temos nossa hipótese re-escrita como: $\forall x,\ [\sim C(x) \vee \sim P(x)] \rightarrow \sim C(x)$. Pelas leis de DeMorgan, temos a nossa hipótese re-escrita como:

$$\forall x,\ \sim \big(C(x) \wedge P(x)\big) \rightarrow \sim C(x),$$

ou seja, para qualquer x, se x não é corvo preto, então x não é corvo. Logo, um corvo branco serve para confirmar que "todos os corvos são pretos".

(H) Paradoxo de Richard

Julio Richard propôs em 1905 um paradoxo tratando dada definição real. Diz que um número real é finitamente definível se ele pode ser definido por uma sentença em linguagem natural (isto é: uma combinação finita de letras do alfabeto mais um número finito de sinais tipográficos). Se incluímos o branco para separar palavras, podemos enumerar essas combinações finitas de um conjunto finito de símbolos usando a ordem lexicográfica (ordem do dicionário) do seguinte modo: Duas seqüências (frases) de comprimento diferente, o comprimento decide a ordem, sendo que a menor vem antes, e duas seqüências de mesmo comprimento, a ordem lexicográfica estendida aos sinais tipográficos mais o símbolo branco decide a ordem.

Agora, considere a sentença: "Seja d o número real, cuja parte inteira é 'zero', e n-ésimo dígito decimal é 1, se o n-ésimo dígito decimal do n-ésimo número na tabela é zero, e zero em outro caso". Então o número d é finitamente definível, mas ele é diferente de todos os números da tabela, que é uma contradição, pois a tabela lista todos os números finitamente definível.

(I) Paradoxo do Barbeiro

Numa cidade havia só um barbeiro e o barbeiro "só fazia a barba de quem não se barbeava". Pergunta: Quem fazia a barba do barbeiro?

Note que o barbeiro não pode se barbear, pois ele só faz a barba de quem não se barbeia. Mas, se ele não se barbear, o barbeiro faz sua barba. Ocorre que o barbeiro é ele mesmo. Então, de qualquer forma, temos uma contradição.

(J) Uma mãe, em visita com seu filho ao jardim zoológico, por descuido deixa um crocodilo pegar seu filho. Diante da aflição e da imploração da mãe, o crocodilo resolve dar uma chance a ela e põe

a seguinte questão: "Ele devolverá o filho se ela adivinhar se ele vai comer ou vai devolver o filho para ela". Como ela conhecia lógica, vendo a pergunta mal posta, deu uma resposta de modo a, pelo menos, salvar o filho, qualquer que fosse a intenção do crocodilo. Qual foi a resposta dada pela mãe?

(K) Os habitantes de um antigo reino, quando morriam, subiam até um ponto no caminho para a eternidade, onde havia uma bifurcação e o caminho se dividia em dois. Um era o caminho do céu, o outro do inferno.

Nesta bifurcação, ora havia um anjo que era verdadeiro, belo, etc: era a verdade; ora estava ali a mentira e, por isso, era mentiroso, cheio de contradições como, por exemplo, também era belo e, por isso, ninguém sabia qual era o anjo verdadeiro e qual era o anjo mentiroso. Chegando aí, as pessoas tinham direito de fazer só uma pergunta para saber qual era o caminho do céu e seguir viagem para lá ou, por azar, ir para o inferno.

Que pergunta pode ser feita ao anjo de modo que te diz com certeza o caminho do céu, independente de ser o anjo verdadeiro ou mentiroso?

(L) O queijo suíço tem muitos buracos. Quanto mais queijo, mais buraco. Logo, quanto mais queijo, menos queijo.

(M) Um velho ditado afirma: "Toda idéia fixa está errada. Inclusive esta".

(N) Você pode provar que seu colega não está aqui, do seguinte modo: Escolha duas cidades diferentes desta onde vocês estão (digamos Paris e Londres, se for o caso). Pergunte a ele: Você está em Londres? Se ele não for sincero e dizer que está, você responde que então ele não está aqui. Se ele for sincero responderá que não. Dê mais uma "chance"perguntando se ele está em Paris. Novamente se ele disser que está, então ele não está aqui. Se ele disser que não está, você diz: Bem, se você não está em Londres e não está em Paris, então você está em outro lugar, concorda? Ele deve responder que sim. Ai você arremata dizendo: então, se você está em outro lugar, você não está aqui!

BIBLIOGRAFIA

[1] Carnielli W. e Epstein, R. L. *Computabilidade Funções Computáveis, Lógica e os Fundamentos da MATEMÁTICA*. Editora UNESP, 2006.
[2]. Cutland, N.: *Computability, An introduction to recursive function theory* - Cambridge University Press, 1980.
[3]. Domingues, Hygino H. e Iezzi, G. *Álgebra Moderna*, Atual Editora, 4ª Edição, 2003.
[4]. Dornhoff, L.L. & Hohn, F.E. *Applied Modern Algebra*, Macmillan Publishing Co., Inc. N. York, 1978.
[5]. Lipschutz, S. *Teoria dos Conjuntos*, Coleção Schaum - ao Livro Técnico S. A., Rio de Janeiro, 1968.
[6]. Péter, R.,: *Recursive Functions*, Academic Press, 1967.
[7]. Whitesitt, J.E. *Algebra Booleana y sus aplicaciones*, Compánia Editorial Continental, S.A., México - España - Argentina - Chile, 1971. Tradução de Laura Bustamante Llaca.

SOBRE OS AUTORES

A Professora Aparecida é licenciada em Ciências em 1977 e em matemática em 1978 pelo IBILCE/UNESP S.J.Rio Preto-SP. É mestre e doutora em matemática, formada pelo IMECC/UNICAMP. Foi bolsista de Iniciação Científica pelo CNPq na graduação e durante o mestrado. Orientou alunos na Pós-Graduação do Departamento e vários alunos de graduação. Sua área de pesquisa é Álgebra Comutativa e Jogos no Ensino da Matemática. Atualmente é coordenadora regional da OBMEP.

O Professor Clotilzio é licenciado em Ciências em 1977 e em matemática em 1978 pelo IBILCE/UNESP S.J.Rio Preto-SP. É mestre (1982) e doutor (1994) em matemática, formado pelo IMECC/UNICAMP. Fez Pós-Doutorado no IMECC/UNICAMP no primeiro semestre de 2009. Foi bolsista de Iniciação Científica pela Fapesp na graduação, bolsista do CNPq durante o mestrado e, bolsista do PICD, durante parte do doutorado. Orientou alunos nos cursos de graduação e de Pós-Graduação do Departamento de matemática IBILCE/UNESP, no qual é docente deste de 1982. Tem publicações na área de teoria algébrica de formas quadráticas sobre corpos e sobre álgebras de quatérnios, sua área de pesquisa. Tem como hobby pesquisas sobre o passado, presente e destino futuro da raça Humana e ciências Metatrônicas, baseadas nos Livros do Conhecimento: As chaves de Enoch e Pistis Sophia conforme publicações da ACADEMIA PARA CIÊNCIA FUTURA, do qual é membro.

ISBN 978-85-98605-88-3