Para meus pais e meus filhos

Agradecimentos

Agradeço a voce Marcia a oportunidade de conhecer a área onde faço pesquisa. Voce é uma profissional séria e competente. Foi bom trabalharmos juntas esses anos todos.

Dalcidio, voce confiou no meu trabalho. Foi uma das melhores experiências na minha vida trabalhar com o grupo de matemática computacional da UFRGS. Gostaria de aprender com voce como desenvolver um grupo produtivo.

Graças ao meu orientador nesse tempo do meu doutourado fui capaz de num mesmo dia experimentar um amplo espectro de sentimentos que variaram de uma grande admiração ao ódio mortal! Mas reconheço hoje que isso fez parte do processo. Graças a ele continuei aprendendo mesmo depois da tese pronta. Realmente as emoções entre orientador e orientando ficam por vezes bastante difíceis, mas isso também faz parte do processo. Sei agora que Rafael confia no meu trabalho e tenho seu respeito como profissional. Rafael, peço desculpas por alguma coisa, qualquer coisa, que tenha feito de errado. Valeu!

Para voces meus amigos daqui, da UFBA, da UFC, da UFPR, da UFRGS, do Centro de Informática e do Depto. de Matemática da Universidade do Minho em Portugal quaisquer palavras são supérfluas. Meu trabalho leva uma parcela do nosso convívio. Voces sabem dos meus sentimentos por voces.

O CNPq me financiou durante uma parte do meu doutorado. Nesse período, nenhuma consulta minha ficou sem resposta, nenhum atrazo na bolsa e principalmente, na passagem de volta. Meus sinceros agradecimentos.

O Depto. de Informática/UFPE é quase perfeito. O quase fica por conta do acervo com respeito a livros e periódicos. Só sabe o que é ser um pós-graduando no DI, quem viveu essa incrível experiência. Desejo sinceramente que o espírito que norteou as lideranças inicais do DI, se faça presente sempre.

Por alguma razão nasci nesse país tão cheio de contrastes. Mais ainda, nasci no Nordeste! Certamente esse fato contribuiu para eu fazer minha tese. Porque ser Nordestino é ser um forte.

Resumo

A teoria da probabilidade é um ramo da matemática relacionado com fenômenos aleatórios. Tal como é conhecida atualmente foi axiomatizada por Kolmogorov após os trabalhos de Lebesgue sobre teoria da medida e integração. A formalização do conceito de probabilidade é suportado fundamentalmente pelas noções de conjuntos, relações e funções e o sistema de números reais. O cálculo das probabilidades fundamenta-se nas analogias entre medida de um conjunto e integral de uma função com probabilidade de um evento e esperança matemática de uma variável aleatória, respectivamente.

Computar probabilidades em situações práticas envolve números e, conseqüentemente, problemas numéricos. Problemas numéricos na computação científica originam-se primordialmente da impossibilidade de se operar com os números reais diretamente, pois tem-se que representar uma grandeza contínua (a reta real) de forma discreta (palavras de máquina). O sistema de ponto flutuante é uma aproximação prática dos números reais. Infelizmente, como um sistema algébrico, suas características são extremamente pobres quando comparadas com o dos números reais.

Esta tese propõe uma metodologia para estender a probabilidade real de tal forma a possibilitar seu cálculo automático através do uso de intervalos, limitando os erros computacionais e mantendo uma semântica consistente entre a probabilidade e os resultados intervalares obtidos. A probabilidade usual, clássica, é referida como a probabilidade real e a aqui proposta como a probabilidade intervalar.

O primeiro passo para alcançar o objetivo de obter a probabilidade intervalar é usar conceitos de extensões intervalares de funções reais, propostos por Moore e Acioly. A partir da definição do que seja um espaço de probabilidade intervalar, prova-se que a extensão proposta tem propriedades similares às da probabilidade real. Nesse sentido, a probabilidade intervalar estende a probabilidade real sendo esta uma restrição da primeira.

A especificação do tipo intervalo usando a linguagem algébrica OBJ3 foi feita e utilizada para demonstrar teoremas fundamentais da matemática intervalar e também da probabilidade intervalar. Tal especificação pode servir de base para a prova de programas em qualquer sistema lógico ou provador de teoremas que use o tipo intervalo assim como viabiliza a implementação do tipo intervalo, como primitivo, em uma linguagem funcional. Essa implementação abre perspectivas na computação científica para a definição de programas que sejam provados corretos e que possuam aritmética confiável.

Abstract

Historically, the calculus of probabilities is linked to games, where the probability of a given event is defined as the ratio between the number of favourable cases (number of occurences of the event) and the total number of possible cases. In this century, probability and statistics have gained a central role in all branches of science. In physics, Heisenberg's principle shows that in the sub-atomic world it is impossible to determine the position of any given particle at a certain time, but that there is a *probability* of finding it at a position at a given time. All quantum physics, the major responsible for the scientific development of the 20th century, is based on the notion of probability.

Probability theory as we know today, was axiomatized by Kolmogorov after the works of Lebesgue. The formal background of probability rests on set theory and makes use of relations and functions of the real numbers set.

Computing probabilities in practice envolves floating-point numbers and, in consequence, numerical problems. The discrete representation of the real numbers (a continous set) in a finite number of machine words gives birth most of the problems in scientific computation. The floating-point numbers as an algebraic system is extremely poor, if compared to the real numbers. Thus, calculating probabilities suffers from the same problems one faces in scientific computing.

In this thesis, we generalize the concept of probability to *interval probability*. This generalisation is conservative in respect to the axioms of probabilities on reals, as it keeps the semantics of "classical" probabilities. At the same time the axioms of interval theory are also observed.

Conteúdo

Lista de Símbolos

Ω	espaço de resultados elementares, espaço amostral
ω	evento simples, resultado elementar
A, B	eventos aleatórios, eventos
A^c	evento complementar de A
$P(A)$	probabilidade de A
$P_{\mathbb{IR}}(A)$	probabilidade intervalar de A
X	variável aleatória
$\sim$	se distribui, a variável aleatória tem distribuição
$\mathcal{A}$	σ-álgebra
$\mathcal{B}$	σ-álgebra de Borel
$\square$	arredondamento
$\triangledown$	arredondamento direcionado para baixo
$\triangle$	arredondamento direcionado para cima
sup	supremo
inf	ínfimo
$\mathbb{N}$	conjunto dos números naturais
$\mathbb{R}$	conjunto dos números reais
$\mathbb{C}$	conjunto dos números complexos
a, b, x, y	números reais
$\mathbb{O}$,	elemento neutro aditivo
$\mathbb{1}$,	elemento neutro multiplicativo
π	número pi
$\mathbb{IR}$	conjunto dos intervalos reais, conjunto dos intervalos
$X = [x_1, x_2]$, $A = [a_1, a_2]$	intervalos
$\mathrm{IV}\mathbb{R}$	espaço dos intervalos cujas componentes são vetores de números reais
$\mathrm{IM}\mathbb{R}$	espaço dos intervalos cujos componentes são matrizes de números reais
D	números de ponto flutuante de precisão dupla
S	números de ponto flutuante de precisão simples
$\mathrm{S}(b, l, e_{min}, e_{max})$	sistema de ponto flutuante
IS	intervalos cujos limites são números de ponto flutuante de precisão simples
VD	vetores cujos elementos são números de pontos flutuante de precisão dupla
VS	vetores cujos elementos são números de pontos flutuante de precisão simples
MD	matrizes cujos elementos são números de pontos flutuante de precisão dupla
MS	matrizes cujos elementos são números de ponto flutuante de precisão simples

$\approx$	aproximadamente igual
$\neq$	diferente
$\top$	topo ou maior elemento
$\perp$	bottom ou menor elemento
$\circ$	operação de composição
$*$	operação binária
$\boxast$	operação binária no *screen*
I_d	função identidade
$\emptyset$	conjunto vazio
∞	infinito
$\Leftrightarrow$	se e somente se
$\Rightarrow$	implica
$\subseteq$	inclusão
$\subset$	inclusão estrita
$\cap$	interseção
$\cup$	união
$\in$	pertence
$\notin$	não pertence
$<$	menor
$>$	maior
$\leq$	menor ou igual
$\geq$	maior ou igual
$\sqsubseteq$	ordem de informação
$\ll$	ordem forte de aproximação
$\forall$	para todo ou qualquer que seja
$\blacksquare$	término de demonstração

Lista de Definições

Lista de Figuras

Capítulo 1

Introdução

Historicamente, o cálculo de probabilidade começou no século dezessete, na França, com a correspondência mantida entre Pascal e Fermat sobre dois problemas de jogos de azar propostos pelo nobre francês Chevalier de Méré [Sne89, Gne75, Lo5, Lar82].

No século XX, a probabilidade e a estatística ganharam um papel fundamental em todos os ramos da ciência. Na física, o princípio da incerteza de Heisenberg mostra que no mundo sub-atômico é impossível determinar a posição de uma partícula em um momento específico, mas que existe uma *probabilidade* de se encontrar uma partícula em determinado local em dado instante. Toda a física quântica, maior responsável pelo desenvolvimento científico deste século, é baseada em probabilidade. De forma semelhante, a química, a biologia e outros ramos do conhecimento humano.

A teoria da probabilidade [Kol50, Fel68, Bre69, Bur72, Chu74, Bil79] é um ramo da matemática relacionado com fenômenos aleatórios; esses têm a propriedade de, se repetidos infinitas vezes sob um conjunto específico de condições, conduzirem ao mesmo resultado. Tal como é conhecida atualmente foi axiomatizada por Kolmogorov [Kol50] após os trabalhos de Lebesgue [Rud76] sobre teoria da medida e integração. A formalização do conceito de probabilidade tem por base as noções de conjuntos, relações e funções e o sistema de números reais. O cálculo das probabilidades fundamenta-se nas analogias entre medida de um conjunto e integral de uma função com probabilidade de um evento e esperança matemática de uma variável aleatória, respectivamente. A formalização do conceito de probabilidade começa com um espaço abstrato e desenvolve-se a partir desse. O conceito de variável aleatória porém, transforma-se rapidamente em um tema central da teoria. A razão para isto vem do fato que na maioria das situações experimentais o interesse é atribuir um número real ao resultado do experimento.

Computar probabilidades em situações práticas envolve números e, conseqüentemente, problemas numéricos. Problemas numéricos na computação científica originam-se primordialmente da impossibilidade de se operar com os números reais diretamente, pois tem-se que representar uma grandeza contínua (a reta real) de forma discreta (palavras de máquina). O sistema de ponto flutuante [Cod88, Gol91, Knu81, Ste74, Ste81] é uma aproximação prática dos números reais. Infelizmente, como um sistema algébrico, suas características são extremamente pobres quando comparadas com o dos números reais.

Uma alternativa bastante difundida atualmente para solucionar problemas numéricos, não só de imprecisão do dado em si (altura, peso, tempo, etc) como erros de arredondamento, truncamento e a propagação do erro numa seqüência de operações aritméticas é a matemática intervalar [Moo66, Moo79]. A teoria da probabilidade e a análise intervalar são enfoques clássicos para a representação de “imperfeição” na informação. A análise intervalar relaciona-se com inexatidão numérica, enquanto a teoria da probabilidade com problemas aleatórios.

A matemática intervalar [Sun58, Moo66, Moo79] fornece uma ferramenta para estimar e controlar erros numéricos automaticamente. Ao invés de aproximar um número real x por um número de máquina, x é aproximado por um intervalo X, tendo números de máquina como limites inferior e superior. O intervalo X contém o valor x. A amplitude do intervalo pode ser usada como uma medida da qualidade da aproximação. Os cálculos entretanto tem que ser efetuados usando intervalos ao invés de números reais e as operações aritméticas tem de ser substituídas pelas operações sobre intervalos.

Por exemplo, considere a representação de 1/3 com quatro dígitos significativos. O arredondamento para o mais próximo resulta em 0.3333, o qual pode ser substituído pelo intervalo [0.3333,0.3334], usando os arredondamentos direcionados [KM81, Kul83, KM86]. Aparentemente esse valor intervalar é mais impreciso que o valor verdadeiro, porém é mais confiável desde que revela o nível de incerteza presente; ele também mostra que 0.3333 é uma subestimação do valor exato. A representação intervalar provê informação acerca da exatidão do valor computado o que um único número não o pode fazer.

A aritmética intervalar com os arredondamentos direcionados fornece limites rigorosos para o contradomínio de operações e funções. Há uma diferença qualitativa em computação científica desde que os resultados são intervalos nos quais os resultados exatos estão obrigatoriamente incluídos.

A análise intervalar pode ser usada para produzir computação numérica autovalidável, também chamada análise automática do erro. Isto é feito quando se computa um intervalo que tem a garantia de conter o valor teoricamente correto mas desconhecido. Dificuldades numéricas que aparecem durante a avaliação de expressões aritméticas tais como cancelamento e arredondamentos podem, em alguns casos, levar a intervalos com grande amplitude. Nestes casos, embora se tenha a garantia que o intervalo resultante contém o verdadeiro porém desconhecido valor, sua utilidade prática pode não ser tão valiosa. Bons algoritmos intervalares produzem intervalos com amplitude muito pequena.

Como dito anteriormente, o cálculo da probabilidade é feito sobre os reais, portanto o cálculo automático da probabilidade sofre dos problemas de representação já mencionados. O uso da aritmética intervalar para representar probabilidades além de exigir cuidados computacionais para manter a amplitude dos intervalos a menor possível, impõe consistência com os axiomas da teoria da probabilidade.

Esta tese propõe uma metodologia para estender a probabilidade real de tal forma a possibilitar seu cálculo automático através do uso de intervalos, limitando os erros computacionais e mantendo uma semântica consistente entre a probabilidade e os resultados intervalares obtidos. A probabilidade usual, clássica, é referida como a probabilidade real e a aqui proposta como a probabilidade intervalar.

O primeiro passo para alcançar o objetivo de obter uma probabilidade intervalar consistente é usar conceitos de extensões intervalares de funções reais, propostos por Moore e Acioly [Moo66, Moo79, Aci91, Aci96]. A partir da definição do que seja um espaço de probabilidade intervalar, prova-se que a extensão proposta tem propriedades similares às da probabilidade real. Nesse sentido, a probabilidade intervalar estende a probabilidade real sendo esta uma restrição da primeira.

Para a obtenção de um método matematicamente correto e que resolva problemas numéricos através de técnicas intervalares, várias aritméticas intervalares foram estudadas. Para o trabalho aqui desenvolvido, a aritmética escolhida é a definida por Moore [Moo66, Moo79], uma vez que a aritmética de exatidão máxima [KM81, Kul83, KM86] está nela baseada.

A especificação do tipo intervalo usando a linguagem algébrica OBJ3 [GWM+93] foi feita para provar teoremas da matemática intervalar usados em provas da probabilidade intervalar. Tal especificação e técnicas de prova podem servir de base para a prova de programas em qualquer sistema lógico ou provador de teoremas que use o tipo intervalo assim como viabiliza a implementação do tipo intervalo, como primitivo, em uma linguagem funcional. Essa implementação abre perspectivas na computação científica para a definição de programas que sejam provados corretos e que possuam aritmética confiável.

Esta tese está organizada em cinco capítulos, sumarizados a seguir.

No capítulo 2 define-se o espaço dos intervalos, aritmética e topologia. A aritmética intervalar usada nesta tese é a proposta em [Moo66, Moo79], porém existem outras que, de certa forma, são extensões da inicialmente definida por Moore [Moo66, Moo79]. Essas extensões encontram-se sucintamente descritas. A razão da escolha da aritmética intervalar de Moore neste trabalho está nele devidamente fundamentada.

O capítulo 3 descreve a aritmética de exatidão máxima [KM81, Kul83, KM86] para todos os espaços da computação numérica. Este capítulo é uma das contribuições desta tese a área pois apresenta uma compilação de toda a produção científica a ela relacionada, com uniformidade de tratamento e notacional, sendo básico para esta tese porque cálculos com a probabilidade intervalar são efetuados através dos conceitos nele definidos.

O capítulo 4 é outra contribuição original desta tese pois relaciona pela primeira vez na literatura questões referentes à implementação do tipo intervalo em linguagens funcionais. Ao final do capítulo é apresentada a especificação do tipo intervalo em uma linguagem algébrica e vários teoremas da matemática intervalar são provados a partir dessa especificação. A idéia relacionada com essa especificação, é usá-la para provar automaticamente teoremas da matemática intervalar, mais especificamente, da probabilidade intervalar definida no capítulo seguinte.

O capítulo 5 é o central desta tese. Nele associam-se a probabilidade e intervalos de forma inédita. Mostra-se como a probabilidade intervalar pode ser vista como uma extensão da probabilidade real e esta como uma restrição da probabilidade intervalar. O conceito de extensões intervalares de funções reais é amplamente utilizado. As variáveis aleatórias de Bernoulli, Binomial e Poisson [Fel68, Jam81, Bre69] são redefinidas à luz do novo enfoque. O último exemplo do capítulo mostra como a probabilidade intervalar é usada para validar a probabilidade real.

No capítulo 6 tem-se a análise dos trabalhos correlatos [GV94, VBS90, Vos88, Vos92, WK94, Kre95], o balanço das contribuições desta tese, bem como propostas de trabalhos futuros.

Capítulo 2

Intervalos como Espaço Algébrico e Topológico

Neste capítulo é definido o espaço dos intervalos assim como as suas operações. Em seguida, à aritmética intervalar de Moore [Moo66, Moo79], outras são descritas, que são extensões da proposta por Moore. Na verdade, o primeiro trabalho conhecido na literatura sobre intervalos, incluindo aritmética, entre outros tópicos, é devido a Sunaga [Sun58]. Aparentemente Sunaga e Moore desenvolveram trabalho similar quase na mesma época, mas em lugares distintos. Porém, na literatura, sempre que se fala em aritmética intervalar, as referências são para Moore. Após visto o intervalo algebricamente, é apresentada sua topologia.

A aritmética intervalar é uma ferramenta matemática para a solução de problemas relacionados com erros numéricos na computação científica. Por aritmética intervalar entende-se um sistema algébrico consistindo do conjunto formado de todos os intervalos fechados da reta real, com algumas operações definidas sobre ele. Ao invés de algoritmos numéricos usuais para resolver certos problemas matemáticos, usam-se algoritmos intervalares desenvolvidos para produzir intervalos como resultados, em lugar de números reais, os quais: (i) devem ser confiáveis no sentido que incluem a solução exata do problema original; (ii) devem ter como resposta um intervalo com amplitude tão pequena quanto possível.

Antes de Moore, os espaços da computação numérica basicamente eram os reais, complexos, vetores de reais, vetores de complexos, matrizes de reais, etc. Depois das idéias de Moore problemas começaram a ser resolvidos, ou propostos, de forma intervalar, sendo assim acrescidos ao conjunto dos espaços da computação numérica o espaço dos intervalos de reais, intervalos de complexos, etc. Há vários tipos de erros em computações matemáticas: incerteza nos dados, erros de arredondamento, erros de aproximações, etc. A análise intervalar fornece cotas inferiores e superiores (um intervalo) que contém estes erros em quantidades computadas. A matemática intervalar praticamente começou com a publicação do livro de R. E. Moore, Interval Analysis, em 1966 [Moo66]. O trabalho de Moore transformou uma idéia simples numa ferramenta viável para análise de erro. O uso da análise intervalar limita o efeito do erro, seja qual for a sua fonte, incluindo erros de aproximação e de arredondamentos [Han92].

Neumaier[Neu87] cita vários exemplos evidenciando a importância do intervalo. Hansen [Han92] afirma que:

> The introduction of interval analysis is the single most important advance in numerical analysis other than the advent of the modern computer and high-level languages. The success of its original purpose of error analysis is enough to make this true. However, interval analysis has had other successes. The most important one was making it possible to solve a previously insoluble problem—the general global optimization problem. Less important, but significant, is improving algorithms by making them more reliable and robust. Every course in numerical analysis should contain a discussion of interval analysis and its use in bounding errors in computed quantities.

Seguem-se os conceitos algébricos e topológicos usados neste trabalho.

2.1 Intervalo: Definição, Igualdade e Relações de Ordem

O conjunto de todos os $x \in \mathbb{R}$ satisfazendo a condição $a_1 \leq x \leq a_2$ é chamado um *intervalo*, [Sun58, Moo66, Moo79] e é denotado por

$$[a_1, a_2] = \{x \in \mathbb{R} \mid a_1 \leq x \leq a_2\}$$

O espaço dos intervalos, $\mathbb{IR}$, é então,

$$\mathbb{IR} = \{[a_1, a_2] \mid a_1 \leq a_2,\ a_1, a_2 \in \mathbb{R}\}$$

Um elemento de $\mathbb{IR}$ é chamado um *intervalo*. De acordo com Sunaga [Sun58], o pioneiro na área da análise intervalar,

> the interval concept is on the bordeline linking pure mathematics with reality and pure analysis with applied analysis.

Sejam $X = [x_1, x_2]$, $Y = [y_1, y_2]$, $Z = [z_1, z_2]$ e $W = [w_1, w_2]$ intervalos.

2.1.1 Igualdade

Os intervalos X e Y são iguais se e só se $x_1 = y_1$ e $x_2 = y_2$.

2.1.2 Relações de Ordem

Há na literatura [Sun58, Moo66, Moo79, KM81, Aci91] vários tipos de relações de ordem definidas sobre $\mathbb{IR}$. Entre essas, tem-se uma extensão da relação de ordem $<$ definida sobre o conjunto dos números reais. Esta extensão foi definida por Moore [Moo66, Moo79] e é como segue:

$$X < Y \Leftrightarrow x_2 < y_1$$

Desde que intervalos de reais são também conjuntos, outra relação de ordem que pode ser definida [Sun58, Moo66, Moo79] é $\subseteq$ dada a seguir:

$$X \subseteq Y \Leftrightarrow y_1 \leq x_1 \text{ e } x_2 \leq y_2$$

A relação de ordem definida por Kulisch e Miranker [KM81] é a ordem $\leq$, dada por

$$X \leq Y \Leftrightarrow x_1 \leq y_1 \text{ e } x_2 \leq y_2$$

Observe-se que $<$ é somente transitiva [Moo66, Moo79] e que $\subseteq$ e $\leq$ são ambas transitivas, reflexivas e anti-simétricas [Sun58, Moo66, Moo79].

Os símbolos $\langle \mathrm{I\!I\!R}, < \rangle$, $\langle \mathrm{I\!I\!R}, \subseteq \rangle$ e $\langle \mathrm{I\!I\!R}, \leq \rangle$ indicam o espaço dos intervalos com as relações de ordem $<$, $\subseteq$ e $\leq$, respectivamente. Desde que $\subseteq$ e $\leq$ são relações de ordem parcial [DP90], $\langle \mathrm{I\!I\!R}, \subseteq \rangle$ e $\langle \mathrm{I\!I\!R}, \leq \rangle$ são chamados conjuntos parcialmente ordenados [DP90].

A declaração de que o valor computado de π=3.14 está correto até a segunda casa decimal pode ser reescrita dizendo-se que π pertence a um intervalo fechado de $\mathbb{R}$. Considerando-se a coleção de todos os intervalos fechados da forma $[a, b] \subseteq \mathbb{R}$, define-se uma ordem nesta coleção da seguinte forma: sejam $X = [a, b]$ e $Y = [c, d]$; $X \leq Y$ se e só se $Y \subseteq X$. Então, se $\pi \in X$, $\pi \in Y$ e $X \leq Y$ significa que, para π, Y contém pelo menos tanta informação quanto X. Esta ordem é denominada ordem de informação [DP90]. Uma ordem similar a esta é utilizada por Acioly [Aci91]. Dada a ordem parcial completa $\langle D, \sqsubseteq, \ll, \perp \rangle$, onde $\ll$ é uma ordem forte e $\perp$ é o primeiro elemento de D, para quaisquer $x, y \in D$ a relação $x \sqsubseteq y$ é uma relação de informação, isto é, x e y são informações sobre alguma entidade, sendo que y dá no mínimo tanta informação quanto x.

2.2 Estrutura Algébrica

As operações aritméticas no espaço dos intervalos são [Sun58, Moo66, Moo79]:

$X + Y = [x_1 + y_1, x_2 + y_2]$
$X - Y = [x_1 - y_2, x_2 - y_1]$
$X \cdot Y = [\min\{x_1y_1, x_1y_2, x_2y_1, x_2y_2\}, \max\{x_1y_1, x_1y_2, x_2y_1, x_2y_2\}]$
$X/Y = X \cdot 1/Y = [x_1, x_2] \cdot [1/y_2, 1/y_1],\ 0 \notin Y$

As referências [Sun58, Moo66, Moo79, AH83] mostram as seguintes propriedades algébricas das operações aritméticas intervalares definidas anteriormente:

(a) $X + Y = Y + X$
(b) $X + (Y + Z) = (X + Y) + Z$
(c) $0 \in X - X$
(d) $X \cdot Y = Y \cdot X$
(e) $X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$
(f) $1 \in X/X,\ 0 \notin X$
(g) $X \cdot (Y + Z) \subseteq X \cdot Y + X \cdot Z$ (subdistributividade)
(h) Se $X \subseteq Y$ e $Z \subseteq W$ então $X * Z \subseteq Y * W$, $* \in \{+, -, \cdot, /\}$ (inclusão monotonicidade).

A estrutura algébrica $\langle \mathrm{I\!I\!R}, +, \cdot \rangle$ não é um corpo. Diferente de um corpo que tem inversos aditivo e multiplicativo, $\mathrm{I\!I\!R}$ tem elementos *negativo* e *recíproco*, respectivamente:

$$-X = -[x_1, x_2] = [-x_2, -x_1] = \{-x \mid x \in X\}$$

$$1/X = [1/x_2, 1/x_1] = \{1/x \mid x \in X,\ 0 \notin X\}$$

Há algumas conseqüências imediatas da definição das operações aritméticas sobre $\mathbb{IR}$.

Lema 2.1 Dados X e Y intervalos em $\mathbb{IR}$, $X = Y \Leftrightarrow -X = -Y$.

Demonstração. $-X = -Y \Leftrightarrow [-x_2, -x_1] = [-y_2, -y_1] \Leftrightarrow -x_2 = -y_2$ and $-x_1 = -y_1 \Leftrightarrow x_2 = y_2$ e $x_1 = y_1 \Leftrightarrow [x_1, x_2] = [y_1, y_2] \Leftrightarrow X = Y$. ■

O lema 2.2, a seguir, é um caso particular da propriedade da inclusão monotônica.

Lema 2.2 Dados $X, Y, Z, W \in \mathbb{IR}$, se $X = Y$ e $Z = W$ então $X + Z = Y + W$.

Prova. Sejam X, Y, Z e W intervalos de $\mathbb{IR}$. Por hipótese, $x_1 = y_1$, $x_2 = y_2$, $z_1 = w_1$, $z_2 = w_2$. Portanto $x_1 + z_1 = y_1 + w_1$ and $x_2 + z_2 = y_2 + w_2$. Então $X + Z = Y + W$ como requerido. ■

Lema 2.3 Dados os intervalos X, Y, Z e

(a) $X = Y - Z$

(b) $X = Y + (-Z)$

(c) $x_1 + x_2 = y_1 + y_2 - z_1 - z_2$

as seguintes implicações são verdadeiras: **(a)** $\Rightarrow$ **(b)** e **(b)** $\Rightarrow$ **(c)**.

Demonstração.

(i) **(a)** $\Rightarrow$ **(b)**: $X = Y - Z = [y_1, y_2] - [z_1, z_2] = [y_1 - z_2, y_2 - z_1] = [y_1, y_2] + [-z_2, -z_1] = Y + (-Z)$.

(ii) **(b)** $\Rightarrow$ **(c)**: $X = Y + (-Z) \Rightarrow [x_1, x_2] = [y_1, y_2] + [-z_2, -z_1] = [y_1 - z_2, y_2 - z_1] \Leftrightarrow x_1 = y_1 - z_2$ e $x_2 = y_2 - z_1$. Mas isto implica que $x_1 + x_2 = y_1 + y_2 - z_1 - z_2$. ■

Nota-se que há uma sobrecarga no operador (*operator overloading*) com respeito aos símbolos que representam as operações aritméticas. Por exemplo, o símbolo $+$ entre os intervalos X e Y tem um significado diferente (semântica) que o mesmo símbolo entre os números reais x e y,

$+_{\mathbb{R}} : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ é tal que $+_{\mathbb{R}}(x, y) = x +_{\mathbb{R}} y$
$+_{\mathbb{IR}} : \mathbb{IR} \times \mathbb{IR} \to \mathbb{IR}$ é tal que $+_{\mathbb{IR}}([x_1, x_2], [y_1, y_2]) = [x_1 +_{\mathbb{R}} y_1, x_2 +_{\mathbb{R}} y_2]$

Assumindo-se a sobrecarga nos operadores os índices $\mathbb{R}$ e $\mathbb{IR}$ serão usados explicitamente apenas se houver dúvidas sobre qual espaço o operador aritmético está definido.

Além da aritmética intervalar proposta por Moore e Sunaga [Sun58, Moo66, Moo79] existem outras. Essas são citadas a seguir. Enfatiza-se que a aritmética intervalar de exatidão máxima [KM81] utiliza a aritmética definida em [Sun58, Moo66, Moo79].

2.2.1 A Aritmética de Kahan

Kahan [Kah68] define uma aritmética intervalar a partir do conjunto dos reais estendidos. Portanto na aritmética de Kahan os extremos dos intervalos podem assumir os valores $-\infty$ e $+\infty$.

Dados X, Y, V e W elementos do conjunto dos intervalos estendidos e $* \in \{+, -, \cdot, /\}$, algumas propriedades da aritmética de Kahan são:

$X * [-\infty, +\infty] = [-\infty, +\infty] * X = [-\infty, +\infty]$
$X * (Y \cup V) = (X * Y) \cup (X * V)$
$(X \cup Y) * (V \cup W) = (X * V) \cup (X * W) \cup (Y * V) \cup (Y * W)$
$(X \cup Y) * V = (X * V) \cup (Y * V)$

2.2.2 A Aritmética de Markov

Markov [Mar77a, Mar78] define as operações de subtração e divisão, respectivamente, por

$$X - Y = [\min\{x_1 - y_1, x_2 - y_2\}, \max\{x_1 - y_1, x_2 - y_2\}] \tag{1}$$

$$X/Y = \begin{cases} [\min\{x_1/y_1, x_2/y_2\}, \max\{x_1/y_1, x_2/y_2\}] & 0 \notin X, 0 \notin Y \\ 1/y_2[x_1, x_2] & 0 \in X, 0 \notin Y \end{cases} \tag{2}$$

Nota-se que $X - X = 0$ e $X/X = 1$ se $0 \notin X$, diferentemente de Moore, onde $0 \in X - X$ e $1 \in X/X$, se $0 \notin X$. Em [Mar77a, Mar78], Markov prova propriedades de $\mathbb{IR}$, com as operações de adição e multiplicação como em Moore e a subtração e divisão como em (1) e (2). Aplicações dessa aritmética podem ser encontradas em [Mar77b, Mar81].

2.2.3 A Aritmética de Bauch

Bauch [Bau90] define um novo tipo de número, denominado intervalos de tolerância (*tolerance intervals*), T-intervalos.

Sejam $\underline{x}$ e $\overline{x}$ números reais tais que $\underline{x} \in \underline{X}$ e $\overline{x} \in \overline{X}$, onde $\underline{X}, \overline{X}$ são elementos de $\mathbb{IR}$. A quádrupla

$$[\underline{X}, \overline{X}] = [x_1, x_2; x_3, x_4]$$

com $x_1 \leq x_2 \leq x_4$ e $x_1 \leq x_3 \leq x_4$ denota os chamados T-intervalos.

As operações aritméticas com os T-intervalos são definidas por:

$[\underline{X}, \overline{X}] + [\underline{Y}, \overline{Y}] = [\underline{X} + \underline{Y}; \overline{X} + \overline{Y}]$
$[\underline{X}, \overline{X}] - [\underline{Y}, \overline{Y}] = [\underline{X} - \overline{Y}, \overline{X} - \underline{Y}]$
$[\underline{X}, \overline{X}] \cdot [\underline{Y}, \overline{Y}] = [\underline{C}, \overline{C}]$
$[\underline{X}, \overline{X}] / [\underline{Y}, \overline{Y}] = [\underline{D}, \overline{D}]$

os T-intervalos $[\underline{C}, \overline{C}]$ e $[\underline{D}, \overline{D}]$, tem como limites intervalos obtidos de acordo com as regras usuais de multiplicação e divisão de intervalos, respectivamente.

Bauch [Bau90] define os T-intervalos para computar simultaneamente aproximações interiores (*inner*) e exteriores (*outer*) para problemas de valores inicias em equações diferenciais ordinárias.

2.2.4 A Aritmética de Acioly

A aritmética de Acioly [Aci91] é realizada de forma similar à de Moore. Acioly [Aci91, Aci96] compatibiliza a propriedade da inclusão monotônica e conceitos topológicos. A inclusão monotonicidade é amplamente usada em algoritmos intervalares. A métrica proposta por Moore gera um espaço topológico de Hausdorff. A idéia subjacente à inclusão monotonicidade é a de aproximação, porém a topologia de Hausdorff separa pontos. Portanto são conceitos incompatíveis. Adicionalmente, intervalos tem sido usados para "enclausurar" números reais "difíceis" de serem alcançados por razões de ordem numérica. Assim, dados dois intervalos contendo o mesmo número real, intuitivamente o "melhor" intervalo é o que tem menor amplitude. Acioly [Aci91, Aci96] usa fatos como esse para enfatizar que intervalos são aproximações de números reais. Nesse sentido a topologia de Hausdorff não pode ser usada, sendo então preterida em favor da topologia de Scott [Smy92]. Como conseqüência resultados obtidos usando a inclusão monotônica também o são usando topologia e vice-versa.

2.3 Intervalos como Conjuntos

Um intervalo é um conjunto de números reais. Intervalos vistos como conjuntos são importantes na definição de seqüências encaixadas e refinamentos mais eficientes.

A *interseção* entre os intervalos X e Y é definida por,

$$X \cap Y = \begin{cases} \emptyset & \text{se } x_1 > y_2 \text{ ou } x_2 < y_1 \\ [\max(x_1, y_1), \min(x_2, y_2)] & \text{caso contrário} \end{cases}$$

e a *união* por,

$$X \cup Y = [\min(x_1, y_1), \max(x_2, y_2)]$$

2.4 Estrutura Topológica

O *valor absoluto* [Moo66, Moo79, AH83] de um intervalo X é definido por:

$$|X| = \max\{|x_1|, |x_2|\}$$

e sua *amplitude* [Moo66, Moo79, AH83] por:

$$w(X) = x_2 - x_1$$

Em muitas situações é importante se dispor do conceito de convergência de seqüências de intervalos. Neste caso é necessário se ter uma função distância definida sobre $\mathbb{IR}$. Inicialmente, considera-se uma topologia sobre $\mathbb{IR}$.

Um *espaço topológico* [Bur72] é um conjunto T com uma *topologia* $\mathcal{T}$ sobre T. Uma topologia é uma coleção de subconjuntos de T, chamados *conjuntos abertos*, com as propriedades:

(a) $\emptyset,\ T \in \mathcal{T}$

(b) se $A_i \in \mathcal{T}, i = 1, \cdots, n$ então $\cap_{i=1}^{n} A_i \in \mathcal{T}$

(c) se $\mathcal{D} \subset \mathcal{T}$ então $\cup\{A \mid A \in \mathcal{D}\} \in \mathcal{T}$

Moore [Moo66, Moo79] define uma métrica sobre o espaço dos intervalos como se segue.

Sejam X e Y intervalos em $\mathbb{IR}$. A *distância* entre X e Y definida por,

$$d(X,Y) = \max\{\mid x_1 - y_1 \mid, \mid x_2 - y_2 \mid\}$$

é uma métrica sobre $\mathbb{IR}$. Então $\langle \mathbb{IR}, d\rangle$ é um *espaço métrico.*

Sabe-se que uma métrica pode ser usada para definir uma topologia $\mathcal{T}$ sobre um conjunto T da seguinte forma: dados $t \in T$ e $\epsilon \in \mathbb{R}$, $\epsilon > 0$, a vizinhança de t de raio ϵ é definida pelo conjunto

$$\mathcal{N}(t,\epsilon) = \{u \mid d(t,u) < \epsilon\}$$

Sobre $\mathbb{IR}$ a vizinhança de X de raio ϵ é definida por

$$\mathcal{N}_{\mathbb{IR}}(X,\epsilon) = \{Y \in \mathbb{IR} \mid d(X,Y) < \epsilon\}$$

i.e.,

$$\mathcal{N}_{\mathbb{IR}}(X,\epsilon) = \{Y \in \mathbb{IR} \mid x_1 - \epsilon < y_1 < x_1 + \epsilon,\ x_2 - \epsilon < y_2 < x_2 + \epsilon\}$$

Como um exemplo, seja $X = [1,2]$ um intervalo em $\mathbb{IR}$ e $\epsilon = 0.001$ um dado número real. Então

$$\mathcal{N}_{\mathbb{IR}}([1,2], 0.001) = \{Y \in \mathbb{IR} \mid 0.999 < y_1 < 1.001,\ 1.999 < y_2 < 2.001\}$$

O conceito de um conjunto aberto em uma topologia $\mathcal{T}$ também pode ser estendido a $\mathbb{IR}$. Dado um subconjunto $A \subset T$, A é um conjunto aberto se $\forall a \in A$, $\exists \mathcal{N}(a,\epsilon) \subset A$. Sobre o conjunto $\mathbb{IR}$, A é um conjunto aberto se $\forall X \subset A$, $\exists \mathcal{N}_{\mathbb{IR}}(X,\epsilon) \subset A$.

Com a métrica d, $\mathbb{IR}$ é um *espaço topológico* e os conceitos de convergência e continuidade podem ser usados da mesma forma que para o espaço métrico $\mathbb{R}$. Portanto, se $X_n = [x_{n_1}, x_{n_2}]$ e $X = [x_1, x_2]$,

$$\lim_{n\to\infty} X_n = X \Leftrightarrow \lim_{n\to\infty} x_{n_1} = x_1 \text{ e } \lim_{n\to\infty} x_{n_2} = x_2$$

$\langle \mathbb{IR}, d\rangle$ é um *espaço métrico completo* e as operações aritméticas são funções contínuas [AH83], i.e., se $\lim_{n\to\infty} X_n = X$, $\lim_{n\to\infty} Y_n = Y$, $* \in \{+,-,\cdot,/\}$, então $\lim_{n\to\infty}(X_n * Y_n) = X * Y$.

2.5 Conclusões

A matemática intervalar é uma solução para problemas práticos relacionados com vários tipos de erros em computações numéricas. O trabalho pioneiro na área é de Sunaga [Sun58], porém apenas a partir de Moore [Moo66, Moo79] e da proposta de Kulisch e Miranker [KM79, KM81, Kul83, KM86] para a aritmética computacional de exatidão máxima a matemática intervalar começou seu real desenvolvimento.

Capítulo 3

A Aritmética de Exatidão Máxima

Este capítulo apresenta a aritmética de exatidão máxima desde os seus fundamentos até a sua definição no espaço dos intervalos. Resultados similares para matrizes e complexos de intervalos estão contidos no Apêndice B [KM79, KM81]. O texto sumariza uma intensa atividade de pesquisa, ocorrida a partir da década de sessenta, nessa área. A extensa revisão bibliográfica aqui vista é *per se* uma contribuição relevante, pois com o nível de abrangência e profundidade enfocados a autora desconhece publicação similar.

A probabilidade intervalar proposta nesta tese, envolve cálculos com o tipo intervalo. Portanto as operações aritméticas sobre o tipo tem de ser realizadas com exatidão máxima em computadores. Aritmética de exatidão máxima significa que o resultado da operação ou é um número de máquina ou está entre dois números de máquina consecutivos. Portanto neste capítulo é apresentada a aritmética de exatidão máxima [KM79, KM81, Kul83, KM86] para todos os espaços da computação numérica. As estruturas algébricas que fundamentam a definição da aritmética de exatidão máxima encontram-se descritas no Apêndice A. As principais características dos padrões IEEE 754 e IEEE 854 para as representações dos números de ponto flutuante podem ser encontradas no Apêndice C.

A Figura 3.1 a seguir lista todos os espaços da computação numérica do ponto de vista da aritmética de alta exatidão ou a aritmética computacional avançada [KM81, KM79, AH83, Cla79, Kul83, KM86]. Segue-se uma descrição dos elementos que a compõem.

		$\mathbb{R}$	$\supset$	D	$\supset$	S
		V$\mathbb{R}$	$\supset$	VD	$\supset$	VS
		M$\mathbb{R}$	$\supset$	MD	$\supset$	MS
P$\mathbb{R}$	$\supset$	I$\mathbb{R}$	$\supset$	ID	$\supset$	IS
PV$\mathbb{R}$	$\supset$	IV$\mathbb{R}$	$\supset$	IVD	$\supset$	IVS
PM$\mathbb{R}$	$\supset$	IM$\mathbb{R}$	$\supset$	IMD	$\supset$	IMS
		$\mathbb{C}$	$\supset$	$\mathbb{C}$D	$\supset$	$\mathbb{C}$S
		V$\mathbb{C}$	$\supset$	V$\mathbb{C}$D	$\supset$	V$\mathbb{C}$S
		M$\mathbb{C}$	$\supset$	M$\mathbb{C}$D	$\supset$	M$\mathbb{C}$S
P$\mathbb{C}$	$\supset$	I$\mathbb{C}$	$\supset$	I$\mathbb{C}$D	$\supset$	I$\mathbb{C}$S
PV$\mathbb{C}$	$\supset$	IV$\mathbb{C}$	$\supset$	IV$\mathbb{C}$D	$\supset$	IV$\mathbb{C}$S
PM$\mathbb{C}$	$\supset$	IM$\mathbb{C}$	$\supset$	IM$\mathbb{C}$D	$\supset$	IM$\mathbb{C}$S

Figura 3.1: Espaços da Computação Numérica

- **D** e **S** representam os conjuntos dos números de ponto flutuante de precisão dupla (D) e simples (S). VD e VS é o conjunto dos vetores cujos elementos são números de ponto flutuante de precisão dupla e simples, respectivamente. MD e MS, conjunto das matrizes cujos elementos são números de ponto flutuante de precisão dupla e simples, respectivamente.

- $\mathbb{R}$, conjunto dos números reais. V$\mathbb{R}$, espaço dos vetores cujas componentes são números reais. M$\mathbb{R}$, espaço das matrizes cujos elementos são números reais.

- $\mathbb{C}$, conjunto dos números complexos. V$\mathbb{C}$, espaço dos vetores cujas componentes são números complexos. M$\mathbb{C}$, espaço das matrizes cujos elementos são números complexos. V$\mathbb{C}$D, M$\mathbb{C}$S, conjuntos dos vetores e matrizes complexas de ponto flutuante de precisão dupla e simples, respectivamente.

- **I$\mathbb{R}$**, espaço dos intervalos de reais. Os elementos da tabela iniciados por I indicam espaços de intervalos. Assim IV$\mathbb{R}$, por exemplo, é o espaço dos intervalos cujas componentes são vetores de números reais; IS, é o conjunto dos intervalos cujos limites são números de ponto flutuante de precisão simples.

- Os espaços iniciados por P indicam conjunto das partes. PV$\mathbb{R}$, por exemplo, é o conjunto das partes do espaço dos vetores cujas componentes são números reais.

Um computador digital é uma máquina de propósito geral, cuja informação é armazenada e processada de forma discreta em palavras com número fixos de dígitos binários (bits). Os bits de informação em sua memória podem ser usados para representar notas musicais, letras de um alfabeto, elementos de um conjunto finito, números inteiros, números racionais, partes de um grafo, etc. Quando se usa computadores para representar as letras de um alfabeto, não há erro de representação, pois símbolos discretos são associados biunivocamente. O problema de erro de representação surge quando o objetivo é se representar, por exemplo, os números reais.

O conjunto dos reais é um corpo ordenado [McC60, Lim76]. O fato dos reais constituirem um corpo possibilita que nele sejam resolvidas equações do tipo $a \cdot x = b, a \neq 0$, onde a solução única é $x = a^{-1} \cdot b$. Por razões de ordem prática, os computadores, em geral, representam os valores numéricos com um número constante de bits. No caso dos reais, é necessário substituí-los por um outro conjunto que os simule, usualmente o dos números de ponto flutuante. O problema porém é que o conjunto dos números de ponto flutuante [Cod88, Gol91, Knu81, Ste74], diferentemente dos reais, não tem propriedades algébricas que garantam os resultados dos cálculos efetuados. Por exemplo, a soma de dois números de grande magnitude pode dar *overflow* ou seja, nem sempre a soma de dois números de ponto flutuante é sequer um número de ponto flutuante.

A aritmética de exatidão máxima [KM79, KM81, Kul83, KM86] foi desenvolvida para computação científica. Ela fornece um método axiomático para as operações aritméticas realizadas em computadores que captura propriedades essenciais associadas com arredondamentos em computações, construindo um sistema de axiomas para problemas gerais que permite várias aplicações; seu grande mérito é propor uma forma de operar números reais representados por números de máquina preservando uma estrutura algébrica chamada de *anelóide* ou *vetóide*. A forma de operar valores mantendo essa estrutura algébrica é através de *semimorfismo* [KM79, KM81, Kul83, KM86]. Semimorfismos são arredondamentos com algumas características básicas. Contudo a definição de semimorfismo pressupõe conjuntos onde a existência de supremos e ínfimos seja garantida.

A proposta e o desenvolvimento da aritmética computacional avançada deve-se não somente à definição dos anelóides, vetóides e semimorfismo, mas também à introdução por Moore [Moo66, Moo79], na década de 60, do *intervalo*. Erros em medições, erros de arredondamentos e controle do erro podem ser resolvidos através de intervalos. Uma área de pesquisa com amplo espectro de aplicações, além do potencial de desenvolvimento teórico, tem progredido a partir dos trabalhos de Moore.

3.1 Screens

Nesta seção é definido o que significa um conjunto $\mathrm{S} \subseteq \mathrm{R}$ ser um *screen* de R. Intuitivamente, um subconjunto S de R é um *screen* de R se R é "visto" através de S. A grande importância do estudo de *screens* no escopo deste trabalho, deve-se ao fato que o sistema de números de ponto flutuante (S ou D) é um screen para o conjunto dos números reais. Não é possível operar (com precisão fixa) os reais em qualquer sistema de computação existente, pois este dispõe apenas dos números de máquina, os quais formam um conjunto finito enquanto os reais são não enumeráveis. Assim, os reais são vistos através dos números de ponto flutuante.

Definição 3.1.1 Seja R um conjunto ordenado e $a \in \mathrm{R}$. Sejam $\mathrm{U}(a)$ e $\mathrm{L}(a)$, respectivamente, os conjuntos dos limites superiores e inferiores de a,

$$\mathrm{L}(a) = \{x \in \mathrm{R} \mid x \leq a\}$$

$$\mathrm{U}(a) = \{x \in \mathrm{R} \mid a \leq x\}$$

Seja $\mathrm{S} \subseteq \mathrm{R}$. S é um *screen* de R, se para todo $a \in \mathrm{R}$:

(a) **(S1L)** $\quad \mathrm{L}(a) \cap \mathrm{S} \neq \emptyset$

(b) **(S1U)** $\quad \mathrm{U}(a) \cap \mathrm{S} \neq \emptyset$

(c) **(S2L)** $\quad \exists l_0 \in \mathrm{L}(a) \cap \mathrm{S}$ tal que para todo $x \in \mathrm{L}(a) \cap \mathrm{S},\ x \leq {l_0}_{\mathrm{L}(a)\cap\mathrm{S}}$

(d) **(S2U)** $\quad \exists u_0 \in \mathrm{U}(a) \cap \mathrm{S}$ tal que para todo $x \in \mathrm{U}(a) \cap \mathrm{S},\ {u_0}_{\mathrm{U}(a)\cap\mathrm{S}} \leq x$

A figura a seguir ilustra a definição de *screen*.

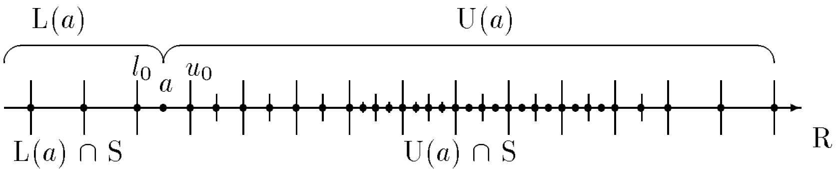

Figura 3.2: Ilustração da Definição de *Screen*

Se apenas (a) e (c) acontecem S é um *semiscreen inferior*; se apenas (b) e (d) acontecem, S é um *semiscreen superior*.

Exemplo 3.1.2 Sejam $\mathbb{R}$, o conjunto dos números reais e $S(b, l, e_{min}, e_{max})$ um sistema de ponto flutuante (ver apêndice C para detalhes). Tem-se que:

- para cada $x \in \mathbb{R}$, $\mid x \mid \leq * \cdot d_1 d_2 \ldots d_l \cdot b^{e_{max}},\ d_i = b - 1,\ i = 1, ..., l$, existem limites inferiores para x em S e existem limites superiores para x em S;
- o conjunto dos limites inferiores de x em S tem um maior elemento e o conjunto dos limites superiores de x em S tem um menor elemento.

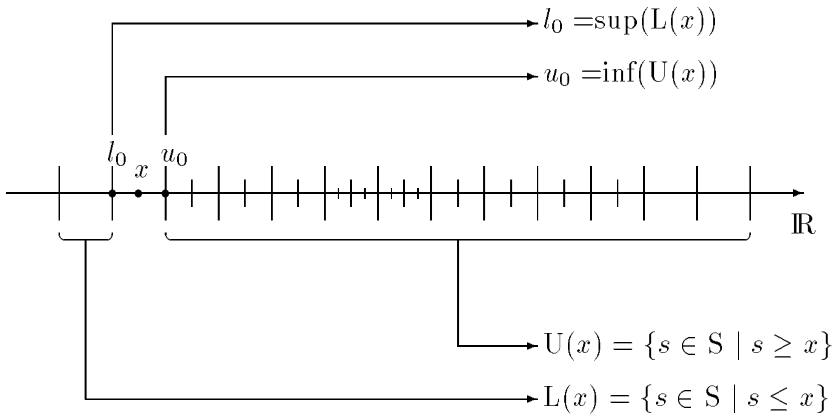

Figura 3.3: Um *Screen* para os Números Reais

3.1.1 Arredondamentos

Sejam l_0 e u_0 da definição 3.1.1. Para todo $a \in \mathrm{R}$ definindo-se as funções $\varphi : \mathrm{R} \to \mathrm{S}$ e $\psi : \mathrm{R} \to \mathrm{S}$ por

(**RL**) $\quad \varphi(a) = l_{0_{\mathrm{L}(a) \cap \mathrm{S}}}$

(**RU**) $\quad \psi(a) = u_{0_{\mathrm{U}(a) \cap \mathrm{S}}}$

Lema 3.1.3 Seja R um conjunto ordenado e S um *screen* de R. As funções φ e ψ têm as seguintes propriedades:

(a) Para todo $a \in \mathrm{S}$,

(**R1L**) $\quad \varphi(a) = a$

(**R1U**) $\quad \psi(a) = a$

(b) Para todo $a, b \in \mathrm{R}$,

(**R2L**) $\quad a \leq b \Rightarrow \varphi(a) \leq \varphi(b)$

(**R2U**) $\quad a \leq b \Rightarrow \psi(a) \leq \psi(b)$

(c) Para todo $a \in \mathrm{R}$,

(**R3L**) $\quad \varphi(a) \leq a$

(**R3U**) $\quad \psi(a) \geq a$

Demonstração. Com relação à função ψ:

(a) $\mathrm{U}(a) = \{x \in \mathrm{R} \mid a \leq x\}$. Seja $a \in \mathrm{U}(a)$; $a \in \mathrm{S}$, por hipótese, logo $a \in \mathrm{U}(a) \cap \mathrm{S}$. Como $\langle \mathrm{S}, \leq \rangle$ é um *screen*, $\mathrm{U}(a) \cap \mathrm{S}$ tem um menor elemento, logo $\mathrm{U}(a) \cap \mathrm{S} = u_{0_{\mathrm{U}(a) \cap \mathrm{S}}} = a$. Mas $\psi(a) = u_{0_{\mathrm{U(a)} \cap \mathrm{S}}}$, por definição. Portanto $\psi(a) = a$.

(b) $a \leq b \Rightarrow \mathrm{U}(b) \subseteq \mathrm{U}(a) \Rightarrow \mathrm{U}(b) \cap \mathrm{S} \subseteq \mathrm{U}(a) \cap \mathrm{S} \Rightarrow u_{0_{\mathrm{U}(a) \cap \mathrm{S}}} \leq u_{0_{\mathrm{U}(b) \cap \mathrm{S}}} \Rightarrow \psi(a) \leq \psi(b)$.

(c) Por definição $\psi(a)$ é o maior de todos os elementos de R que são menores ou iguais a a, logo $a \leq \psi(a)$.

Demonstração de forma dual para φ. ∎

$\langle \mathrm{S}, \leq \rangle$ é um *screen inferior* se apenas φ está definida e um *screen superior* se apenas ψ está definida.

Teorema 3.1.4 Seja R um reticulado completo e $\mathrm{S} \subseteq \mathrm{R}$.

(a) S é um *screen* inferior de R se e só se S é um sup-semireticulado completo.

(b) S é um *screen* superior de R se e só se S é um inf-semireticulado completo.

(c) S é um *screen* de R se e só se S é um subreticulado completo.

Este teorema relaciona *screens* e reticulados. Prova em [KM79, KM81].

Teorema 3.1.5 Seja R um reticulado completo, S um *screen* de R e $\varphi : \mathrm{R} \to \mathrm{S}$ e $\psi : \mathrm{R} \to \mathrm{S}$ definidas por

(RL) $\varphi(a) = \sup(\mathrm{L}(a) \cap \mathrm{S}),\ \forall a \in \mathrm{R}$

(RU) $\psi(a) = \inf(\mathrm{U}(a) \cap \mathrm{S}),\ \forall a \in \mathrm{R}$

Então, para todo $\mathrm{A} \subseteq \mathrm{S}$,

$$\inf_{\mathrm{S}}\mathrm{A} = \varphi(\inf_{\mathrm{R}}\mathrm{A})$$

$$\sup_{\mathrm{S}}\mathrm{A} = \psi(\sup_{\mathrm{R}}\mathrm{A})$$

Demonstração. (com relação à função ψ)

$\forall a \in \mathrm{A}, a \leq \sup_{\mathrm{R}}\mathrm{A} \Rightarrow \psi(a) \leq \psi(\sup_{\mathrm{R}}\mathrm{A}) \Rightarrow a \leq \psi(\sup_{\mathrm{R}}\mathrm{A})$.

Por conseguinte,

$$\sup_{\mathrm{S}}\mathrm{A} \leq \psi(\sup_{\mathrm{R}}\mathrm{A}) \tag{1}$$

Sabe-se que, $\forall \mathrm{A} \subseteq \mathrm{S}, \sup_{\mathrm{R}}\mathrm{A} \leq \sup_{\mathrm{S}}\mathrm{A}$. Logo $\psi(\sup_{\mathrm{R}}\mathrm{A}) \leq \psi(\sup_{\mathrm{S}}\mathrm{A})$. Mas $\sup_{\mathrm{S}}\mathrm{A} \in \mathrm{S}$, portanto $\psi(\sup_{\mathrm{S}}\mathrm{A}) \leq \sup_{\mathrm{S}}\mathrm{A}$. Então,

$$\psi(\sup_{\mathrm{R}}\mathrm{A}) \leq \sup_{\mathrm{S}}\mathrm{A} \tag{2}$$

Considerando (1) e (2) o teorema está provado. Demonstração similar para φ. ■

No teorema anterior, se S é apenas um *screen* inferior então só φ está definida; se S é um *screen* superior, apenas ψ está definida.

Definição 3.1.6 Seja R um conjunto e $\mathrm{S} \subseteq \mathrm{R}$. Um mapeamento $\square : \mathrm{R} \to \mathrm{S}$ é chamado um *arredondamento* se para todo $a \in \mathrm{S}$,

(R1) $\square a = a$

Definição 3.1.7 Seja R um reticulado completo, S um *screen* para R e $\square : \mathrm{R} \to \mathrm{S}$ um arredondamento.

(a) $\square$ é um *arredondamento monótono* se para todo $a, b \in \mathrm{R}$,

(R2) $a \leq b \Rightarrow \square a \leq \square b$

(b) $\square$ é um *arredondamento direcionado para baixo* se para todo $a \in \mathrm{R}$,

(R3L) $\square a \leq a$

(c) $\square$ é um *arredondamento direcionado para cima* se para todo $a \in \mathrm{R}$,

(R3U) $a \leq \square a$.

Se S é um *screen* inferior, valem só (a) e (b). Se S é um *screen* superior, são válidas (a) e (c). Na definição 3.1.6, R é um conjunto ordenado, isto é, o mapeamento arredondamento apenas pressupõe ordem. Quando R e S são estruturas com mais propriedades, definição 3.1.7, tem-se monotonicidade e direcionamentos.

O teorema a seguir mostra um arredondamento que satisfaz as propriedades (**R1**), (**R2**) e (**R3**).

Teorema 3.1.8

(a) Seja R um reticulado completo, S um *screen* inferior de R e $\square : \mathrm{R} \to \mathrm{S}$ um arredondamento.
$\square$ é um arredondamento monótono direcionado para baixo se e só se para todo $a \in \mathrm{R}$,

(**RL**) $\square a = \sup(\mathrm{L}(a) \cap \mathrm{S})$

(b) Seja R um reticulado completo, S um *screen* superior de R e $\square : \mathrm{R} \to \mathrm{S}$ um arredondamento.
$\square$ é um arredondamento monótono direcionado para cima se e só se para todo $a \in \mathrm{R}$,

(**RU**) $\square a = \inf(\mathrm{U}(a) \cap \mathrm{S})$

Demonstração.

(a) ($\Rightarrow$) De acordo com o lema 3.1.3 um mapeamento, $\square$, definido por (**RL**) satisfaz (**R1L**), (**R2L**), (**R3L**). Portanto $\square$ é um arredondamento monótono direcionado para baixo.

($\Leftarrow$) Por (**R3L**), $\square a \leq a \Rightarrow a \in \mathrm{L}(a) \cap \mathrm{S}$. Por hipótese, S é um *screen* inferior, portanto, usando o teorema 3.1.4 (a), S é um sup-semireticulado completo o que implica $\sup(\mathrm{L}(a) \cap \mathrm{S}) \in \mathrm{S}$. Seja x qualquer, mas tal que $x \in \mathrm{L}(a) \cap \mathrm{S}$. Logo, $x \leq a$. Por (**R2L**), $\square x \leq \square a$ e por (**R1L**) $\square x = x$, logo $x \leq \square a \Rightarrow \square a$ é o maior elemento de $\mathrm{L}(a) \cap \mathrm{S} \Rightarrow \square a = \sup(\mathrm{L}(a) \cap \mathrm{S})$.

(b) Prova-se de forma dual. ∎

Como supremos e ínfimos, quando existem, são únicos, *existe apenas um arredondamento monótono direcionado para baixo e um arredondamento monótono direcionado para cima, quando o arredondamento é definido sobre um conjunto que tenha a estrutura de reticulado e assuma valores em um screen* (inferior/superior). Portanto, para estes únicos arredondamentos serão usados os símbolos,

$\bigtriangledown$, *arredondamento monótono direcionado para baixo,*

$\bigtriangleup$, *arredondamento monótono direcionado para cima,*

de forma que, para todo $a \in \mathrm{R}$, as regras (**RL**) e (**RU**) do teorema 3.1.8 são agora denotadas por

(**RL**) $\bigtriangledown a = \sup(\mathrm{L}(a) \cap \mathrm{S})$

(**RU**) $\bigtriangleup a = \inf \mathrm{U}(a) \cap \mathrm{S})$

Exemplo 3.1.9 Sejam S(10,3,−3,3) e $a = 2.324$; então $\bigtriangledown a = 2.32 = 0.232 \times 10^1$ e $\bigtriangleup a = 2.33 = 0.233 \times 10^1$.

Teorema 3.1.10 Seja R um reticulado completo.

(a) Sejam $\langle \mathrm{S}, \leq \rangle$ e $\langle \mathrm{D}, \leq \rangle$ *screen*s inferiores de $\langle \mathrm{R}, \leq \rangle$, com $\mathrm{S} \subset \mathrm{D} \subset \mathrm{R}$ e os arredondamentos monótonos direcionados para baixo $\bigtriangledown : \mathrm{R} \to \mathrm{S}$, $\bigtriangledown_1 : \mathrm{R} \to \mathrm{D}$ e $\bigtriangledown_2 : \mathrm{D} \to \mathrm{S}$. Então, para todo $a \in \mathrm{R}$,

$$\bigtriangledown a = \bigtriangledown_2(\bigtriangledown_1 a)$$

(b) Sejam $\langle \mathrm{S}, \leq \rangle$ e $\langle D, \leq \rangle$ *screens* superiores de $\langle \mathrm{R}, \leq \rangle$, com $\mathrm{S} \subset \mathrm{D} \subset \mathrm{R}$ e os arredondamentos monótonos direcionados para cima $\bigtriangleup : \mathrm{R} \to \mathrm{S}$, $\bigtriangleup_1 : \mathrm{R} \to \mathrm{D}$ e $\bigtriangleup_2 : \mathrm{D} \to \mathrm{S}$ arredondamentos monótonos direcionados para cima. Então, para todo $a \in \mathrm{R}$,

$$\bigtriangleup a = \bigtriangleup_2(\bigtriangleup_1 a)$$

Demonstração.

(a) $\mathrm{S} \subset \mathrm{D} \Rightarrow \mathrm{L}(a) \cap \mathrm{S} \subset \mathrm{L}(a) \cap \mathrm{D} \Rightarrow \sup(\mathrm{L}(a) \cap \mathrm{S}) \leq \sup(\mathrm{L}(a) \cap \mathrm{D}) \Rightarrow$

$$\bigtriangledown a \leq \bigtriangledown_1 a \tag{3}$$

Aplicando $\bigtriangledown_2$ em (3), tem-se que $\bigtriangledown_2(\bigtriangledown a) \leq \bigtriangledown_2(\bigtriangledown_1 a)$. Mas, $\bigtriangledown_2(\bigtriangledown a) = \bigtriangledown a$, logo

$$\bigtriangledown a \leq \bigtriangledown_2(\bigtriangledown_1 a) \tag{4}$$

Por (**R3L**), $\bigtriangledown_2(\bigtriangledown_1 a) \leq \bigtriangledown_1 a \leq a \Rightarrow$

$$\bigtriangledown_2(\bigtriangledown_1 a) \leq a \tag{5}$$

Aplicando $\bigtriangledown$ em (5), $\bigtriangledown(\bigtriangledown_2(\bigtriangledown_1 a)) \leq \bigtriangledown a$. Mas $\bigtriangledown(\bigtriangledown_2(\bigtriangledown_1 a)) = \bigtriangledown_2(\bigtriangledown_1 a)$, de (**R1L**). Logo,

$$\bigtriangledown_2(\bigtriangledown_1 a) \leq \bigtriangledown a \tag{6}$$

De (4) e (6) conclui-se que

$$\bigtriangledown a = \bigtriangledown_2(\bigtriangledown_1 a)$$

(b) Prova-se de forma dual. ■

Em aplicações práticas, S é o conjunto de números de ponto flutuante de precisão simples e D, dupla, sobre o mesmo computador [KM79, KM81].

Exemplo 3.1.11 Sejam $\mathrm{R}=[0,8] \subset \mathbb{R}$, $\mathrm{S}(10,1,0,1)$, $\mathrm{D}(10,2,0,1)$, $\square : \mathrm{R} \to \mathrm{S}$, $\square_1 : \mathrm{R} \to \mathrm{D}$, $\square_2 : \mathrm{D} \to \mathrm{S}$, os arredondamentos para o mais próximo ou, se ponto médio, para o extremo superior. Se a=2.46 então $\square a = 2$, $\square_1 a = 2.5$, $\square_2(\square_1 a) = \square_2 2.5 = 3$. Logo, $\square a \neq \square_2(\square_1 a)$, isto é, a igualdade $\bigtriangledown a = \bigtriangledown_2(\bigtriangledown_1 a)$ do teorema anterior não é verdadeira. Nota-se que $\square$ não é um arredondamento direcionado para baixo pois não é verdade que $\square a \leq a$ para todo $a \in \mathrm{R}$; se $a = 2.79$ então $\square a = 3$ e portanto $\square a \not\leq a$.

O teorema a seguir mostra a importância dos arredondamentos direcionados para obtenção de exatidão máxima.

Teorema 3.1.12 Seja R um reticulado completo totalmente ordenado, S um *screen* de R, $\nabla : \mathrm{R} \to \mathrm{S}$ e $\triangle : \mathrm{R} \to \mathrm{S}$ os arredondamentos monótonos direcionados. Então para todo $a \in \mathrm{R}$ *não existe* $b \in \mathrm{S}$ tal que $\nabla a < b < \triangle a$.

Demonstração. $\nabla a = \sup(\mathrm{L}(a) \cap \mathrm{S})$ e $\triangle a = \inf(\mathrm{U}(a) \cap \mathrm{S})$. Supondo que existe $b \in \mathrm{S}$ tal que $\sup(\mathrm{L}(a) \cap \mathrm{S}) < b$ ou $\inf(\mathrm{U}(a) \cap \mathrm{S}) > b$. Mas $\sup(\mathrm{L}(a) \cap \mathrm{S}) < b < \inf(\mathrm{U}(a) \cap \mathrm{S})$ implica que ou ∇a não é o $\sup(\mathrm{L}(a) \cap \mathrm{S})$, ou $\triangle a$ não é o $\inf(\mathrm{U}(a) \cap \mathrm{S})$. Absurdo. ∎

A importância de R ser um conjunto totalmente ordenado como hipótese do teorema anterior é para garantir que todos os elementos são comparáveis, isto é, ou $\nabla a \leq b$ ou $\triangle a \geq b$.

Qual o significado de exatidão máxima? O teorema 3.1.12, mostra que entre os valores convenientemente arredondados de a não existe elemento no *screen*. Com os dados do exemplo 3.1.9 tem-se que $0.232 \times 10^1 < 2.324 < 0.233 \times 10^1$.

3.1.2 Operações Aritméticas e Arredondamentos

Esta seção relaciona-se com o problema de como operações que são definidas em um conjunto R, podem ser aproximadas em um subconjunto de R, S. Sobre computadores as operações aritméticas têm caracteristícas algébricas diferentes da usual (usual no sentido das definidas sobre a reta); portanto algum tipo de técnica tem que ser usada para que resultados obtidos na máquina sejam tão próximos dos verdadeiros quanto possível.

A terna $\langle \mathrm{R}, *, \leq \rangle$ é um *grupóide ordenado* se $\langle \mathrm{R}, * \rangle$ é um grupóide, $\langle \mathrm{R}, \leq \rangle$ é um conjunto ordenado e para todo $a, b, c \in \mathrm{R}$, vale a propriedade

(OA) $\quad a \leq b \Rightarrow a * c \leq b * c \text{ e } c * a \leq c * b$

Kulisch e Miranker [KM79, KM81] referem-se a esta propriedade como a propriedade de compatibilidade entre a estrutura algébrica e a estrutura de ordem; esta propriedade é equivalente a

$$a \leq b \text{ e } c \leq d \Rightarrow a * c \leq b * d,\ \forall a, b, c, d \in \mathrm{R}$$

Mais geralmente, tem-se um grupo ordenado ou anel ordenado, etc. $\langle \mathbb{R}, +, \leq \rangle$ é um grupo ordenado; $\langle \mathbb{R}, +, \cdot, \leq \rangle$ é um anel ordenado.

Definição 3.1.13 Seja $\langle \mathrm{R}, \leq \rangle$ um reticulado completo, $\langle \mathrm{R}, * \rangle$ um grupóide e $\langle \mathrm{S}, \leq \rangle$ um *screen* inferior ou superior de R.

(a) Um grupóide $\langle \mathrm{S}, \boxast \rangle$ é chamado um *screen grupóide* se

(RG1) $\quad a * b \in \mathrm{S} \Rightarrow a \boxast b = a * b,\ \forall a, b \in \mathrm{S}$

(b) $\langle \mathrm{S}, \boxast \rangle$ é um *screen grupóide monótono* se

(RG2) $\quad a * b \leq c * d \Rightarrow a \boxast b \leq c \boxast d,\ \forall a, b, c, d \in \mathrm{S}$

(c) $\langle \mathrm{S}, \boxast \rangle$ é um *screen grupóide inferior* se

(RG3L) $\quad a \boxast b \leq a * b,\ \forall a, b \in \mathrm{S}$

(d) $\langle \mathrm{S}, \boxast \rangle$ é um *screen grupóide superior* se

$$\textbf{(RG3U)} \qquad a * b \leq a \boxast b, \forall a, b \in \mathrm{S}$$

Exemplo 3.1.14 Este exemplo ilustra as operações envolvidas de definição 3.1.13. Sejam R, S e $\Box$ como no exemplo 3.1.11.

$$+ : \mathrm{R} \times \mathrm{R} \rightarrow \mathrm{R}$$

$$(2.3264\ ,\ 5.223) \mapsto 2.3264 + 5.223 = 7.5494$$

$$(1.03\ ,\ 0.2) \mapsto 1.03 + 0.2 = 1.23$$

$$\Box : \mathrm{R} \rightarrow \mathrm{S}$$

$$\Box(7.5498) = 8$$

$$\Box(1.23) = 1$$

$$\boxplus : \mathrm{S} \times \mathrm{S} \rightarrow \mathrm{S}$$

$$(8, 1) \mapsto 8 \boxplus 1 = 9$$

O teorema seguinte mostra *screens* grupóides que satisfazem às propriedades (**RG1**), (**RG2**), (**RG3L**) e (**RG3U**) da definição 3.1.13.

Teorema 3.1.15 Sejam $\langle \mathrm{R}, \leq \rangle$ um reticulado completo, $\langle \mathrm{R}, * \rangle$ um grupóide, $\langle \mathrm{S}, \leq \rangle$ um *screen* inferior (ou superior) ou um *screen* de $\langle \mathrm{R}, \leq \rangle$, o mapeamento $\Box : \mathrm{R} \rightarrow \mathrm{S}$ e $\boxast$ uma operação sobre S definida por

$$\textbf{(RG)} \qquad a \boxast b = \Box(a * b), \forall a, b \in \mathrm{S}$$

(a) Se $\Box$ tem as propriedades (**R1**), (**R2**), (**R3L**) e (**R3U**) então $\langle \mathrm{S}, \boxast \rangle$ tem as propriedades (**RG1**), (**RG2**), (**RG3L**) e (**RG3U**).

(b) Se $\langle \mathrm{R}, * \rangle$ tem elemento neutro à direita $\mathbb{1} \in \mathrm{S}$, então $\langle \mathrm{S}, \boxast \rangle$ é um *screen* grupóide inferior (superior) monótono se e só se $\boxast$ é definida por (**RG**), com $\Box$ tendo as propriedades (**R1**), (**R2**), (**R3L**) e (**R3U**).

Demonstração.

(a) Sejam $a, b, c, d \in \mathrm{S}$, onde $\langle \mathrm{S}, \leq \rangle$ é um *screen* inferior.

$$\begin{aligned}
& a \boxast b = a * b = \Box(a * b) \\
& a * b \leq c * d \overset{(R2)}{\Rightarrow} \Box(a * b) \leq \Box(c * d) = \mathrm{a} \boxast b \leq c \boxast d \\
& a \boxast b = \Box(a * b) \overset{(R3L)}{\leq} a * b \Rightarrow a \boxast b \leq a * b \\
& a \boxast b = \Box(a * b) \overset{(R3U)}{\geq} a * b \Rightarrow a \boxast b \geq a * b.
\end{aligned}$$

(b) ($\Leftarrow$) Se $\boxast$ é definida por (**RG**) e $\square$ tem as propriedades (**R1**), (**R2**) e (**R3**) então foi mostrado em (a) que $\langle \mathrm{S}, \boxast \rangle$ tem as propriedades (**RG1**), (**RG2**), (**RG3L**) e (**RG3U**) e portanto, pela definição 3.1.13, $\langle \mathrm{S}, \boxast \rangle$ é um *screen* grupóide inferior/superior monótono.

($\Rightarrow$) Supondo válidas (**RG1**), (**RG2**), (**RG3L**), (**RG3U**) e (**RG**) e $\mathbb{1}$ elemento neutro de $\langle \mathrm{R}, * \rangle$ e $\langle \mathrm{S}, \boxast \rangle$; provando verdadeiras (**R1**), (**R2**), (**RG3L**).

Como $\mathbb{1} \in \mathrm{S}$, $\forall a \in \mathrm{S}$, $\square a = \square(a * \mathbb{1}) \overset{(RG)}{=} a \boxast \mathbb{1} = a$.

Sejam $a, b \in \mathrm{S}$. Então

$$\begin{aligned} a \leq b \quad & \Rightarrow \quad a * \mathbb{1} \leq b * \mathbb{1} \\ & \overset{(RG2)}{\Rightarrow} \quad a \boxast \mathbb{1} \leq b \boxast \mathbb{1} \\ & \overset{(RG)}{\Rightarrow} \quad \square(a * \mathbb{1}) \leq \square(b * \mathbb{1}) \\ & \Rightarrow \quad a \leq b \end{aligned}$$

$\forall a, b \in \mathrm{S}, a \boxast b \overset{(RG3)}{\leq} a * b$

Em particular se $b = \mathbb{1}$, $a \boxast \mathbb{1} \leq a * \mathbb{1} \overset{(RG)}{\Rightarrow} \square(a * \mathbb{1}) \leq a * \mathbb{1} \Rightarrow \square a \leq a$

Prova-se de forma similar que $\langle \mathrm{S}, \boxast \rangle$ é um *screen* grupóide superior monótono. ∎

Como os arredondamentos monótonos direcionados, para baixo e para cima, são únicos e como os *screens* grupóides monótonos, inferior e superior, são definidos através desses arredondamentos então existe um único *screen* grupóide monótono inferior e um único *screen* grupóide monótono superior. Portanto são usados os símbolos especiais $\mathbin{\triangledown\!\!\!\!\!*}$ e $\mathbin{\vartriangle\!\!\!\!\!*}$ para denotar operações aritméticas nestes grupóides. Tem-se então,

$$\begin{gathered} \langle \mathrm{S}, \mathbin{\triangledown\!\!\!\!\!*}, \leq \rangle, \text{ o } \textit{screen grupóide monótono inferior}, \\ \langle \mathrm{S}, \mathbin{\vartriangle\!\!\!\!\!*}, \leq \rangle, \text{ o } \textit{screen grupóide monótono superior}. \end{gathered}$$

Tem-se então que, para todo $a, b \in \mathrm{S}$, a propriedade (**RG**) do teorema 3.1.15, definida usando estes símbolos especiais é,

(**RG**) $\quad a \mathbin{\triangledown\!\!\!\!\!*} b = \triangledown(a * b)$
(**RG**) $\quad a \mathbin{\vartriangle\!\!\!\!\!*} b = \vartriangle(a * b)$

O teorema a seguir mostra propriedades adicionais dos grupóides quando estes são ordenados.

Teorema 3.1.16 Seja $\langle \mathrm{R}, *, \leq \rangle$ um grupóide completamente ordenado com elemento neutro à direita $\mathbb{1} \in \mathrm{R}$.

(a) Seja $\langle \mathrm{S}, \mathbin{\triangledown\!\!\!\!\!*}, \leq \rangle$, o *screen* grupóide monótono inferior. Então para todo $a, b \in \mathrm{R}$,

$$(\triangledown a) \mathbin{\triangledown\!\!\!\!\!*} (\triangledown b) \leq \triangledown(a * b) \leq a * b \tag{7}$$

(b) Seja $\langle \mathrm{S}, \mathbin{\vartriangle\!\!\!\!\!*}, \leq \rangle$, o *screen* grupóide monótono superior. Então para todo $a, b \in \mathrm{R}$,

$$a * b \leq \vartriangle(a * b) \leq (\vartriangle a) \mathbin{\vartriangle\!\!\!\!\!*} (\vartriangle b) \tag{8}$$

Demonstração.

(a) $(\triangledown a) \,\triangledown\!\!\!\!*\, (\triangledown b) \overset{(RG)}{=} \triangledown(\triangledown a * \triangledown b) \overset{(R3L)}{\leq} \triangledown(a * b) \overset{(R3L)}{\leq} a * b.$

(b) Prova-se de forma dual. ■

3.2 Semimorfismo e o Método Horizontal de Definição da Aritmética em Computadores

Nesta seção é definido o que é semimorfismo. Em seguida é dada a definição e os fundamentos do chamado método horizontal de definição da aritmética em computadores. Sucintamente, este método define a aritmética no *screen* através de um mapeamento que faz com que propriedades algébricas de interesse do ponto de vista numérico sejam preservadas.

3.2.1 Semimorfismo

A questão que se coloca de modo geral, com respeito a uma computação científica, é como operações aritméticas que são definidas numa estrutura $\langle \mathrm{R}, *, \leq \rangle$ podem ser mais bem aproximadas em uma outra estrutura $\langle \mathrm{S}, \boxast, \leq \rangle$, com $\mathrm{S} \subseteq \mathrm{R}$. Tomando como exemplo o conjunto dos reais, $\mathbb{R}$, sabe-se que $\langle \mathbb{R}, +, \cdot, \leq \rangle$ é um corpo [Lim76, McC60]. As operações aritméticas nos reais, quando realizadas em computadores, têm que ser aproximadas em $\mathrm{S} \subseteq \mathbb{R}$, onde S é um sistema de ponto flutuante de determinada máquina. Além disso, essa aproximação não pode ser realizada por meio de um isomorfismo, nem por meio de um homomorfismo. A aritmética de alta exatidão [KM79, KM81, Kul83, KM86], define uma técnica que permite aproximar as operações aritméticas definidas nos reais, no *screen*.

Seja $\square : \mathrm{R} \to \mathrm{S}$ tal que $\square a = a,\ \forall a \in \mathrm{S}$. O mapeamento $\square$, visto no capítulo anterior, é denominado arredondamento. Homomorfismos preservam operações nas transformações entre estruturas, mas $\square$ não é um homomorfismo como pode ser visto através do exemplo a seguir [KM79, KM81].

Exemplo 3.2.1 $\mathrm{R}=\mathbb{R}$ e $\mathrm{S}(10,1,-1,1)$; $\square$ é o arredondamento para o mais próximo ou, se ponto médio para o extremo superior e $\boxplus$ a operação de adição em S. Sejam $a, b \in \mathbb{R}$, $a = 0.34$ e $b = 0.54$. Então

$$\square a = \square 0.34 = 0.3$$

$$\square b = \square 0.54 = 0.5$$

$$\square(a+b) = \square(0.34 + 0.54) = \square 0.88 = 0.9$$

$$(\square a) \boxplus (\square b) = (\square 0.34) \boxplus (\square 0.54) = 0.3 \boxplus 0.5 = 0.8$$

Logo,

$$\square(a+b) \neq \square(a) \boxplus \square(b).$$

Os comentários que se seguem são importantes, pois vão ilustrar algumas das características que um mapeamento entre R e $\mathrm{S} \subseteq \mathrm{R}$ deve ter de forma que se mantenham propriedades algébricas de interesse.

(a) O exemplo anterior mostra que dados $a, b \in \mathrm{R}$, de modo geral não se tem,

$$\square(a * b) = \square a \circledast \square b \tag{9}$$

Portanto uma idéia é que (9) seja válida considerando apenas $a, b \in \mathrm{S}$.

(b) Adicionalmente, do ponto de vista de preservação da ordem, é importante a manutenção da monotonicidade, isto é,

$$\forall a, b \in \mathrm{R}, a \leq b \Rightarrow \square a \leq \square b$$

(c) Sabe-se que 0 e 1 pertencem a S, ou mais geralmente quando necessário,

$$\mathbb{0}, \mathbb{1} \in \mathrm{S}$$

(d) $-a \in \mathrm{S},\ \forall a \in \mathrm{S}$

(e) Supondo (9), $a, b \in \mathrm{R}$, $b = -\mathbb{1} \in \mathrm{S}$, a operação multiplicação $(\cdot)$ em R e $\boxdot$ a mesma em S, tem-se que:

$$\square(a \cdot b) = \square(a \cdot -\mathbb{1}) = \square(-a) \tag{10}$$

$$\square a \boxdot \square b = \square a \boxdot (-\mathbb{1}) = -\square a \tag{11}$$

De (10) e (11) conclui-se que, $\forall a, b \in \mathrm{R}$,

$$\square(-a) = -\square a$$

Em anelóides e vetóides existe um operador menos (definição A.6.5). Este operador é utilizado para estender os conceitos de *screen* e arredondamentos. Estes conceitos são básicos para a definição de semimorfismo.

Definição 3.2.2 Seja $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq \rangle$ um anelóide (ou vetóide), $\langle \mathrm{R}, \leq \rangle$ um reticulado completo e $\langle \mathrm{S}, \leq \rangle$ um *screen* inferior (superior) ou *screen* de $\langle \mathrm{R}, \leq \rangle$; $\langle \mathrm{S}, \leq \rangle$ é um *screen simétrico* se

(S3) $(\mathbb{0}, \mathbb{1} \in \mathrm{S})$ e $(-a \in \mathrm{S},\ \forall a \in \mathrm{S})$

Definição 3.2.3 Seja $\langle \mathrm{R}, \leq \rangle$ um reticulado completo e $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico de $\langle \mathrm{R}, \leq \rangle$. O arredondamento $\square : \mathrm{R} \to \mathrm{S}$ é um *arredondamento anti-simétrico* se

(R4) $\square(-a) = -\square a,\ \forall a \in \mathrm{R}$

Definição 3.2.4 Seja $\langle \mathrm{R}, \leq \rangle$ um reticulado completo, $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq \rangle$ um anelóide (ou vetóide), $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico inferior (superior) ou *screen* simétrico de $\langle \mathrm{R}, \leq \rangle$, $\square : \mathrm{R} \to \mathrm{S}$ e para cada operação $*$ definida em R, uma operação $\circledast$ definida em S por

(RG) $a \circledast b = \square(a * b),\ \forall a, b \in \mathrm{S}$

onde $\Box$ tem as seguintes propriedades

(R1)	$\Box a = a, \ \forall a \in \mathrm{S}$
(R2)	$a \leq b \Rightarrow \Box a \leq \Box b, \ \forall a, b \in \mathrm{R}$
(R4)	$\Box(-a) = -\Box a, \ \forall a \in \mathrm{R}$

$\Box$ definida por (**RG**) e satisfazendo (**R1**), **R2**) e (**R4**) é um *semimorfismo*.

Será visto que quando R é um espaço de intervalos, uma propriedade adicional é acrescida à definição de semimorfismo. Esta propriedade vai definir os arredondamentos direcionados nos extremos do intervalo.

O teorema a seguir mostra uma dependência entre os arredondamentos $\bigtriangledown$ e $\bigtriangleup$.

Teorema 3.2.5 Seja $\langle R, +, .\rangle$ um anelóide (ou vetóide) completamente e fracamente ordenado, S um *screen* simétrico de R, $\bigtriangledown : \mathrm{R} \rightarrow \mathrm{S}$ e $\bigtriangleup : \mathrm{R} \rightarrow \mathrm{S}$ os arredondamentos monótonos direcionados para baixo e para cima, respectivamente. Então para todo $a \in \mathrm{R}$,

$$\bigtriangledown a = - \bigtriangleup (-a)$$

$$\bigtriangleup a = - \bigtriangledown (-a)$$

O teorema anterior mosta que os arredondamentos $\bigtriangledown$ e $\bigtriangleup$ são interdependentes e não anti-simétricos; apenas a implementação de um deles é necessária quando ambos devem ser implementados.

Exemplo 3.2.6 Se S(10,3,−3,3) e a=2.316; tem-se que:

$$\bigtriangleup a = 2.32, \ \bigtriangleup(-a) = \bigtriangleup(-2.316) = -2.31$$

$$\bigtriangledown a = 2.31, \ \bigtriangledown(-a) = \bigtriangledown(-2.316) = -2.32$$

$$\bigtriangledown a = \bigtriangledown 2.316 = 2.31 = -(-2.31) = - \bigtriangleup (-a)$$

$$\bigtriangleup a = \bigtriangleup 2.316 = 2.32 = -(-2.32) = - \bigtriangledown (-a)$$

O lema a seguir define as características algébricas e de ordem do *screen* quando a aritmética é definida por semimorfismo.

Lema 3.2.7 Seja $\langle \mathrm{R}, \leq\rangle$ um reticulado completo, $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}\rangle$ um anelóide, $\langle \mathrm{S}, \leq\rangle$ um *screen* simétrico inferior(superior) ou *screen* simétrico de $\langle \mathrm{R}, \leq\rangle$ e $\Box : \mathrm{R} \rightarrow \mathrm{S}$ um semimorfismo. Então,

(a) $\forall a, b, c, d \in \mathrm{S}$ e $* \in \{+, \cdot\}$ tem-se que

(a1) (**RG1**) $\quad a \boxast b = a * b$
(a2) (**RG2**) $\quad a * b \leq c * d \Rightarrow a \boxast b \leq c \boxast d$
(a3) $-a = (-\mathbb{1}) \boxdot a$ (12)

(b) $\langle \mathrm{S}, \boxplus, \boxdot\rangle$ tem as seguintes propriedades:

(b1) $a \boxplus \mathbb{0} = \mathbb{0} \boxplus a = a, \ \forall a \in \mathrm{S}$
(b2) $a \boxdot \mathbb{1} = \mathbb{1} \boxdot a = a, \ \forall a \in \mathrm{S}$
(b3) $a \boxdot \mathbb{0} = \mathbb{0} \boxdot a = \mathbb{0}$

(b51) $(-\mathbb{1}) \boxplus \mathbb{1} = \mathbb{0}$
(b52) $(-\mathbb{1}) \boxdot (-\mathbb{1}) = \mathbb{1}$
(b53) $(-\mathbb{1}) \boxdot (a \boxdot b) = ((-\mathbb{1}) \boxdot a) \boxdot b = a \boxdot ((-\mathbb{1}) \boxdot b), \ \forall a, b \in \mathrm{S}$
(b54) $(-\mathbb{1}) \boxdot (a \boxplus \mathrm{b}) = ((-\mathbb{1}) \boxdot a) \boxplus ((-\mathbb{1}) \boxdot b), \ \forall a, b \in \mathrm{S}$

(c) Se $\langle \mathrm{S}, \boxplus, \boxdot \rangle$ é um anelóide, então (**RG**), (**RG1**), (**RG2**) são válidas para a subtração e (12) estabelece a identidade do operador $-$(menos) em R e S.

(d) Se $\square$ é direcionado para baixo, estão $\forall a, b \in$S,

(**RG3L**) $\qquad a \boxed{*} b \leq a * b$

e se é direcionado para cima, então

(**RG3U**) $\qquad a * b \leq a \boxed{*} b$

(e) Se $\langle \mathrm{S}, \boxplus, \boxdot \rangle$ é um anelóide então (**RG3L**) e (**RG3U**) são válidas para a subtração.

(f) Se $\langle \mathrm{R}, +, \cdot, \leq \rangle$ é um anelóide fracamente ordenado, então em $\langle \mathrm{S}, \boxplus, \boxdot, \leq \rangle$ também vale que, para todo $a, b, c \in \mathrm{S}$,

$$a \leq b \Rightarrow a \boxplus c \leq b \boxplus c \tag{13}$$

$$a \leq b \Rightarrow (-\mathbb{1})\, b \leq (-\mathbb{1}) a \tag{14}$$

(g) Se $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq \rangle$ é um anelóide ordenado, então em $\langle \mathrm{S}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1}, \leq \rangle$ além de (13) e (14) também é verdade que $\forall a, b, c \in \mathrm{S}$, se $\mathbb{0} \leq a \leq b$ e $c \geq \mathbb{0}$ então

$$a \boxdot c \leq b \boxdot c \ \text{ e } \ c \boxdot a \leq c \boxdot b \tag{15}$$

Demonstração.

(a) **(a1)** $a \boxed{*} b \overset{(RG)}{=} \square(a * b) \overset{(R1)}{=} a * b$

(a2) $a \boxed{*} b \overset{(RG),(R1)}{=} a * b \leq c * d \overset{(RG),(R1)}{=} c \boxed{*} d$

(a3) $(-\mathbb{1}) \boxed{*} a \overset{(RG)}{=} \square((-\mathbb{1}) \cdot a) = \square(-a) \overset{(R4)}{=} -\square a \overset{(R1)}{=} -a \in \mathrm{S}$, por (**S3**)

(b) Como, por hipótese, $\square$ é um semimorfismo, $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1} \rangle$ é um anelóide e $\langle \mathrm{S}, \leq \rangle$ é um *screen* simétrico de $\langle \mathrm{R}, \leq \rangle$ então as propriedades de (b1), (b2), (b3), (b5.1) e (b5.2) são facilmente demonstradas bastando usar (**RG**).

(c) $a \boxminus b = a \boxplus (-b) = \square(a + (-b)) = \square(a - b) = a - b$

$a \boxminus b = a - b \leq c - d = c \boxminus d$

(d)/(e) Se $\square$ é direcionado para baixo então

$\Box(a * b) \leq a * b,\ \forall a, b \in \mathrm{R}$ e $* \in \{+, -, \cdot\}$

Mas $\Box(a * b) = a \boxast b$ por (**RG**), então $a \boxast b \leq a * b$.

De modo dual no caso do arredondamento ser direcionado para cima.

(f)/(g) $a \leq b \Rightarrow a + c \leq b + c \overset{(\mathbf{RG1})}{\Rightarrow} a \boxplus c \leq b \boxplus c$

De forma similar (14) e (15). ■

O lema a seguir refere-se a anelóides divisão; sua prova é similar à do lema 3.2.7.

Lema 3.2.8 Seja $\langle \mathrm{R}, \leq \rangle$ um reticulado completo, $\langle \mathrm{R}, \mathrm{N}, +, \cdot, / \rangle$ um anelóide divisão onde N é tal que $\mathbb{0} \in \mathrm{N}$. Seja $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico inferior (superior) ou um *screen* simétrico de $\langle \mathrm{R}, \leq \rangle$ e $\Box : \mathrm{R} \rightarrow \mathrm{S}$ um semimorfismo. Então são válidas (a)-(f) do lema anterior considerando $\langle \mathrm{R}, \mathrm{N}, +, \cdot, /, \leq \rangle$, $\langle \mathrm{S}, \mathrm{S} \cap \mathrm{N}, \boxplus, \boxdot, \boxslash, \leq \rangle$ e $* \in \{+, \cdot, /\}$, onde necessário.

É importante compreender o significado dos lemas 3.2.7 e 3.2.8; estes mostram que a estrutura algébrica do *screen* simétrico (S) é a mesma do anelóide (reticulado completo R) quando as operações aritméticas em S são definidas através das operações aritméticas em R por meio do semimorfismo $\Box : \mathrm{R} \rightarrow \mathrm{S}$. Neste sentido anelóides são invariantes com respeito a semimorfismos. Adicionalmente, as propriedades (**S3**), (**RG**), (**R1**), (**R2**) e (**R4**) foram fundamentais na prova de ambos. Se estas propriedades são mudadas e/ou não implementadas, a estrutura algébrica no *screen* é diferente ou não descritível [KM79, KM81].

Definição 3.2.9 Seja $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1} \rangle$ um anelóide, $\langle \mathrm{R}, \leq \rangle$ um reticulado completo e $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico inferior (superior) ou *screen* simétrico de $\langle \mathrm{R}, \leq \rangle$.

(a) $\langle \mathrm{S}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1} \rangle$ é um *screen anelóide* se

(**RG1**)	$a * b \in \mathrm{S} \Rightarrow a \boxast b = a * b,\ \forall a, b \in \mathrm{S}$ e $* \in \{+, -, \cdot\}$
(**RG4**)	$-a = \boxminus a,\ \forall a \in \mathrm{S}$

(b) $\langle \mathrm{S}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1} \rangle$ é um *screen anelóide monótono* se

(**RG2**) $a * b \leq c * d \Rightarrow a \boxast b \leq c \boxast d,\ \forall a, b, c, d \in \mathrm{S}$ e $* \in \{+, -, \cdot\}$

(c) $\langle \mathrm{S}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1} \rangle$ é um *screen anelóide inferior* se

(**RG3L**) $a \boxast b \leq a * b,\ \forall a, b \in \mathrm{S}$ e $* \in \{+, -, \cdot\}$

(d) $\langle \mathrm{S}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1} \rangle$ é um *screen anelóide superior* se

(**RG3U**) $a * b \leq a \boxast b,\ \forall a, b \in \mathrm{S}$ e $* \in \{+, -, \cdot\}$

Definição 3.2.10 Seja $\langle \mathrm{R}, \mathrm{N}, +, \cdot, /, \mathbb{0}, \mathbb{1} \rangle$ um anelóide divisão, $\langle \mathrm{R}, \leq \rangle$ um reticulado completo e $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico inferior (superior) ou *screen* simétrico de $\langle \mathrm{R}, \leq \rangle$.

(a) $\langle S, \mathrm{S}\cap\mathrm{N}, \boxplus, \boxdot, \boxslash, \mathbb{0}, \mathbb{1}\rangle$ é um *screen anelóide divisão* se

$$(\mathbf{RG3}) \qquad a/b \in \mathrm{S} \Rightarrow a \boxslash b = a/b,\ \forall a \in \mathrm{S} \text{ e } b \in \mathrm{S} - \mathrm{S}\cap\mathrm{N}$$

(b) $\langle \mathrm{S}, \mathrm{S}\cap\mathrm{N}, \boxplus, \boxdot, \boxslash, \mathbb{0}, \mathbb{1}\rangle$ é um *screen anelóide divisão monótono* se

$$(\mathbf{RG2}) \qquad a/b \leq c/d \Rightarrow a \boxslash b \leq c \boxslash d,\ \ \forall a, c \in \mathrm{S} \text{ e } b, d \in \mathrm{S} - \mathrm{S}\cap\mathrm{N}$$

(c) $\langle \mathrm{S}, \mathrm{S}\cap\mathrm{N}, \boxplus, \boxdot, \boxslash, \mathbb{0}, \mathbb{1}\rangle$ é um *screen anelóide divisão inferior* se

$$(\mathbf{RG3L}) \qquad a \boxslash b \leq a/b,\ \forall a \in \mathrm{S} \text{ e } b \in \mathrm{S}-\mathrm{S}\cap\mathrm{N}$$

(d) $\langle \mathrm{S}, \mathrm{S}\cap\mathrm{N}, \boxplus, \boxdot, \boxslash, \mathbb{0}, \mathbb{1}\rangle$ é um *screen anelóide divisão superior* se

$$(\mathbf{RG3U}) \qquad a/b \leq a \boxslash b,\ \forall a \in \mathrm{S} \text{ e } b \in \mathrm{S} - \mathrm{S}\cap\mathrm{N}$$

Existem definições similares às 3.2.9 ou 3.2.10 para vetóides.

Se o anelóide é linearmente ordenado, o teorema A.6.6 e o lema 3.2.7 são usados para se obter o seguinte teorema.

Teorema 3.2.11 Seja $\langle \mathrm{R}, +, \cdot, \leq, \mathbb{0}, \mathbb{1}\rangle$ um anelóide completamente e totalmente ordenado, $\langle \mathrm{S}, \leq\rangle$ um *screen* simétrico de $\langle \mathrm{R}, \leq\rangle$ e $\square : \mathrm{R} \to \mathrm{S}$ um semimorfismo. Então $\langle \mathrm{S}, \boxplus, \boxdot, \leq, \mathbb{0}, \mathbb{1}\rangle$ é um *screen* anelóide monótono completamente e totalmente ordenado.

A importância deste teorema pode ser compreendida através do seguinte fato. Se $\mathrm{R}=\mathbb{R}$, $\mathrm{D}\supseteq\mathrm{S}$ é o conjunto de números de ponto flutuante de precisão estendida e $\square : \mathbb{R} \to \mathrm{D}$ é um semimorfismo, então $\langle \mathrm{D}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ terá as mesmas propriedades algébricas e de ordem de $\langle \mathbb{R}, +, \cdot, \mathbb{0}, \mathbb{1} \leq\rangle$. Considerando agora $\langle \mathrm{D}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1}, \leq\rangle$, $\mathrm{S}\subseteq\mathrm{D}$ pontos flutuantes de precisão simples e $\square : \mathrm{D} \to \mathrm{S}$, então $\langle \mathrm{S}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ terá as mesmas propriedades algébricas e de ordem de $\langle \mathrm{D}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1}, \leq\rangle$, isto é,

$\langle \mathbb{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ anelóide completamente e totalmente ordenado	$\overset{semimorfismo}{\overset{\square}{\to}}$	$\langle \mathrm{D}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ *screen* anelóide monótono completamente e totalmente ordenado	$\overset{semimorfismo}{\overset{\square}{\to}}$	$\langle \mathrm{S}, \boxplus, \boxdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ *screen* anelóide monótono completamente e totalmente ordenado

Figura 3.4: Transformações Garantidas por Semimorfismo

3.2.2 O Método Horizontal de Definição da Aritmética em Computadores

Segundo Kulisch e Miranker [KM79, KM81] basicamente há dois métodos de definição da aritmética em computadores:

- Método Vertical. Assume-se que a aritmética é definida de alguma forma em cada conjunto da primeira linha da Figura 3.1.

$$\begin{array}{ccccc} \mathbb{R} & \rightarrow & D & \rightarrow & S \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{C} & & \mathbb{C}\mathrm{D} & & \mathbb{C}\mathrm{S} \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{M}\mathbb{C} & & \mathrm{M}\mathbb{C}\mathrm{D} & & \mathrm{M}\mathbb{C}\mathrm{S} \end{array}$$

Figura 3.5: Definição Vertical da Aritmética

Neste método as operações em M$\mathbb{C}$D e M$\mathbb{C}$S são definidas através das operações em D e S e as fórmulas usuais para a aritmética de matrizes de complexos. Na maioria dos computadores este é o método de adição e multiplicação para matrizes de ponto flutuante.

- Método Horizontal. O método horizontal de definição das operações aritméticas em computadores [KM79, KM81] é aquele que faz uso do conceito de semimorfismo. O sentido de definição das operações aritméticas é,

$$\begin{array}{ccccc} \mathbb{R} & \rightarrow & D & \rightarrow & S \\ \downarrow & & & & \\ \mathbb{C} & \rightarrow & \mathbb{C}D & \rightarrow & \mathbb{C}S \\ \downarrow & & & & \\ M\mathbb{C} & \rightarrow & M\mathbb{C}D & \rightarrow & M\mathbb{C}S \end{array}$$

Figura 3.6: Definição Horizontal da Aritmética

A fórmula básica para a definição do método horizontal é (**RG**) [Grü80]. Para a implementação de (**RG**), quando $a * b$ não é representável, este é substituído por um valor aproximado $a\tilde{*}b$ tal que

$$a \boxast b = \square(a * b) = \square(a\tilde{*}b).$$

As operações definidas por (**RG**) e um arredondamento com as propriedades (**R1**)-(**R3L**) ou (**R3U**) produzem resultados de exatidão máxima em um sentido que é dependente do arredondamento [KM86]. Tomando como exemplo o conjunto dos reais, $\mathbb{R}$, e o *screen* S, entre um valor correto $x * y \in \mathbb{R}$ e uma sua aproximação $x \boxast y \in$ S, nenhum outro valor no *screen* é encontrado. Isto é justificado pelo seguinte. Dados $s_1, s_2 \in$ S, s_1 e s_2 consecutivos e

$$s_1 \leq x * y \leq s_2$$

$$\text{por } (\mathbf{R2}),\ \ \square s_1 \leq \square(x * y) \leq \square s_2$$

$$\text{por } (\mathbf{R1}),\ s_1 \leq \square(x * y) \leq s_2$$

$$\text{por } (\mathbf{RG}),\ s_1 \leq x \boxast y \leq s_2$$

Donde,

$$x \boxast y = s_1 \text{ ou } x \boxast y = s_2$$

Os resultados que conduzem ao método horizontal de definição da aritmética basicamente mostram a invariância na estrutura algébrica e a preservação da ordem com respeito aos espaços nas linhas da Figura 3.1, quando são usados semimorfismos.

Teorema 3.2.12 Seja $\langle \mathrm{R}, \leq \rangle$ um reticulado completo, $\langle \mathrm{R}, +, \cdot \rangle$ um anelóide, $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico inferior (superior) ou um *screen* simétrico de $\langle \mathrm{R}, \leq \rangle$ e $\square : \mathrm{R} \rightarrow \mathrm{S}$ um arredondamento anti-simétrico e monótono. Sejam os espaços produto $\mathrm{V}_n\mathrm{R}{=}\mathrm{R}{\times}\mathrm{R}{\times} \cdots {\times}\mathrm{R}$ e $\mathrm{V}_n\mathrm{S}{=}\mathrm{S}{\times}\mathrm{S}{\times} \cdots {\times}\mathrm{S}$ tal que $\mathrm{V}_n\mathrm{S} \subseteq \mathrm{V}_n\mathrm{R}$. Então

(a) $\langle \mathrm{V}_n\mathrm{R}, \leq \rangle$ é um reticulado completo se a relação de ordem é definida componente a componente.

(b) $\langle \mathrm{V}_n\mathrm{S}, \leq \rangle$ é um *screen* simétrico inferior (superior) ou, um *screen* simétrico de $\langle \mathrm{V}_n\mathrm{R}, \leq \rangle$.

(c) Seja o mapeamento

$$\square_n : \mathrm{V}_n\mathrm{R} \rightarrow \mathrm{V}_n\mathrm{S}$$

definido $\forall \alpha = (a_1, a_2, \cdots, a_n) \in \mathrm{V}_n\mathrm{R}$ por,

$$\square_n \alpha = \begin{pmatrix} \square a_1 \\ \square a_2 \\ \cdots \\ \square a_n \end{pmatrix}$$

Então $\square_n$ é um arredondamento anti-simétrico e monótono.

Demonstração.

(a) $\langle \mathrm{R}, \leq \rangle$ é um reticulado completo por hipótese; o produto de reticulados completos é um reticulado completo, logo $\langle \mathrm{V}_n\mathrm{R}, \leq \rangle$ é um reticulado completo.

(b) $\langle \mathrm{S}, \leq \rangle$, $\mathrm{S} \subseteq \mathrm{R}$ é um reticulado completo, logo $\langle \mathrm{V}_n\mathrm{S}, \leq \rangle$ é um reticulado completo. Como por hipótese $\langle \mathrm{S}, \leq \rangle$ é um *screen* de $\langle \mathrm{R}, \leq \rangle$, supremos em S coincidem com supremos em R, portanto o vetor de supremos tomado em $\mathrm{V}_n\mathrm{S}$ é igual ao vetor de supremos em $\mathrm{V}_n\mathrm{R}$. Como $\langle \mathrm{S}, \leq \rangle$ é um *screen* simétrico, os vetores $\underline{\mathbb{0}}$, $\underline{\mathbb{1}} \in V_n\mathrm{S}$ e $\forall \alpha \in \mathrm{V}_n\mathrm{S}$, $-\alpha \in \mathrm{V}_n\mathrm{S}$, o que implica ser $\langle \mathrm{V}_n\mathrm{S}, \leq \rangle$ um *screen* simétrico de $\langle \mathrm{V}_n\mathrm{R}, \leq \rangle$.

(c) $\square : \mathrm{R} \rightarrow \mathrm{S}$ é definida componente a componente, logo $\square_n{:}\mathrm{V}_n\mathrm{R} \rightarrow \mathrm{V}_n\mathrm{S}$ satisfaz (**R1**), (**R2**) e (**R4**). Assim $\square_n$ é anti-simétrico e monótono. ■

Desde que a relação de ordem e o arredondamento sejam definidos convenientemente, o teorema anterior permanece válido trocando vetores por matrizes.

Os seguintes dois teoremas definem a aritmética por meio de semimorfismo nos conjuntos das segunda, terceira e quarta colunas da Figura 3.1.

Teorema 3.2.13 Seja $\langle \mathrm{R}, +, \cdot, \leq \rangle$ um anelóide, $\langle \mathrm{R}, \leq \rangle$ um reticulado completo, $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico de $\langle \mathrm{R}, \leq \rangle$. Seja também $\langle \mathrm{S}, \boxplus, \boxdot, \leq \rangle$ o anelóide definido por um semimorfismo $\square : \mathrm{R} \to \mathrm{S}$ e $\langle \mathrm{M}_n\mathrm{R}, +, \cdot, \leq \rangle$ o anelóide das matrizes $n \times n$ sobre R. As operações aritméticas em $\mathrm{M}_n\mathrm{S}$ são especificadas pelo semimorfismo $\square : \mathrm{M}_n\mathrm{R} \to \mathrm{M}_n\mathrm{S}$ definido por

$$\square \mathrm{A} = (\square a_{ij}), \forall \mathrm{A} = (a_{ij}) \in \mathrm{M}_n\mathrm{R}$$

onde

(**RG**) $$\mathrm{A} \boxast \mathrm{B} = \square(\mathrm{A} * \mathrm{B}),\ \forall \mathrm{A},\mathrm{B} \in \mathrm{M}_n\mathrm{S} \text{ e } * \in \{+, \cdot\}$$

Então

(a) $\langle \mathrm{M}_n\mathrm{S}, \boxplus, \boxdot, \leq \rangle$ é um *screen* anelóide monótono de $\langle \mathrm{M}_n\mathrm{R}, +, \cdot, \leq \rangle$.

(b) Se o arredondamento $\square : \mathrm{R} \to \mathrm{S}$ é direcionado para cima então $\langle \mathrm{M}_n\mathrm{S}, \boxplus, \boxdot, \leq \rangle$ é um *screen* anelóide superior; se o arredondamento é direcionado para baixo então $\langle \mathrm{M}_n\mathrm{S}, \boxplus, \boxdot, \leq \rangle$ é um *screen* anelóide inferior.

(c) Se $\langle \mathrm{R}, +, \cdot, \leq \rangle$ é um anelóide fracamente ordenado então $\langle \mathrm{M}_n\mathrm{S}, \boxplus, \boxdot, \leq \rangle$ é um *screen* anelóide fracamente ordenado de $\langle \mathrm{M}_n\mathrm{R}, +, \cdot, \leq \rangle$; se $\langle \mathrm{R}, +, \cdot, \leq \rangle$ é um anelóide ordenado então $\langle \mathrm{M}_n\mathrm{S}, \boxplus, \boxdot, \leq \rangle$ é um anelóide ordenado de $\langle \mathrm{M}_n\mathrm{R}, +, \cdot, \leq \rangle$.

Demonstração.

(a) Usar o lema 3.2.7 (b) e (c), o teorema 3.2.12 e para provar ($\mathrm{P6}_{\mathrm{ALD}}$) da definição A.6.1 ver [KM79, KM81].

(b) Usar o lema 3.2.7 (d).

(c) Usar o lema 3.2.7 (f) e (g).

Exemplo 3.2.14 Este exemplo ilustra semimorfismo no caso do espaço das matrizes 2×2. Sejam

$$\mathrm{M}_2\mathbb{R} = \{\mathrm{A} = (a_{ij}) \mid a_{ij} \in \mathbb{R}\}$$
$$\mathrm{M}_2\mathrm{S} = \{\mathrm{A} = (a_{ij}) \mid a_{ij} \in \mathrm{S}\}$$
$$\square : \mathrm{M}_2\mathbb{R} \to \mathrm{M}_2\mathrm{S}$$
$$\square \mathrm{A} = (\square a_{ij}),\ \forall \mathrm{A} \in \mathrm{M}_2\mathbb{R}$$
$$\mathrm{A} \boxplus \mathrm{B} = \square(\mathrm{A}+\mathrm{B})$$

onde + é uma operação em $\mathrm{M}_2\mathbb{R}$ e $\boxplus$, em $\mathrm{M}_2\mathrm{S}$. Sejam A,B $\in M_2\mathbb{R}$ tais que

$$\mathrm{A} = \begin{pmatrix} e & \pi \\ 7 & \sqrt[2]{3} \end{pmatrix}$$

$$\mathrm{B} = \begin{pmatrix} \sqrt[2]{5} & 2 \\ 3.16 & \sqrt[2]{11} \end{pmatrix}$$

Então

$$
\begin{aligned}
A + B &= \begin{pmatrix} e + \sqrt[2]{5} & \pi + 2 \\ 7 + 3.16 & \sqrt[2]{3} + \sqrt[2]{11} \end{pmatrix} \\
A \boxplus B &= \square \begin{pmatrix} e + \sqrt[2]{5} & \pi + 2 \\ 7 + 3.16 & \sqrt[2]{3} + \sqrt[2]{11} \end{pmatrix} \\
&= \begin{pmatrix} \square(e + \sqrt[2]{5}) & \square(\pi + 2) \\ \square(10.16) & \square(\sqrt[2]{3} + \sqrt[2]{11}) \end{pmatrix}
\end{aligned}
$$

O teorema anterior mostrou um *screen* e suas propriedades para o anelóide das matrizes $n \times n$ obtido através de operações aritméticas definidas por semimorfismo. O teorema a seguir tem objetivos similares ao anterior mas envolvendo complexos.

Teorema 3.2.15 Seja $\langle \mathrm{R}, +, \cdot \rangle$ um anelóide, $\langle \mathrm{R}, \leq \rangle$ um reticulado completo, $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico de $\langle \mathrm{R}, \leq \rangle$ e $\langle \mathrm{S}, \boxplus, \boxdot \rangle$ um anelóide definido pelo semimorfismo $\square : \mathrm{R} \to \mathrm{S}$. Seja $\langle \mathrm{CR}, +, \cdot \rangle$ o anelóide de pares (a, b) sobre R e as operações em CS especificadas pelo semimorfismo $\square : \mathrm{CR} \to \mathrm{CS}$ definido por

$$\square\alpha = (\square a_1, \square a_2), \ \forall \alpha = (a_1, a_2) \in \mathrm{CR}$$

e

(RG) $$\alpha \boxast \beta = \square(\alpha * \beta), \ \forall \alpha, \beta \in \mathrm{CS} \text{ e } * \in \{+, \cdot\}$$

Então,

(a) $\langle \mathrm{CS}, \boxplus, \boxdot \rangle$ é um *screen* anelóide monótono de $\langle \mathrm{CR}, +, \cdot \rangle$.

(b) Se o arredondamento $\square : \mathrm{R} \to \mathrm{S}$ é direcionado para cima, então $\langle \mathrm{CS}, \boxplus, \boxdot \rangle$ é um anelóide *screen* superior de $\langle \mathrm{CR}, +, \cdot \rangle$; se o arredondamento é direcionado para baixo, então $\langle \mathrm{CS}, \boxplus, \boxdot \rangle$ é um *screen* inferior.

(c) Se $\langle \mathrm{R}, +, \cdot, \leq \rangle$ é um anelóide fracamente ordenado então $\langle \mathrm{CS}, \boxplus, \boxdot, \leq \rangle$ é um *screen* anelóide fracamente ordenado de $\langle \mathrm{CR}, +, \cdot, \leq \rangle$.

(d) Sejam $\langle \mathrm{R}, \mathrm{N}, +, \cdot, / \rangle$, $\langle \mathrm{CR}, \overline{N}, +, \cdot, \leq \rangle$ onde $\overline{\mathrm{N}} = \{(c_1, c_2) \in \mathrm{CR} \mid c_1 c_1 + c_2 c_2 \in \mathrm{N}\}$ e $\langle \mathrm{S}, \mathrm{S} \cap \mathrm{N}, \boxplus, \boxdot, \boxslash \rangle$ o anelóide divisão definido pelo semimorfismo $\square : \mathrm{R} \to \mathrm{S}$. Se a divisão por um elemento $\beta \in$CS é definida pelo semimorfismo (RG), onde $\beta \notin \overline{N} \cap$CS, então $\langle \mathrm{CS}, \overline{N} \cap \mathrm{CS}, \boxplus, \boxdot, \boxslash \rangle$ é um *screen* anelóide divisão monótono de $\langle \mathrm{CR}, +, \cdot, \leq \rangle$.

Demonstração.

(a) Usando o teorema 3.2.12, por (b) $\langle \mathrm{CS}, \leq \rangle$ é um *screen* simétrico de $\langle \mathrm{CR}, \leq \rangle$ e por (c) $\square : \mathrm{CM} \to \mathrm{CS}$ é um arredondamento anti-simétrico e monótono. Usando o lema 3.2.7, por (a) e (b) provam-se as propriedades P1-P5 da definição de anelóide (definição A.6.1) e por (c) prova-se (RG1), (RG2) e (RG4). Para provar (P6) da definição A.6.1, [KM79, KM81].

(b) Usar o lema 3.2.7 (d).

(c) Usar o lema 3.2.7 (f) e (g).

(d) Usar o lema 3.2.8. ■

Sejam $\mathbb{R}$, D e S, respectivamente, os conjuntos dos reais, dos pontos flutuantes de precisão dupla (D) e simples (S); considerando também os espaços das matrizes quadradas formadas de elementos de cada um desses espaços, $M_n\mathbb{R}$, M_nD e M_nS. O teorema 3.2.13 garante as seguintes passagens:

$$M_n\mathbb{R} \to M_nD$$
$$M_n\mathbb{R} \to M_nS$$

Porém o problema é como definir a função abaixo.

$$M_nD \to M_nS$$

De modo geral isto é visto a seguir.

Seja um arredondamento anti-simétrico e monótono

$$\Diamond : D \to S$$

e o semimorfismo

$$\Diamond : M_nD \to M_nS$$

definido por

$$\Diamond A = (\Diamond a_{ij}),\ \forall A = (a_{ij}) \in M_nD$$

e

$$A \mathbin{\Diamond\!\!\!\!\ast} B = \Diamond(A \boxast B),\ \forall A,B \in M_nS \text{ e } \ast \in \{+,\cdot\}.$$

Tomando a composição

(RG) $\quad \Diamond \circ \Box : R \to S$

esta composição é também um arredondamento direcionado anti-simétrico e monótono; seja então o semimorfismo

$$\Diamond \circ \Box : M_nR \to M_nS$$

tal que

(RG) $\quad A \mathbin{\Diamond\!\!\!\!\ast} B = \Diamond(\Box(A \ast B)),\ \forall A,B \in M_nR \ \text{ e } \ast \in \{+,\cdot\}$

Então $\langle M_nS, \mathbin{\Diamond\!\!\!\!+}, \mathbin{\Diamond\!\!\!\!\cdot}, \leq\rangle$ é um anelóide satisfazendo todas as propriedades do lema 3.2.7.

Qual a importância desse fato? Supondo que cálculos intermediários estejam sendo efetuados em precisão dupla e que resultados sejam exibidos em precisão simples, tem-se então como fazer essas passagens e se manter similar estrutura algébrica.

Essas considerações valem não somente para os espaços em questão, mas também para transformações em outros casos tais como

$$\mathrm{CD} \to \mathrm{CS}$$

A Figura 3.7 a seguir sumariza os resultados que justificam as transformações entre alguns dos espaços da computação numérica quando estas transformações são fundamentadas no conceito de semimorfismo.

$\mathbb{R}$	$\xrightarrow{T3.2.11}$	D	$\xrightarrow{T3.2.11}$	S
$V\mathbb{R}$	$\xrightarrow{T3.2.13}$	VD	$\xrightarrow{L3.2.7}$	VS
$M\mathbb{R}$	$\xrightarrow{T3.2.13}$	MD	$\xrightarrow{L3.2.7}$	MS
$\mathbb{C}$	$\xrightarrow{T3.2.15}$	$\mathbb{C}$D	$\xrightarrow{L3.2.8}$	$\mathbb{C}$S
$V\mathbb{C}$	$\xrightarrow{T3.2.13}$	$V\mathbb{C}$D	$\xrightarrow{L3.2.7}$	$V\mathbb{C}$S
$M\mathbb{C}$	$\xrightarrow{T3.2.13}$	$M\mathbb{C}$D	$\xrightarrow{L3.2.7}$	$M\mathbb{C}$S

Figura 3.7: Transformações Justificadas por Semimorfismos

A aritmética de exatidão máxima definida através de semimorfismo não prescinde de um cálculo exato do *produto interno* ou *produto escalar*. Uma tradicional computação do produto interno de dois vetores $\mathbf{x}$ e $\mathbf{y}$, cada um com n componentes, em aritmética de ponto flutuante usual, envolve $(2n-1)$ arredondamentos o que pode levar a um cancelamento catastrófico de dígitos significantes. Ao lado da perda de exatidão, um considerável acúmulo de tempo de processamento pode ser requerido para realizar operações intermediárias como composição, decomposição, normalização, etc. Adicionalmente, operações de *load* e *store* podem ter de ser feitas desnecessariamente. Por estas razões, nos últimos anos vários algoritmos sobre o assunto têm sido propostos e analisados [Sil87, BG83] de modo que se tenha a garantia de exatidão máxima na implementação do produto escalar. De modo geral dados dois vetores $\mathbf{x}$ e $\mathbf{y}$ cada um com n componentes de ponto flutuante e um modo de arredondamento $\square$, o resultado, s, de uma operação de produto escalar é:

$$s = \square(\tilde{s}) = \square(\mathbf{x} \cdot \mathbf{y}) = \square(\sum_{i=1}^{n}(x_i \cdot y_i)), \quad n \geq 1.$$

onde todas as operações são realizadas com exatidão máxima, de acordo com a definição de semimorfismo. O valor $\tilde{s}$ é um valor intermediário com uma precisão infinita.

3.3 Aritmética Intervalar

Nesta seção o conceito de semimorfismo é estendido aos espaços cujos elementos são intervalos; isto significa que a aritmética computacional proposta por [KM79, KM81], denominada de método horizontal, agora estará definida para todos os espaços da Figura 3.1. Para os conjuntos intervalos da Figura 3.1 são fornecidas fórmulas explícitas para a computação do intervalo resultante em termos dos limites dos intervalos operandos.

Teorema 3.3.1 Se $\langle \mathrm{R}, \leq \rangle$ é um reticulado completo então $\langle \mathrm{IR}, \leq \rangle$ é um reticulado completo.

Demonstração. $\langle \mathrm{IR}, \leq \rangle$ é um conjunto ordenado, e $\mathrm{IR} \subseteq \mathrm{R} \times \mathrm{R}$. Portanto $\langle \mathrm{IR}, \leq \rangle$ é um reticulado completo, onde dado qualquer $\mathrm{S} \subseteq \mathrm{IR}$ e $\mathrm{A} = [a_1, a_2] \in \mathrm{S}$, tem-se que, respectivamente,

$$\inf \mathrm{S} = [\inf a_1, \inf a_2]$$

$$\sup \mathrm{S} = [\sup a_1, \sup a_2]$$

■

Exemplo 3.3.2 Seja $\langle \mathbb{R}, \leq \rangle$, $\mathbb{R}^\infty = \mathbb{R} \cup \{-\infty, +\infty\}$. Então $\langle \mathbb{R}^\infty, \leq \rangle$ é um reticulado completo. Considerando $\langle \mathrm{I}\mathbb{R}^\infty, \leq \rangle$ e $\mathrm{S} \subseteq \mathrm{I}\mathbb{R}^\infty$ tal que

$$\mathrm{S} = \{[1/2^n, 1] \mid n \geq 0\} = \{[1,1], [1/2, 1], [1/4, 1], \cdots\}$$

Logo,

$$\inf \mathrm{S} = [\inf\{1/2^n\}, \inf\{1\}] = [0, 1]$$

e

$$\sup \mathrm{S} = [\sup\{1/2^n\}, \sup\{1\}] = [1, 1].$$

Teorema 3.3.3 Se $\langle \mathrm{R}, \leq \rangle$ é um reticulado completo, então

(a) $\langle \mathrm{IR}, \subseteq \rangle$ é um reticulado completo. Dados $\mathrm{A} \subseteq \mathrm{IR}$, e $[b_1, b_2] \in \mathrm{B}$, tem-se que

$$\inf \mathrm{A}_{\mathrm{IR}} = \left[\begin{matrix} \sup b_1 \\ \mathrm{B} \in \mathrm{A} \end{matrix} \quad , \quad \begin{matrix} \inf b_2 \\ \mathrm{B} \in \mathrm{A} \end{matrix}\right]$$

$$\sup \mathrm{A}_{\mathrm{IR}} = \left[\begin{matrix} \inf b_1 \\ \mathrm{B} \in \mathrm{A} \end{matrix} \quad , \quad \begin{matrix} \sup b_2 \\ \mathrm{B} \in \mathrm{A} \end{matrix}\right]$$

(b) Seja $\overline{\mathrm{IR}} = \mathrm{IR} \cup \{\emptyset\}$. Então $\langle \overline{\mathrm{IR}}, \subseteq \rangle$ é um *screen* superior para $\langle \mathrm{PR}, \subseteq \rangle$.

Demonstração.

(a) Como por hipótese $\langle \mathrm{IR}, \subseteq \rangle$ é um reticulado completo, qualquer $\mathrm{A} \subseteq \mathrm{IR}$ tem supremo e ínfimo. Sejam os seguintes elementos de IR,

$$\mathrm{L} = \left[\begin{matrix} \sup b_1 \\ \mathrm{B} \in \mathrm{A} \end{matrix} \quad , \quad \begin{matrix} \inf b_2 \\ \mathrm{B} \in \mathrm{A} \end{matrix}\right]$$

$$\mathrm{U} = \left[\begin{matrix} \inf b_1 \\ B \in S \end{matrix} \quad , \quad \begin{matrix} \sup b_2 \\ B \in S \end{matrix}\right]$$

Para todo $\mathrm{B} \in \mathrm{A}$, $\sup b_{1_i} \geq b_1$ e $\inf b_{2_i} \leq b_2$ o que implica $\mathrm{L} \subseteq \mathrm{B}$. De forma similar conclui-se que $\mathrm{B} \subseteq \mathrm{U}$. Então L é uma cota inferior para A e U uma superior. Supondo L' e U' outras cotas para A, por construção, $\mathrm{L}' \subseteq \mathrm{L}$ e $\mathrm{U} \subseteq \mathrm{U}'$. Isto significa que L é a maior e U a menor das cotas inferiores e superiores, respectivamente, para A. Logo $\mathrm{L} = \inf_{\mathrm{IR}} \mathrm{A}$ e $\mathrm{U} = \sup_{\mathrm{IR}} \mathrm{A}$.

(b) Seja $\mathrm{A} \in \mathrm{PR}$ e $\mathrm{U(A)}$ o conjunto dos limites superiores de A. Tem-se que (i) $\mathrm{U(A)} \cap \overline{\mathrm{IR}} \neq \emptyset$ pois $\mathrm{U} \in \mathrm{U(A)} \cap \overline{\mathrm{IR}}$, U definido em (a); (ii) adicionalmente $\mathrm{U} \subseteq \mathrm{B}$ qualquer que seja $\mathrm{B} \in \mathrm{U(A)} \cup \overline{\mathrm{IR}}$. Logo $\langle \overline{\mathrm{IR}}, \subseteq \rangle$ é um *screen* superior para $\langle \mathrm{PR}, \subseteq \rangle$. ■

Exemplo 3.3.4 Considerando os dados do exemplo 3.3.2, mas agora $\langle \mathrm{IIR}^{\infty}, \subseteq \rangle$, tem-se que

$$\inf_{\mathrm{IIR}^{\infty}} \mathrm{S} = [\sup\{1/2^n\}, \inf\{1\}] = [1,1]$$

e

$$\sup_{\mathrm{IIR}^{\infty}} \mathrm{S} = [\inf\{1/2^n\}, \sup\{1\}] = [0,1]$$

Como $\langle \overline{\mathrm{IR}}, \subseteq \rangle$ é um *screen* superior para $\langle \mathrm{PR}, \subseteq \rangle$ [KM79, KM81] pode-se considerar o arredondamento monótono direcionado para cima

$$\square : \mathrm{PR} \to \overline{\mathrm{IR}} \tag{16}$$

definido pelas propriedades,

(**R1**)	$\square \mathrm{A} = \mathrm{A},\ \forall \mathrm{A} \in \overline{\mathrm{IR}}$
(**R2**)	$\mathrm{A} \subseteq \mathrm{B} \Rightarrow \square \mathrm{A} \subseteq \square \mathrm{B},\ \forall \mathrm{A,B} \in \mathrm{PR}$
(**R3**)	$\mathrm{A} \subseteq \square \mathrm{A},\ \forall \mathrm{A} \in \mathrm{PR}$

O teorema a seguir mostra propriedades deste arredondamento.

Teorema 3.3.5 Seja $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq \rangle$ um anelóide completamente e fracamente ordenado. Então,

(a) $\langle \overline{\mathrm{IR}}, \subseteq \rangle$ é um *screen* superior simétrico de $\langle \mathrm{PR}, +, \cdot, \subseteq \rangle$.

(b) (**R**) $$\square \mathrm{A} = \inf_{\overline{\mathrm{IR}}} (\mathrm{U(A)} \cap \overline{\mathrm{IR}}) = \begin{bmatrix} \inf a & , & \sup a \\ a \in \mathrm{A} & & a \in \mathrm{A} \end{bmatrix}, \forall \mathrm{A} \in \mathrm{PR}$$

(c) O arredondamento monótono direcionado para cima definido em (16) é um mapeamento anti-simétrico.

Demonstração.

(a) $\mathbb{0}, \mathbb{1} \in \mathrm{R} \Rightarrow$

$$[\mathbb{0}, \mathbb{0}],\ [\mathbb{1}, \mathbb{1}] \in \overline{\mathrm{IR}} \tag{17}$$

Seja $\mathrm{A}=[a_1, a_2] \in \mathrm{IR}$.

$$-\mathrm{A} = (-\mathbb{1}) \cdot \mathrm{A} = \{(-\mathbb{1}) \cdot x \mid x \in \mathrm{A}\} = \{x \mid -a_2 \leq x \leq -a_1\} \in \mathrm{IR} \tag{18}$$

Portanto, como $\overline{\mathrm{IR}}$ satisfaz (17) e (18), $\langle \overline{\mathrm{IR}}, \subseteq \rangle$ é um *screen* simétrico para $\langle \mathrm{PR}, \subseteq \rangle$.

(b) Pelo Teorema 3.1.8

$$\square \mathrm{A} = \inf_{\overline{\mathrm{IR}}} (\mathrm{U(A)} \cap \overline{\mathrm{IR}})$$

$\mathrm{A} \subseteq \begin{bmatrix} \inf a & , & \sup a \\ a \in \mathrm{A} & & a \in A \end{bmatrix}$. Seja $\mathrm{B}= [b_1, b_2] \in \mathrm{IR}$ tal que $\mathrm{A} \subseteq \mathrm{B}$.

Logo $b_1 \leq a \leq b_2,\ \forall a \in \mathrm{A}$ e portanto, $b_1 \leq \inf a_{a \in \mathrm{A}}$ e $\sup a_{a \in \mathrm{A}} \leq b_2$.

Então $\begin{bmatrix} \inf a & , & \sup a \\ a \in \mathrm{A} & & a \in \mathrm{A} \end{bmatrix} \subseteq [a_1, a_2]$, o que significa,

$$\begin{bmatrix} \inf a & , & \sup a \\ a \in \mathrm{A} & & a \in \mathrm{A} \end{bmatrix} = \inf_{\overline{\mathrm{IR}}}(\mathrm{U(A)} \cap \overline{\mathrm{IR}})$$

(c) $\square\mathrm{A} = \begin{bmatrix} \inf a & , & \sup a \\ a \in \mathrm{A} & & a \in \mathrm{A} \end{bmatrix} \Rightarrow -\square\mathrm{A} = \begin{bmatrix} -\sup a & , & -\inf a \\ a \in \mathrm{A} & & a \in \mathrm{A} \end{bmatrix}$

$\square(-\mathrm{A}) = \begin{bmatrix} -\sup a & , & -\inf a \\ a \in A & & a \in A \end{bmatrix} = -\square\mathrm{A}.$

Logo,

(**R4**) $\square(-\mathrm{A}) = -\square\mathrm{A},\ \forall \mathrm{A} \in \mathrm{PR}$ ■

Quais as condições para a proposição de um semimorfismo? Recapitulando: uma estrutura de anelóide (ou vetóide) com uma ordem que a torne um reticulado completo, um *screen* (superior ou inferior) simétrico e um mapeamento (arredondamento) entre o anelóide (vetóide) e o *screen* que defina as operações no *screen* e satisfaça algumas propriedades (projeção, monotonicidade, inclusão e anti-simetria). Então, considerando o arredondamento definido em (16),

$$\square : \mathrm{PR} \to \overline{\mathrm{IR}}$$

e para cada operação $*$ em PR, tem-se $\boxed{*}$ em $\overline{\mathrm{IR}}$ tal que

(**RG**) $\mathrm{A} \boxed{*} \mathrm{B} = \square(\mathrm{A} * \mathrm{B}) = [\inf(a * b), \sup(a * b)],\ \forall \mathrm{A,B} \in \overline{\mathrm{IR}}$

onde $\square$ satisfaz

(**R1**) $\square\mathrm{A} = \mathrm{A}, \forall \mathrm{A} \in \overline{\mathrm{IR}}$
(**R2**) $\mathrm{A} \subseteq \mathrm{B} \Rightarrow \square\mathrm{A} \subseteq \square\mathrm{B},\ \forall \mathrm{A,B} \in \mathrm{PR}$
(**R3**) $\mathrm{A} \subseteq \square\mathrm{A}, \forall \mathrm{A} \in \mathrm{PR}$
(**R4**) $\square(-\mathrm{A}) = -\square\mathrm{A}$

Portanto, $\square$ é um *semimorfismo.*

$\langle \mathrm{PR}, \subseteq \rangle$ é um reticulado completo, $\langle \overline{\mathrm{IR}}, \subseteq \rangle$ é um *screen* superior de $\langle \mathrm{PR}, \subseteq \rangle$, $\square$ é definido por (**RG**) e satisfaz (**R1**), (**R2**) e (**R3**) portanto, $\forall \mathrm{A,B,C,D} \in \overline{\mathrm{IR}}$, pelo teorema 3.1.15, $\langle \overline{\mathrm{IR}}, \boxed{*} \rangle$ tem as propriedades,

(**RG1**) $\mathrm{A}*\mathrm{B} \in \overline{\mathrm{IR}} \Rightarrow \mathrm{A} \boxed{*} \mathrm{B} = \mathrm{A}*\mathrm{B}$
(**RG2**) $\mathrm{A} * \mathrm{B} \subseteq \mathrm{C} * \mathrm{D} \Rightarrow \mathrm{A} \boxed{*} \mathrm{B} \subseteq \mathrm{C} \boxed{*} \mathrm{D}$
(**RG3**) $\mathrm{A} * \mathrm{B} \subseteq \mathrm{A} \boxed{*} \mathrm{B}$

No início desta seção, a hipótese básica sobre $\langle \mathrm{R}, \leq \rangle$ é que seja um conjunto ordenado. Nas operações aritméticas definidas no teorema a seguir todos os operandos são comparáveis com $[\mathbb{O},\mathbb{O}]$ com respeito a relação de ordem $\leq$. Este teorema mostra como as operações aritméticas no *screen* são definidas através do semimorfismo proposto anteriormente [KM79, KM81].

Teorema 3.3.6 Sejam $\langle \mathrm{R}, +, \cdot, \mathbb{O}, \mathbb{1}, \leq \rangle$ e $\langle \mathrm{R}, \mathrm{N}, +, \cdot, /, \mathbb{O}, \mathbb{1}, \leq \rangle$ anelóides completamente e fracamente ordenados. Se as operações aritméticas em IR são definidas pelo semimorfismo

$\square : \mathrm{PR} \to \overline{\mathrm{IR}}$ então $\langle \mathrm{IR}, \boxplus, \boxdot, [\mathbb{0},\mathbb{0}], [\mathbb{1},\mathbb{1}], \leq, \subseteq \rangle$ e $\langle \mathrm{IR}, \tilde{\mathrm{N}}, \boxplus, \boxdot, \boxslash, [\mathbb{0},\mathbb{0}], [\mathbb{1},\mathbb{1}], \leq, \subseteq \rangle$ com $\tilde{\mathrm{N}}=\{\mathrm{A} \in \mathrm{IR} \mid \mathrm{A} \cap \mathrm{N} \neq \emptyset\}$ tornam-se anelóides completamente e fracamente ordenados com respeito à relação de ordem $\leq$ e, dados A$= [a_1, a_2]$ e B$= [b_1, b_2]$ pertencentes a IR,

$\mathrm{A} \boxplus \mathrm{B}= [a_1 + b_1, a_2 + b_2]$
$\mathrm{A} \boxminus \mathrm{B} = \mathrm{A}+(-\mathrm{B})=[a_1 - b_2, a_2 - b_1]$

$$\mathrm{A} \boxdot \mathrm{B} = \begin{cases} [a_1b_1, a_2b_2], & \mathrm{A} \geq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathrm{B} \geq [\mathbb{0},\mathbb{0}] \\ [a_2b_2, a_1b_1], & \mathrm{A} \leq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathrm{B} \leq [\mathbb{0},\mathbb{0}] \\ [a_1b_2, a_2b_1], & \mathrm{A} \leq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathrm{B} \geq [\mathbb{0},\mathbb{0}] \\ [a_2b_1, a_1b_2], & \mathrm{A} \geq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathrm{B} \leq [\mathbb{0},\mathbb{0}] \end{cases}$$

Se $\mathrm{B} \in \mathrm{IR}-\tilde{\mathrm{N}}$,

$$\mathrm{A} \boxslash \mathrm{B} = \begin{cases} [a_1/b_2, a_2/b_1], & \mathrm{A} \geq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathrm{B} > [\mathbb{0},\mathbb{0}] \\ [a_2/b_2, a_1/b_1], & \mathrm{A} \geq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathrm{B} < [\mathbb{0},\mathbb{0}] \\ [a_1/b_1, a_2/b_2], & \mathrm{A} \leq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathrm{B} > [\mathbb{0},\mathbb{0}] \\ [a_2/b_1, a_1/b_2], & \mathrm{A} \leq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathrm{B} < [\mathbb{0},\mathbb{0}] \end{cases}$$

$\mathrm{A} \boxast \mathrm{B}$ é expresso em termos dos limites (inferior e superior) dos intervalos operandos. Adicionalmente, os intervalos são comparáveis com $[\mathbb{0},\mathbb{0}]$. A seguir será visto como são definidas as operações aritméticas quando os intervalos operandos são não-comparáveis com $[\mathbb{0},\mathbb{0}]$. O lema seguinte caracteriza intervalos não-comparáveis.

Lema 3.3.7 Seja $\langle \mathrm{R}, \leq \rangle$ um conjunto totalmente ordenado, IR o conjunto dos intervalos sobre R e $\langle \mathrm{IR}, \leq \rangle$. Sejam A$= [a_1, a_2]$ e B$= [b_1, b_2]$ elementos de IR. A e B são não-comparáveis com respeito à ordem $\leq$ se e só se

$$a_1 < b_1 \leq b_2 < a_2$$

ou

$$b_1 < a_1 \leq a_2 < b_2$$

Demonstração. Não é verdade que $[a_1, a_2] \leq [b_1, b_2]$, pois neste caso obrigatoriamente $a_1 \leq b_1$ e $a_2 \leq b_2$, o que é falso por hipótese. Da mesma forma, também não é verdade que $[b_1, b_2] \leq [a_1, a_2]$.
■

De acordo com o lema visto, A e B são intervalos não comparáveis com respeito à ordem $\leq$ se e só se $\mathrm{A} \subset \mathrm{B}$ ou $\mathrm{B} \subset \mathrm{A}$.

Pelo lema 3.3.7, os intervalos não-comparáveis com $[\mathbb{0},\mathbb{0}]$ correspondem àqueles onde $\mathbb{0}$ é um ponto no interior do intervalo. O teorema a seguir define as operações aritméticas $\boxdot$ e $\boxslash$ nestes casos. Os resultados para $\boxplus$ e $\boxminus$ são os mesmos uma vez que, para essas operações, não há necessidade de comparação entre os intervalos operandos.

Teorema 3.3.8 Seja $\langle \mathrm{R}, \mathrm{N}, +, \cdot, /, \mathbb{0}, \mathbb{1}, \leq \rangle$ um anelóide divisão completamente e totalmente ordenado e $\langle \mathrm{IR}, \tilde{\mathrm{N}}, \boxplus, \boxdot, \boxslash, [\mathbb{0},\mathbb{0}], [\mathbb{1},\mathbb{1}], \leq, \subseteq \rangle$, com $\tilde{\mathrm{N}}=\{\mathrm{A} \in \mathrm{IR} \mid \mathrm{A} \cap \mathrm{N} \neq \emptyset\}$, um anelóide divisão completamente e totalmente ordenado. Então, dados A$= [a_1, a_2]$, B$= [b_1, b_2]$ pertencentes a IR,

$\mathrm{A} \boxplus \mathrm{B}= [a_1 + b_1, a_2 + b_2]$
$\mathrm{A} \boxminus \mathrm{B} = \mathrm{A}+(-\mathrm{B})=[a_1 - b_2, a_2 - b_1]$

$$\mathrm{A} \boxdot \mathrm{B} = \begin{cases} [a_2b_1, a_2b_2], & \mathrm{A} \geq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathbb{0} \in \mathrm{B} \\ [a_1b_2, a_1b_1], & \mathrm{A} \leq [\mathbb{0},\mathbb{0}] \quad \text{e} \quad \mathbb{0} \in \mathrm{B} \\ [a_1b_2, a_2b_2], & \mathbb{0} \in \mathrm{A} \quad \text{e} \quad \mathrm{B} \geq [\mathbb{0},\mathbb{0}] \\ [a_2b_1, a_1b_1], & \mathbb{0} \in \mathrm{A} \quad \text{e} \quad \mathrm{B} \leq [\mathbb{0},\mathbb{0}] \\ [\min(a_1b_2, a_2b_1), \max(a_1b_1, a_2b_2)], & \mathbb{0} \in \mathrm{A} \quad \text{e} \quad \mathbb{0} \in \mathrm{B} \end{cases}$$

Se $\mathrm{B} \in \mathrm{IR} - \tilde{\mathrm{N}}$,

$$\mathrm{A} \boxslash \mathrm{B} = \begin{cases} \text{indefinido}, & \mathbb{0} \in \mathrm{B} \\ [a_1/b_1, a_2/b_2], & \mathbb{0} \in \mathrm{A} \quad \text{e} \quad \mathrm{B} > [\mathbb{0},\mathbb{0}] \\ [a_2/b_2, a_1/b_1], & \mathbb{0} \in \mathrm{A} \quad \text{e} \quad \mathrm{B} < [\mathbb{0},\mathbb{0}] \end{cases}$$

Como consequência dos teoremas 3.3.6 e 3.3.8 tem-se o seguinte corolário.

Corolário 3.3.9 Seja $\langle \mathrm{R}, +, \cdot, /, \mathbb{0}, \mathbb{1}, \leq \rangle$ um anelóide divisão completamente e totalmente ordenado. Dados A= $[a_1, a_2]$, B= $[b_1, b_2]$ pertencentes a IR tem-se que

$$\mathrm{A} \boxast \mathrm{B} = \square(\mathrm{A} * \mathrm{B}) = [\min_{i,j=1,2}(a_i * b_j), \max_{i,j=1,2}(a_i * b_j)]$$

onde $* \in \{+, -, \cdot, /\}$.

3.3.1 Aritmética Intervalar em um Screen

Seja, por exemplo, $\mathbb{R}$ o conjunto dos números reais e $\mathbb{IR}$ o conjunto dos intervalos reais. Supondo que cálculos devam ser feitos usando elementos de $\mathbb{IR}$. De modo geral, os elementos de $\mathbb{IR}$ não são representáveis, uma vez que elementos de $\mathbb{R}$ também não o são. Portanto, os elementos de $\mathbb{IR}$ devem ser aproximados por meio de um *screen*, que de forma natural, é IS. Esta aproximação porém deve (i) conter o verdadeiro valor, isto é, conter o valor que está sendo aproximado e (ii) ser tão próxima quanto possível do verdadeiro valor. Isto será feito definindo as operações aritméticas através de um semimorfismo conveniente, como descrito a seguir.

Sejam $\langle \mathrm{R}, \leq \rangle$ um reticulado completo, $\langle \mathrm{S}, \leq \rangle$ um *screen* de $\langle \mathrm{R}, \leq \rangle$ e IS o conjunto de todos os intervalos da forma,

$$[a_1, a_2] = \{x \in \mathrm{R} \mid a_1 \leq x \leq a_2, \;\; a_1, a_2 \in \mathrm{S}\}$$

Teorema 3.3.10 Seja $\langle \mathrm{R}, \leq \rangle$ um reticulado completo e $\langle \mathrm{S}, \leq \rangle$ um *screen* de $\langle \mathrm{R}, \leq \rangle$. Então

(a) $\langle \mathrm{IS}, \subseteq \rangle$ é um reticulado completo.

Dados $\mathrm{A} \subseteq \mathrm{IS}$ e $\mathrm{B} = [b_1, b_2] \in \mathrm{IS}$, tem-se que

$$\inf_{\mathrm{IS}}\mathrm{A} = \left[\sup_{\mathrm{B} \in \mathrm{A}} b_1 \quad , \quad \inf_{\mathrm{B} \in \mathrm{A}} b_2 \right]$$

e

$$\sup_{\mathrm{IS}}\mathrm{A} = \left[\inf_{\mathrm{B} \in \mathrm{A}} b_1 \quad , \quad \sup_{\mathrm{B} \in \mathrm{A}} b_2 \right]$$

(b) Seja $\overline{\mathrm{IS}} = \mathrm{IS} \cup \{\emptyset\}$. Então $\langle \overline{\mathrm{IS}}, \subseteq \rangle$ é um *screen* de $\langle \overline{\mathrm{IR}}, \subseteq \rangle$.

A prova deste teorema é similar à do teorema 3.3.3.

O importante a ser salientado no teorema 3.3.10 é o *screen* proposto para um espaço de intervalos. Considerando o espaço de intervalos de reais, por exemplo, um *screen* neste caso é um espaço de intervalos cujos extremos são números de ponto flutuante.

Desde que já se tem estruturas algébricas e de ordem convenientes, o próximo passo é propor um arredondamento que permita definir um semimorfismo através do qual operações aritméticas sejam definidas.

Seja o arredondamento monótono direcionado para cima

$$\Diamond : \overline{\mathrm{IR}} \rightarrow \overline{\mathrm{IS}} \tag{19}$$

tal que,

(**R1**)	$\Diamond\mathrm{A} = \mathrm{A},\ \forall \mathrm{A} \in \overline{\mathrm{IS}}$
(**R2**)	$\mathrm{A} \subseteq \mathrm{B} \Rightarrow \Diamond\mathrm{A} \subseteq \Diamond\mathrm{B},\ \forall \mathrm{A,B} \in \overline{\mathrm{IR}}$
(**R3**)	$\mathrm{A} \subseteq \Diamond\mathrm{A},\ \forall \mathrm{A} \in \overline{\mathrm{IR}}$

O teorema a seguir mostra propriedades deste arredondamento.

Teorema 3.3.11 Seja $\langle \mathrm{R}, +, \cdot, \mathbb{O}, \mathbb{1}, \leq \rangle$ um anelóide completamente e fracamente ordenado , $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico de $\langle \mathrm{R}, +, \cdot, \mathbb{O}, \mathbb{1}, \leq \rangle$ e $\langle \mathrm{IR}, \boxplus, \boxdot \rangle$ o anelóide definido pelo semimorfismo $\Box : \mathrm{PR} \rightarrow \overline{\mathrm{IR}}$. Então

(a) $\langle \overline{\mathrm{IS}}, \subseteq \rangle$ é um *screen* simétrico de $\langle \overline{\mathrm{IR}}, \boxplus, \boxdot \rangle$.

(b) (**R**) $\quad \Diamond\mathrm{A} = \inf(\mathrm{U(A)} \cap \overline{\mathrm{IR}}) = [\bigtriangledown a_1, \bigtriangleup a_2],\ \forall \mathrm{A} = [a_1, a_2] \in \overline{\mathrm{IS}}$

(c) O arredondamento monótono direcionado para cima definido em (19) é anti-simétrico.

A prova é similar a do teorema 3.3.5.

O arredondamento monótono direcionado para cima definido em (19) satisfaz (**R1**), (**R2**), (**R3**), (**R4**). É necessário então definir as operações aritméticas em $\overline{\mathrm{IS}}$ (de acordo com (**RG**) da definição de semimorfismo). Isto é feito a seguir.

No seguinte desenho, os sinais abaixo das setas representam os mapeamentos entre os espaços e os sinais abaixo das siglas dos espaços, representam as operações nos espaços obtidos através dos mapeamentos (arredondamentos) bem definidos.

$$\begin{array}{ccccc} \mathrm{PR} & \rightarrow & \overline{\mathrm{IR}} & \rightarrow & \overline{\mathrm{IS}} \\ * & \Box & \boxast & \Diamond & \circledast \end{array}$$

Para quaisquer elementos A e B pertencentes a IS e $* \in \{+, \cdot, /\}$ tem-se que:

$$\begin{aligned} \mathrm{A} \circledast \mathrm{B} &= \Diamond(\mathrm{A} \boxast \mathrm{B}) \\ &= \Diamond(\Box(\mathrm{A} * \mathrm{B})) \\ &= \Diamond([\inf(\mathrm{A} * \mathrm{B}), \sup(\mathrm{A} * \mathrm{B})] \\ &= [\bigtriangledown\inf(\mathrm{A} * \mathrm{B}), \bigtriangleup\sup(\mathrm{A} * \mathrm{B})] \end{aligned}$$

Logo, a (**RG**), para este arredondamento, é definida por

(RG) $\qquad A \mathbin{\Diamond\!\!\!\!\ast} B = [\bigtriangledown\inf(A * B), \bigtriangleup\sup(A * B)],\ \forall A,B \in \overline{IS}$

Como é então definido o semimorfismo neste caso? Considerando o arredondamento proposto em (19),

$$\Diamond : \overline{IR} \to \overline{IS}$$

onde para cada operação $*$ em $\overline{IR}$, tem-se $\mathbin{\Diamond\!\!\!\!\ast}$ em $\overline{IS}$ tal que

(RG) $\qquad A \mathbin{\Diamond\!\!\!\!\ast} B = [\bigtriangledown\inf(A * B), \bigtriangleup\sup(A * B)],\ \forall A,B \in \overline{IS}$

com $\Diamond$ satisfazendo

(R1) $\qquad \Diamond A = A,\ \forall A \in \overline{IS}$
(R2) $\qquad A \subseteq B \Rightarrow \Diamond A \subseteq \Diamond B,\ \forall A,B \in \overline{IR}$
(R3) $\qquad A \subseteq \Diamond A,\ \forall A \in \overline{IR}$
(R4) $\qquad \Diamond(-A) = -\Diamond A$

Então $\Diamond$ *é um semimorfismo.*

O teorema 3.1.15 mostra que, para todo A,B,C,D $\in$ IS, a operação $\mathbin{\Diamond\!\!\!\!\ast}$ tem as seguintes propriedades,

(RG1) $\qquad A \boxast B \in \overline{IS} \Rightarrow A \mathbin{\Diamond\!\!\!\!\ast} B = A \boxast B$
(RG2) $\qquad A \boxast B \subseteq C \boxast D \Rightarrow A \mathbin{\Diamond\!\!\!\!\ast} B \subseteq C \mathbin{\Diamond\!\!\!\!\ast} D$
(RG3) $\qquad A \boxast B \subseteq A \mathbin{\Diamond\!\!\!\!\ast} B$

Lema 3.3.12 Seja $\langle R, +, \cdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ um anelóide completamente e fracamente ordenado e $\langle S, \leq\rangle$ um *screen* simétrico de $\langle R, +, \cdot, \mathbb{0}, \mathbb{1}, \leq\rangle$. Sejam os semimorfismos $\Box : PR \to \overline{IR}$ e $\Diamond : \overline{IR} \to \overline{IS}$. Então

(a) Em $\langle IS, \mathbin{\Diamond\!\!\!\!+}, \mathbin{\Diamond\!\!\!\!\cdot}\rangle$, somente os intervalos pontuais satisfazem a propriedade $(P5_{ALD})$ da definição A.6.1.

(b) Se todo elemento $X \in IS$ que satisfaz $(P5_{ALD})$ e para o qual também vale que: $\forall A,B \in IS,\ A \leq B \Rightarrow XB \leq XA$ pertence a $\langle L, \leq\rangle$, onde L é um subconjunto totalmente ordenado de IS, então $\langle IS, \mathbin{\Diamond\!\!\!\!+}, \mathbin{\Diamond\!\!\!\!\cdot}, [\mathbb{0},\mathbb{0}], [\mathbb{1},\mathbb{1}]\ \leq\rangle$ é um anelóide fracamente ordenado.

(c) Se $\langle R, +, \cdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ é um anelóide ordenado, então, sob as hipóteses em (b), $\langle IS, \mathbin{\Diamond\!\!\!\!+}, \mathbin{\Diamond\!\!\!\!\cdot}, \leq\rangle$ também é um anelóide ordenado.

(d) Se $\langle R, N, +, \cdot, /, \mathbb{0}, \mathbb{1}, \leq\rangle$ é um anelóide divisão completamente ordenado (fracamente ordenado) então, sob as hipóteses em (b), $\langle IS, \overline{N}, \mathbin{\Diamond\!\!\!\!+}, \mathbin{\Diamond\!\!\!\!\cdot}, \mathbin{\Diamond\!\!\!\!/}, [\mathbb{0},\mathbb{0}], [\mathbb{1},\mathbb{1}], \leq\rangle$, com $\overline{N} = \{A \in IS \mid A \cap N \neq \emptyset\}$ também é um anelóide divisão completamente ordenado (fracamente ordenado).

Demonstração.

(a) Pelo teorema 3.3.6, existe $X \in IS$ tal que

$$X \mathbin{\Diamond\!\!\!\!\ast} [\mathbb{1},\mathbb{1}] = [\mathbb{0},\mathbb{0}] \tag{20}$$

$$\mathrm{X}\odot\mathrm{X} = [\mathbb{1},\mathbb{1}] \tag{21}$$

$$\mathrm{X}\odot(\mathrm{A}\odot\mathrm{B}) = (\mathrm{X}\odot\mathrm{A})\odot\mathrm{B} = \mathrm{A}\odot(\mathrm{X}\odot\mathrm{B}) \tag{22}$$

$$\mathrm{X}\odot(\mathrm{A}\oplus\mathrm{B}) = (\mathrm{X}\odot\mathrm{A})\oplus(\mathrm{X}\odot\mathrm{B}) \tag{23}$$

Por (20) e seja $\mathrm{X} = [x_1, x_2]$,

$$\mathrm{X}\oplus[\mathbb{1},\mathbb{1}] = \Diamond(\mathrm{X}\boxplus[\mathbb{1},\mathbb{1}])) = \mathrm{X}\boxplus[\mathbb{1},\mathbb{1}] = [x_1, x_2] + [\mathbb{1},\mathbb{1}] = [\mathbb{0},\mathbb{0}] \Leftrightarrow x_1 = x_2 = -1 \tag{24}$$

$\Diamond$ e $\Box$ são arredondamentos monótonos direcionados para cima; portanto da igualdade (24) conclui-se que X$= [x, x]$.

De forma similar prova-se (21).

Como o X que satisfaz (20), (21), (22) e (23) é o mesmo, então X é um intervalo degenerado em todos os casos.

(b) Supondo que existe um X$\in$S tal que X satisfaz (20), (21), (22) e (23) e também que

$$\mathrm{A} \leq \mathrm{B} \Rightarrow \mathrm{XB} \leq \mathrm{XA}, \forall \mathrm{A},\mathrm{B} \in \mathrm{IS} \tag{25}$$

Além disso, X$\in \langle \mathrm{L}, \leq\rangle$ onde todos os elementos de L são comparáveis por hipótese. Pelo item (a), X é um ponto. Logo, para que $\langle \mathrm{IS},\oplus,\odot,[\mathbb{0},\mathbb{0}],[\mathbb{1},\mathbb{1}] \leq\rangle$ seja um anelóide fracamente ordenado basta mostrar que X é único. Supondo que existem X e Y satisfazendo todas essas condições, que X$\leq$Y e como são pontos, X$= x$ e Y$= y$.

$$x \leq y \tag{26}$$

multiplicando (26) por x e aplicando (25),

$$xy \leq xx \Rightarrow xy \leq \mathbb{1}$$

multiplicando (26) por y e aplicando (25),

$$yy \leq yx \Rightarrow \mathbb{1} \leq yx.$$

Como $x, y \in \mathrm{L}$,

$$xy = yx = \mathbb{1}.$$

Considerando que

$$xy = \mathbb{1}$$

e multiplicando por x,

$$xxy = x\,\mathbb{1}$$

$$\mathbb{1}\,y = x\,\mathbb{1} \Rightarrow y = x.$$

(c) Para mostrar que $\langle \text{IS}, \diamondplus, \diamonddot, [\mathbb{0},\mathbb{0}], [\mathbb{1},\mathbb{1}]\ \leq \rangle$ é um anelóide ordenado basta mostrar que $\diamond : \overline{\text{IR}} \rightarrow \overline{\text{IS}}$ é monotônico com respeito à ordem $\leq$ (lema 3.2.7). Sejam A$= [a_1, a_2]$, B$= [b_1, b_2]$. Então A $\leq$ B $\Leftrightarrow$ $(a_1 \leq b_1$ e $a_2 \leq b_2) \Rightarrow (\bigtriangledown a_1 \leq \bigtriangledown b_1$ e $\triangle a_2 \leq \triangle b_2) \Rightarrow ([\bigtriangledown a_1, \triangle a_2] \leq [\bigtriangledown b_1, \triangle b_2]) \Rightarrow \diamond\text{A} \leq \diamond\text{B}$.

(d) Similar a (c) (lema 3.2.8). ∎

Seja $\langle \text{R}, *, \subseteq \rangle$ um anelóide. Da definição A.6.4, $\langle \text{R}, *, \subseteq \rangle$ é *inclusamente ordenado* se para quaisquer A,B,C,D $\in$R, A $\subseteq$ B e C $\subseteq$ D $\Rightarrow$ A $*$ C $\subseteq$ B $*$ D.

O teorema a seguir é uma aplicação do lema 3.3.12.

Teorema 3.3.13 Seja $\langle \text{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq \rangle$ um anelóide completamente e totalmente ordenado e $\langle \text{S}, \leq \rangle$ um *screen* simétrico de $\langle \text{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq \rangle$. Sejam os semimorfismos $\square$: PR $\rightarrow \overline{\text{IR}}$ e $\diamond : \overline{\text{IR}} \rightarrow \overline{\text{IS}}$. Então,

(a) $\langle \text{IS}, \diamondplus, \diamonddot, [\mathbb{0},\mathbb{0}], [\mathbb{1},\mathbb{1}], \leq, \subseteq \rangle$, com respeito à ordem $\leq$ é um anelóide completamente ordenado e com respeito à $\subseteq$, é um anelóide *screen* superior monótono inclusamente ordenado de IR.

(b) Se $\langle \text{R}, \text{N}, +, \cdot, /, \mathbb{0}, \mathbb{1}, \leq \rangle$ é um anelóide divisão então $\langle \text{IS}, \overline{N}, \diamondplus, \diamonddot, \diamondslash, [\mathbb{0},\mathbb{0}], [\mathbb{1},\mathbb{1}], \leq, \subseteq \rangle$, onde $\overline{N} \stackrel{\text{def}}{=} \{\text{A} \in \text{IS} \mid \mathbb{0} \in \text{A}\}$ é um anelóide divisão ordenado com respeito a ordem $\leq$ e um anelóide divisão *screen* superior inclusamente ordenado monótono com respeito a ordem $\subseteq$.

Kulisch e Miranker [KM79, KM81] enfatizam que uma aplicação central do teorema 3.3.13 é o conjunto dos intervalos que formam o *screen*, IS, para os intervalos de reais. A definição e a realização das operações aritméticas no *screen* IS são mostradas a seguir.

Seja $\mathbb{R}$, o conjunto dos números reais e S um conjunto de números de ponto flutuante, $\langle \mathbb{R} \cup \{-\infty, +\infty\}, +, \cdot, 0, 1, \leq \rangle$ um anelóide completamente e totalmente ordenado e $\langle \text{S}, \leq \rangle$ um *screen* de $\langle \mathbb{R} \cup \{-\infty, +\infty\}, +, \cdot, 0, 1, \leq \rangle$. Sabe-se que, dados A$= [a_1, a_2]$, B$= [b_1, b_2]$, $* \in \{+, -, \cdot, /\}$,

$$\square : \text{P}\mathbb{R} \rightarrow \overline{\text{I}\mathbb{R}}$$

$$\text{A} \boxast \text{B} = \square(\text{A} * \text{B}) = [\min_{i,j=1,2}(a_i * b_j), \max_{i,j=1,2}(a_i * b_j)]$$

(esta igualdade vem do corolário 3.3.9). Seja o semimorfismo,

$$\Diamond : \overline{\mathrm{IIR}} \to \overline{\mathrm{IS}}$$

então, dados A=$[a_1, a_2]$ e B=$[b_1, b_2]$ tem-se que:

$$\begin{aligned}
\mathrm{A} \mathbin{\Diamond_{*}} \mathrm{B} &= \Diamond(\mathrm{A} \boxast \mathrm{B}) \\
&= \Diamond(\Box(\mathrm{A} * \mathrm{B})) \\
&= \Diamond([\min_{i,j=1,2}(a_i * b_j), \max_{i,j=1,2}(a_i * b_j)]) \\
&= [\triangledown \min_{i,j=1,2}(a_i * b_j), \vartriangle \max_{i,j=1,2}(a_i * b_j)] \\
&= [\min_{i,j=1,2}(a_i \mathbin{\triangledown_{*}} b_j), \max_{i,j=1,2}(a_i \mathbin{\vartriangle_{*}} b_j)] && (27) \\
&= [\min_{i,j=1,2} \triangledown(a_i * b_j), \max_{i,j=1,2} \vartriangle(a_i * b_j)] && (28)
\end{aligned}$$

Em (27) estão definidas como as operações aritméticas são realizadas no *screen* conveniente para o espaço dos intervalos reais. Considerando os resultados dos teoremas 3.3.6 e 3.3.8 e por (27) e (28), as operações no *screen* são sumarizadas a seguir. É conveniente enfatizar que $a \mathbin{\triangledown_{*}} b$, por exemplo, significa tomar os verdadeiros valores reais de a e b, em seguida operar fazendo o arredondamento direcionado para baixo.

Dados A=$[a_1, a_2]$, B=$[b_1, b_2] \in$ IS tem-se que:

$\mathrm{A} \mathbin{\Diamond_{+}} \mathrm{B}=[a_1 \mathbin{\triangledown_{+}} b_1, a_2 \mathbin{\vartriangle_{+}} b_2] = [\triangledown(a_1 + b_1), \vartriangle(a_2 + b_2)]$
$\mathrm{A} \mathbin{\Diamond_{-}} \mathrm{B}=[a_1 \mathbin{\triangledown_{-}} b_2, a_2 \mathbin{\vartriangle_{-}} b_1] = [\triangledown(a_1 - b_2), \vartriangle(a_2 - b_1)]$

$$\mathrm{A} \mathbin{\Diamond_{\cdot}} \mathrm{B} = \begin{cases}
[a_1 \mathbin{\triangledown_{\cdot}} b_1, a_2 \mathbin{\vartriangle_{\cdot}} b_2] = [\triangledown(a_1.b_1), \vartriangle(a_2.b_2)], & \mathrm{A} \geq [0,0], \quad \mathrm{B} \geq [0,0] \\
[a_2 \mathbin{\triangledown_{\cdot}} b_1, a_1 \mathbin{\vartriangle_{\cdot}} b_2] = [\triangledown(a_2.b_1), \vartriangle(a_1.b_2)], & \mathrm{A} \geq [0,0], \quad \mathrm{B} \leq [0,0] \\
[a_2 \mathbin{\triangledown_{\cdot}} b_1, a_2 \mathbin{\vartriangle_{\cdot}} b_2] = [\triangledown(a_2.b_1), \vartriangle(a_2.b_2)], & \mathrm{A} \geq [0,0], \quad 0 \in \mathrm{B} \\
[a_1 \mathbin{\triangledown_{\cdot}} b_2, a_2 \mathbin{\vartriangle_{\cdot}} b_1] = [\triangledown(a_1.b_2), \vartriangle(a_2.b_1)], & \mathrm{A} \leq [0,0], \quad \mathrm{B} \geq [0,0] \\
[a_2 \mathbin{\triangledown_{\cdot}} b_2, a_1 \mathbin{\vartriangle_{\cdot}} b_1] = [\triangledown(a_2.b_2), \vartriangle(a_1.b_1)], & \mathrm{A} \leq [0,0], \quad \mathrm{B} \leq [0,0] \\
[a_1 \mathbin{\triangledown_{\cdot}} b_2, a_1 \mathbin{\vartriangle_{\cdot}} b_1] = [\triangledown(a_1.b_2), \vartriangle(a_1.b_1)], & \mathrm{A} \leq [0,0], \quad 0 \in \mathrm{B} \\
[a_1 \mathbin{\triangledown_{\cdot}} b_2, a_2 \mathbin{\vartriangle_{\cdot}} b_2] = [\triangledown(a_1.b_2), \vartriangle(a_2.b_2)], & 0 \in \mathrm{A}, \quad \mathrm{B} \geq [0,0] \\
[a_2 \mathbin{\triangledown_{\cdot}} b_1, \mathrm{a}_1 \mathbin{\vartriangle_{\cdot}} b_1] = [\triangledown(a_2.b_1), \vartriangle(a_1.b_1)], & 0 \in \mathrm{A}, \quad \mathrm{B} \leq [0,0] \\
[\min(a_1 \mathbin{\triangledown_{\cdot}} b_2, a_2 \mathbin{\triangledown_{\cdot}} b_1), \max(a_1 \mathbin{\vartriangle_{\cdot}} b_1, a_2 \mathbin{\vartriangle_{\cdot}} b_2)] & 0 \in \mathrm{A}, \quad 0 \in \mathrm{B}
\end{cases}$$

$$\mathrm{A} \mathbin{\Diamond_{/}} \mathrm{B} = \begin{cases}
[a_1 \mathbin{\triangledown_{/}} b_2, a_2 \mathbin{\vartriangle_{/}} b_1] = [\triangledown(a_1/b_2), \vartriangle(a_2/b_1)], & \mathrm{A} \geq [0,0], \quad \mathrm{B} > [0,0] \\
[a_2 \mathbin{\triangledown_{/}} b_2, a_1 \mathbin{\vartriangle_{/}} b_1] = [\triangledown(a_2/b_2), \vartriangle(a_1/b_1)], & \mathrm{A} \geq [0,0], \quad \mathrm{B} < [0,0] \\
\text{indefinida}, & \mathrm{A} \geq [0,0], \quad 0 \in \mathrm{B} \\
[a_1 \mathbin{\triangledown_{/}} b_1, a_2 \mathbin{\vartriangle_{/}} b_2] = [\triangledown(a_1/b_1), \vartriangle(a_2/b_2)], & \mathrm{A} \leq [0,0], \quad \mathrm{B} > [0,0] \\
[a_2 \mathbin{\triangledown_{/}} b_1, a_1 \mathbin{\vartriangle_{/}} \mathrm{b}_2] = [\triangledown(a_2/b_1), \vartriangle(a_1/b_2)], & \mathrm{A} \leq [0,0], \quad \mathrm{B} < [0,0] \\
\text{indefinida}, & \mathrm{A} \leq [0,0], \quad 0 \in \mathrm{B} \\
[a_1 \mathbin{\triangledown_{/}} b_1, a_2 \mathbin{\vartriangle_{/}} b_1] = [\triangledown(a_1/b_1), \vartriangle(a_2/b_1)], & 0 \in \mathrm{A}, \quad \mathrm{B} > [0,0] \\
[a_2 \mathbin{\triangledown_{/}} b_2, a_1 \mathbin{\vartriangle_{/}} b_2] = [\triangledown(a_2/b_2), \vartriangle(a_1/b_2)], & 0 \in \mathrm{A}, \quad \mathrm{B} < [0,0] \\
\text{indefinida}, & 0 \in \mathrm{A}, \quad 0 \in \mathrm{B}
\end{cases}$$

3.4 Exemplos

Os exemplos a seguir ilustram as vantagens das aplicações de métodos intervalares e da aritmética de exatidão máxima.

Exemplo 3.4.1 Este exemplo é de [Böh83]. O problema consiste na avaliação do polinômio,

$$P(x) = 23616x^5 - 161522x^4 + 401773x^3 - 406754x^2 + 87511x + 66576$$

para valores de x entre 1.7800 e 1.7810. Os resultados estão sumarizados abaixo; PF significa Ponto Flutuante e IEM, Intervalos e Exatidão Máxima

x	resultados em PF	resultados em	IEM
1.7800	0	-5.12000000000	E-8
1.7801	-1.4 E-6	-3.4094229723^{9}_{8}	E-8
1.7802	2.6 E-6	-2.0535703802^{9}_{8}	E-8
1.7803	-2.3 E-6	-1.0434985373^{2}_{1}	E-8
1.7804	3.5 E-6	-3.58579593216	E-9
1.7805	-1.5 E-6	3.35013000000	E-10
1.7806	2.2 E-6	1.76748822016	E-9
1.7807	-1.5 E-6	1.26860318112	E-9
1.7808	-1.9 E-6	-4.87713669120	E-10
1.7809	8.0 E-7	-2.71055054816	E-9
1.7810	-5.0 E-7	-4.49198400000	E-9

O grau do polinômio é 5, logo P(x) tem 5 zeros [Gon79]. Nos intervalos (1.7801,1.7802), (1.7802,1.7803), (1.7803,1.7804), (1.7804,1.7805), (1.7805,1.7806), (1.7806,1.7807), (1.7808,1.7809), (1.7809,1.7810) existe pelo menos um x tal que P(x)=0 [Apo60] . Portanto, através dos resultados em PF, P(x) tem pelo menos 8 zeros no intervalo (1.7800,1.7810)! Usando um algoritmo intervalar e métodos de exatidão máxima, os resultados mostram apenas a existência de pelo menos duas raízes no mesmo intervalo.

Exemplo 3.4.2 Dados $x = 0.3459$ e $y = 0.3460$, elementos do sistema de ponto flutuante S(10,4,$-$9,9), calcular o desvio padrão, σ, entre eles. Sabe-se que $\sigma \geq 0$. A expressão para o cálculo de σ é,

$$\sigma = +1/2\sqrt{x^2 + y^2 - 2xy}$$

que avaliada para os valores dados fornece como resposta

$$\sigma = (1/2)\sqrt{-10^{-4}}$$

o que é um absurdo! A resposta para o mesmo problema obtida através de métodos intervalares e de máxima exatidão é

$$\sigma = (1/2)[10^{-4}, 10^{-4}]$$

3.5 Conclusões

Métodos intervalares [Moo66, Moo79, AH83] podem tratar problemas envolvendo dados imprecisos. A Análise Intervalar resolve problemas de otimização global, tais como o método de Newton intervalar para resolver sistemas de equações não lineares. Este método pode ser usado para encontrar e limitar todas as soluções em uma dada região. Hansen [Han92] mostra que, através do método de Newton intervalar prova-se a existência e unicidade de uma solução de um sistema não linear de equações em uma dada região. Intervalos reais são usualmente realizados em computadores de tal forma que seus limites são escolhidos como números de máquina, isto é, números de ponto flutuante com uma precisão fixa. A aritmética intervalar é implementada pelo uso das operações de ponto flutuante com arredondamentos direcionados. A disponibilidade de arredondamentos direcionados e operações intervalares, são ferramentas essenciais em computadores, quando, entre outros, tem-se o objetivo de controlar os erros numéricos.

As idéias de Kulisch e Miranker [Kul73, KM79, KM81, Kul83, KM86, KB83] aqui tratadas mostram que uma correta implementação de uma aritmética em computadores depende de desenvolvimentos teóricos. O conceito de semimorfismo é fundamental. As estruturas dos espaços ocorrendo em cálculos efetuados em computadores são invariantes com respeito a semimorfismos. Considerando os espaços envolvendo matrizes ou vetóides, o produto escalar de dois vetores é de importância básica. É necessário executar esta operação com máxima exatidão, isto é, o computador tem de ser capaz de determinar a soma n-ária de produtos de números de ponto flutuante de tal forma que resultados computados difiram de no máximo uma ou meia unidade no último dígito da mantissa.

Se todas as operações nos espaços da Figura 3.1 forem definidas por semimorfismo, as estruturas algébricas naqueles espaços são preservadas tanto quanto possível, portanto tem-se resultados de exatidão máxima. Portanto, Bohlender e Grüner [BG83] propõem, para a realização de uma aritmética exata, que:

- não haja número de máquina entre o resultado exato e o valor computado
- em todos os espaços da computação numérica as operações sejam exatamente arredondadas
- os subespaços precisam ter pelo menos as propriedades de anelóide ou vetóide
- problemas numéricos que sejam exatamente representáveis tem de ser exatamente representáveis na máquina
- tem de ser possível implementar novos algoritmos numéricos que computem resultados garantidos
- todas as características da aritmética tem de ser acessível a linguagens de programação de alta ordem
- os requerimentos de exatidão não devem levar a uma perda de velocidade
- a memória tem de ser utilizada economicamente e a construção tem de ser modular
- a portabilidade deve ser mantida.

Atualmente é bastante grande o número de trabalhos publicados acerca de aritmética computacional e computação científica. Alguns tópicos abordados são: aritmética computacional para métodos de verificação, aritmética de hardware para métodos de verificação, funções padrão com máxima exatidão, métodos de verificação, programação paralela, supercomputadores e linguagens de programação para computação científica, entre outros.

Capítulo 4

Linguagens de Programação e Computação Científica

Provas e cálculos concernentes à probabilidade intervalar proposta nesta tese, envolvem linguagens de programação que tenham o tipo intervalo e as operações sobre o tipo implementados com exatidão máxima. Como será visto a seguir, já existem extensões de linguagens de programação procedurais com essa característica, que permitem computações em todos os espaços da computação numérica (Figura 3.1, capítulo 3). O trabalho [LCC95] analisa, de forma pioneira, a introdução do tipo intervalo como primitivo nas linguagens funcionais.

Este capítulo inicialmente enfoca aspectos gerais relacionados com conceitos de linguagens de programação com verificação automática dos resultados. Em seguida, aborda aspectos do paradigma funcional que o qualifica para computação científica. Ao final, é apresentada a especificação do tipo intervalo em OBJ3 e a prova automática de teoremas da matemática intervalar. A importância da especificação do tipo intervalo em OBJ3 transcende em muito as provas apresentadas neste capítulo. Na realidade, a especificação apresentada é um modelo que poderá ser facilmente seguido e adaptado para outras linguagens e outros ambientes de prova de programas. Da mesma maneira, as provas aqui apresentadas podem ser mimificadas na prova de corretude de outros programas ou teoremas que façam uso do tipo intervalo. A especificação adotada também serve para a inclusão de mais alto nível do tipo de dado intervalo em linguagens que permitam ao usuário definir novos tipos algébricos. Desse modo apresenta-se aqui uma significativa contribuição para a engenharia de *software*, numa perspectiva em que programas devem ser *provados corretos* e que tal não faz sentido se a aritmética adotada não for confiável, tornando-se mandatória a adoção de uma aritmética tal como a intervalar aqui adotada.

4.1 Tipos de Dados e Polimorfismo

Toda linguagem possui um conjunto de tipos pré-definidos, chamados tipos *básicos*. Sobre os tipos básicos, *contrutores*, tais como o produto cartesiano e a união disjunta, formam novos tipos ditos *estruturados*. Os tipos implementados na linguagem são chamados tipos *primitivos*, que podem ser básicos, como booleanos ou inteiros, ou estruturados como listas. Na maior parte das linguagens imperativas os tipos dos dados são declarados. Supondo uma linguagem imperativa onde o tipo intervalo esteja introduzido, se a variável X por exemplo é declarada no começo do programa como sendo um intervalo, então durante toda a execução do programa, X é um intervalo. Este tipo de linguagem possui um sistema de tipos *estático*, pois o tipo das variáveis não muda em tempo de execução.

No caso específico de funções, rigorosamente falando, a função depende do seu domínio, para que ela possa ser completamente especificada. Através do uso de *polimorfismo* pode-se especificar toda uma classe de funções através de uma única definição. Por exemplo, a função que retira a cabeça de uma lista de inteiros é de natureza diferente da função que seleciona a cabeça de uma lista de booleanos. Os tipos das duas funções são, respectivamente:

```
 Hd.int ::  [int] -> int
Hd.bool ::  [bool] -> bool
```

Ora, a "natureza" do seletor Hd independe do tipo da lista. Utilizando-se polimorfismo é possível obter este caráter unificador de todas as funções Hd, que seria do tipo:

```
Hd ::  [ * ] -> *
```

O polimorfismo permite detectar grande parte dos erros de programas, aumentando a sua confiabilidade.

4.2 Requisitos de Linguagens para Computação Científica

A confiabilidade de uma computação numérica pressupõe validade das expressões matemáticas envolvidas, precisão numérica compatível com a aplicação e garantia de que os erros acumulados não superam limites previamente estabelecidos. As dificuldades em gerar automaticamente resultados confiáveis faz com que muitos aplicativos numéricos operem de modo iterativo, com o operador controlando os resultados intermediários. Cálculos em tempo real ou de grande complexidade, no entanto, inviabilizam este modo de operação. Por outro lado, a interferência humana só pode ser descartada com a completa automação do controle do erro, o que requer validação do algoritmo e da implementação.

Operar os números reais de modo rápido e confiável tem sido um desafio para os programadores e projetistas de computadores porque as unidades aritméticas dos processadores operam com precisões pré-fixadas enquanto a aritmética dos reais produz resultados de precisão arbitrária. Uma representação interna ideal dos números reais deve manter as propriedades algébricas necessárias à validação dos resultados. Adicionalmente, envolve aspectos de *hardware* e/ou *software* que assegurem alto desempenho às máquinas. A facilidade de programação também deve ser considerada; provê meios para representar os dados inexatos. Os conflitos embutidos nestes requisitos tem levado a diferentes representações dos reais, usadas pelos sistemas de computação, cada uma delas com suas vantagens relativas. A medida em que aumenta a complexidade dos problemas tratados surgem novos desafios a serem atendidos, tendo como limitação o poder computacional das arquiteturas e a capacidade de extração de paralelismo [CCL95].

Kulisch e seus colaboradores [KM81, Kul83, KM86, KB83] mostram que uma correta implementação de uma aritmética em computadores depende de desenvolvimentos teóricos. O conceito de semimorfismo é fundamental. As estruturas dos espaços ocorrendo em cálculos numéricos (Figura 3.1, capítulo 3) efetuados em computadores são invariantes com respeito a semimorfismos. Considerando os espaços envolvendo matrizes ou vetóides, o produto escalar de dois vetores é de importância básica. É necessário realizar esta operação com máxima exatidão, isto é, o computador tem de ser capaz de determinar a soma n-ária de produtos de números de ponto flutuante de tal forma que resultados computados difiram de no máximo uma ou meia unidade no último dígito da mantissa.

Como foi visto no capítulo anterior, intervalos reais são usualmente implementados em computadores de tal forma que seus limites são escolhidos como números de máquina, isto é, números de ponto flutuante com uma precisão fixa. A aritmética intervalar é implementada pelo uso das operações de ponto flutuante com arredondamentos direcionados.

As linguagens que fazem uso de aritméticas de precisão fixa introduziram os conceitos de arredondamento, *overflow* e *underflow* como parte delas próprias, refletindo a aritmética implementada na arquitetura. Nelas passa-se a ter um erro associado às operações aritméticas que, propagado através dos cálculos, pode contaminar os resultados. Os procedimentos que asseguram a validação dos resultados envolvem o controle do erro. A disponibilidade de arredondamentos direcionados e operações intervalares, são ferramentas essenciais em computadores, quando, entre outros, tem-se o objetivo de controlar erros de arredondamento.

As linguagens de programação que possuem o tipo intervalo como primitivo implementam métodos intervalares por *software*, assegurando assim que o resultado exato está contido no intervalo que o representa, fornecendo portanto um mecanismo de verificação automática do erro. Para isso é necessário que o arredondamento do extremo inferior do intervalo seja feito na direção de menos infinito e o do extremo superior, na direção de mais infinito. A adoção do padrão IEEE 754 [Cod88, Gol91, Ste81], descrito no apêndice C desta tese, pelos fabricantes de arquiteturas, já possibilita que linguagens usem os arredondamentos disponíveis no *hardware*. Na ausência da observância de tal padrão, toda a aritmética, incluindo os arredondamentos, serão realizados por *software*. Espera-se que em futuro próximo arquiteturas comerciais adotem o intervalo como tipo primitivo de máquina, possibilitando que muitas das operações que hoje são feitas por *software* tornem-se mais eficientes, através da sua implementação direta em *hardware*, inclusive fazendo uso do paralelismo de fina granularidade existente na aritmética intervalar.

O intervalo, além de ser adequado à representação do erro inerente aos dados inexatos, serve para medir o erro decorrente dos arredondamentos. Uma vantagem adicional é que as ocorrências de *overflow* e *underflow* passam a ser vistas como casos de arredondamentos, explicitamente previstos nas linguagens e possíveis de serem manipulados simbolicamente, e não como exceções, indicando erro de *hardware*. Se comparada à aritmética de ponto flutuante, o custo computacional da aritmética intervalar é mais alto. São necessários dois números do tipo ponto flutuante para representar cada intervalo e as operações aritméticas são mais complexas. O custo da implementação do produto escalar com máxima exatidão é alto devido a soma n-ária envolvida.

Matemáticos usam o mesmo operador infixo para denotar operações aritméticas em espaços diferentes. Também nomes de funções idênticos são usados em funções padrão para diferentes tipos de dados.

A análise das necessidades computacionais [Gud92, Rum94, Boh94] mostra que as linguagens de programação para computação científica devem possuir:

- operadores definidos pelo usuário, pelo menos pela superposição de operadores padrão ou permitindo a definição de novos;

- dados estruturados como resultado de operadores e funções;
- identificadores de funções sobrecarregáveis (*overloadable*;)
- arrays dinâmicos;
- disponibilidade de arredondamentos direcionados para a aritmética intervalar;
- conceito de módulo;
- subrotinas com tipos parametrizáveis.
- conceito de subtipo;
- polimorfismo.

Nós [CCCL95] argumentamos que *computação científica* tem o significado de computação confiável: representar e operar os espaços da computação numérica [Moo66, Moo79, KM81] (entre outros os números reais, números complexos, matrizes reais, intervalos de reais, matrizes de intervalos) em computadores digitais através de linguagens de programação que além dos tipos e operações usuais sobre tipos, permitam a validação dos resultados.

4.3 Linguagens de Programação XSC

Linguagens de programação do paradigma imperativo, consideradas tradicionais, como ALGOL, FORTRAN, PL/I, PASCAL ou MODULA dispõem somente dos tipos de dados numéricos elementares e das operações associadas a esses tipos. Mesmo quando operações com números complexos estão disponíveis, elas são baseadas nas operações sobre números reais. Todas as operações sobre intervalos devem ser definidas e implementadas pelo usuário na forma de subrotinas; operações aritméticas sobre vetores, matrizes, vetores e matrizes de complexos e intervalos sobre todos estes conjuntos são ainda mais difíceis de serem definidas. Cada ocorrência de uma operação em um algoritmo ocasiona uma chamada de rotina, o que é notacionalmente inconveniente, complicado e dispendioso em termos de consumo de tempo. Uma forma de resolver muitas dificuldades na implementação de algoritmos numéricos envolvendo todos os espaços da computação científica (Figura 3.1), é desenvolver extensões dessas linguagens.

As linguagens de programação que têm tipos adicionais implementados, são usualmente denominadas na literatura com a extensão XSC, que significa "e**X**tended **S**cientific **C**omputation" [Shi93].

Além de um grande número de tipos de dados pré-definidos e a definição das respectivas operações aritméticas com máxima exatidão, as linguagens XSC [Shi93] satisfazem, entre outros, os requisitos básicos para computação científica apresentados na seção anterior.

Atualmente, existem pelo menos três desenvolvimentos de linguagens e de seus correspondentes compiladores que contém todos os conceitos para programação com verificação automática de resultado. Tais linguagens são ACRITH-XSC [Wal92], Pascal-XSC [HNR92] e C-XSC[Law92]. O ACRITH-XSC é uma extensão da linguagem FORTRAN-77. O Pascal-XSC e o C-XSC são extensões das linguagens Pascal e C++, respectivamente. Do ponto de vista da computação científica essas linguagens implementam a mesma aritmética computacional e são igualmente confiáveis. As diferenças de eficiência ou sintáticas estão fora do escopo desta tese.

4.4 Linguagens Funcionais

O paradigma de programação funcional, como o próprio nome indica, significa *programação através de funções* [Hug89]. Definições podem ser entendidas como na matemática elementar. Programação funcional simplifica a execução de expressões sem qualquer mudança em seu estado, pois programas funcionais trabalham com valores e não com estados. Quando uma função é chamada, o argumento é substituído por seu parâmetro formal; o parâmetro formal indica no corpo onde substituir o argumento. O nome do parâmetro formal não tem outro significado e nada significa fora da definição da função [Pau91].

Em linguagens imperativas ou procedurais o cálculo de expressões pode não satisfazer as leis da álgebra. O cálculo de

$$f(E1 + E2) - g(E3)$$

pode ser diferente do cálculo de

$$-g(E3) + f(E1 + E2)$$

Portanto, uma das vantagens da implementação de métodos numéricos em linguagens funcionais é a *transparência referencial*. A transparência referencial das linguagens funcionais garante que as leis usuais da algébra são satisfeitas [Pau91]. Por exemplo

$$E_1 + E_2$$

pode ser substituída por

$$E_2 + E_1$$

porque a comutatividade que é válida na adição é mantida na linguagem. Porém isto é válido para os inteiros, não para a aritmética dos reais (ponto flutuante). A vantagem da implementação do semimorfismo é a preservação de uma estrutura algébrica (anelóide ou vetóide). Portanto, se métodos intervalares e de exatidão máxima são implementados em linguagens funcionais, a estrutura algébrica de anelóide ou vetóide não somente é preservada através do semimorfismo como na linguagem devido à transparência referencial.

Muitas expressões matemáticas têm uma estrutura recursiva. Por exemplo, podemos definir a função fatorial como no *script* abaixo:

```
fat 0 = 1,
fat n = n * fat (n-1).
```

A definição de fatorial de n invoca a própria função fatorial, tendo como argumento $n - 1$. Em programas funcionais, os valores das variáveis são obtidos ou quando uma função é chamada ou por definição. Portanto, não podem ser atualizados, mas chamadas recursivas podem produzir mudanças nos valores dos argumentos, porque este tipo de alteração de valor ocorre "internamente" ao mecanismo de avaliação, sem interferência do usuário. Recursão elimina o *baroque looping constructs* das linguagens procedurais [Pau91], tornando os programas mais legíveis. Muitos algoritmos numéricos convencionais são recursivos. Esta afirmação é verdadeira também para algoritmos intervalares.

Uma característica importante das linguagens funcionais, é serem de *alta ordem*, isto é funções podem receber funções como argumentos e retornar funções como resultados [Pau91]. Exemplos de funções de alta ordem são o cálculo da derivada e da integral de uma dada função real $f(x)$. Em programação funcional expressões consistem principalmente da aplicação de funções. Nesse sentido os termos *functional programming* e *applicative programming* têm o mesmo significado.

4.4.1 Estilo de Programação

Lins et al [LCC95] apresentam argumentos que justificam o desenvolvimento de extensões de linguagens funcionais para computação científica. Analisando, por exemplo, um problema bastante comum em cálculo numérico que é a avaliacão de uma expressão aritmética e para a solução deste problema o Algoritmo 1 a seguir proposto por Böhm [Böh83].

Algoritmo 1

$$
\begin{array}{lll}
1. & \text{approximate solution} & \\
 & x_0^0 := p_0; & (1) \\
 & x_i^0 := x_{i-1}^0 \boxdot t \boxplus \ , p_i,\ i = 1, \ldots, n) & (2) \\
2. & \text{iteration} & \\
 & k := 0; & \\
 & \text{repeat } k := k + 1; & \\
 & \text{if } k > 1 \text{ then } x^k := mid(X^k); & \\
 & d^k := \diamond(p - \sum_{i=0}^{k-1} Ax_i); & \\
 & X_0^k := d_0^k; & (3) \\
 & X_i^k := X_{i-1}^k \odot t \oplus \ , d_i^k,\ i = 1, \ldots, n; & (4) \\
 & Y^k := \diamond(X_n^k + \sum_{i=0}^{k-1} x_n^i) & \\
 & \text{until } (\triangle(diam(X_n^k)) < \delta \cdot \mid Y^k \mid) & (5) \\
 & \text{or } (Y = 0) \text{ or } (\text{underflow and } k \geq 10). &
\end{array}
$$

O problema refere-se a avaliação do polinômio

$$p(x) = \sum_{i=0}^{n} p_{n-i} x^i,\ p \in S$$

em um ponto $t \in S$, com exatidão máxima. Basicamente o algoritmo contém uma aproximação inicial, procedimento iterativo e regra de parada. Este algoritmo é visto relacionando os seguintes aspectos:

- Numéricos. Problemas da manipulação de números de ponto flutuante e vantagens dos métodos intervalares e de exatidão máxima;
- Programação Funcional. Características de programação funcional relevantes para métodos numéricos.

Recursividade: A recursividade pode ser observada em (4). Nota-se também que a implementação de um algoritmo como este em uma linguagem funcional, é a forma natural como um matemático ou analista numérico está habituado a calcular.

Alta Ordem: Observando-se a expressão (5), que é a regra de parada do algoritmo, sabe-se da aritmética de exatidão máxima que $\triangle$ e diam(X) são funções. Portanto $\triangle$ é uma função que recebe uma função como argumento e retorna um real. É uma das principais características de linguagens funcionais serem de alta ordem o que neste caso condiz com o algoritmo intervalar proposto. Convém enfatizar que esta regra de parada é um critério canônico de parada de algoritmos intervalares [Moo66, Moo79].

Polimorfismo: A questão do polimorfismo pode ser vista nas expressões (1), (2), (3) e (4) ; (1) e (2) são expressões envolvendo constantes, variáveis e operações com reais. (3) e (4) são expressões envolvendo constantes, variáveis e operações com intervalos. O destaque porém é que as expressões sintaticamente são as mesmas. A depender como seja a tradução entre o paradigma imperativo para o funcional pode-se ver, também, o relacionamento acima como um caso de sobrecarga de operadores (*operator overloading*).

Programas funcionais dizem "o que" fazer ao invés do "como" fazer característica da programação imperativa. É desnecessário enfatizar que programas confiáveis exigem uma aritmética confiável. Possivelmente, essa linha de raciocínio seja o motivo pelo qual o paradigma funcional está na vanguarda da computação científica.

A colocação do tipo intervalo em uma linguagem funcional pode ter como objetivos:

- a implementação de algoritmos intervalares,
- a prova de teoremas.

Se o objetivo é implementar algoritmos, a decisão seguinte é se o tipo intervalo é implementado com precisão fixa ou infinita. Se a precisão do tipo é infinita, o estilo funcional *lazy* permite que conjuntos sejam definidos intencionalmente, isto é, através de sua lei de formação. Isso possibilita o aparecimento de conjuntos infinitos. Como um intervalo tem como limites, inferior e superior, números reais, a idéia é que se use reais preguiçosos. Porém isso, pode tornar a implementação de algoritmos ineficientes. Se a precisão do tipo é fixa, a aritmética de alta exatidão [KM81] precisa ser implementada. A aritmética intervalar é uma alternativa à aritmética de precisão infinita a um custo computacional mais baixo. A introdução do tipo intervalo em linguagens funcionais, proposta em [LCC95], oferece uma solução simples para tornar programas numéricos mais confiáveis.

Quando o objetivo é usar uma linguagem para provar teoremas automaticamente, OBJ3 [GWM+93] pode ser uma ferramenta útil. Foi esta o provador automático usado na especificação do tipo intervalo na seção a seguir [CSB95b, CSB95a]. Outra linguagem de especificação poderia ser usada, tal como EML [SRC93, San88, ST91].

O desenvolvimento dos computadores trouxe de volta a questão da representação numérica. É próprio do *hardware* operar com um número pré-fixado de bits. Em se tratando dos números inteiros a precisão fixa tem como única consequência a possibilidade de *overflow*. Maiores dificuldades surgem com os reais pois quaisquer que sejam os limites impostos à excursão, haverá um conjunto infinito de números reais dos quais apenas uma pequena parte pode ser representada.

Os sistemas numéricos de ponto flutuante e intervalar são exemplos conhecidos de sistemas que operam com precisão fixa. A grande vantagem da representação intervalar é facilitar a implementação dos métodos auto-validáveis.

4.5 Introdução a OBJ3

OBJ3 é o último em uma série de sistemas OBJ, todos baseados em lógica equacional de primeira ordem. Uma detalhada descrição de OBJ3 pode ser encontrada em [GWM+93]. Nesta seção é dada uma sucinta descrição do sistema.

OBJ3 é uma linguagem declarativa de propósito geral especialmente útil para especificação e prototipagem. Uma especificação em OBJ3 é uma coleção de módulos de duas espécies: *theories* e *objects*. Uma teoria tem semântica *loose*, no sentido que define uma variedade de modelos. Um objeto tem semântica *tight* ou *standard*, isto é, define a menos de isomorfismo um específico modelo–sua álgebra inicial [GTWW77]. Por exemplo, a especificação usual dos números naturais, descreve precisamente o que se entende pelos números naturais. Como uma teoria, descreve qualquer modelo que satisfaça as propriedades requeridas. Nesse sentido os inteiros poderiam ser um modelo. Uma das conseqüências da distinção entre uma teoria e um objeto é que indução pode ser usada para um objeto, mas não para uma teoria.

Um módulo (um objeto ou teoria) é a unidade da especificação. Compreende uma assinatura e um conjunto de equações (possivelmente condicionais). Essas equações são considerdas regras de reescrita e computações são acompanhadas por reescrita de termos, de forma usual.

Uma notação elaborada para definir assinaturas é fornecida. Como OBJ3 é baseado em *order sorted algebra* [GM89], provê a noção de subsort (subtipo), que é extremamente conveniente na prática. Por exemplo, declarando `Integer` como um subsort de `Float` nenhuma função de conversão é necessária para transformar inteiro em float. Sorts e subsorts são declarados, respectivamente, por

$$\texttt{sorts}\ \langle SortIdList\rangle\ .$$
$$\texttt{subsort}\ \langle SortIdList\rangle < \langle SortIdList\rangle\ .$$

Uma sintaxe *mixfix* geral pode ser usada para definir operadores; usuários podem definir qualquer sintaxe incluindo prefix, posfix e infix. O argumento e valores de um operador são declarados quando sua forma sintática é declarada. A sintaxe geral para um operador é

$$\texttt{op}\ \langle OpForm\rangle : \langle SortList\rangle\ \texttt{->}\ \langle Sort\rangle\ .$$

Adicionalmente, operadores podem ter atributos para descrever propriedades úteis tais como associatividade, comutatividade e identidade. Isto torna possível documentar as principais propriedades de um operador ao nível da declaração. Como conseqüência o número de equações que necessita ser fornecido pelo usuário, pode ser reduzido em muitos casos. Mais importante ainda é que OBJ3 provê reescrita módulo esses atributos.

Módulos podem ser parametrizados por teorias que definem então a estrutura e propriedades requeridas de um parâmetro real para dar significado a instanciação. A instanciação de um módulo genérico requer um *view*–uma função das entidades no requerimento da teoria às entidades nos parâmetros reais (módulo). Como exemplo, um objeto para descrever conjuntos de elementos arbitrários, `SET`, pode ser parametrizado por uma teoria que requer que o módulo argumento tenha (pelo menos) um sort. Estão esse módulo pode ser instanciado para se obter conjuntos de elementos do tipo desejado.

Afora os mecanismos para definir e instanciar módulos genéricos, OBJ3 provê meios para importar e combinar módulos de outros módulos. Por exemplo, `A + B` cria um novo módulo que combina a assinatura e as equações de `A` and `B`.

OBJ3 também pode ser usado como um provador de teoremas. Em particular, computações são acompanhadas por reescrita de termos, que é um método de dedução amplamente aceito. Se as regras de reescrita forem *confluent* e *terminating*, sua exaustiva aplicação funciona como um procedimento de decisão para a teoria: a equivalência de duas expressões pode sempre ser determinada pela redução de ambas a sua forma normal. A equivalência acontece quando as duas formas normais são (sintaticamente) as mesmas. Esse modo de prova é normalmente chamado de *automático*. A estratégia para provas de teoremas consiste em mostrar que todas as reduções avaliadas fornecem como resposta `true`.

Muitas vezes porém, aplicações não satisfazem propriedades desejáveis no sentido de a reescrita automática de termos reduzir-se a expressões equivalentes, ou então o processo pode não terminar. Entretanto OBJ3 também provê mecanismos para a aplicação de regras de uma forma controlada pelo usuário.

4.6 Especificação do Tipo Intervalo em OBJ3

A introdução de tipos de dados em linguagens de programação pode ter diferentes objetivos. No caso da computação científica a introdução de um determinado tipo usualmente tem como objetivo o desenvolvimento de algoritmos numéricos envolvendo o tipo.

Esta seção descreve sucintamente um trabalho de pesquisa relacionado com a introdução de tipo intervalo em uma liguagem funcional, mas com o objetivo de provar teoremas da matemática intervalar [CSB95b, CSB95a]. Do ponto de vista da matemática intervalar as provas aqui feitas podem ser encontradas nas referências sobre o assunto, como em [Moo66, Moo79, AH83]. A contribuição e originalidade deste trabalho consiste em usar uma linguagem algébrica para especificar o tipo intervalo e para desenvolver provas mecanicamente, ou como denominado atualmente, provas assistidas por computador. OBJ3 é um provador de teoremas amplamente usado, como pode ser visto em [Sam93].

Para provar a corretude de qualquer programa em OBJ3 que faça uso do `type interval`, o usuário pode fazer uso da biblioteca aqui desenvolvida. Portanto esta é o núcleo para qualquer uma outra desenvolvida em OBJ3, que também pode ser facilmente traduzida para qualquer outro sistema provador de teoremas, seguindo-se os passos aqui apresentados.

A teoria `INTERVAL` precisa incluir variáveis booleanas e reais, respectivamente `BOOL` e `REAL`, com seus respectivos operadores. OBJ3 tem módulos que implementam essas duas álgebras. Adicionalmente, dadas as características do tipo intervalo, é necessário usar conjuntos de números reais. Isto pode ser feito especificando a teoria de conjuntos como um módulo genérico (parametrizado pelo tipo de elementos). Então este módulo genérico pode ser instanciado com o módulo `REAL`. Além da declaração do tipo de elementos, é necessário definir uma ordem total entre elementos, porque a teoria usa propriedades de conjuntos, tal como o máximo (`max`) e o mínimo (`min`) de um conjunto.

`INTERVAL` contém uma descrição do tipo (sort) `INTERVAL` como também de seus operadores unários e binários. O módulo `BOOL` é importado usando a cláusula `protecting`, o que significa que `INTERVAL` não adiciona novos elementos a esta álgebra e que nenhum elemento distinto em `BOOL` (tais como true e false) são identificados em `INTERVAL`. Como o módulo `SET` é genérico, pode ser importado para `INTERVAL` depois de ser instanciado; nesse caso particular, este módulo é instanciado com o módulo `REAL`, porque o interesse é conjunto de números reais. A ênfase em conjuntos de números reais é para compatibilizar conhecimento teóricos com termos usados. Por exemplo, sabe-se que a operação aritmética de adição entre números reais é associativa, o que, geralmente, não é verdade para números de ponto flutuante.

A relação `subsort` declara que intervalos podem ser representados como conjuntos. Esta facilidade de OBJ3 é particularmente útil na definição de interseção de intervalos, quando o resultado de alguma operação pode ser o conjunto vazio. O construtor do tipo interval (`[_,_]`) é um operador parcial pois o limite inferior de um intervalo tem de ser menor ou igual ao limite superior. Os símbolos `[prec 2]`, `[prec 4]`, `[prec 5]` e `[prec 6]` são as precedências dos operadores recíproco, negação, multiplicação e subtração. Isto significa, por exemplo que a precedência da negação é mais baixa que a precedência da multiplicação em têrmos que envolvem ambas. As propriedades adicionais dos operadores são descritas pelas equações (`eq`) e equações condicionais (`cq`). É possível associar um nome (label) às equações.

Segue-se a especificação do tipo intervalo e exemplos de como usá-la. As computações são através de reescrita de termos, usando as equações na teoria. Todos os detalhes das provas podem ser encontrados em [Cam95].

```
th INTERVAL is

  protecting BOOL .
  protecting SET[REAL] .

  sort Interval .
  subsort Interval < Set .

  op-as [_,_]    : Real Real -> Interval  for [x1,x2] if  x1 <= x2 .
  op _+_         : Interval Interval -> Interval [prec 6] .
  op -_          : Interval -> Interval [prec 4] .
  op _-_         : Interval Interval -> Interval [prec 6] .
  op _*_         : Interval Interval -> Interval [prec 5] .
  op _ -1        : Interval -> Interval [prec 2] .
  op _/_         : Interval Interval -> Interval [prec 5] .
  op w_          : Interval -> Real .
  op absi_       : Interval -> Real .
  op pm_         : Interval -> Real .
  op d           : Interval Interval -> Real .
  op _om_        : Interval Interval -> Bool .
  op _ok_        : Interval Interval -> Bool .
  op _inc_       : Interval Interval -> Bool .
  op _/\_        : Interval Interval -> Interval .
  op _\/_        : Interval Interval -> Interval .
  op _pertains_ : Real Interval -> Bool .

  [add]  eq [x1,x2] + [x3,x4] = [x1 + x3, x2 + x4] .
  [sym]  eq - [x1,x2] = [- x2, - x1 ] .
  [dif]  eq A - B = A + - B .
  [eq]   eq [x1, x2] == [x3, x4] = (x1 == x3) and (x2 == x4) .
  [mult] eq [x1,x2] * [x3,x4] = [min({x1 * x3} U {x1 * x4} U
                                     {x2 * x3} U {x2 * x4}),
                                 max({x1 * x3} U {x1 * x4} U
                                     {x2 * x3} U {x2 * x4})] .
  [rec]  eq [x1,x2] -1 = [1 / x2, 1 / x1] .
  [div]  eq A / B = A  * B -1 .
  [wid]  eq w [x1,x2] = x2 - x1 .
  [abs]  eq absi [x1,x2] = max({abs(x1)} U {abs(x2)}) .
```

```
  [dist] eq d([x1,x2] , [x3,x4]) = max({abs(x1 - x3)} U {abs (x2 - x4)}) .
  [pm]   eq pm [x1,x2] = (x1 + x2) / 2 .
  [om]   cq [x1,x2] om [x3,x4] = true if x2 < x3 .
  [ok]   cq [x1,x2] ok [x3,x4] = true if x1 <= x3 and  x2 <=  x4 .
  [inc]  eq [x1,x2] inc [x3,x4] = if x3 <= x1 and  x2 <= x4
                                    then true
                                    else false
                                  fi .
  [int]  eq [x1,x2] /\ [x3,x4] = if x1 > x4 or x2 < x3
                                    then {}
                                    else [max ({x1} U {x3}),
                                          min({x2}  U{x4})]
                                 fi .
  [uni]  eq [x1,x2] \/ [x3,x4] = if ([x1,x2] /\ [x3,x4]) == {}
                                    then {}
                                    else [min ({x1} U {x3}),
                                          max({x2}  U{x4})]
                                 fi .
  [pert] cq x1 pertains [x2,x3] = true if x2 <= x1 and x1 <=  x3 .

endth
```

Os exemplos a seguir ilustram o uso da teoria `INTERVAL`. Na seção a seguir a teoria `INTERVAL` será usada para provar teoremas.

Exemplo 4.6.1 Este exemplo avalia o negativo de um termo na teoria `INTERVAL`. O termo a ser avaliado é

```
reduce - [-4,-2] .
```

O sistema retorna:

```
==========================================
reduce in INTERVAL : - [- 4.0,- 2.0]
rewrites: 3
result Interval: [2.0,4.0]
==========================================
```

O comando `reduce` ou (`red`) é executado pela aplicação de regras de reescrita. Neste exemplo o sistema fez 5 passos de reescrita. O resultado é o intervalo [2.0,4.0].

Exemplo 4.6.2 Dados os intervalos X=[1,2], Y=[3,4], Z=[-3.5,0] e W=[-3,0], avaliar a expressão

$$((X^{-1} * (-Y)) \cap Z)$$

e comparar o intervalo resultante com W, usando a ordem proposta [KM81]. O comando é

```
red (( [1,2] -1 * -[3,4]) /\ [-3.5,0]) ok [-3,0] .
```

O sistema retorna:

```
==========================================
reduce in INTERVAL : ([1.0,2.0] -1 * - [3.0,4.0]) /\ [-3.5,0.0] ok
    [-3.0,0.0]
rewrites: 63
result Bool: true
==========================================
```

4.7 Provando Teoremas

Os teoremas a seguir dizem respeito às propriedades algébricas, topológicas e de conjuntos, quando intervalos são vistos como conjuntos, do espaço dos intervalos. No capítulo 2 algumas dessas foram referidas, porém as constantes nos teoremas a seguir compõem um conjunto mais exaustivo. Todas são provadas usando a teoria `INTERVAL`. As provas com todos os detalhes podem ser encontrados em [Cam95]. Aqui são apresentados apenas alguns exemplos. A teoria `INTERVAL` que aparece ao final corresponde à teoria inicial, mas com todas as propriedades dos operadores, que foram provadas automaticamente, colocadas ao nível da especificação. Sejam X, Y e Z intervalos.

Teorema 4.7.1 Propriedades Algébricas

(a) $X + Y = Y + X$ (comutatividade da adição)

(b) $X + (Y + Z) = (X + Y) + Z$ (associatividade da adição)

(c) $X + 0 = X$ (elemento neutro aditivo)

(d) $0 \in X - X$

(e) $X * Y = Y * X$ (comutatividade da multiplicação)

(f) $X * (Y * Z) = (X * Y) * Z$ (associatividade da multiplicação)

(g) $X * 1 = X$ (elemento neutro multiplicativo)

(h) $1 \in X/X, 0 \notin X$

(i) $X * (Y + Z) \subseteq X * Y + X * Z$ (subdistributividade)

Teorema 4.7.2 Intervalos como Conjuntos

(a) $X \cap Y = Y \cap X$ (cumutatividade da interseção)

(b) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ (associatividade da interseção)

(c) $X \cup Y = Y \cup X$ (comutatividade da união)

(d) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$ (associatividade da união)

Teorema 4.7.3 **Propriedades Topológicas**

(a) $X \subseteq Y \Rightarrow w(X) \leq w(Y)$

(b) $w(X+Y) = w(X) + w(Y)$

(c) $w(X-Y) = w(X) + w(Y)$

(d) $d(X,Y) = 0 \Leftrightarrow X = Y$

(e) $d(X,Y) = d(Y,X)$

(f) $d(X,Z) \leq d(X,Y) + d(Y,Z)$

(g) $\mid X \mid \geq 0$

(h) $\mid X \mid = 0 \Leftrightarrow X = [0,0]$

(i) $\mid X+Y \mid \leq \mid X \mid + \mid Y \mid$

(j) $\mid X*Y \mid = \mid X \mid * \mid Y \mid$

(k) $X \subseteq Y \Rightarrow \mid X \mid \leq \mid Y \mid$

Em todas as provas a seguir, a primeira parte corresponde ao arquivo de entrada. A segunda parte começando por `OBJ>` e por `OBJ> ev (dribble)` é o *output* do sistema. A última informação precisa ser sempre `result Bool: true`. Além do resultado, o sistema escreve o número de regras de reescrita aplicadas. Nestas provas o arquivo de entrada é `Proof<n>.obj` , onde `n=1,...,24`, (pois são 24 resultados que são provados), que corresponde ao número da prova. A seqüência de comandos para OBJ3 ler o arquivo de entrada e imprimir o resultado no arquivo de saída é

```
OBJ> ev (dribble "Proof<n>.out")
OBJ> in Proof<n>.obj
OBJ> ev (dribble)
```

Na seqüência de provas abaixo sejam $X = [x_1, x_2]$, $Y = [x_3, x_4]$, $Z = [x_5, x_6]$.

A seguir são apresentados exemplos de provas relacionadas com as propriedades algébricas da aritmética intervalar. A aritmética usada é como definida em Moore [Moo66, Moo79] ou Acioly [Aci91].

4.7.1 $X + Y = Y + X$, comutatividade da adição

```
open .
ops 'x1 'x2 'x3 'x4 : -> Float .
red ['x1, 'x2] + ['x3, 'x4] == ['x3, 'x4] +  ['x1, 'x2] .
close

OBJ>
in Proof1.obj
==========================================
open
==========================================
ops 'x1 'x2 'x3 'x4 : -> Float .
==========================================
reduce in INTERVALO : ['x1,'x2] + ['x3,'x4] == ['x3,'x4] + ['x1,'x2]
```

```
rewrites: 6
result Bool: true
==========================================
close
OBJ> ev (dribble)
```

■

A prova foi concluída após 6 passos de reescrita, quando o resultado foi `true`.

4.7.2 $1 \in X/X,\ 0 \notin X$

Esta prova considera todos os possíveis valores para os extremos do intevalo $[x_1, x_2]$.

```
open .
ops 'x1 'x2 : -> Float .
eq 'x1 <= 'x2 = true .
eq 'x2 <= 'x1 = false .
eq 'x1 <= 0 = false .
eq 'x2 <= 0 = false .
red 1 pertains (['x1, 'x2] / ['x1, 'x2]) .
eq 'x1 <= 0 = true .
eq 'x2 <= 0 = false .
red 1 pertains (['x1, 'x2] / ['x1, 'x2]) .
eq 'x1 <= 0 = true .
eq 'x2 <= 0 = true .
red 1 pertains (['x1, 'x2] / ['x1, 'x2]) .
close

OBJ>
in Proof8
==========================================
open
==========================================
ops 'x1 'x2 : -> Float .
==========================================
eq 'x1 <= 'x2 = true .
==========================================
eq 'x2 <= 'x1 = false .
==========================================
eq 'x1 <= 0 = false .
==========================================
eq 'x2 <= 0 = false .
==========================================
reduce in INTERVALO : 1.0 pertains ['x1,'x2] / ['x1,'x2]
rewrites: 47
result Bool: true
==========================================
eq 'x1 <= 0 = true .
==========================================
eq 'x2 <= 0 = false .
==========================================
reduce in INTERVALO : 1.0 pertains ['x1,'x2] / ['x1,'x2]
```

```
rewrites: 47
result Bool: true
==========================================
eq 'x1 <= 0 = true .
==========================================
eq 'x2 <= 0 = true .
==========================================
reduce in INTERVALO : 1.0 pertains ['x1,'x2] / ['x1,'x2]
rewrites: 47
result Bool: true
==========================================
close
OBJ> ev (dribble)
```

■

Na seguinte propriedade intervalos são vistos como conjuntos.

4.7.3 $X \cap Y = Y \cap X$, comutatividade da interseção

```
open .
ops 'x1 'x2 'x3 'x4 : -> Float .
eq 'x1 <= 'x2 = true .
eq 'x2 <= 'x1 = false .
eq 'x3 <= 'x4 = true .
eq 'x4 <= 'x3 = false .
eq 'x2 > 'x3 = true .
eq 'x1 < 'x4 = true .
eq 'x3 > 'x2 = false .
eq 'x4 < 'x1 = false .
eq 'x1 > 'x4 = false .
eq 'x2 < 'x3 = false .
eq 'x1 <= 'x3 = true .
eq 'x3 <= 'x1 = false .
eq 'x2 <= 'x4 = false .
eq 'x4 <= 'x2 = true .
red ['x1, 'x2] /\ ['x3, 'x4] == ['x3, 'x4] /\ ['x1, 'x2] .

OBJ>
in Proof10
==========================================
open
==========================================
ops 'x1 'x2 'x3 'x4 : -> Float .
==========================================
eq 'x1 <= 'x2 = true .
==========================================
eq 'x2 <= 'x1 = false .
==========================================
eq 'x3 <= 'x4 = true .
==========================================
eq 'x4 <= 'x3 = false .
```

```
==========================================
eq 'x2 > 'x3 = true .
==========================================
eq 'x1 < 'x4 = true .
==========================================
eq 'x3 > 'x2 = false .
==========================================
eq 'x4 < 'x1 = false .
==========================================
eq 'x1 > 'x4 = false .
==========================================
eq 'x2 < 'x3 = false .
==========================================
eq 'x1 <= 'x3 = true .
==========================================
eq 'x3 <= 'x1 = false .
==========================================
eq 'x2 <= 'x4 = false .
==========================================
eq 'x4 <= 'x2 = true .
==========================================
reduce in INTERVALO : ['x1,'x2] /\ ['x3,'x4] == ['x3,'x4] /\ ['x1,'x2]
rewrites: 30
result Bool: true
==========================================
close
OBJ> ev (dribble)
```

■

A seguir algumas provas relacionadas com a amplitude de intervalos.

4.7.4 $X \subseteq Y \Rightarrow w(X) \leq w(Y)$

```
open .
ops 'x1 'x2 'x3 'x4 : -> Float .
eq 'x1 <= 'x2 = true .
eq 'x2 <= 'x1 = false .
eq 'x3 <= 'x4 = true .
eq 'x4 <= 'x3 = false .
eq 'x1 <= 'x3 = false .
eq 'x3 <= 'x1 = true .
eq 'x2 <= 'x4 = true .
eq 'x4 <= 'x2 = false .
red  if (['x1, 'x2] inc ['x3, 'x4])
then w ['x1, 'x2] <= w ['x3, 'x4]
else true
     fi .
close

OBJ>
in Proof14
```

```
==========================================
open
==========================================
ops 'x1 'x2 'x3 'x4 : -> Float .
==========================================
eq 'x1 <= 'x2 = true .
==========================================
eq 'x2 <= 'x1 = false .
==========================================
eq 'x3 <= 'x4 = true .
==========================================
eq 'x4 <= 'x3 = false .
==========================================
eq 'x1 <= 'x3 = false .
==========================================
eq 'x3 <= 'x1 = true .
==========================================
eq 'x2 <= 'x4 = true .
==========================================
eq 'x4 <= 'x2 = false .
==========================================
reduce in INTERVALO : if ['x1,'x2] inc ['x3,'x4] then w ['x1,'x2] <=
    w ['x3,'x4] else true fi
rewrites: 20
result Bool: true
==========================================
close
OBJ> ev (dribble)
```

■

4.7.5 $w(X + Y) = w(X) + w(Y)$

```
open .
ops 'x1 'x2 'x3 'x4 : -> Float .
eq 'x1 <= 'x2 = true .
eq 'x2 <= 'x1 = false .
eq 'x3 <= 'x4 = true .
eq 'x4 <= 'x3 = false .
red w(['x1, 'x2] + ['x3, 'x4]) == w ['x1, 'x2] + w ['x3, 'x4] .
close

OBJ>
in Proof15
==========================================
open
==========================================
ops 'x1 'x2 'x3 'x4 : -> Float .
==========================================
reduce in INTERVALO : w ['x1,'x2] + ['x3,'x4] == w ['x1,'x2] + w ['x3,
    'x4]
rewrites: 15
```

```
result Bool: true
==========================================
close
OBJ> ev (dribble)
```

■

4.7.6 $w(X - Y) = w(X) + w(Y)$

```
open .
ops 'x1 'x2 'x3 'x4 : -> Float .
red w(['x1, 'x2] - ['x3, 'x4]) == w ['x1, 'x2] + w ['x3, 'x4] .
close

OBJ>
in Proof16
==========================================
open
==========================================
ops 'x1 'x2 'x3 'x4 : -> Float .
==========================================
reduce in INTERVALO : w ['x1,'x2] - ['x3,'x4] == w ['x1,'x2] + w ['x3,
    'x4]
rewrites: 18
result Bool: true
==========================================
close
OBJ> ev (dribble)
```

■

As provas seguintes dizem respeito a conceitos topológicos tais como, por exemplo, distância.

4.7.7 $d(X, Y) = 0$ se e só se $X = Y$

```
open .
ops X Y : -> Interval .
ops 'x1 'x2 'x3 'x4 : -> Float .
eq 'x1 <= 'x2 = true .
eq 'x3 <= 'x4 = true .
eq 'x2 <= 'x1 = false .
eq 'x4 <= 'x3 = false .
eq 'x1 == 'x3 = true .
eq 'x2 == 'x4 = true .
red if ( d(['x1, 'x2], ['x3, 'x4]) == 0 )
      then ['x1, 'x2] == ['x3, 'x4]
      else true
    fi .
close

OBJ>
```

```
in Proof17
==========================================
open
==========================================
ops X Y : -> Intervalo .
==========================================
ops 'x1 'x2 'x3 'x4 : -> Float .
==========================================
eq 'x1 <= 'x2 = true .
==========================================
eq 'x3 <= 'x4 = true .
==========================================
eq 'x2 <= 'x1 = false .
==========================================
eq 'x4 <= 'x3 = false .
==========================================
eq 'x1 == 'x3 = true .
==========================================
eq 'x2 == 'x4 = true .
==========================================
reduce in INTERVALO : if d(['x1,'x2],['x3,'x4]) == 0.0 then ['x1,'x2]
==
    ['x3,'x4] else true fi
rewrites: 17
result Bool: true
==========================================
close
OBJ> ev (dribble)
```

■

4.7.8 $\mid X \mid \geq 0$

Esta prova considera todos os possíveis valores para os extremos do intervalo $[x_1, x_2]$.

```
open .
ops 'x1 'x2 : -> Float .
eq 'x1 <= 'x2 = true .
eq 'x2 <= 'x1 = false .
eq 'x1 <= 0 = true .
eq 'x2 <= 0 = false .
eq 'x2 <= - 'x1 = false .
red not (absi (['x1, 'x2]) <= 0) .
eq 'x1 <= 0 = false .
eq 'x2 <= 0 = false .
red not (absi (['x1, 'x2]) <= 0) .
eq 'x1 <= 0 = true .
eq 'x2 <= 0 = true .
eq - 'x2 <= 'x1 = false .
red not (absi (['x1, 'x2]) <= 0) .
close

OBJ>
```

```
in Proof20
==========================================
open
==========================================
ops 'x1 'x2 : -> Float .
==========================================
eq 'x1 <= 'x2 = true .
==========================================
eq 'x2 <= 'x1 = false .
==========================================
eq 'x1 <= 0 = true .
==========================================
eq 'x2 <= 0 = false .
==========================================
eq 'x2 <= - 'x1 = false .
==========================================
reduce in INTERVALO : not absi ['x1,'x2] <= 0.0
rewrites: 13
result Bool: true
==========================================
eq 'x1 <= 0 = false .
==========================================
eq 'x2 <= 0 = false .
==========================================
reduce in INTERVALO : not absi ['x1,'x2] <= 0.0
rewrites: 13
result Bool: true
==========================================
eq 'x1 <= 0 = true .
==========================================
eq 'x2 <= 0 = true .
==========================================
eq - 'x2 <= 'x1 = false .
==========================================
reduce in INTERVALO : not absi ['x1,'x2] <= 0.0
rewrites: 15
result Bool: true
==========================================
close
OBJ> ev (dribble)
```

■

4.8 Teoria Enriquecida

Como mencionado anteriormente, a `theory INTERVAL` é agora paresentada com todas as propriedades que foram provadas a partir da especificação inicial.

```
th INTERVAL is

  protecting BOOL .
```

```
protecting SET[REAL] .

sort Interval .
subsort Interval < Set .

op-as [_,_]   : Real Real -> Interval  for [x1,x2] if  x1 <= x2 .
op _+_        : Interval Interval -> Interval [prec 6] [comm  assoc id: [0,0]] .
op -_         : Interval -> Interval [prec 4] .
op _-_        : Interval Interval -> Interval [prec 6] .
op _*_        : Interval Interval -> Interval [prec 5] [comm  assoc id: [1,1]] .
op _ -1       : Interval -> Interval [prec 2] .
op _/_        : Interval Interval -> Interval [prec 5] .
op w_         : Interval -> Real .
op absi_      : Interval -> Real .
op pm_        : Interval -> Real .
op d          : Interval Interval -> Real .
op _om_       : Interval Interval -> Bool .
op _ok_       : Interval Interval -> Bool .
op _inc_      : Interval Interval -> Bool .
op _/\_       : Interval Interval -> Interval [comm assoc] .
op _\/_       : Interval Interval -> Interval [comm assoc] .
op _pertains_ : Real Interval -> Bool .


[add]  eq [x1,x2] + [x3,x4] = [x1 + x3, x2 + x4] .
[sym]  eq - [x1,x2] = [- x2, - x1 ] .
[dif]  eq A - B = A + - B .
[eq]   eq [x1, x2] == [x3, x4] = (x1 == x3) and (x2 == x4) .
[mult] eq [x1,x2] * [x3,x4] = [min({x1 * x3} U {x1 * x4} U
                                   {x2 * x3} U {x2 * x4}),
                               max({x1 * x3} U {x1 * x4} U
                                   {x2 * x3} U {x2 * x4})] .
[rec]  eq [x1,x2] -1 = [1 / x2, 1 / x1] .
[div]  eq A / B = A  * B -1 .
[wid]  eq w [x1,x2] = x2 - x1 .
[abs]  eq absi [x1,x2] = max({abs(x1)} U {abs(x2)}) .
[dist] eq d([x1,x2] , [x3,x4]) = max({abs(x1 - x3)} U {abs (x2 - x4)}) .
[pm]   eq pm [x1,x2] = (x1 + x2) / 2 .
[om]   cq [x1,x2] om [x3,x4] = true if x2 < x3 .
[ok]   cq [x1,x2] ok [x3,x4] = true if x1 <= x3 and  x2 <=  x4 .
[inc]  eq [x1,x2] inc [x3,x4] = if x3 <= x1 and  x2 <= x4
                                  then true
                                  else false
                                fi .
[int]  eq [x1,x2] /\ [x3,x4] = if x1 > x4 or x2 < x3
                                  then {}
                                  else [max ({x1} U {x3}),
                                        min({x2}  U{x4})]
                               fi .
[uni]  eq [x1,x2] \/ [x3,x4] = if ([x1,x2] /\ [x3,x4]) == {}
                                  then {}
                                  else [min ({x1} U {x3}),
                                        max({x2}  U{x4})]
```

```
                                fi .
  [pert] cq x1 pertains [x2,x3] = true if x2 <= x1 and x1 <=  x3 .

endth
```

4.9 Conclusões

Existe um grande interesse da comunidade científica pelo desenvolvimento de sistemas de provas baseados em computação simbólica que venham se somar às técnicas de validação de algoritmos fundamentadas no produto interno ótimo e na aritmética de exatidão máxima. A biblioteca desenvolvida aqui contribui para mostrar como provas da matemática intervalar podem ser feitas usando uma linguagem de programação como um provador de teoremas. Isso implica, entre outros, na validação de algoritmos ou programas. Validação ou verificação tem caracterizado um esforço da computação científica para gerar, paralelamente a algoritmos numéricos, resultados computacionais corretos dentro de um rigor matemático.

Capítulo 5

A Probabilidade Intervalar

Neste capítulo é definido um *espaço de probabilidade intervalar*. Neste espaço a *probabilidade intervalar* é proposta a partir do conceito de extensões de funções reais [Moo66, Moo79, Aci91, Aci96]. Basicamente, a probabilidade intervalar consiste em substituir a probabilidade real por um intervalo que a contenha e as operações sobre o conjunto dos números reais pelas correspondentes sobre o conjunto dos intervalos.

Inicialmente são apresentados conceitos básicos de probabilidade [Kol50, Fel68, Bre69, Bur72, Chu74, Bil79] e exemplos mostrando erros numéricos quando probabilidades são calculadas. A seguir é definido o espaço de probabilidade intervalar com a função probabilidades intervalar satisfazendo específicas propriedades ou axiomas. Resultados relacionados com o conceito proposto são provados e as variáveis aleatórias de Bernoulli, Binomial e Poisson [Fel68, Bre69, Jam81] são vistas à luz do novo enfoque.

5.1 Noções Básicas de Probabilidade

Esta seção contém noções de probabilidade [Kol50, Fel68, Bre69, Bur72, Chu74, Bil79]. Os conceitos aqui apresentados são fundamentais para o desenvolvimento da teoria das probabilidades e para a probabilidade intervalar proposta nesta tese. Serão apresentados erros numéricos detectados a partir da computação de algumas probabilidades específicas, que ilustram a necessidade de se propor a probabilidade intervalar.

A Teoria da Probabilidade é o ramo da matemática relacionado com *fenômenos aleatórios*, os quais apresentam as seguintes características: (i) podem ser repetidos sob as mesmas condições; (ii) apresentam um conjunto de possíveis resultados; (iii) quando realizado um grande número de vezes, apresentam uma regularidade. Um exemplo clássico é o lançamento de uma moeda. A teoria da probabilidade desenvolve uma estrutura matemática formal para o tratamento dos fenômenos aleatórios. Sua construção axiomática foi proposta por Kolmogorov [Kol50].

O conjunto dos possíveis resultados de um experimento aleatório é chamado *espaço amostal* e é denotado por Ω. Seja $\mathcal{A}$ uma família de subconjuntos de Ω. Os subconjuntos de Ω são chamados *eventos*. Um evento é um elemento A em $\mathcal{A}$. Do ponto de vista matemático $\mathcal{A}$ é apenas uma coleção especificada de subconjuntos de Ω. Serão associadas probabilidades apenas aos elementos $A \in \mathcal{A}$, isto é, aos eventos.

A questão seguinte é definir qual a estrutura da coleção $\mathcal{A}$. Inicialmente pode-se supor que $\mathcal{A}$ seja fechada com respeito a uniões e interseções finitas. Dizer que o evento A não ocorre significa dizer que ocorre seu complementar, A^c. Assim, exige-se também que a classe $\mathcal{A}$ seja fechada com respeito a complementações. Conclui-se, então que $\mathcal{A}$ deve ter uma estrutura algébrica. Porém, por razões matemáticas, $\mathcal{A}$ deve ser uma classe mais restritiva, isto é, $\mathcal{A}$ deve ser fechada com respeito a uniões enumeráveis. Exige-se, portanto, que $\mathcal{A}$ seja uma σ-álgebra.

Definição 5.1.1 Uma coleção $\mathcal{A}$ de subconjuntos de Ω é uma *σ-álgebra* se os seguintes axiomas são satisfeitos:

(A1) $\Omega \in \mathcal{A}$
(A2) $A \in \mathcal{A} \Rightarrow A^c \in \mathcal{A}$
(A3) Se A_n está em $\mathcal{A}$, $n = 1, 2, ...,$ então $\cup_{n=1}^{\infty} A_n \in \mathcal{A}$

A axiomática da teoria das probabilidades fundamenta-se nas analogias entre medida de um conjunto e probabilidade de um evento, na integral de uma função e esperança matemática de uma variável aleatória. Como uma disciplina matemática pode e deve ser desenvolvida a partir dos axiomas propostos. Isto significa que todo desenvolvimento adicional deve ser baseado exclusivamente nos axiomas.

Definição 5.1.2 Um *espaço de probabilidade* é uma quádrupla $\langle \mathcal{A}, \mathbb{R}, \Omega, P \rangle$, onde $\mathcal{A}$ é uma família de conjuntos, $\mathbb{R}$ é o conjunto dos números reais, Ω é um elemento destacado de $\mathcal{A}$, o qual corresponde ao espaço amostral e $P : \mathcal{A} \to \mathbb{R}$ é uma medida sobre $\mathcal{A}$ assumindo valores no conjunto dos reais, satisfazendo os seguintes axiomas [Kol50, Fel68, Bur72, Chu74, Bil79]:

(A1) $P(A) \geq 0, \forall A \in \mathcal{A}$

(A2) $P(\Omega) = 1$

(A3) (σ-aditividade). Se A_n é uma coleção contável de subconjuntos de $\mathcal{A}$ disjuntos dois a dois, então $P(\cup_{n=1}^{\infty} A_n) = \sum_{n=1}^{\infty} P(A_n)$

Observa-se que o conjunto de axiomas acima é usualmente proposto, porém não é o único [Kol50, Fel68, Bur72, Chu74, Bil79]. Um outro equivalente, é o seguinte:

(A1) $P(A) \geq 0, \forall\ A \in \mathcal{A}$

(A2) $P(\Omega) = 1$

(A3) Se $A_k \in \mathcal{A}$, $k = 1, 2, ..., n$, $A_i \cap A_j = \emptyset$, $\forall i \neq j$, então $P(\cup_{k=1}^{n} A_k) = \sum_{k=1}^{n} P(A_k)$

(A4) Se $A_n \in \mathcal{A}$, $n = 1, 2, ...$ é uma sequência de elementos de $\mathcal{A}$ decrescente para o vazio, então $\lim_{n\to\infty} P(A_n) = 0$

Dos axiomas vistos tem-se, dentre outras, como conseqüências, onde todos os conjuntos são membros de $\mathcal{A}$, o seguinte:

(a) $P(\emptyset) = 0$

(b) $P(A) \leq 1$

(c) $P(A^c) = 1 - P(A)$

(d) $A \subseteq B \Rightarrow P(A) \leq P(B)$

(e) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

(f) $A \subseteq B \Rightarrow P(B - A) = P(B) - P(A)$

(g) Propriedade monotônica: se A_n é uma seqüência crescente ou decrescente com limite A, então $P(A_n) \to P(A)$

(h) Desigualdade de Boole: $P(\cup_{n=1}^{\infty} A_n) \leq \sum_{n=1}^{\infty} P(A_n)$

Observa-se que o conceito de probabilidade é suportado fundamentalmente pelas noções de conjuntos, relações e funções e o sistema de números reais. A teoria da probabilidade começa com um espaço abstrato de probabilidades, e desenvolve-se a partir desse. O conceito de variável aleatória, visto a seguir, dada a sua importância, transforma-se rapidamente em um tema central da teoria. A razão para isto deve-se ao fato de que na maioria das situações experimentais o interesse é atribuir um número real ao resultado do experimento.

Definição 5.1.3 Uma *variável aleatória* X [Fel68, Bre69, Jam81] em um espaço de probabilidade $\langle \mathcal{A}, \mathbb{R}, \Omega, P \rangle$ é uma função real definida sobre Ω, $X : \Omega \to \mathbb{R}$, tal que $\{\omega \in \Omega \mid X(\omega) \leq x\} \in \mathcal{A}$ para todo $x \in \mathbb{R}$.

Definição 5.1.4 Uma variável aleatória X é *discreta* se seu contradomínio é um subconjunto finito ou infinito enumerável $\{x_1, x_2, ...\}$ de números reais tal que $\{\omega \mid X(\omega) = x_i\}$ é um evento para todo i. A *função de de probabilidade* para a variável aleatória X é uma função real p_k definida por $p_k = P(X = k) = P(\{\omega \in \Omega \mid X(\omega) = k\})$.

Variáveis aleatórias associadas a contagens de objetos são exemplos de variáveis aleatórias discretas. Existem situações contudo que naturalmente as variáveis aletórias discretas são inadequadas para representá-las. Como exemplo podem ser citadas mensurações relacionadas com grandezas físicas tais como peso, altura, tempo, temperatura e voltagem. Essas grandezas assumem valores reais acarretando a necessidade da definição de um outro tipo de variável aleatória.

Definição 5.1.5 Uma variável aleatória X em um espaço de probabilidade $\langle \mathcal{A}, \mathbb{R}, \Omega, P \rangle$ é denominada variável aleatória *contínua* se existe uma função real $f(x) \geq 0$ tal que $F_X(x) = \int_{-\infty}^{x} f(t)d(t), \forall x \in \mathbb{R}$, onde $F_X(x) = P(X \leq x) = P(\{\omega \in \Omega \mid X(\omega) \leq x\})$.

A seguir são definidas as funções de probabilidade das variáveis aleatórias discretas de Bernoulli, Binomial e Poisson [Fel68, Bre69, Jam81], que são usadas para evidenciar como erros numéricos distorcem resultados teóricos [Fel68, Bre69, Jam81].

Definição 5.1.6 (Bernoulli) Uma variável aleatória de Bernoulli [Fel68, Bre69, Jam81] tem probabilidade de "sucesso" p e de "fracasso" $q = 1 - p$. Sua função de probabilidade é

$$p_k = P(X = k) = p^k q^{1-k}, \ k = 0, 1$$

Definição 5.1.7 (Binomial) Para ensaios de Bernoulli a probabilidade $b(k; n, p)$ [Fel68, Bre69, Jam81] de que n deles resultem em k sucessos e $n - k$ fracassos vale

$$p_k = P(X = k) = \binom{n}{k} p^k q^{n-k}, \ k = 0, \ldots, n$$

Definição 5.1.8 (Poisson) A função de probabilidade de uma variável aleatória de Poisson [Fel68, Bre69, Jam81] com parâmetro $\lambda > 0$, $\lambda \in \mathbb{R}$ é

$$p_k = P(X = k) = \frac{e^{-\lambda}\lambda^k}{k!}, \ k = 0, 1, \ldots.$$

5.1.1 Problemas Numéricos no Cálculo de Probabilidades

Nos exemplos 5.1.9, 5.1.10 e 5.1.11 a seguir X é uma variável aleatória discreta. Para essas variáveis se $p_k = P(X = k)$, $k \in R_X \subseteq \mathbb{R}$, onde R_X é o contradomínio da variável aleatória, (i) $p_k \geq 0$ e (ii) $\sum_{k \in R_X} p_k = 1$.

Exemplo 5.1.9 Seja X uma variável de Bernoulli [Fel68, Bre69, Jam81]. Se $p_1 = p = 1/31$, então $p_2 = q = 30/31$. Obviamente $p_k \geq 0$, $k = 1, 2$ e $p_1 + p_2 = 1$. Os resultados a seguir são obtidos a partir de aproximações para p e q.

$p_1 = p = 1/31 = 0.032258...$
$p_2 = q = 30/31 = 0.967741...$
Se $p_1 \approx 0.032$ e $p_2 \approx 0.968$, $p_1 + p_2 = 1.000$
Se $p_1 \approx 0.0322$ e $p_2 \approx 0.9677$, $p_1 + p_2 = 0.9999$

Considerando as aproximações com 3 e 4 dígitos, mas normalizadas:

$p_1 \approx 0.322 \cdot 10^{-1}$, $p_2 \approx 0.968$, $p_1 + p_2 = 1.0002 \approx 1.000$
$p_1 \approx 0.03226 \cdot 10^{-1}$, $p_2 \approx 0.9677$, $p_1 + p_2 = 0.99996 \approx 1.000$

O ponto importante a ser observado neste exemplo é que $1/31$ sendo um número racional ou tem uma representação decimal finita ou é uma dízima periódica. Porém, pode não ser possível encontrar a parte que se repete ou esta pode ser maior que a capacidade de representação do sistema de ponto flutuante da máquina. Portanto, tomar uma aproximação para o valor da probabilidade é fundamental.

Exemplo 5.1.10 Dado o número de repetições independentes de um experimento, um inteiro $n \geq 0$ e o evento observado A. A variável aleatória X que conta o número de ocorrências de A durante as n repetições do experimento tem distribuição binomial. Se $n = 3$ e $p = 1/3$, então

$$p_k = P(X = k) = \binom{3}{k}(1/3)^k(2/3)^{n-k}, k = 0, \ldots, 3$$

As probabilidades p_k serão computadas de diferentes formas.

(a) Usando durante os cálculos os números racionais $p = 1/3$ e $q = 2/3$

$p_0 = 8/27$
$p_1 = 4/9$
$p_2 = 2/9$
$p_3 = 1/27$
$\sum_{k=0}^{3} P(X = k) = 1$

(b) Nos resultados anteriores, obtendo-se números decimais arredondados,

$p_0 = 0.296296... \approx 0.2963$
$p_1 = 0.444444... \approx 0.4444$
$p_2 = 0.222222... \approx 0.2222$
$p_3 = 0.037037... \approx 0.0370$
$\sum_{k=0}^{3} P(X = k) \approx 0.9999 \neq 1$

(c) Tomando valores arredondados para p e q no início $p \approx 0.3333$ e $q \approx 0.6667$ fazendo os cálculos com todos os dígitos e arredondando-se os resultados obtém-se,

$p_0 = 0.296330752963 \approx 0.2963$
$p_1 = 0.444444441111 \approx 0.4444$
$p_2 = 0.222188888889 \approx 0.2222$
$p_3 = 0.037025927037 \approx 0.0370$
$\sum_{k=0}^{3} P(X = k) = 0.9999 \neq 1$

Exemplo 5.1.11 Seja X uma variável aleatória tendo distribuição de Poisson com parâmetro $\lambda = 2$ e $e = 2.7$, (2.7 é uma aproximação para e).

$$p_k = P(X = k) = \frac{2.7^{-2}2^k}{k!}, k = 0, 1, \ldots$$

$p_0 \approx 0.137$
$p_1 \approx 0.274$
$p_2 \approx 0.274$
$p_3 \approx 0.183$
$p_4 \approx 0.0914 = 0.914 \cdot 10^{-1}$
$p_5 \approx 0.0366 = 0.366 \cdot 10^{-1}$
$p_6 \approx 0.0122 = 0.122 \cdot 10^{-1}$
$\sum_{k=0}^{4} P(X = k) = 1.0082 \approx 1.01 > 1$

Exemplo 5.1.12 Suponha que se tem um espaço amostral $\Omega = \{\omega_1, \omega_2, \omega_3\}$, onde as probabilidades dos eventos elementares são

$$P(\omega_1) = 1/\pi, P(\omega_2) = 1/\sqrt{7}, P(\omega_3) = 1 - (1/\pi + 1/\sqrt{7})$$

Se $\pi \approx 3.14$ e $\sqrt{7} \approx 2.64$, então

$$P(\omega_1) \approx 0.318, P(\omega_2) \approx 0.379, P(\omega_3) \approx 1 - (0.318 + 0.379) \approx 0.303$$

Se $\pi \approx 3.1416$ e $\sqrt{7} \approx 2.6458$, então

$$P(\omega_1) \approx 0.31831, P(\omega_2) \approx 0.37796, P(\omega_3) \approx 1 - (0.31831 + 0.37796) \approx 0.30373$$

As aproximações tomadas para π e $\sqrt{7}$ são exatamente representáveis. Portanto os erros que ocorreram nos cálculos foram erros de arredondamento ou de truncamento. Sabe-se que o aumento da precisão não necessariamente implica qualquer garantia na corretude dos dígitos coincidentes

[Rum88]. No caso deste exemplo o aumento da precisão modificou o valor de $P(\omega_2)$ (diferença no terceiro dígito da mantissa, com respeito às probabilidades anteriores).

Os exemplos anteriores mostram como erros numéricos influem na computação das probabilidades. O resultado da soma de todas as probabilidades relacionadas com os valores que uma dada variável aleatória X pode assumir é 1. Porém, dependendo de como os cálculos sejam efetuados, isto não acontece.

5.2 Extensões Intervalares

A probabilidade intervalar usa a definição e resultados sobre extensões intervalares de funções reais. Em virtude disto seguem-se conceitos básicos pertinentes ao assunto. Detalhes podem ser encontrados em [Moo66, Moo79, Aci91].

Definição 5.2.1 Seja $g : \mathbb{R}^n \to \mathbb{R}$ tal que $(x_1, \cdots, x_n) \mapsto g(x_1, \cdots, x_n)$. Uma extensão intervalar de g é uma função $G : \mathbb{IR}^n \mapsto \mathbb{IR}$ tal que $G([x_1, x_1] \cdots, [x_n, x_n]) = g(x_1, \cdots, x_n)$.

Existem várias extensões intervalares de uma função real f. Isto acontece porque expressões racionais que são equivalentes na aritmética real podem não o ser na aritmética intervalar, como mostra o exemplo a seguir.

Exemplo 5.2.2 Seja a função real $f(x) = x(1-x)$. Sabe-se que

$$x(1-x) = x - x^2 = x - x \cdot x$$

Porém, tem-se como extensões intervalares para f,

$$F_1(X) = X \cdot (1 - X)$$

$$F_2(X) = X - X^2$$

$$F_3(X) = X - X \cdot X$$

Observa-se que:

$$\begin{aligned} F_1([0,1]) &= [0,1] \cdot (1 - [0,1]) \\ &= [0,1] \cdot ([1,1] - [0,1]) \\ &= [0,1] \cdot [0,1] \\ &= [0,1] \end{aligned}$$

No cálculo de $F_2([0,1])$, a seguir, é usada a potência de intervalos, definida em Moore [Moo79] por:

$$X = [x_1, x_2]^n = \begin{cases} [x_1^n, x_2^n], & \text{se } x_1 > 0 \text{ ou } n \text{ é ímpar} \\ [x_2^n, x_1^n], & \text{se } x_2 < 0 \text{ e } n \text{ é par} \\ [0, \mid X \mid^n], & \text{se } 0 \in X \text{ e } n \text{ é par} \end{cases}$$

$$\begin{aligned} F_2([0,1]) &= [0,1] - [0,1]^2 \\ &= [0,1] - [0,1] \\ &= [-1,1] \end{aligned}$$

$$\begin{aligned} F_3([0,1]) &= [0,1] - [0,1] \cdot [0,1] \\ &= [0,1] - [0,1] \\ &= [-1,1] \end{aligned}$$

Nota-se que o *range* de $f(x)$ para $x \in [0,1]$ varia entre 0 e 1/2. Portanto, as extensões intervalares contém o *range* de f. A diferença está em alguns resultados serem melhores que outros no sentido de que se tem, neste caso, $[0,1/2] \subset [0,1] \subset [-1,1]$.

Então, extensões intervalares para uma dada função real f sempre contém o *range* de $f(x)$ para x em um dado intervalo. A questão que permanece é qual extensão intervalar tem resultado mais próximo desse *range*.

Moore e Acioly [Moo66, Moo79, Aci91, Aci96] mostram que funções racionais de variáveis reais têm extensões intervalares canônicas, bastando para isso substituir as variáveis reais por intervalos e as operações aritméticas sobre os números reais pelas correspondentes sobre os intervalos. Então,

(a) Seja I_d a função identidade definida por:

$$I_d : \mathbb{R} \to \mathbb{R}$$

$$I_d(x) = x$$

Uma extensão intervalar para I_d é:

$$I_D : \mathbb{IR} : \mathbb{IR}$$

$$I_D(X) = X$$

(b) Com respeito às operações aritméticas, $*$, $* \in \{+,-,\cdot,/\}$, tem-se, respectivamente, que:

$$* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

$$*(x,y) = x * y$$

$$* : \mathbb{IR} \times \mathbb{IR} \to \mathbb{IR}$$

$$*(X,Y) = X * Y$$

O exemplo a seguir ilustra um aumento na amplitude dos intervalos numa seqüência de operações aritméticas, decorrente dos arredondamentos direcionados.

Exemplo 5.2.3 Sejam os reais 0.2 e 0.3. Se são somados e em seguida tomado um intervalo não-degenerado contendo o resultado da operação tem-se, com 2 dígitos decimais, [0.49,0.51]. Se a cada valor é associado um intervalo não-degenerado e em seguida estes são somados, tem-se [0.19,0.21]+[0.29,0.31]=[0.48,0.52].

Definição 5.2.4 Sejam x, y números reais, $* \in \{+,-,\cdot,/\}$ e:

$$F_{I_d} : \mathbb{R} \to \mathbb{IR}$$

$$F_{I_d}(x) = X,\ x \in X \qquad (1)$$

$$F_* : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{IR} \times \mathbb{IR}$$
$$F_*(x * y) = X * Y \tag{2}$$

Em (1), a função F_{I_d} "estende" um número real para um intervalo e em (2), as operações sobre os reais para as operações sobre os intervalos. Pode-se ver F como um funtor de tradução entre a categoria cujos objetos são reais e as flecha são as funções de variável real e a categoria cujos objetos são intervalos e cujas flechas são funções sobre intervalos. Pode-se também definir o funtor F^{-1} que traduz o intervalo em um número real. F^{-1} é um funtor de esquecimento (*forgetful functor*) e faz a escolha de um real no intervalo para a tradução do intervalo.

É natural pensar que dado $x \in \mathbb{R}$, existe uma infinidade de intervalos X com a propriedade que $x \in X$. Todavia deve ser enfatizado que é sempre possível encontrar um único, basta tomar o intervalo de exatidão máxima que contém x, $[\bigtriangledown x, \triangle x]$.

5.3 Probabilidade Intervalar

Os problemas numéricos vistos anteriormente mostraram como resultados em probabilidade podem ser distorcidos devido aos erros numéricos habituais tais como não representatividade do número real no sistema de ponto flutuante, arredondamento ou truncamento.

Nesta tese é proposto um método para calcular uma denominada *probabilidade intervalar* ou uma *extensão intervalar para a probabilidade* ou ainda uma *validação da probabilidade* para resolver problemas dessa natureza. Tal método é suportado teoricamente pelos trabalhos de Moore [Moo66, Moo79], Kulisch e Miranker [KM81, KM86] e Acioly [Aci91].

Do ponto de vista matemático, a idéia de probabilidade intervalar consiste em dada uma probabilidade, um número real $P(A) = p$, p é substituído por um intervalo que o contém. Do ponto de vista da implementação, p sendo não representável em um específico sistema de ponto flutuante, é substituído pelo menor intervalo que o contém propriamente. Com respeito a ambos pontos de vista, o intervalo não é uma probabilidade, apenas contém o valor da probabilidade, isto é, é uma aproximação da probabilidade exata.

Substituir simplesmente um valor real por um intervalo e as operações sobre os números reais pelas operações sobre o espaço dos intervalos não é suficiente para resolver esses problemas, desde que, entre outros, a estrutura algébrica dos números reais e a dos intervalos não é a mesma. Por exemplo, se $x \in \mathbb{R}$, sabe-se que $x - x = 0$, enquanto que se $X \in \mathbb{IR}$, prova-se que $0 \in X - X$. Portanto, condições adicionais tem que ser introduzidas capazes de preservar a semântica da função probabilidade.

A análise intervalar será útil em dois sentidos. Inicialmente como uma ferramenta conveniente e computacionalmente eficiente para limitar e controlar os erros numéricos. Em segundo lugar para tratar a imprecisão envolvida em modelos probabilísticos. O método proposto mostra que valores não representáveis de probabilidades pertencem a intervalos que, se necessário, podem ter amplitude tão pequena quanto possível.

A aplicação da computação intervalar [KK95] em métodos numéricos para verificação automática dos resultados, tem merecido a atenção de vários pesquisadores, não somente pelos desafios teóricos que esses métodos apresentam como tambem pelo potencial de aplicações práticas. O uso da aritmética intervalar [Sun58, Moo66, Moo79] com os arredondamentos direcionados [KM81, KM86] contém o resultado exato da computação de tal forma que erros de arredondamento, truncamento ou nos dados são rigorosamente limitados (*enclosured*).

A probabilidade intervalar proposta neste trabalho resolve problemas numéricos associados com o cálculo de probabilidades reais. Enfatiza-se ainda que a probabilidade intervalar é uma extensão da probabilidade real, mas que mantém toda a consistência semântica do cálculo probabilístico, buscando para isso recursos da análise intervalar [Sun58, Moo66, Moo79, Aci91, Aci96] e da aritmética de exatidão máxima [KM81, KM86]

O espaço dos intervalos contém os números reais. A teoria intervalar desenvolvida por Moore [Moo66, Moo79] e Acioly [Aci91, Aci96] suporta que cálculos sejam resolvidos no espaço dos números reais ou no espaço dos intervalos. Funções que são definidas dos reais nos reais podem ser estendidas para terem como domínio $\mathbb{IR}$ e contradomínio $\mathbb{IR}$ e se necessário restritas aos reais. Acioly [Aci91, Aci96] mostra que qualquer função contínua de $\mathbb{R}$ em $\mathbb{R}$ tem uma extensão contínua de $\mathbb{IR}$ em $\mathbb{IR}$. Além desse resultado, Acioly [Aci96] também mostra que qualquer função monotônica definida no espaço dos intervalos de extremos racionais pode ser estendida para o espaço dos intervalos de extremos reais. Para a probabilidade intervalar aqui proposta isto significa que basta considerar, se necessário, os intervalos de extremos racionais de exatidão máxima em um específico sistema de ponto flutuante.

A probabilidade intervalar é realizada através de uma peculiar composição de funções, envolvendo extensões intervalares de funções reais. Inicialmente a um evento é associada a probabilidade real p. Em seguida, a p é associado um intervalo que a contém. Da mesma forma que uma extensão canônica para um número real é um intervalo que o contenha, assim também uma extensão natural para a probabilidade real é a probabilidade intervalar. Nesse sentido, a probabilidade real é a restrição da probabilidade intervalar e esta a extensão da probabilidade real. Então, se necessário, a probabilidade real é estendida para a probabilidade intervalar ou a probabilidade intervalar é restrita para a real.

A probabilidade intervalar portanto *aproxima* a probabilidade real. Essa aproximação deve ser vista sob dois aspectos. Inicialmente, pela própria filosofia inerente à matemática intervalar quando relacionada com a matemática real. Em seguida pelo fato de como extensões intervalares de funções reais não são únicas e como para se ter função é necessário unicidade no conjunto imagem, a aproximação intervalar tomada para um real x, sempre será um intervalo que difira de x a menos de um dado ε, o qual é um número real tão pequeno quanto se queira.

5.3.1 Fundamentos

Definição 5.3.1 Seja $\mathcal{A}$ uma σ-álgebra, P a função probabilidade e a função $P_{\mathbb{IR}}$ definida por

$$P_{\mathbb{IR}} : \mathcal{A} \to \mathbb{IR}$$

$$P_{\mathbb{IR}}(A) = (F \circ P)(A) \tag{3}$$

onde F é como na definição 5.2.4.

Portanto, $P_{\mathbb{IR}}$ associa a cada elemento $A \in \mathcal{A}$ um intervalo X com a propriedade que dada a probabilidade do evento A, $P(A) = p \in \mathbb{R}$, tem-se que $p \in X$. Observe que o intervalo X pode ser degenerado. Como comentado anteriormente, podem existir várias extensões intervalares para uma dada função real f, porém com respeito a (3), ou $F = F_{I_d}$ associa um intervalo X tal que $p \in X$, ou $F = F_*$ corresponde a extensões de operações aritméticas sobre os números reais.

Lema 5.3.2 Seja Ω o espaço amostral, $\mathcal{A}$ uma σ-álgebra de subconjuntos de Ω e a função probabilidade P. Seja ε um número real tal que $\varepsilon > 0$. A função $P_{\mathbb{IR}}$ satisfaz as seguintes propriedades:

(a) Dada $P(A) = p$, $P_{\mathbb{IR}}(A) = X$, $p \in X$

(b) $P_{\mathbb{IR}}(\Omega) = 1_\varepsilon$, onde $1_\varepsilon = [1-\varepsilon, 1+\varepsilon]$, $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$

(c) $P_{\mathbb{IR}}(\emptyset) = 0_\varepsilon$, onde $0_\varepsilon = [-\varepsilon, +\varepsilon]$, $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$

(d) Se $A \cap B = \emptyset$ então $P_{\mathbb{IR}}(A \cup B) = P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B)$

(e) Dada a seqüência $A_1, A_2, \cdots$, com $A_i \cap A_j = \emptyset$, $\forall i \neq j$, então

$$P_{\mathbb{IR}}(\cup_{n=1}^{\infty} A_n) = \sum_{n=1}^{\infty} P_{\mathbb{IR}}(A_n)$$

Demonstração.

(a) $P_{\mathbb{IR}}(A) = (F \circ P)(A) = F(P(A)) = F(p) = X, \ p \in X$

(b) $P_{\mathbb{IR}}(\Omega) = (F \circ P)(\Omega) = F(P(\Omega)) = F(1) = 1_\varepsilon$

(c) $P_{\mathbb{IR}}(\emptyset) = (F \circ P)(\emptyset) = F(P(\emptyset)) = F(0) = 0_\varepsilon$

(d) Se $A \cap B = \emptyset$, $P(A) = x$, $P(B) = y$

$$\begin{aligned} P_{\mathbb{IR}}(A \cup B) &= (F \circ P)(A \cup B) \\ &= F(P(A \cup B)) \\ &= F(P(A) + P(B)) \\ &= F(x+y) \\ &= X + Y \end{aligned}$$

onde, $x \in X$ e $y \in Y$.

$$P_{\mathbb{IR}}(A) = (F \circ P)(A) = F(P(A)) = F(x) = X, \ x \in X$$

$$P_{\mathbb{IR}}(B) = (F \circ P)(B) = F(P(B)) = F(y) = Y, \ y \in Y$$

$$P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B) = X + Y$$

Então,

$$P_{\mathbb{IR}}(A \cup B) = P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B)$$

(e) Desde que a extensão acima é válida para dois elementos, usando-se indução prova-se que também é válida para todo natural $n, n+1, \ldots$. Portanto tem-se que:

$$P_{\mathrm{IIR}}(\cup_{n=1}^{\infty} A_n) = \sum_{n=1}^{\infty} P_{\mathrm{IIR}}(A_n)$$

■

Definição 5.3.3 Um *espaço de probabilidade intervalar* é uma sêxtupla $\langle \mathcal{A}, \mathbb{R}, \mathrm{I}\mathbb{R}, \Omega, P, P_{\mathrm{I}\mathbb{R}} \rangle$, onde $\mathcal{A}$ é uma família de conjuntos, Ω é um elemento destacável de $\mathcal{A}$, $\mathbb{R}$ é o conjunto dos números reais aqui destacado, $\mathrm{I}\mathbb{R}$ é o espaço dos intervalos, P uma função probabilidade e $P_{\mathrm{I}\mathbb{R}} : \mathcal{A} \to \mathrm{I}\mathbb{R}$ é uma função satisfazendo as seguintes propriedades:

(A1) $\forall A \in \mathcal{A}$ se $P(A) \in \mathbb{R}$, então $P_{\mathrm{I}\mathbb{R}}(A) \in \mathrm{I}\mathbb{R}$

(A2) $1 \in P_{\mathrm{I}\mathbb{R}}(\Omega)$

(A3) $0 \in P_{\mathrm{I}\mathbb{R}}(\emptyset)$

(A4) Se $A_1, A_2, \ldots$ é uma seqüência de elementos de $\mathcal{A}$ com $A_i \cap A_j = \emptyset$ para todo $i \neq j$, então $P_{\mathrm{I}\mathbb{R}}(\cup_{n=1}^{\infty} A_n) = \sum_{n=1}^{\infty} P_{\mathrm{I}\mathbb{R}}(A_n)$

A função $P_{\mathrm{I}\mathbb{R}}$ satisfazendo as propriedades A1, A2, A3 e A4 acima é denominada uma *probabilidade intervalar* ou uma *extensão intervalar de P* ou ainda uma *validação para P*.

Por analogia com a probabilidade real, as propriedades A1, A2, A3 e A4 também são chamadas axiomas. A propriedade (A4) é denominada σ-aditividade.

O sistema de axiomas A1-A4 é consistente. Basta considerar $\Omega = \{\omega\}$ e $\mathcal{A}$ o conjunto das partes de Ω.

Observa-se que a menos de $P_{\mathrm{I}\mathbb{R}}(\emptyset)$, quaisquer outras probabilidades intervalares, podem sem perda de generalidade ser consideradas como tendo extremos inferiores números reais maiores ou iguais a zero.

5.3.2 Propriedades

Os lemas a seguir são ferramentas úteis na obtenção de resultados sobre a probabilidade intervalar.

Lema 5.3.4 Seja a seqüência de intervalos $X_n = [x_{n_1}, x_{n_2}]$, $n = 1, 2, \cdots$ tal que $\lim_{n\to\infty} x_{n_1} = x_1$ e $\lim_{n\to\infty} x_{n_2} = x_2$. Então $x_1 \leq x_2$ e $\lim_{n\to\infty} X_n = [x_1, x_2]$.
Demonstração. Suponha $x_1 \geq x_2$. Então

$$\lim_{n\to\infty} x_{n_1} > \lim_{n\to\infty} x_{n_2} \Rightarrow \lim_{n\to\infty} x_{n_1} - \lim_{n\to\infty} x_{n_2} > 0 \Rightarrow \lim_{n\to\infty}(x_{n_1} - x_{n_2}) > 0 \Rightarrow$$

$$\exists n_0 \in \mathbb{N} \mid \forall n \geq n_0, x_{n_1} - x_{n_2} > 0$$

Isto leva a uma contradição, porque pode-se ter $x_{n_1} > x_{n_2}, \forall n \geq n_0$. Portanto segue-se que $\lim_{n\to\infty} X_n = [x_1, x_2]$. ■

Lema 5.3.5 Se $x_{n_1} \leq x_{n_2}$, $\underline{X}_1 = \sum_{n=1}^{\infty} x_{n_1} < \infty$, $\overline{X}_2 = \sum_{n=1}^{\infty} x_{n_2} < \infty$, então

$$\sum_{n=1}^{\infty} x_{n_1} \leq \sum_{n=1}^{\infty} x_{n_2}$$

Demonstração. Sejam $\underline{s}_k = \sum_{n=1}^{k} x_{n_1}$ e $\overline{s}_k = \sum_{n=1}^{k} x_{n_2}$ somas parciais das séries $\underline{X}_1$ e $\overline{X}_2$, respectivamente. Então, $\underline{s}_k < \overline{s}_k$, $\forall k$. Desde que $\underline{X}_1 = \lim_{k\to\infty} \underline{s}_k$, $\overline{X}_2 = \lim_{k\to\infty} \overline{s}_k$ e $\underline{X}_1, \overline{X}_2 < \infty$, usando o lema 5.3.4 o resultado segue-se. ∎

Lema 5.3.6 Se $\sum_{n=1}^{\infty} x_{n_1} < \infty$ e $\sum_{n=1}^{\infty} x_{n_2} < \infty$ com $x_{n_1} < x_{n_2}$, $\forall n \geq 1$, então

$$\sum_{n=1}^{\infty} [x_{n_1}, x_{n_2}] = [\sum_{n=1}^{\infty} x_{n_1}, \sum_{n=1}^{\infty} x_{n_2}].$$

Demonstração. Aplicando a adição de intervalos e o lema 5.3.4 tem-se,

$$\begin{aligned}
\sum_{n=1}^{\infty} [x_{n_1}, x_{n_2}] &= \lim_{k\to\infty} \sum_{n=1}^{k} [x_{n_1}, x_{n_2}] \\
&= \lim_{k\to\infty} [\sum_{n=1}^{k} x_{n_1}, \sum_{n=1}^{k} x_{n_2}] \\
&= \lim_{k\to\infty} [\underline{s}_k, \overline{s}_k] \\
&= [\lim_{k\to\infty} \underline{s}_k, \lim_{k\to\infty} \overline{s}_k] \\
&= [\sum_{n=1}^{\infty} x_{n_1}, \sum_{n=1}^{\infty} x_{n_2}]
\end{aligned}$$

∎

Exemplo 5.3.7 $X_n = [1/n, (n+1)/n]$, $\lim_{n\to\infty} 1/n = 0$, $\lim_{n\to\infty} (n+1)/n = 1$

$$\lim_{n\to\infty} [1/n, (n+1)/n] = [\lim_{n\to\infty} 1/n, \lim_{n\to\infty} (n+1)/n] = [0, 1] \in \mathrm{I\!IR}.$$

Exemplo 5.3.8 $X_n = [p^n, (1-p)^n]$, $n \geq 0$ e $0 < p \leq 0.5$

$$\sum_{n=0}^{\infty} p^n = 1/(1-p)$$

$$\sum_{n=0}^{\infty} (1-p)^n = 1/p$$

$$\sum_{n=0}^{\infty} X_n = \sum_{n=0}^{\infty} [p^n, (1-p)^n] = [\sum_{n=0}^{\infty} p^n, \sum_{n=0}^{\infty} (1-p)^n] = [1/(1-p), 1/p] \in \mathrm{I\!IR}$$

Neste exemplo, para se ter $X_n \in \mathrm{I\!IR}$, a condição $0 < p \leq 0.5$ precisa ser satisfeita. Se $p = 0.7$, $1 - p = 0.3$ e portanto $X_n \notin \mathrm{I\!IR}$.

Proposição 5.3.9 Se $P_{\mathbb{IR}}(\cup_{k=1}^{n} A_k) = \sum_{k=1}^{n} P_{\mathbb{IR}}(A_n)$, então

$$w(P_{\mathbb{IR}}(\cup_{k=1}^{n} A_k)) = \sum_{k=1}^{n} w(P_{\mathbb{IR}}(A_k))$$

Demonstração. Usando indução, primeiro prova-se que o resultado é verdade para $n = 2$ e em seguida o passo geral. Como a prova para $n = 2$ foi feita no capítulo 4 usando a teoria `INTERVAL`, segue-se o passo indutivo.
Assuma que $w(P(\cup_{k=1}^{n-1})) = \sum_{k=1}^{n-1} w(P(A_k))$. Então

$$\begin{aligned}
w(P_{\mathbb{IR}}(\cup_{k=1}^{n})) &= w(P_{\mathbb{IR}}(\cup_{k=1}^{n-1})) + w(P_{\mathbb{IR}}(A_n)) \\
&= \sum_{k=1}^{n-1} w(P_{\mathbb{IR}}(A_k)) + w(P_{\mathbb{IR}}(A_n)) \\
&= \sum_{k=1}^{n} w(P_{\mathbb{IR}}(A_k))
\end{aligned}$$

■

Proposição 5.3.10 Se $\{A_n\}_{n\in\mathbb{N}}$ é tal que $A_1 \subset A_2 \subset \cdots$, $A = \cup_{n=1}^{\infty} A_n = \lim_{n\to\infty} A_n$ então

$$P_{\mathbb{IR}}(A) = \lim_{n\to\infty} P_{\mathbb{IR}}(A_n).$$

Demonstração. Defina $B_1 = A_1$, $B_n = A_n \cap A_{n-1}^c$, $n \geq 2$. Então $\{B_n\}_{n\in\mathbb{N}}$ é tal que $B_i \cap B_j = \emptyset, i \neq j$, $A_n = \cup_{k=1}^{n} B_k$, e $A = \cup_{k=1}^{\infty} B_k$. Adicionalmente,
$P_{\mathbb{IR}}(A_n) = P_{\mathbb{IR}}(\cup_{k=1}^{n} B_k) = \sum_{k=1}^{n} P_{\mathbb{IR}}(B_k)$ e $P_{\mathbb{IR}}(A) = P_{\mathbb{IR}}(\cup_{k=1}^{\infty} B_k) = \sum_{k=1}^{\infty} P_{\mathbb{IR}}(B_k)$, onde $P_{\mathbb{IR}}(B_k) = [b_{k_1}, b_{k_2}]$. Então,

$$\begin{aligned}
\lim_{n\to\infty} P_{\mathbb{IR}}(A_n) &= \lim_{n\to\infty} \sum_{k=1}^{n} P_{\mathbb{IR}}(B_k) \\
&= \lim_{n\to\infty} \sum_{k=1}^{n} [b_{k_1}, b_{k_2}] \\
&= \lim_{n\to\infty} [\sum_{k=1}^{n} b_{k_1}, \sum_{k=1}^{n} b_{k_2}] \\
&= [\lim_{n\to\infty} \sum_{k=1}^{n} b_{k_1}, \lim_{n\to\infty} \sum_{k=1}^{n} b_{k_2}] \\
&= [\sum_{k=1}^{\infty} b_{k_1}, \sum_{k=1}^{\infty} b_{k_2}] \\
&= \sum_{k=1}^{\infty} [b_{k_1}, b_{k_2}] \\
&= \sum_{k=1}^{\infty} P_{\mathbb{IR}}(B_k) \\
&= P_{\mathbb{IR}}(A)
\end{aligned}$$

■

Definição 5.3.11 Seja $A \in \mathcal{A}$ e $P_{\mathbb{IR}}(A) = [a_1, a_2]$. A probabilidade intervalar do evento complementar, $P_{\mathbb{IR}}(A^c)$ é definida por

$$P_{\mathbb{IR}}(A^c) = 1_\varepsilon - P_{\mathbb{IR}}(A)$$

Da definição anterior tem-se que

$$P_{\mathbb{IR}}(A^c) = [1-\varepsilon, 1+\varepsilon] - [a_1, a_2] = [1 - a_2 - \varepsilon, 1 - a_1 + \varepsilon]$$

Observa-se que

$$P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(A^c) = [1 - (a_2 - a_1) - \varepsilon, 1 - (a_2 - a_1) + \varepsilon]$$

então quanto menor a amplitude de $P_{\mathbb{IR}}(A)$, melhor a de $P_{\mathbb{IR}}(A^c)$ e mais próxima de 1 a soma das duas probabilidades intervalares.

A probabilidade intervalar estende a probabilidade real, quando necessário. Adicionalmente, a restrição da probabilidade intervalar é uma probabilidade real. Nesse sentido, note que dados $P_{\mathbb{IR}}(A) = [a_1, a_2]$ e $P_{\mathbb{IR}}(A^c) = [1 - (a_2 - a_1) - \varepsilon, 1 - (a_2 - a_1) + \varepsilon]$, existem $p \in P_{\mathbb{IR}}(A)$, $p = (a_1 + a_2)/2$ e $q \in P_{\mathbb{IR}}(A^c)$, $q = 1 - (a_1 + a_2)/2$ tais que $p + q = 1$.

Sabe-se da teoria dos conjuntos que dado um conjunto A, $(A^c)^c = A$. Com respeito à probabilidade real tem-se que se $P(A) = p$, $P(A^c) = 1 - p$ e portanto $P((A^c)^c) = p$. Assim, $P((A^c)^c) = P(A)$. A seguir será visto que a probabilidade intervalar satisfaz igualdade similar a menos de um erro.

Proposição 5.3.12 $P_{\mathbb{IR}}((A^c)^c) \approx P_{\mathbb{IR}}(A)$.
Demonstração. Se $P_{\mathbb{IR}}(A) = [a_1, a_2]$ então $P_{\mathbb{IR}}(A^c) = 1_\varepsilon - P_{\mathbb{IR}}(A) = [1 - a_2 - \varepsilon, 1 - a_1 - \varepsilon]$ e $P_{\mathbb{IR}}((A^c)^c) = 1_\varepsilon - P_{\mathbb{IR}}(A^c) = [1-\varepsilon, 1+\varepsilon] - [1 - a_2 - \varepsilon, 1 - a_1 + \varepsilon] = [a_1 - \delta, a_2 + \delta]$. Desde que δ é tão próximo de zero quanto se arbitre, a proposição está provada. ■

Proposição 5.3.13 Se $\{A_n\}_{n\in\mathbb{N}}$ é tal que $A_1 \supset A_2 \supset \cdots$, $A = \cap_{n=1}^{\infty} A_n = \lim_{n\to\infty} A_n$ então

$$P_{\mathbb{IR}}(A) = \lim_{n\to\infty} P_{\mathbb{IR}}(A_n) + [-\delta, +\delta].$$

Demonstração. Se $A_1 \supset A_2 \supset \cdots$ e $A = \cap_{n=1}^{\infty} A_n$, então $A_1^c \subset A_2^c \subset \cdots$ com $A = \cup_{n=1}^{\infty} A_n^c$. Em virtude da proposição 5.3.10, $\lim_{n\to\infty} P_{\mathbb{IR}}(A_n^c) = P_{\mathbb{IR}}(A^c)$. Sabe-se que

$$P_{\mathbb{IR}}(A_n^c) = 1_\varepsilon - P_{\mathbb{IR}}(A_n) = [1 - a_{n_2} - \varepsilon, 1 - a_{n_1} + \varepsilon],$$

$$P_{\mathbb{IR}}(A^c) = [1 - a_2 - \varepsilon, 1 - a_1 + \varepsilon].$$

Então, tem-se que $\lim_{n\to\infty} a_{n_1} = a_1$ e $\lim_{n\to\infty} a_{n_2} = a_2$. Portanto,

$$\begin{aligned}
\lim_{n\to\infty} P_{\mathbb{IR}}(A_n) &= \lim_{n\to\infty} (1_\varepsilon - P_{\mathbb{IR}}(A_n^c)) \\
&= \lim_{n\to\infty} ([1-\varepsilon, 1+\varepsilon] - [1 - a_{n_2} - \varepsilon, 1 - a_{n_1} + \varepsilon]) \\
&= \lim_{n\to\infty} [a_{n_1} - \delta, a_{n_2} + \delta] \\
&= [\lim_{n\to\infty} (a_{n_1} - \delta), \lim_{n\to\infty} (a_{n_2} + \delta)] \\
&= [a_1 - \delta, a_2 + \delta]
\end{aligned}$$

■

Para realizar operações de comparações torna-se necessário definir uma relação de ordem. Foi visto no capítulo 2 que no espaço dos intervalos tem-se definidas as relações de ordem $<$, $\leq$ e $\subseteq$, sendo as duas últimas ordens parciais [DP90]. No espaço dos conjuntos a relação de ordem usual é $\subseteq$. A proposição a seguir vai mostrar qual das ordens entre intervalos mantém o sentido da ordem entre eventos.

Proposição 5.3.14 Seja $\langle \mathbb{IR}, \leq \rangle$ o conjunto $\mathbb{IR}$ com a ordem $\leq$. Se $A \subseteq B$ então

$$P_{\mathbb{IR}}(A) \leq P_{\mathbb{IR}}(B).$$

Demonstração. Seja A um conjunto não-vazio e $A \subseteq B$, então $B = A \cup (A^c \cap B)$ portanto $P_{\mathbb{IR}}(B) = P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(A^c \cap B)$. Dadas as probabilidades intervalares $P_{\mathbb{IR}}(A) = [a_1, a_2]$, $P_{\mathbb{IR}}(B) = [b_1, b_2]$ e $P_{\mathbb{IR}}(A^c \cap B) = [c_1, c_2]$,

$$[b_1, b_2] = [a_1, a_2] + [c_1, c_2] = [a_1 + c_1, a_2 + c_2]$$

Desde que $[c_1, c_2]$ é tal que $c_1 \geq 0$, então

$$b_1 \geq a_1 \text{ e } b_2 \geq a_2 \tag{4}$$

A última equação implica que $P_{\mathbb{IR}}(A) \leq P_{\mathbb{IR}}(B)$. Se $A = \emptyset$, tem-se que $[b_1, b_2] = [-\varepsilon, +\varepsilon] + [c_1, c_2]$.
■

Portanto, de acordo com a proposição anterior, a ordem a ser usada é a ordem parcial $\leq$. Nota-se que:

(a) Seja $\langle \mathbb{IR}, < \rangle$ o conjunto $\mathbb{IR}$ com a ordem $<$. Em (4), se $a_2 < b_1$, i.e., $a_1 \leq a_2 < b_1$, então

$$P_{\mathbb{IR}}(A) < P_{\mathbb{IR}}(B).$$

(b) Seja $\langle \mathbb{IR}, \subseteq \rangle$ o conjunto $\mathbb{IR}$ com a ordem $\subseteq$. Em (4), se $a_1 = b_1$ então $P_{\mathbb{IR}}(A) \subseteq P_{\mathbb{IR}}(B)$. Usando a amplitude dos intervalos, $P_{\mathbb{IR}}(A) \subseteq P_{\mathbb{IR}}(B) \Rightarrow w(A) \leq w(B)$.

Uma das propriedades da probabilidade real é que se $A \subseteq B$ então $P(A) \leq P(B)$. A seguir será visto que resultado similar vale para a probabilidade intervalar mas em uma situação bastante particular.

Proposição 5.3.15 Sejam $A, B \in \mathcal{A}$ onde $A \subseteq B$. Sejam $P_{\mathbb{IR}}(A) = [a_1, a_2]$ e $P_{\mathbb{IR}}(B) = [b_1, b_2]$. Se $a_1 = a_2 = a$ então $P_{\mathbb{IR}}(B - A) = P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A)$.
Demonstração. $A \subseteq B$, então da proposição 5.3.15, $P_{\mathbb{IR}}(A) \leq P_{\mathbb{IR}}(B)$, i.e.,

$$a_1 \leq b_1 \text{ e } a_2 \leq b_2$$

Sabe-se que $B = A \cup (A^c \cap B)$ onde $A \cap (A^c \cap B) = \emptyset$. Portanto,

$$P_{\mathbb{IR}}(B) = P_{\mathbb{IR}}(A \cup (A^c \cap B)) = P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(A^c \cap B).$$

Contudo, $A^c \cap B = B - A$, então $P_{\mathbb{IR}}(B) = P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B-A)$. Tomando $P_{\mathbb{IR}}(B-A) = [c_1, c_2]$, então $[b_1, b_2] = [a_1, a_2] + [c_1, c_2] = [a_1 + c_1, a_2 + c_2]$. Portanto, $c_1 = b_1 - a_1$ e $c_2 = b_2 - a_2$.
$P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A) = [b_1, b_2] - [a_1, a_2] = [b_1 - a_2, b_2 - a_1]$.
Tem-se então que:

$$P_{\mathbb{IR}}(B - A) = P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A)$$

se e somente se

$$b_1 - a_2 = b_1 - a_1$$
$$b_2 - a_1 = b_2 - a_2$$

e portanto, $a_1 = a_2 = a$. ∎

Proposição 5.3.16 Se $P_{\mathbb{IR}}(A) = [a_1, a_2]$, $P_{\mathbb{IR}}(B) = [b_1, b_2]$ então
$P_{\mathbb{IR}}(A \cup B) = P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A \cap B)$ desde que $P_{\mathbb{IR}}(A \cap B) = P(A \cap B) = [a, a]$.
Demonstração. Observa-se que $A \cup B = A \cup (A^c \cap B)$ onde $A \cap (A^c \cap B) = \emptyset$. Contudo,

$$P_{\mathbb{IR}}(A \cup B) = P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(A^c \cap B). \tag{5}$$

Adicionalmente, $A^c \cap B = B - (A \cap B)$. Então, se $P_{\mathbb{IR}}(A \cap B) = P(A \cap B) = [a, a]$ tem-se da proposição 5.3.15 que

$$P_{\mathbb{IR}}(A^c \cap B) = P_{\mathbb{IR}}(B - (A \cap B)) = P_{\mathbb{IR}}(B) - P(A \cap B).$$

Substituindo-se (5) o resultado segue-se. ∎

Proposição 5.3.17 Se $P_{\mathbb{IR}}(A \cup B) = P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A \cap B)$ então

$$w(P_{\mathbb{IR}}(A \cup B)) = w(P_{\mathbb{IR}}(A)) + w(P_{\mathbb{IR}}(B)) + w(P_{\mathbb{IR}}(A \cap B)).$$

Demonstração. A prova desta proposição envolve soma e amplitudes de intervalos. Provas desse tipo foram feitas com a teoria `INTERVAL`, no capítulo 4.

Proposição 5.3.18 $P_{\mathbb{IR}}(\cup_{k=1}^{n} A_k) \leq \sum_{k=1}^{n} P_{\mathbb{IR}}(A_k)$.
Demonstração. Seja $n = 2$. $A_1 \cup A_2 = A_1 \cup (A_1^c \cap A_2)$. Então

$$P_{\mathbb{IR}}(A_1 \cup A_2) = P_{\mathbb{IR}}(A_1 \cup (A_1^c \cap A_2)) = P_{\mathbb{IR}}(A_1) + P_{\mathbb{IR}}(A_1^c \cap A_2).$$

Mas, $A_1^c \cap A_2 \subseteq A_2 \Rightarrow P_{\mathbb{IR}}(A_1^c \cap A_2) \leq P_{\mathbb{IR}}(A_2)$, então

$$P_{\mathbb{IR}}(A_1 \cup A_2) \leq P_{\mathbb{IR}}(A_1) + P_{\mathbb{IR}}(A_2).$$

Agora, usando indução, $P_{\mathbb{IR}}(\cup_{k=1}^{n} A_k) = P_{\mathbb{IR}}((\cup_{k=1}^{n-1} A_k) \cup A_n) \leq \sum_{k=1}^{n-1} P_{\mathbb{IR}}(A_k) + P_{\mathbb{IR}}(A_n)$. ∎

A proposição 5.3.19 a seguir é a correspondente extensão intervalar da "continuidade no vazio" da probabilidade real.

Proposição 5.3.19 Seja $A_n \in \mathcal{A}$, $\forall n \in \mathbb{N}$ tal que $A_1 \supset A_2 \supset \ldots$ e $\lim_{n\to\infty} A_n = \emptyset$. Então $\lim_{n\to\infty} P_{\mathbb{IR}}(A_n) = 0_\varepsilon$.

Demonstração. $A = \lim_{n\to\infty} A_n = \emptyset$. Pela proposição 5.3.13, $\lim_{n\to\infty} P_{\mathrm{IIR}}(A_n) = P_{\mathrm{IIR}}(\lim_{n\to\infty} A_n) = P_{\mathrm{IIR}}(A)$. Como $A = \emptyset$ e $P_{\mathrm{IIR}}(A) = 0_\varepsilon$, a proposição está provada. ■

Exemplo 5.3.20 Com os dados do exemplo 5.1.12 foram computados usando a linguagem C, em estações Sun SPARC com versão do sistema operacional 4.1.2. O padrão IEEE754 [Cod88, Gol91, Ste81] está implementado nesses sistemas. Os resultados estão mostrados a seguir, em precisão simples e estendida com os arredondamentos direcionados, respectivamente, $\triangle$ e $\triangledown$, e para o número de máquina mais próximo, *default*.

	$P(\omega_1)$	$P(\omega_2)$	$P(\omega_3)$
$\triangledown$	0.318309	0.377964	0.303725
default	0.318310	0.377964	0.303726
$\triangle$	0.318310	0.377965	0.303726
$\triangledown$	0.318309886183	0.377964473009	0.303725640806
default	0.318309886184	0.377964473009	0.303725640807
$\triangle$	0.318309886184	0.377964473010	0.303725640807

Com estes dados as probabilidades intervalares são:

$$P_{\mathrm{IIR}}(\omega_1) = [0.318309, 0.318310]$$

$$P_{\mathrm{IIR}}(\omega_2) = [0.377964, 0.377965]$$

$$P_{\mathrm{IIR}}(\omega_3) = [0.303725, 0.303726]$$

5.4 Conjecturas

A proposição 5.3.15 é válida em uma situação particular. Porém, os exemplos a seguir ilustram outros resultados que podem ser obtidos.

Exemplo 5.4.1 Seja $\Omega = \{\omega_1, \omega_2, \omega_3, \omega_4\}$, onde as probabilidades dos eventos elementares são dadas por $P(\omega_1) = P(\omega_2) = P(\omega_3) = 1/10$ e $P(\omega_4) = 7/10$. Se $A = \{\omega_2, \omega_3\}$ e $B = \{\omega_2, \omega_3, \omega_4\}$ então,

$$\begin{aligned} P_{\mathrm{IIR}}(A) &= P_{\mathrm{IIR}}(\{\omega_2, \omega_3\}) \\ &= P_{\mathrm{IIR}}(\omega_2) + P_{\mathrm{IIR}}(\omega_3) \\ &= [0.1, 0.1] + [0.1, 0.1] \\ &= [0.2, 0.2] \end{aligned}$$

$$\begin{aligned} P_{\mathrm{IIR}}(B) &= P_{\mathrm{IIR}}(\{\omega_2, \omega_3, \omega_4\}) \\ &= P_{\mathrm{IIR}}(\omega_2) + P_{\mathrm{IIR}}(\omega_3) + P_{\mathrm{IIR}}(\omega_4) \\ &= [0.1, 0.1] + [0.1, 0.1] + [0.7, 0.7] \\ &= [0.9, 0.9] \end{aligned}$$

$P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A) = [0.9, 0.9] - [0.2, 0.2] = [0.7, 0.7]$
$B - A = \{\omega_4\} \Rightarrow P_{\mathbb{IR}}(B - A) = P_{\mathbb{IR}}(\omega_4) = [0.7, 0.7]$
Neste caso tem-se então que

$$P_{\mathbb{IR}}(B - A) = P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A)$$

Apesar de terem sido usados intervalos (em geral as máquinas não usam a aritmética racional), o resultado está coerenta com a proposição 5.3.16 pois os intervalos são degenerados.

Exemplo 5.4.2 Seja agora $\Omega = \{\omega_1, \omega_2, \omega_3, \omega_4\}$, onde as probabilidades dos eventos elementares são dadas por $P(\omega_1) = 1/3$, $P(\omega_2) = 1/6$, $P(\omega_3) = 1/12$ e $P(\omega_4) = 5/12$. Tem-se então que:

$P(\omega_1) = [0.33, 0.34]$
$P(\omega_2) = [0.16, 0.17]$
$P(\omega_3) = [0.083, 0.084]$
$P(\omega_4) = [0.41, 0.42]$

Se $A = \{\omega_2, \omega_3\}$ e $B = \{\omega_2, \omega_3, \omega_4\}$ então,

$$\begin{aligned} P_{\mathbb{IR}}(A) &= P_{\mathbb{IR}}(\{\omega_2, \omega_3\}) \\ &= P_{\mathbb{IR}}(\omega_2) + P_{\mathbb{IR}}(\omega_3) \\ &= [0.16, 0.17] + [0.083, 0.084] \\ &= [0.243, 0.254] \end{aligned}$$

$$\begin{aligned} P_{\mathbb{IR}}(B) &= P_{\mathbb{IR}}(\omega_2, \omega_3, \omega_4) \\ &= P_{\mathbb{IR}}(\omega_2) + P_{\mathbb{IR}}(\omega_3) + P_{\mathbb{IR}}(\omega_4) \\ &= [0.16, 0.17] + [0.083, 0.084] + [0.41, 0.42] \\ &= [0.653, 0.674] \end{aligned}$$

$P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A) = [0.653, 0.674] - [0.243, 0.254] = [0.399, 0.431]$
$B - A = \{\omega_4\} \Rightarrow P_{\mathbb{IR}}(B - A) = P_{\mathbb{IR}}(\omega_4) = [0.41, 0.42]$

$P_{\mathbb{IR}}(A) = [0.243, 0.254]$
$P_{\mathbb{IR}}(B) = [0.653, 0.674]$
$P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A) = [0.399, 0.431]$
$P_{\mathbb{IR}}(B - A) = [0.41, 0.42]$

Portanto,

$$P_{\mathbb{IR}}(B - A) \subseteq P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A)$$

Desde que operações aritméticas intervalares tendem a aumentar a amplitude dos intervalos, o esperado é que $P_{\mathbb{IR}}(B - A)$ seja “menor”, de acordo com alguma relação de ordem, que
$P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A)$.

Os dados do exemplo 5.4.2 podem ser usados para ilustrar resultado similar para a expressão

$$P_{\mathbb{IR}}(A \cup B) = P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A \cap B)$$

que foi provada apenas na situação particular de $P_{\mathbb{IR}}(A \cap B)$ ser um número real.

Exemplo 5.4.3

$$\begin{aligned}
P_{\mathbb{IR}}(A \cup B) &= P_{\mathbb{IR}}(\omega_2, \omega_3, \omega_4) \\
&= P_{\mathbb{IR}}(\omega_2) + P_{\mathbb{IR}}(\omega_3) + P_{\mathbb{IR}}(\omega_4) \\
&= [0.16, 0.17] + [0.083, 0.084] + [0.41, 0.42] \\
&= [0.653, 0.674]
\end{aligned}$$

$A \cap B = A$. Portanto,

$$\begin{aligned}
P_{\mathbb{IR}}(A \cap B) &= P_{\mathbb{IR}}(A) \\
&= P_{\mathbb{IR}}(\{\omega_2, \omega_3\}) \\
&= P_{\mathbb{IR}}(\omega_2) + P_{\mathbb{IR}}(\omega_3) \\
&= [0.16, 0.17] + [0.083, 0.084] \\
&= [0.243, 0.254]
\end{aligned}$$

$P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A \cap B) = [0.243, 0.254] + [0.653, 0.674] - [0.243, 0.254] = [0.642, 0.685]$
Tem-se então que:

$$P_{\mathbb{IR}}(A \cup B) \subseteq P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A \cap B)$$

5.5 Variáveis Aleatórias

Nesta seção é estudado o problema de como calcular probabilidades intervalares no contexto de variáveis aleatórias, mais especificamente, das variáveis de Bernoulli, Binomial e Poisson [Fel68, Bre69, Jam81]. Probabilidades intervalares para essas variáveis podem se tornar necessárias quando, seus parâmetros não estão bem definidos ou seus valores não são representáveis.

A função de probabilidade para variáveis aleatórias discretas, $P(X = k)$, $k \in R_X$, onde R_X é o contra-domínio da variável aleatória, satisfaz as seguintes condições:

(a) $P(X = k) \geq 0, \forall k \in R_X$

(b) $\sum_{k \in R_X} P(X = k) = 1$

A definição a seguir estende essas condições para o caso intervalar.

Definição 5.5.1 Seja X uma variável aleatória discreta com uma função de probabilidade $P(X = k), k \in R_X$. A *função de probabilidade intervalar* ou a *extensão intervalar para a função de probabilidade real* , $P_{\mathbb{IR}}(X = k)$, satisfaz as seguintes propriedades:

(a) $P_{\mathbb{IR}}(X = k) \in \mathbb{IR}$

(b) $1 \in \sum_{k \in R_X} P_{\mathbb{IR}}(X = k)$

5.5.1 Distribuição de Bernoulli

Um experimento aleatório é realizado e é observada a ocorrência de um evento A, onde $P(A) = p$. A variável aleatória de Bernoulli, X, assume o valor 1 com probabilidade p e 0 com probabilidade $1 - p = q$. Os exemplos 5.5.2, 5.5.3 e 5.5.4 a seguir ilustram problemas numéricos relacionados com os valores de p e/ou q, os quais justificam usar a probabilidade intervalar.

Exemplo 5.5.2 Sejam $S(10, 4, -1, 1)$ e $p = 0.25$. Neste caso não é necessário tomar as extensões intervalares para p e q pois ambos são representáveis no sistema de ponto flutuante dado.

Exemplo 5.5.3 Se $S(10, 3, -1, 1)$ e $p = 0.0625 = 0.625 \cdot 10^{-1}$ então o valor de q não é representável no sistema de ponto flutuante dado, sendo necessário arredondá-lo, $q = 1 - 0.0625 = 0.9376 \approx 0.938$.

Exemplo 5.5.4 Se $S(10, 3, -1, 1)$ e $p = 1/31$ o quociente precisa ser arredondado, isto é, $p \approx 0.03225 = 0.3225 \cdot 10^{-1}$.

Para a variável de Bernoulli, probabilidades intervalares correspondem apenas a extensões intervalares para p e q. A definição a seguir formaliza este fato.

Definição 5.5.5 Seja X uma variável aleatória de Bernoulli tal que $P(X = 1) = P(A) = p$ e $P(X = 0) = P(A^c) = 1 - p = q$. Então a *função de probabilidade intervalar de Bernoulli* ou *distribuição intervalar de Bernoulli* é definida por

$$P_{\mathbb{IR}}(X = 1) = P_{\mathbb{IR}}(A) = p_{\mathbb{IR}}$$

$$P_{\mathbb{IR}}(X = 0) = P_{\mathbb{IR}}(A^c) = q_{\mathbb{IR}}$$

Note que dado $P_{\mathbb{IR}}(A) = [p_1, p_2]$ e usando-se a definição 5.4.1, tem-se:

$$p_{\mathbb{IR}} = P_{\mathbb{IR}}(X = 1) = [p_1, p_2]$$

$$q_{\mathbb{IR}} = P_{\mathbb{IR}}(X = 0) = [1 - p_2 - \varepsilon, 1 - p_1 + \varepsilon]$$

$$\sum_{k=0}^{1} P_{\mathbb{IR}} = [1 - (p_2 - p_1) - \varepsilon, 1 + (p_2 - p_1) + \varepsilon]$$

$$1 \in [1 - (p_2 - p_1) - \varepsilon, 1 + (p_2 - p_1) + \varepsilon]$$

As probabilidades intervalares para os dados dos problemas 5.5.3 e 5.5.4 são, respectivamente,

(a)

$$p_{\mathbb{IR}} = [0.625 \cdot 10^{-1}, 0.625 \cdot 10^{-1}]$$

$$q_{\mathbb{IR}} = [1 - 0.625 \cdot 10^{-1} - \varepsilon, 1 - 0.625 \cdot 10^{-1} + \varepsilon] = [0.937 - \varepsilon, 0.938 + \varepsilon]$$

(b)

$$p_{\mathrm{IR}} = [0.322 \cdot 10^{-1}, 0.323 \cdot 10^{-1}]$$

$$q_{\mathrm{IR}} = [1 - 0.323 \cdot 10^{-1} - \varepsilon, 1 - 0.322 \cdot 10^{-1} + \varepsilon] = [0.967 - \varepsilon, 0.968 + \varepsilon]$$

5.5.2 Distribuição Binomial

Seja a distribuição binomial de parâmetros n e p, como na definição 5.1.7. O exemplo a seguir ilustra situações quando arredondamentos tornam-se necessários.

Exemplo 5.5.6 Sejam $S(10, 4, -1, 1)$, $n = 2$ e $p = 0.233$. Então $q = 0.767$ e

$$p_k = P(X = k) = \binom{2}{k} 0.233^k 0.767^{n-k}, k = 0, \ldots, 2$$

$p_0 = 0.588289 \approx 0.5883$
$p_1 = 0.357422 \approx 0.3574$
$p_2 = 0.542890 \approx 0.5429$
$\sum_{k=0}^{2} P(X = k) \approx 1.488601 \approx 1.488 \neq 1$

Os valores $p = 0.233$ e $q = 0.767$ são elevados, respectivamente, às potências k e $n-k$, $k = 0, \cdots, n$; os resultados extrapolam o número de dígitos da mantissa ($l = 4$), sendo necessário arredondamentos. Como n, k e $\binom{n}{k}$ são números inteiros, uma extensão intervalar para a distribuição binomial toma intervalos para p e q e as operações aritméticas intervalares.

Os lemas a seguir são usados em provas da extensão intervalar da distribuição binomial.

Lema 5.5.7 Sejam $X = [x_1, x_2]$ e $Y = [y_1, y_2]$ onde $x_1 \geq 0$ e $y_1 \geq 0$. Tem-se que

$$(X + Y)^n = [(x_1 + y_1)^n, (x_2 + y_2)^n]$$

Demonstração.

$$\begin{aligned}
(X + Y)^2 &= ([x_1, x_2] + [y_1, y_2])^2 \\
&= [x_1 + y_1, x_2 + y_2]^2 \\
&= [x_1 + y_1, x_2 + y_2][x_1 + y_1, x_2 + y_2] \\
&= [\min M, \max M] \\
&= [(x_1 + y_1)^2, (x_2 + y_2)^2] \qquad (6)
\end{aligned}$$

Sendo $M = \{(x_1 + y_1)^2, (x_1 + y_1)(x_2 + y_2), (x_2 + y_2)(x_1 + y_1), (x_2 + y_2)^2\}$, segue-se (6). O resultado para n é obtido por indução. ■

Lema 5.5.8 Se a, b, c e d são números reais maiores ou iguais a zero, então

$$([a, b] + [c, d])^n = \sum_{k=0}^{n} \binom{n}{k} [a, b]^k [c, d]^{n-k} \qquad (7)$$

Demonstração. Seja $n = 2$. Então

$$([a, b] + [c, d]))^2 = [(a + c)^2, (b + d)^2]. \qquad (8)$$

$$\begin{aligned}
[a,b]^2 + 2[a,b][c,d] + [c,d]^2 &= [a,b][a,b]2[a,b][c,d] + [c,d][c,d] \\
&= [a^2, b^2] + 2[ac, bd] + [c^2, d^2] \\
&= [(a+c)^2, (b+d)^2] \qquad (9)
\end{aligned}$$

De (8) e (9) segue-se que (7) é verdade para $n = 2$. Usando-se indução, prova-se para n. ∎

Lema 5.5.9 Seja A um evento tal que $P_{\mathrm{IIR}}(A) = [p_1, p_2]$ e $P_{\mathrm{IIR}}(A^c) = [1 - p_2 - \varepsilon, 1 - p_1 + \varepsilon]$. Então

$$1 \in ([p_1, p_2] + [1 - p_2 - \varepsilon, 1 - p_1 + \varepsilon])^n$$

Demonstração. Seja $n = 2$. Então

$$\begin{aligned}
([p_1, p_2] + [1 - p_2 - \varepsilon, 1 - p_1 + \varepsilon])^2 &= [1 - (p_2 - p_1) - \varepsilon, 1 + (p_2 - p_1) + \varepsilon]^2 \\
&= [(1 - (p_2 - p_1) - \varepsilon)^2, (1 + (p_2 - p_1) + \varepsilon])^2] \qquad (10)
\end{aligned}$$

$$[p_1, p_2] + [1 - p_2 - \varepsilon, 1 - p_1 + \varepsilon])^2 \supseteq [(1 - (p_2 - p_1)^2 - \varepsilon_1, (1 + (p_2 - p_1)^2 + \varepsilon_2] \qquad (11)$$

ε_1 e ε_2 correspondem ao resultado das operações aritméticas envolvendo ε, p_1 e p_2. Como $0 \leq p_1 \leq p_2 \leq 1$, tem-se que $(p_2 - p_1)^2 \leq p_2 - p_1$ e então 1 pertence ao intervalo em (11). Consequentemente, 1 também pertence ao intervalo em (10). O resultado para n segue-se por indução. ∎

Definição 5.5.10 Seja $P(A) = p$ e X uma variável aleatória que conta o número de ocorrências de A nas n repetições independentes do experimento. A *função de probabilidade intervalar binomial* ou a *distribuição intervalar binomial* é definida por

$$P_{\mathrm{IIR}}(X = k) = \binom{n}{k} p_{\mathrm{IIR}}^k q_{\mathrm{IIR}}^{n-k}, k = 0, \cdots, n$$

Note que, sendo $p_{\mathrm{IIR}} = [p_1, p_2]$ e $q_{\mathrm{IIR}} = [1 - p_2 - \varepsilon, 1 - p_1 + \varepsilon]$,

$$\begin{aligned}
\sum_{k=0}^{n} P_{\mathrm{IIR}}(X = k) &= \sum_{k=0}^{n} \binom{n}{k} p_{\mathrm{IIR}} k q_{\mathrm{IIR}}^{n-k} \\
&= (p_{\mathrm{IIR}} + q_{\mathrm{IIR}})^n \\
&= ([p_1, p_2] + [1 - p_2 - \varepsilon, 1 - p_1 + \varepsilon])^n \\
&= [1 - (p_2 - p_1) - \varepsilon, 1 + (p_2 - p_1) + \varepsilon]^n
\end{aligned}$$

Pelo lema 5.5.9, o intervalo acima contém 1.

Exemplo 5.5.11 Supondo $X \sim B(3, 1/3)$ e $S(10, 3, -1, 1)$. Então

$$p_{\mathrm{IIR}} = [0.333, 0.334]$$

$$1 - p_{\mathrm{IIR}} = q_{\mathrm{IIR}} = [0.666 - \varepsilon, 0.667 + \varepsilon]$$

$$P_{\mathrm{IIR}}(X = k) = \binom{3}{k} [0.333, 0.334]^k [0.666 - \varepsilon, 0.667 + \varepsilon]^{3-k}, k = 0, \cdots, 3$$

$P_{\mathbb{IR}}(X = 0) = [0.295 - \varepsilon, 0.297 + \varepsilon]$
$P_{\mathbb{IR}}(X = 1) = [0.443 - \varepsilon, 0.446 + \varepsilon]$
$P_{\mathbb{IR}}(X = 2) = [0.222 - \varepsilon, 0.223 + \varepsilon]$
$P_{\mathbb{IR}}(X = 3) = [0.369 \cdot 10^{-1}, 0.372 \cdot 10^{-1}]$
$\sum_{k=0}^{3} P_{\mathbb{IR}}(X = k) = [0.997 - \delta, 1.00 + \delta]$

5.5.3 Distribuição de Poisson

Como visto na definição 5.1.8, a função de probabilidade de uma variável aleatória de Poisson é

$$P(X = k) = \frac{e^{-\lambda}\lambda^k}{k!}, k = 0, 1, \ldots, \lambda \in \mathbb{R}$$

onde a prova que $\sum_{k=0}^{\infty} P(X = k) = 1$ está baseada no fato que $\sum_{k=0}^{\infty} \frac{\lambda^k}{k!} = e^{\lambda}$. Os exemplos a seguir mostram erros numéricos na computação de probabilidades nessa distribuição.

Exemplo 5.5.12 Supondo $\lambda = 1$, $e = 2.7$, $S(10, 2, -1, 1)$. Então,

$$P(X = k) = \frac{2.7^{-1}}{k!}, k = 0, 1, \ldots$$

$P(X = 0) \approx 0.37$
$P(X = 1) \approx 0.37$
$P(X = 2) \approx 0.18$
$P(X = 3) = 0.12$
$\sum_{k=0}^{4} P(X = k) \approx 1.04 > 1$

Exemplo 5.5.13 Supondo $\lambda = 2$, $e = 2.7$, $S(10, 3, -1, 1)$. Então,

$$P(X = k) = \frac{2.7^{-2}2^k}{k!},\ k = 0, 1, \ldots$$

$P(X = 0) \approx 0.137$
$P(X = 1) \approx 0.274$
$P(X = 2) \approx 0.274$
$P(X = 3) \approx 0.183$
$P(X = 4) \approx 0.0914 = 0.914 \cdot 10^{-1}$
$P(X = 5) \approx 0.0366 = 0.366 \cdot 10^{-1}$
$P(X = 6) \approx 0.0122 = 0.122 \cdot 10^{-1}$
$\sum_{k=0}^{4} P(X = k) = 1.0082 \approx 1.01 > 1$

O método usado para obter as probabilidades intervalares usa extensões intervalares de específicas funções reais.

As funções reais

$$f(\lambda) = e^{-\lambda}, \lambda > 0$$

$$f(k) = \lambda^k, k = 0, 1, \ldots$$

tem as correspndentes extensões intervalares [Moo66, Moo79]

$$[\underline{e^{-\lambda}}\overline{e^{-\lambda}}],$$

$$[\underline{\lambda^k}, \overline{\lambda^k}]$$

Então uma proposta inicial para as probabilidades intervalares de uma distribuição de Poisson é

$$P_{\mathbb{IR}}(X = k) = \frac{[\underline{e^{-\lambda}}, \overline{e^{-\lambda}}][\underline{\lambda^k}, \overline{\lambda^k}]}{k!}, k = 0, 1, \ldots$$

Efetuando-se a multiplicação dos intervalos, tem-se a definição abaixo.

Definição 5.5.14 Seja X uma variável aleatória de Poisson. Então a *função de probabilidade intervalar de Poisson* ou a *distribuição intervalar de Poisson* é definida por

$$P_{\mathbb{IR}}(X = k) = [\underline{\frac{e^{-\lambda}\lambda^k}{k!}}, \overline{\frac{e^{-\lambda}\lambda^k}{k!}}], k = 0, 1, \ldots$$

Note que

$$\begin{aligned}
\sum_{k=0}^{\infty} P_{\mathbb{IR}}(X = k) &= \sum_{k=0}^{\infty} [\underline{\frac{e^{-\lambda}\lambda^k}{k!}}, \overline{\frac{e^{-\lambda}\lambda^k}{k!}}] \\
&= [\sum_{k=0}^{\infty} \underline{\frac{e^{-\lambda}\lambda^k}{k!}}, \sum_{k=0}^{\infty} \overline{\frac{e^{-\lambda}\lambda^k}{k!}}] \\
&= [1, 1].
\end{aligned}$$

Portanto $1 \in \sum_{k=0}^{\infty} P_{\mathbb{IR}}(X = k)$.

Exemplo 5.5.15 Este exemplo é o exercício 8.5, da página 210, proposto em Paul L. Meyer [Mey68]. Uma companhia de seguros descobriu que somente cerca de 0.1 por cento da população está incluída em certo tipo de acidente cada ano. Se seus 10.000 segurados são escolhidos, ao acaso, na população, qual é a probabilidade de que não mais do que 5 de seus clientes venham a estar incluídos em tal acidente no próximo ano?
Seja $S(10, 3, -3, 3)$.

$$P_{\mathbb{IR}}(X = k) = [\underline{\frac{e^{-10}10^k}{k!}}, \overline{\frac{e^{-10}10^k}{k!}}], k = 0, 1, \ldots$$

$P_{\mathbb{IR}}(X = 0) = [0.000, 0.000]$
$P_{\mathbb{IR}}(X = 1) = [0.000, 0.000]$
$P_{\mathbb{IR}}(X = 2) = [0.226 \cdot 10^{-2}, 0.227 \cdot 10^{-2}]$
$P_{\mathbb{IR}}(X = 3) = [0.756 \cdot 10^{-2}, 0.757 \cdot 10^{-2}]$
$P_{\mathbb{IR}}(X = 4) = [0.189 \cdot 10^{-1}, 0.190 \cdot 10^{-1}]$
$P_{\mathbb{IR}}(X = 5) = [0.378 \cdot 10^{-2}, 0.379 \cdot 10^{-2}]$

Portanto,

$$P_{\mathbb{IR}}(X \leq 5) = [0.665 \cdot 10^{-1}, 0.667 \cdot 10^{-1}]$$

A resposta fornecida pelo autor para o problema é $P(X \leq 5) = 0.067$. Os cálculos efetuados com a extensão intervalar controlaram todos os erros numéricos, pois esta é uma característica da aritmética de exatidão máxima.

5.6 Conclusões

A extensão intervalar aqui proposta é uma alternativa teórica e numericamente correta para a validação da probabilidade real. Teórica porque propriedades básicas similares às da probabilidade real são mantidas quando esta é estendida para a probabilidade intervalar. Numérica pois a aritmética (intervalar) de exatidão máxima é desenvolvida de forma a controlar os erros de arredondamento ou truncamento na computação científica.

Com respeito ao erro ε presente em várias expressões da probabilidade intervalar, a nível de inplementação, pode ser considerado como a diferença entre dois números de máquina consecutivos. Nesse caso o número será formado de um número com l dígitos na mantissa, onde $l-1$ são zeros e o último 1.

Capítulo 6

Conclusões e Trabalhos Futuros

Neste capítulo são apontadas as conclusões obtidas nesse trabalho, assim como as perspectivas de desenvolvimentos futuros.

6.1 Trabalhos Correlatos

A autora desta tese desconhece qualquer trabalho similar ao aqui proposto. A seguir é feita uma sucinta exposição de trabalhos em probabilidade e estatística e que usam intervalos.

Em [WK94] a análise intervalar é usada para a computação de probabilidades através de algoritmos numéricos autovalidáveis para as distribuições contínuas normal, gama incompleta, beta incompleta e qui-quadrado não central.

Para o conjunto de possíveis valores de um erro, Kreinovich [Kre95] prova que de esse erro é a soma de um número de componentes independentes e muito pequenas, então seu conjunto de possíveis valores é um intervalo. Nesse artigo Kreinovich associa esses resultados com teoremas limites da estatística matemática.

Cui e Blockley [CB90] usam um intervalo para representar probabilidade com o objetivo de capturar aspectos difusos (*fuzziness*) e incompletude (*incompleteness*).

A matemática intervalar e métodos estatísticos têm sido associados por vários autores.

Voshchinin, Bockov e Sotirov [VBS90] descrevem métodos de análise intervalar de dados com erros experimentais não-estatísticos.

Voshchinin [Vos92] relaciona análise de regressão e "análise de regressão intervalar" assumindo que os valores são intervalos e resolvendo um sistema linear intervalar.

Orlov [Orl92] analisa o desenvolvimento da estatística intervalar na Rússia no período 1980-1990. Esse desenvolvimento foi motivado por problemas do mundo real tais como a estabilidade da inferência estatística com respeito aos desvios admissíveis dos dados iniciais. Como cita Orlov, o desenvolvimento de novos conceitos resultou na proposição de uma nova teoria estatística chamada "estatística realista" (*realistic statistic*), onde, por exemplo, não há estimadores consistentes e o método dos momentos pode ser mais adequado que o de máxima verossimilhança.

Golubkova e Voshchinin [GV94] propõem a análise de regressão intervalar na investigação do relacionamento entre o efeito da mutagenicidade de microorganismos quando na presença de certos produtos químicos.

O exemplo a seguir refere-se à estimação dos parâmetros para modelos de séries temporais. [Nar92] sugere intervalos para representarem valores imprecisos tais como estimativas para um dado parâmetro.

Os dados abaixo são de [BJ76], a menos da coluna correspondente a **MMMI**. Estes dados foram computados usando um outro método de estimação de parâmetros [CC95] e a aritmética de exatidão máxima [KM81]. Então, as estimativas para os parâmetros dos modelos AR(1), AR(2) e ARMA(1,1) foram obtdas através do método dos momentos modificados e aritmética de exatidão máxima – **MMMI** e através do método de máxima verossimilhança com a aritmética de ponto flutuante –**MLFP**. Abaixo de cada valor na coluna MLFP, são dados os correspondentes devio padrão entre parêntesis.

Serie	N	Modelo	Parâmetros	Valor dos Parâmetros	
				MMMI	**MLFP**
A	197	ARMA(1,1)	ϕ_1	0.8818451_2^3	0.92
					($\pm$.04)
			θ_1	0.5143846_1^2	0.58
					($\pm$.08)
C	226	AR(1)	ϕ_1	0.8119850_7^8	0.82
					($\pm$.04)
D	310	AR(1)	ϕ_1	0.8691036_7^8	0.87
					($\pm$.03)
E	100	AR(2)	ϕ_1	1.3921477_7^8	1.42
					($\pm$.07)
			ϕ_2	-0.6945869_9^8	-0.73
					($\pm$.07)
F	70	AR(2)	ϕ_1	-0.3065561_1^0	-0.34
					($\pm$.12)
			ϕ_2	0.1982084_2^3	0.19
					($\pm$.12)

Com respeito à série de tempo A, as estimativas para os parâmetros encontradas por máxima verossimilhança são 0.92 e 0.58. Os verdadeiros e desconhecidos valores de ϕ_1 e θ_1 estão no intervalo de confiança (0.88,0.96) e (0.50,0.66) com um dado nível de significância. Os resultados intervalares mostram que, do ponto de vista numérico, os verdadeiros e desconhecidos valores dos parâmetros pertencem aos intervalos [0.88184512,0.88184513] e [0.51438461, 0.51438462]. Usando o ponto médio dos intervalos como estimativas para os respectivos parâmetros tem-se como modelo ajustado para a série A, $z_t - 0.88184512z_{t-1} = a_t - 0.51438461a_{t-1}$.

6.2 Conclusões

Esta tese propôs uma metodologia própria para estender a probabilidade real de maneira a possibilitar seu cálculo automático através do uso de intervalos, limitando os erros computacionais e mantendo uma semântica consistente entre a probabilidade e os resultados intervalares obtidos.

A probabilidade usual, clássica, foi referida como a probabilidade real e a aqui proposta como a probabilidade intervalar.

O primeiro passo para alcançar o objetivo foi usar conceitos de extensões intervalares de funções reais, propostos por Moore e Acioly [Moo66, Moo79, Aci91, Aci96]. A partir da definição de um espaço de probabilidade intervalar, provou-se que a extensão proposta tem propriedades similares às da probabilidade real. Nesse sentido, a probabilidade intervalar estende a probabilidade real sendo esta uma restrição da primeira.

A probabilidade intervalar aqui proposta mostrou ser uma alternativa numérica e computacional eficiente para a probabilidade real. Probabilidades reais podem ser substituídas por intervalos mantendo as características peculiares do que seja uma probabilidade. A probabilidade intervalar engloba consigo todos os erros que ocorrem em computações numéricas. Além disso, como as operações aritméticas são realizadas com exatidão máxima, os limites dos intervalos são precisos e exatos. Portanto, o intervalo resultante é uma informação confiável.

6.3 Trabalhos Futuros

Os seguintes tópicos podem ser considerados como continuação do trabalho aqui proposto. Basicamente, tais tópicos referem-se à Teoria da Probabilidade, Lógica, Linguagens Funcionais e Teoria dos Domínios.

6.3.1 Teoria da Probabilidade

- No capítulo 5 foram mencionadas duas conjecturas relacionadas com a probabilidade intervalar:

  1. Qual a relação de ordem entre $P_{\mathbb{IR}}(B-A)$ e $P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A)$, quando $A \subseteq B$?
  2. Que relação mais geral pode ser definida entre $P_{\mathbb{IR}}(A \cup B)$ e $P_{\mathbb{IR}}(A) + P_{\mathbb{IR}}(B) - P_{\mathbb{IR}}(A \cap B)$?

  Portanto, uma sugestão de pesquisa nessa linha é encontrar, se possível, relações envolvendo as probabilidades intervalares mencionadas acima.

- A definição da probabilidade condicional no caso real [Jam81, Bur72, Chu74], é o quociente entre duas outras probabilidades onde o denominador é estritamente positivo. Uma extensão natural para o caso intervalar pode ser o quociente entre intervalos mas de tal forma que zero não pertença ao intervalo do denominador. A adequabilidade de tal extensão tem que ser averiguada e fica para trabalhos futuros.

- O conceito de eventos independentes é fundamental na probabilidade real pois é aplicado, entre outros, para a definição de variáveis aleatórias [Bur72, Chu74, Jam81]. Na probabilidade real dois eventos A e B são independentes quando calculados $P(A \cap B)$ e $P(A)P(B)$, os valores resultantes são iguais. Portanto, associado ao conceito de independência, está a multiplicação de reais. Sabe-se que a multiplicação de intervalos é uma operação que resulta um intervalo com amplitude maior que dos intervalos operandos. Portanto é um dos objetivos estudar tal problema.

- Nesta tese mostrou-se como calcular probabilidades intervalares para as variáveis aleatórias discretas de Bernoulli, Binomial e Poisson. Mas além dessas, tem-se outras variáveis discretas, e as contínuas, que são bastante utilizadas em problemas práticos, como por exemplo a exponencial e a normal.

6.3.2 Lógica

O termo *fuzzy logic* tem sido usado para descrever um tipo de matemática que trabalha com graus de incerteza. De certa forma também probabilidade é uma medida de incerteza. Operações aritméticas em *fuzzy sets* [VP95] são como entre intervalos [Sun58, Moo66, Moo79]. Estudar então se existe alguma relação entre a probabilidade aqui proposta e *fuzzy sets* [Wil90, Kaw78, Kaw79, Gai78, DP91, BT87, Pia86, MS84].

6.3.3 Linguagens Funcionais

- No nosso trabalho [LCC95] mostramos dois problemas que devem ser solucionados de forma a se adaptarem os requisitos para computação científica e o paradigma funcional: (i) a introdução do tipo array, que pode quebrar a transparência referencial, e (ii) a inclusão do operador de iteração explícito. Resolvidos esses problemas, entre outros, algoritmos intervalares que são validáveis por definição, também serão validados na linguagem. O estudo de aplicações intervalares em linguagens funcionais é um interessante tema de pesquisa a ser explorado.

- Nesta tese a linguagem OBJ3 foi usada para especificar o tipo intervalo. Uma sugestão para continuação de trabalho nessa linha é especificar os outros espaços da computação numérica (Figura 3.1) que envolvam o tipo intervalo.

- Inicialmente, a formalização do tipo intervalo em OBJ3 teve como um dos objetivo provar teoremas da matemática intervalar usados em provas da probabilidade intervalar. Porém, as provas da probabilidade intervalar requerem técnicas ainda não incluídas na especificação do capítulo 4. Sugere-se então ampliar a especificação proposta de modo a automatizar as provas da probabilidade intervalar.

6.3.4 Domínios

A inclusão monotônica é uma propriedade básica na análise intervalar, porém a topologia proposta por Moore [Moo66, Moo79] não é com ela compatível desde que há funções contínuas nessa topologia que não são monotônicas. Com o objetivo de sanar este problema, [Aci91] propõe a topologia de Scott para o espaço dos intervalos. Portanto, do ponto de vista da validação da probabilidade real como aqui proposto, analisar quais as diferenças que surgem quando do uso das topologias.

Referências Bibliográficas

[Aci91] B. M. Acioly. *Fundamentação computacional da matemática intervalar.* PhD thesis, Porto Alegre, Departamento de Informática Teórica/UFRGS, 1991.

[Aci96] B. M. Acioly. The Scott Interval Analysis. In M. A. Campos, editor, *Recife, II Workshop on Computer Arithmetic, Interval and Symbolic Computation,*, pages 4–6, agosto 1996.

[AH83] G. Alefeld and J. Herzberger. *Introduction to Interval Computation.* New York, Academic Press, 1983.

[Apo60] T. M. Apostol. *Análisis Matemático.* Espanha, Editora Revert; S. A., 1960.

[Bau90] H. Bauch. Solving Ordinary Initial Problems by Means of T-Intervals. *ZAMM Z. angew. Math. Mech.*, 70(6):590–591, 1990.

[BG83] G. Bohlender and K. Grüner. Realization of an Optimal Computer Arithmetic. In U. W. Kulisch and W. L. Miranker, editors, *A New Approach to Scientific Computation*, pages 247–268. Proceedings of Symposium held at IBM Research Center, Yorktown Heights, N. Y., Academic Press, 1983.

[Bil79] P. Billingsley. *Probability and measure.* New York, John Wiley Sons, Inc., 1979.

[BJ76] G. E. Box and G. M.. Jenkins. *Time series analysis forecasting and control.* San Francisco, Holden-Day, 1976.

[Böh83] H. Böhm. Evaluation of Arithmetic Expressions with Maximum Accuracy. In U. W. Kulisch and W. L. Miranker, editors, *A New Approach to Scientific Computation*, pages 121–137. Proceedings of Symposium held at IBM Research Center, Yorktown Heights, N. Y., Academic Press, 1983.

[Boh94] G. Bohlender. Seminar notes. Departamento de Informática, Universidade Federal de Pernambuco , Recife (Brazil), December 1994.

[Bre69] L. Breiman. *Probability and Stochastic Processes.* Boston, Houghton Mifflin Company, 1969.

[BT87] S. B. Boswell and M. S. Taylor. A central limit theorem for fuzzy random variables. *Fuzzy Sets and Systems*, (24):331–344, 1987.

[Bur72] C. W. Burrill. *Measure, integration and probability.* McGraw-Hill Book Company, 1972.

[Cam95] M. A. Campos. Formalizing and Implementing (or Proving) Theorems about Intervals Using OBJ3. Technical Report 002, Departamento de Informática - UFPE - BRASIL, 1995.

[CB90] W. Cui and D. I. Blockley. Interval Probability Theory for Evidential Support. *International Journal of Intelligent Systems*, 5:183–192, 1990.

[CC95] M. A. Campos and M. de B. Correia. Interval and high accuracy results for parameter estimation in time series models. *International Journal of Reliable Computing*, pages 40–43, 1995.

[CCCL95] D. M. Claudio, M. de B. Correia, M. A. Campos, and R. D. Lins. *Linguagens de Programação e Computação Científica*. Canela, XV Congresso da Sociedade Brasileira de Computação, agosto 1995.

[CCL95] M. de B. Correia, M. A. Campos, and R. D. Lins. Paralelismo e Confiabilidade da Aritmética Computacional. *Curitiba, XVI Congresso Ibero Latino Americano sobre Métodos Computacionais em Engenharia*, pages 1375–1384, novembro 1995.

[Chu74] K. L. Chung. *A course in probability theory*. New York, Academic Press, Inc., second edition, 1974.

[Cla79] D. M. Claudio. *Beiträge zur Struktur der Rechnerarithmetik*. PhD thesis, Karlsruhe, Universität Karlsruhe, 1979.

[Cod88] W. J. Cody. Floating-Point Standards, Theory and Practice. In Ramon E. Moore, editor, *Reliability in Computing. The Role of Interval Methods in Scientific Computing*, volume 19 of *Perspectives in Computing*, pages 99–108. Academic Press, Inc., 1988.

[CSB95a] M. A. Campos, A. C. A. Sampaio, and A. H. F. Brainer. Mechanising the Theory of Intervals Using OBJ3. In *International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics*, 1995.

[CSB95b] M. A. Campos, A. C. S. Sampaio, and A. H. F. Brainer. Proving Algebraic Properties of Intervals using OBJ3. *XVIII Congresso Nacional de Matemática Aplicada e Computacional, Curitiba - PR - Brasil*, pages 118–122, 1995.

[DP90] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge, Cambridge University Press, 1990.

[DP91] D Didier and H. Prade. Random sets and fuzzy interval analysis. *Fuzzy Sets and Systems*, 42(1):87–101, 1991.

[Fel68] W. Feller. *An Introduction to Probability Theory and Its Applications*. New York, John Wiley & Sons, Inc., 1968.

[For77] G. E. Forsythe. Pitfalls in Computation, or Why a Math Book Isn't Enough. *Amer. Math. Monthly*, pages 931–955, 1977.

[Gai78] B. R. Gaines. Fuzzy and Probability Uncertainty Logic. *Information and Control*, pages 154–169, 1978.

[GM89] J. Goguen and J. Meseguer. Order sorted algebra i: Equational deduction for multiple inheritance, overloading, exceptions and partial operations. Technical report, SRI International, SRI-CSL-89-10, 1989.

[Gne75] B. V. Gnedenko. *The Theory of Probability.* Moscow, Mir Publishers, 1975.

[Gol91] D. Goldberg. What Every Computer Scientist Should Know About Floating-Point Arithmetic. *ACM Computing Surveys*, 23(1):5–48, March 1991.

[Gon79] A. Gonçalves. *Introdução à Álgebra.* Rio de Janeiro, Projeto Euclides, IMPA, 1979.

[Grü80] K. Grüner. Implementation of Universal Computer Arithmetic with Optimal Accuracy. *Computing*, (24):181–193, 1980.

[GTWW77] J. Goguen, J. Thatcher, E. Wagner, and J. Wright. Initial algebra semantics and continuous algebras. *Journal of the ACM*, 24(1):68–95, 1977.

[Gud92] J. W. von Gudenberg. Programming Language Support for Scientific Computation. *Interval Computations*, (4(6)):116–126, 1992.

[GV94] D. T. Golubkova and A. P. Voshchinin. Some Applications of Interval Regression Analysis in Biometrics. In *International Conference on Interval and Computer-Algebraic Methods in Science and Engineering*, pages 96–98, Interval'94, St-Petersburg, Russia, March 1994.

[GWM+93] J. A. Goguen, T. Winkler, J. Meseguer, K. Futatsigi, and J. P. Jouannaud. Introduction to OBJ. Technical report, SRI Internation, 1993. To appear.

[Han92] E. Hansen. *Global Optimization Using Interval Analysis.* Number 165 in Pure and Applied Mathematics. Marcel Dekker, Inc., 1992.

[HNR92] R. Hammer, M. Neaga, and D. Ratz. PASCAL-XSC, New Concepts for Scientific Computation and Numerical Data Processing. In E. Adams and U. Kulisch, editors, *Scientific Computing with Automatic Result Verification*, volume 189, pages 15–44. Academic Press, Inc., 1992.

[Hug89] J. Hughes. Why Functional Programming Matters. *The Computer Journal*, 32(2):98–107, 1989.

[Jam81] B. R. James. *Probabilidade: um curso em nível intermediário.* Rio de Janeiro, Projeto Euclides, IMPA, 1981.

[Kah68] W. M. Kahan. A more complete interval arithmetic. Lectures Notes for a Summer Course at the University of Michigan, 1968.

[Kah80] W. M. Kahan. Interval Arithmetic Options in the Proposed IEEE Floating Point Arithmetic Standard. In Karl L. E. Nickel, editor, *Interval Mathematics 1980*, pages 99–128. International Symposium on Interval Mathematics, Academic Press, 1980.

[Kaw78] H. Kawakernaak. Fuzzy Random Variables–i. definitions and theorems. *Information Sciences*, (15):1–29, 1978.

[Kaw79] H. Kawakernaak. Fuzzy Random Variables–ii. algorithms and examples for the discrete case. *Information Sciences*, (17):253–278, 1979.

[KB83] U. W. Kulisch and G. Bohlender. Features of a Hardware Implementation of an Optimal Arithmetic. In U. W. Kulisch and W. L. Miranker, editors, *A New Approach to Scientific Computation*, pages 269–290. Proceedings of Symposium held at IBM Research Center, Yorktown Heights, N. Y., Academic Press, 1983.

[KK95] R. B. Kearfott and V. Kreinovich. Applications of interval computations: An introduction. In R. B. Kearfott and V. Kreinovich, editors, *Applications of Interval Computations*, volume 3 of *Applied Optimization*, pages 1–22. Kluwer Academic Publishers, 1995.

[KM79] U. W Kulisch and W. L. Miranker. Computer Arithmetic in Theory and Practice. Technical Report 33658, IBM Thomas L. Watson Research Center, 1979.

[KM81] U. W. Kulisch and W. L. Miranker. *Computer Arithmetic in Theory and Practice.* New York, Academic Press, 1981.

[KM86] U. W. Kulisch and W. L. Miranker. The Arithmetic of the Digital Computer: A New Approach. *SIAM Review*, 28(1):1–40, March 1986.

[Knu81] D. E. Knuth. *The Art of Computer Programming*, volume II. Mass., Addison-Wesley, Reading, 2nd. ed. edition, 1981.

[Kol50] A. N. Kolmogorov. *Foundations of the Theory of Probability.* New York, Chelsea, 1950.

[Kre95] V. Kreinovich. Why intervals? A simple limit theorem that is similar to limit theorems from statistics. *Reliable Computing*, 1(1):33–40, 1995.

[Kul73] U. W. Kulisch. On the Concept of a Screen. *ZAMM*, (53):115–119, 1973.

[Kul83] U. W. Kulisch. A New Arithmetic for Scientific Computation. In U. W. Kulisch and W. L. Miranker, editors, *A New Approach to Scientific Computation*, pages 1–26. Proceedings of Symposium held at IBM Research Center, Yorktown Heights, N. Y., Academic Press, 1983.

[Lar82] H. J. Larson. *Introduction to Probability Theory and Statistical Inference.* New York, John Wiley & Sons, 1982.

[Law92] C. Lawo. C-XSC, a Programming Environment for Verified Scientific Computing. In E. Adams and U. Kulisch, editors, *Scientific Computing with Automatic Result Verification*, volume 189, pages 71–86. Academic Press, Inc., 1992.

[LCC95] R. D. Lins, M. A. Campos, and M. de B. Correia. Functional programming and interval arithmetic. *International Journal of Reliable Computing*, pages 146–150, 1995.

[Lim76] E. L. Lima. *Curso de Análise.* Rio de Janeiro, Projeto Euclides, IMPA, 1976.

[Lo5] M. Loève. *Probability Theory.* London, D. Van Nostrand Company, Inc.,, 1955.

[Mar77a] S. M. Markov. A Non-Standard Subtraction of Intervals. *SERDICA Bulgaricae mathematicae publicationes*, 3:359–370, 1977.

[Mar77b] S. M. Markov. On the Application of Interval Arithmetic in Numerical Analysis and Approximation Theory. In *Constructive Function Theory*, pages 389–393, 1977.

[Mar78] S. M. Markov. On the Extended Interval Arithmetic. *Comptes rendus de l'Acadèmie bulgare des Sciences*, 31(2):163–166, 1978.

[Mar81] S. M. Markov. On the Interval Computation of Elementary Functions. *Comptes rendus de l'Acad'emie bulgare des Sciences*, 34:319–322, 1981.

[McC60] N. H. McCoy. *Introduction to Modern Algebra.* Boston, Allyn and Bacon, Inc., 1960.

[Mey68] P. L. Meyer. *Probabilidade. Aplicações à Estatística.* Rio de Janeiro, Livros Técnicos e Científicos Editora, 1968.

[Moo66] R. E. Moore. *Interval Analysis.* N. J., Prentice Hall Inc., Englewood Cliffs, 1966.

[Moo79] R. E. Moore. *Methods and Applications of Interval Analysis.* SIAM, Philadelphia, Pennsylvania, 1979.

[MS84] M. Miyakoshi and M. Shimbo. A strong law of large numbers for fuzzy random variables. *Fuzzy Sets and Systems*, (12):133–142, 1984.

[Nar92] A. S. Narin'yani. NE-Factors and Natural Pragmatics: What do the Intervals Represent. *Interval Computations*, (4(6)):42–46, 1992.

[Neu87] A. Neumaier. Interval Methods for Systems of Equations. Cambridge, Cambridge University Press, 1987.

[Orl92] A. I. Orlov. Interval statistics. *Interval Computations*, pages 83–91, 1992.

[Pau91] L. C. Paulson. *ML for the Working Programmer.* Cambridge, Cambridge University Press, 1991.

[Pia86] K. Piasecki. Fuzzy probability spaces defined by means of the fuzzy relation "less than". *Fuzzy Sets and Systems*, (19):273–289, 1986.

[Rud76] W. Rudin. *Principles of Mathematical Analysis.* Great Britain, Mc-Graw Hill International Editions, 1976.

[Rum88] S. M. Rump. Algorithms for Verified Inclusions: Theory and Practice. In Ramon E. Moore, editor, *Reliability in Computing The Role of the Interval Methods in Scientific Computing*, pages 109–126. Academic Press, Inc., 1988.

[Rum94] S. M. Rump. Seminar notes. Departamento de Informática, Universidade Federal de Pernambuco, Recife (Brazil), September 1994.

[Sam93] A. C. A. Sampaio. *An Algebraic Approach to Compiler Design.* PhD thesis, Oxford University Computing Laboratory, 1993.

[San88] D. Sannella. A survey of formal software development methods. Technical Report ECS-LFCS-88-56, Laboratory for Foundations of Computer Science, July 1988.

[Shi93] D. Shiriaev. *Fast Automatic Differentiation for Vector Processors and Reduction of the Spatial Complexity in a Source Translation Environment.* PhD thesis, University of Karlsruhe, Germany, 1993.

[Sil87] E. N. Silva. Uma Especificação para a Aritmética de Intervalos. Master's thesis, Departamento de Informática/UFPE, 1987.

[Smy92] M. Smyth. Topology. In D. M. Gabbay S. Abramsky and T. S. E. Mainbaum, editors, *Handbook of Logic in Computer Science*, volume 1. Oxford University Press, 1992.

[Sne89] J. L. Snell. *Introduction to Probability.* Singapore, McGraw-Hill International Edition, 1989.

[SRC93] C. J. A. da Silva, Alencar F. M. R., and M. A. Campos. Uma Especificação da Aritmética Intervalar usando a Lnguagem EML. (unpublished manuscript), 1993.

[ST91] D. Sannella and A. Tarleck. Extended ML: past, present and future. Technical report, ECS-LFCS-91-138, Department of Computer Science, University of Edinburg, 1991.

[Ste74] P. H. Sterbenz. *Floating-Point Computation.* Prentice-Hall, Englewood Cliffs, N. J., 1974.

[Ste81] D. Stevenson. A Proposed Standard for Binary Floating-Point Arithmetic. *Computer*, 14(3):51–62, March 1981.

[Sun58] T. Sunaga. Theory of An Interval Algebra and its Application to Numerical Analysis. *RAAG Memoirs*, (2):29–46, 1958.

[VBS90] A. P. Voshchinin, A. F. Bochkov, and G. R. Sotirov. Method of data analysis with a nonstatistical interval. *Industrial Laboratory (Moscow Power Institute)*, pages 854–860, 1990. Russian Original Vol. 56, No. 7, pp. 76-81.

[Vos88] A. P. Voshchinin. Solution of optimization problems in the interval estimates criterion. *Industrial Laboratory (Moscow Power Institute)*, pages 615–620, 1988. Russian Original, Vol. 16, No. 7, pp. 45-48, 1987.

[Vos92] A. S. Voshchinin. Some Questions of Application of Interval Mathematics in Parameter Estimation and Decision Making. *Interval Computations*, pages 42–46, 1992.

[VP95] S. Valliappan and T. D. Pham. Fuzzy logic applied to numerical modelling of engineering problems. *Computational Mechanics Advances*, 2:213–287, 1995.

[Wal92] W.V. Walter. ACRITH-XSC, A Fortran-like Language for Verified Computing. In E. Adams and U. Kulisch, editors, *Scientific Computing with Automatic Result Verification*, volume 189, pages 45–70. Academic Press, Inc., 1992.

[Wil90] R. C. Williamson. Interval Arithmetic and Probabilistic Arithmetic. In J. C. Ulriich, editor, *Contributions to Computer Arithmetic and Self-Validating Numerical Methods*, pages 67–80. IMACS, 1990.

[WK94] M. C. Wang and W. J. Kennedy. Self-Validating Computations of Probabilities for Selected Central and Noncentral Univariate Probability Functions. *Journal of the American Statistical Association*, pages 878–887, 1994.

Apêndice A

Estruturas Algébricas

Computação numérica necessita do conhecimento do espaço ao qual os números pertencem e das propriedades relativas às operações aritméticas definidas nesse espaço. Isto leva à álgebra. Portanto seguem-se alguns fundamentos algébricos que serão aplicados aos espaços da computação numérica.

A.1 Grupo

Definição A.1.1 Seja R um conjunto não-vazio. Uma *operação binária* sobre R, $*$, é uma função que associa a cada par (a, b), constituído de elementos de R, um elemento $a * b$ em R.

A mais simples estrutura algébrica que se pode pensar é um conjunto não-vazio, R, com uma operação definida em R. Esta operação pode ou não satisfazer qualquer propriedade. Tal estrutura é chamada *grupóide*.

Exemplo A.1.2 Seja $\mathbb{R}$ o conjunto dos números reais. $\langle \mathbb{R}, + \rangle$ é um grupóide com elemento neutro 0 e $\langle \mathbb{R}, \cdot \rangle$ é um grupóide com elemento neutro 1. $\langle \mathbb{R}, - \rangle$ é um grupóide, mas o elemento neutro 0 é apenas à direita ($a - 0 = a, \ \forall a \in \mathbb{R}$).

Definição A.1.3 Seja R um conjunto não-vazio e $*$ uma operação binária definida sobre R. $\langle \mathrm{R}, * \rangle$ é um *grupo* se, para quaisquer $a, b, c \in \mathrm{R}$ tem-se que:

$\mathbf{P1_{GRP}}$: Se $a, b, c \in \mathrm{R}$, então $(a * b) * c = a * (b * c)$
(lei associativa)

$\mathbf{P2_{GRP}}$: Existe $e \in \mathrm{R}$ tal que $e * a = a * e = a, \ \forall a \in \mathrm{R}$
(existência de identidade)

$\mathbf{P3_{GRP}}$: Se $a \in \mathrm{R}$, existe $x \in \mathrm{R}$ tal que $a * x = x * a = e, \ \forall a \in \mathrm{R}$
(existência de inverso)

A.2 Anel

Definição A.2.1 Seja R um conjunto não-vazio sobre o qual estão definidas duas operações binárias, $+$ e $\cdot$, denominadas respectivamente adição e multiplicação, tal que para quaisquer $a, b, c \in \mathrm{R}$ as seguintes propriedades sejam satisfeitas:

P1$_{\mathbf{ANL}}$ **:** $a + b = b + a$
(lei comutativa da adição)

P2$_{\mathbf{ANL}}$ **:** $(a + b) + c = a + (b + c)$
(lei associativa da adição)

P3$_{\mathbf{ANL}}$ **:** Existe $\mathbb{O} \in$ R tal que $a + \mathbb{O} = \mathbb{O} + a = a, \forall a \in$ R
(existência de um zero ou identidade aditiva)

P4$_{\mathbf{ANL}}$ **:** Se $a \in$ R, existe $-a \in$ R tal que $a + (-a) = (-a) + a = \mathbb{O}$
(existência de inverso aditivo)

P5$_{\mathbf{ANL}}$ **:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
(lei associativa da multiplicação)

P6$_{\mathbf{ANL}}$ **:** $a \cdot (b + c) = a \cdot b + a \cdot c, \ \ (b + c) \cdot a = b \cdot a + c \cdot a$
(leis distributivas)

$\langle \mathrm{R}, +, \cdot \rangle$ satisfazendo as propriedades P1$_{\mathrm{ANL}}$-P6$_{\mathrm{ANL}}$ é chamado um *anel.*

Observação. No que segue é adotada a convenção de se escrever xy em lugar de $x \cdot y$.

A.3 Corpo

Definição A.3.1 Um *corpo* $\langle \mathrm{R}, +, \cdot \rangle$ é uma estrutura algébrica onde $\forall a, b, c \in$ R valem as seguintes propriedades:

P1$_{\mathbf{CRP}}$ **:** $a + b = b + a$
(lei comutativa da adição)

P2$_{\mathbf{CRP}}$ **:** $(a + b) + c = a + (b + c)$
(lei associativa da adição)

P3$_{\mathbf{CRP}}$ **:** Existe $\mathbb{O} \ \in$ R tal que $a + \mathbb{O} = \mathbb{O} + a =$ a$, \forall a \in$ R
(existência de um zero ou identidade aditiva)

P4$_{\mathbf{CRP}}$ **:** Se $a \in$ R, existe $-a \in$ R tal que $a + (-a) = (-a) + a = \mathbb{O}$
(existência de inverso aditivo)

P5$_{\mathbf{CRP}}$ **:** $(ab)c = a(bc)$
(lei associativa da multiplicação)

P6$_{\mathbf{CRP}}$ **:** $a(b + c) = ab + ac, \ (b + c)a = ba + ca$
(leis distributivas)

P7$_{\mathbf{CRP}}$: $ab = ba$
(lei comutativa da multiplicação)

P8$_{\mathbf{CRP}}$: Existe $\mathbb{1} \in$ R tal que $\mathbb{1}\, a = a\mathbb{1} = a$, $\forall a \in$ R
(existência de uma unidade)

P9$_{\mathbf{CRP}}$: Se $a \in$ R e $a \neq \mathbb{0}$, então existe $a^{-1} \in$ R tal que $aa^{-1} = a^{-1}a = \mathbb{1}$
(existência de inverso multiplicativo)

A.4 Espaço Vetorial

Definição A.4.1 Seja V um conjunto não vazio e K um corpo. V é um *espaço vetorial* sobre o corpo K se forem dadas:
Uma operação binária de V×V→V com $(\mathbf{a},\mathbf{b})\mapsto\mathbf{a}+\mathbf{b}$ satisfazendo os seguintes axiomas:

P1$_{\mathbf{EVT}}$: $\mathbf{a}+\mathbf{b}=\mathbf{b}+\mathbf{a}$, $\forall$ $\mathbf{a},\mathbf{b} \in$V

P2$_{\mathbf{EVT}}$: $\mathbf{a}+(\mathbf{b}+\mathbf{c})=(\mathbf{a}+\mathbf{b})+\mathbf{c}$, $\forall \mathbf{a}, \mathbf{b}, \mathbf{c} \in$ V

P3$_{\mathbf{EVT}}$: Existe $\mathbf{o} \in$ V tal que $\mathbf{a}+\mathbf{o}=\mathbf{o}+\mathbf{a}=\mathbf{a}$, $\forall$ $\mathbf{a}\in$V

P4$_{\mathbf{EVT}}$: Para todo $\mathbf{a} \in$ V, existe $-\mathbf{a} \in$ V tal que $\mathbf{a}+(-\mathbf{a})=(-\mathbf{a})+\mathbf{a}=\mathbf{o}$

Uma operação binária de K×V→V com $(\alpha,\mathbf{b})\mapsto\alpha\mathbf{b}$ satisfazendo os seguintes axiomas:

P5$_{\mathbf{EVT}}$: $\alpha(\beta\mathbf{a}) = (\alpha\beta)\mathbf{a}$, $\forall\alpha, \beta \in$ K e $\forall\mathbf{a} \in$ V

P6$_{\mathbf{EVT}}$: $\mathbb{1}\, \mathbf{a}=\mathbf{a}$, $\mathbb{1}\in$ K, $\forall\mathbf{a} \in$ V

P7$_{\mathbf{EVT}}$: $(\alpha + \beta)\mathbf{a} = \alpha\mathbf{a} + \beta\mathbf{a}, \forall\alpha, \beta \in$ K e $\forall\mathbf{a} \in$ V

P8$_{\mathbf{EVT}}$: $\alpha(\mathbf{a} + \mathbf{b}) = \alpha\mathbf{a} + \alpha\mathbf{b}, \forall\alpha \in$ K e $\forall\mathbf{a}, \mathbf{b} \in$ V

Os elementos de V são chamados vetores e os de K, escalares.

A.5 Ordem

Definição A.5.1 Seja R um conjunto. Uma *ordem* ou *ordem parcial* sobre R é uma relação binária $\leq$ sobre R tal que para todo $x, y \in$ R,

(a) $x \leq x$

(b) $x \leq y$ e $y \leq x$ implica $x = y$

(c) $x \leq y$ e $y \leq z$ implica $x \leq z$

Estas condições são referenciadas, respectivamente, como *reflexividade*, *anti-simetria* e *transitividade*. Um conjunto com uma relação de ordem $\leq$ é dito um *conjunto ordenado* ou um *conjunto parcialmente ordenado*. Alguns autores usam o termo *poset* (*partially ordered set*). Quando é necessário especificar a ordem escreve-se $\langle \mathrm{R}, \leq \rangle$.

Uma relação de ordem $\leq$ dá origem a uma relação de *desigualdade estrita*: $x < y$ em R se e só se $x \leq y$ e $x \neq y$. Também $x \geq y$ é usado em lugar de $y \leq x$. O símbolo $\|$ é usado para denotar não-comparabilidade, isto é: $x \parallel y$ se $x \nleq y$ e $y \nleq x$. Neste caso se diz que x e y são elementos não-comparáveis.

Seja R um conjunto ordenado. Então R é uma *cadeia* se, para todo $x, y \in$R, ou $x \leq y$ ou $y \leq x$, isto é, quaisquer dois elementos de R são comparáveis. Nomes alternativos para cadeias são *conjunto linearmente ordenado* e *conjunto totalmente ordenado*.

Exemplo A.5.2 Seja R um conjunto qualquer. O conjunto das partes (ou powerset) PR, consistindo de todos os subconjuntos de R, é ordenado com respeito à inclusão de conjuntos. Para A,B $\in$ PR, A$\leq$B se e somente se A$\subseteq$B. Porém $\langle \mathrm{PR}, \subseteq \rangle$ não é uma cadeia pois seja R=$\{1, 2\}$, então $\mathrm{PR} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Em PR, $\{1\} \nsubseteq \{2\}$ e $\{2\} \nsubseteq \{1\}$. Assim $\{1\}$ e $\{2\}$ são não-comparáveis segundo a relação de ordem $\subseteq$.

A.6 Anelóide

Os conceitos a seguir são devidos a [KM81, KM79, Cla79, Kul83, KM86]. Estas estruturas algébricas são básicas pois se repetem nos subconjuntos da direita da Figura 3.1 do capítulo 3, quando sua aritmética é definida através de semimorfismo.

Definição A.6.1 Seja R um conjunto não-vazio sobre o qual estão definidas duas operações binárias, $+$ e $\cdot$, denominadas respectivamente adição e multiplicação, tal que para quaisquer $a, b, c \in$ R as seguintes propriedades sejam satisfeitas:

P1$_{\mathbf{ALD}}$: $a + b = b + a$
(lei comutativa da adição)

P2$_{\mathbf{ALD}}$: Existe $\mathbb{O} \in$ R tal que $a + \mathbb{O} = a, \ \forall a \in$ R
(existência de um zero)

P3$_{\mathbf{ALD}}$: Existe $\mathbb{1} \in \mathrm{R} - \{\mathbb{O}\}$ tal que $a\, \mathbb{1} = \mathbb{1}\, a = a$
(existência de uma unidade)

P4$_{\mathbf{ALD}}$: $a\, \mathbb{O} = \mathbb{O}\, a = \mathbb{O}, \ \forall a \in$ R

P5$_{\mathbf{ALD}}$: Existe um elemento $\mathbf{x} \in$ R tal que

- **P5(a)$_{\mathbf{ALD}}$** : $\mathbf{x} + \mathbb{1} = \mathbb{O}$
- **P5(b)$_{\mathbf{ALD}}$** : $\mathbf{x}\mathbf{x} = \mathbb{1}$
- **P5(c)$_{\mathbf{ALD}}$** : $\mathbf{x}(ab) = (\mathbf{x}a)b = a(\mathbf{x}b)$
- **P5(d)$_{\mathbf{ALD}}$** : $\mathbf{x}(a + b) = (\mathbf{x}a) + (\mathbf{x}b)$

P6$_{\mathbf{ALD}}$: $\mathbf{x}$ é único

A terna $\langle \mathrm{R}, +, \cdot \rangle$ satisfazendo as propriedades P1$_{\mathrm{ALD}}$-P6$_{\mathrm{ALD}}$ é chamado um *anelóide*.
Seja N$\subseteq$R, $\mathbb{O}\in$ N e $/$: R $\times$ (R-N) $\rightarrow$ R. A estrutura $\langle \mathrm{R}, +, \cdot, / \rangle$ é um *anelóide divisão* se a divisão ($/$) é uma operação binária bem definida e também valem:

P7$_{\mathbf{ALD}}$: $a/\mathbb{1}$ = a, $\forall a \in$ R

P8$_{\mathbf{ALD}}$: $\mathbb{O}/a = \mathbb{O}$, $\forall a \in$ (R-N)

P9$_{\mathbf{ALD}}$: $\mathbf{x}(a/b) = (\mathbf{x}a)/b = a/(\mathbf{x}b), \forall a \in$ R, $\forall b \in$ (R-N)

Em um anelóide ou anelóide divisão tem-se três elementos destacáveis: $\mathbb{O}$, $\mathbb{1}$ e $\mathbf{x}$. Em se tratando de $\mathbb{R}$ ou $\mathbb{C}$, respectivamente, os conjuntos dos números reais e complexos, $\mathbf{x} = -1$. São anelóides $\langle \mathbb{R}, +, \cdot \rangle$ e $\langle \mathbb{C}, +, \cdot \rangle$ e, fazendo N=$\{\mathbb{O}\}$, $\langle \mathbb{R}, \mathrm{N}, +, \cdot, / \rangle$ e $\langle \mathbb{C}, \mathrm{N}, +, \cdot, / \rangle$ são anelóides divisão. Comparado com outras estruturas algébricas, nota-se que em um anelóide, além da inexistência das propriedades associativa e distributiva, não se assume a existência de elemento inverso, nem aditivo, nem multiplicativo.

Definição A.6.2 Um anelóide $\langle \mathrm{R}, +, \cdot, \rangle$ é *fracamente ordenado* se R é um conjunto ordenado e $\forall\ a, b, c \in$ R também valem

P10$_{\mathbf{ALD}}$: $a \leq b \Rightarrow a + c \leq b + c$

P11$_{\mathbf{ALD}}$: $a \leq b \Rightarrow \mathbf{x}b \leq \mathbf{x}a$

Definição A.6.3 Um anelóide fracamente ordenado $\langle \mathrm{R}, +, \cdot, \rangle$ é *ordenado* se $\forall\ a, b, c \in$ R,

P12$_{\mathbf{ALD}}$: $\mathbb{O} \leq a \leq b$ e $c > \mathbb{O} \Rightarrow ac \leq bc$ e $ca \leq cb$

Existem definições similares para anelóides divisão.

A idéia de completamento de um reticulado, que será vista posteriormente, é bastante sensível no caso dos reais. $\mathbb{R}$ não é um reticulado completo, necessitando-se para sua completude dos símbolos $+\infty$ e $-\infty$, na forma $\mathbb{R}\cup\{-\infty\}\cup\{+\infty\}$. Com respeito a anelóides, as expressões *anelóide linearmente ordenado*, *anelóide completamente ordenado* e *anelóide completamente e fracamente ordenado* serão usadas indistintamente quando a ordem no anelóide é linear ou completa.

Definição A.6.4 Um anelóide é *inclusamente ordenado* com respeito à ordem parcial $\subseteq$, se $\forall * \in \{+, \cdot\}$ e $\forall\ a, b, c, d \in$ R,

P13$_{\mathbf{ALD}}$: $a \subseteq b$ e $c \subseteq d \Rightarrow a * c \subseteq b * d$

Existem definições similares para anelóides divisão.

Definição A.6.5 Em um anelóide define-se um *operador menos* por

$$-a = \mathbf{x}a,\ \forall a \in \mathrm{R}$$

e uma *subtração* por

$$a - b = a + (-b),\ \forall a, b \in \mathrm{R}$$

[KM79, KM81, Cla79] mostram que em um anelóide, ou anelóide divisão, o operador menos tem as mesmas propriedades que a subtração em $\mathbb{R}$ ou $\mathbb{C}$. É importante enfatizar que $\langle \mathbb{R}, +, \cdot, 0, 1\rangle$ e $\langle \mathbb{C}, +, \cdot, (0,0), (1,0)\rangle$ são anelóides ou anelóides divisão se destacado o zero correspondente a cada um. $\langle \mathbb{R}, +, \cdot, 0, 1, \leq\rangle$ é linearmente ordenado e, se a relação de ordem é definida componente a componente, $\langle \mathbb{C}, +, \cdot, (0,0), (1,0), \leq\rangle$ é um anelóide fracamente ordenado.

Teorema A.6.6 Se R é um anelóide linearmente ordenado, a unicidade do elemento **x** ($P6_{ALD}$), é uma consequência das propriedades $P1_{ALD}$, $P2_{ALD}$, $P3_{ALD}$, $P4_{ALD}$, $P5_{ALD}$,$P10_{ALD}$, $P11_{ALD}$, $P12_{ALD}$.
A prova deste teorema pode ser encontrada nas referências [KM79, KM81].

De modo geral em anelóides não se assume a existência de inverso, nem aditivo, nem multiplicativo. Porém se o anelóide é linearmente ordenado então $a+(-a) = (-a)+a = \mathbb{0}$, isto é, existe um inverso aditivo para todo $a \in \mathrm{R}$.

Seja R um conjunto não vazio e PR, o conjunto das partes de R. Para cada operação $*$ definida sobre R, define-se uma correspondente em PR da seguinte forma,

$$\mathrm{A} * \mathrm{B} = \{\mathrm{a} * \mathrm{b} \mid \mathrm{a} \in \mathrm{A} \text{ e } \mathrm{b} \in \mathrm{B}\},\ \forall \mathrm{A,B} \in \mathrm{PR}$$

Supondo que $\langle \mathrm{R}, *\rangle$ é um grupo, [KM79, KM81] provam que $\langle \mathrm{PR}, *\rangle$ não é um grupo; consequentemente, também não é um anel ou corpo. Entretanto, se R é um anelóide, PR também é um anelóide:

Teorema A.6.7 Se $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}\rangle$ é um anelóide, então $\langle \mathrm{PR}, +, \cdot, \{\mathbb{0}\}, \{\mathbb{1}\}\rangle$ também é um anelóide.
A prova pode ser encontrada nas referências [KM79, KM81].

A importância do teorema A.6.7 é mostrar que a estrutura algébrica anelóide é preservada quando operações são definidas no conjunto das partes. A contrapartida deste fato, como será enfatizado posteriormente, é que operações no conjunto das partes não são implementáveis e que transformações convenientes precisam ser feitas, quando o objetivo é a definição de uma aritmética. Este teorema também é válido se R é um anelóide divisão.

A.7 Matrizes sobre Anelóides

A seguir é visto como é construído um espaço de matrizes sobre anelóides.

Seja o anelóide $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}\rangle$, $\mathrm{M}_{mn}\mathrm{R}$ o conjunto de todas as matrizes com elementos em R e A=(a_{ij}) e B=(b_{ij}), com $i = 1, \ldots, m$ e $j = 1, \ldots, n$, elementos de $\mathrm{M}_{mn}\mathrm{R}$. Se $m = n$, escreve-se $\mathrm{M}_n\mathrm{R}$. Definem-se em $\mathrm{M}_{mn}\mathrm{R}$ as operações de adição e multiplicação de forma usual; a igualdade e a ordem são definidas componente a componente,

$$(a_{ij}) \leq (b_{ij}) \Leftrightarrow a_{ij} \leq b_{ij},\ \forall\ i = 1, \ldots, m\ \forall\ j = 1, \ldots, n$$

Teorema A.7.1 Seja $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ um anelóide. Então $\langle \mathrm{M}_n\mathrm{R}, +, \cdot, O, E, \leq\rangle$ também é um anelóide, onde

$$O = \begin{pmatrix} \mathbb{O} & \mathbb{O} & \dots & \mathbb{O} \\ \mathbb{O} & \mathbb{O} & \dots & \mathbb{O} \\ \dots & \dots & \dots & \dots \\ \mathbb{O} & \mathbb{O} & \dots & \mathbb{O} \end{pmatrix}, E = \begin{pmatrix} \mathbb{1} & \mathbb{O} & \dots & \mathbb{O} \\ \mathbb{O} & \mathbb{1} & \dots & \mathbb{O} \\ \dots & \dots & \dots & \dots \\ \mathbb{O} & \mathbb{O} & \dots & \mathbb{1} \end{pmatrix}, -E = \begin{pmatrix} -\mathbb{1} & \mathbb{O} & \dots & \mathbb{O} \\ \mathbb{O} & -\mathbb{1} & \dots & \mathbb{O} \\ \dots & \dots & \dots & \dots \\ \mathbb{O} & \mathbb{O} & \dots & -\mathbb{1} \end{pmatrix}$$

A prova deste teorema é encontrada em [KM79, KM81].

A.8 Anelóides Complexos

Seja R um anelóide ou anelóide divisão. Qual a estrutura algébrica de um espaço complexo construído a partir de R? Isto é visto a seguir.

Seja $\langle \mathrm{R}, \mathrm{N}, +, \cdot, /, \leq \rangle$ onde R é um anelóide e $\mathrm{N} \subseteq \mathrm{R}$ tal que $\mathbb{O} \in \mathrm{N}$; seja

$$\mathrm{CR}=\{(a,b) \mid a,b \in \mathrm{R}\}$$

e $\overline{\mathrm{N}} \subseteq \mathrm{CR}$ tal que $(\mathbb{O},\mathbb{O}) \in \overline{\mathrm{N}}$. Igualdade, adição, multiplicação, divisão e relação de ordem em CR são definidas $\forall \alpha, \beta \in \mathrm{CR}$, $\alpha = (a_1, a_2)$, $\beta = (b_1, b_2)$, respectivamente, da seguinte forma.

$$\alpha = \beta \Leftrightarrow (a_1, a_2) = (b_1, b_2) \Leftrightarrow a_1 = b_1 \text{ e } a_2 = b_2$$

$$\alpha + \beta = (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

$$\alpha \cdot \beta = (a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$$

$$\alpha / \beta = (a_1, a_2)/(b_1, b_2) = ((a_1 b_1 + a_2 b_2)/b, (a_2 b_1 - a_1 b_2)/b), \; b = b_1 b_1 + b_2 b_2, \; b \in \text{R-N}, \; \beta \in \mathbb{C}\mathrm{R} - \overline{\mathrm{N}}$$

$$\alpha \leq \beta \Leftrightarrow (a_1, a_2) \leq (b_1, b_2) \Leftrightarrow a_1 \leq b_1 \text{ e } a_2 \leq b_2$$

Teorema A.8.1 Seja $\langle \mathrm{R}, +, \cdot, \mathbb{O}, \mathbb{1}, \leq \rangle$ um anelóide (ou anelóide divisão). Então $\langle \mathrm{CR}, +, \cdot, (\mathbb{O},\mathbb{O}), (\mathbb{1},\mathbb{O}), \leq \rangle$ também é um anelóide. Se $\langle \mathrm{R}, +, \cdot, \mathbb{O}, \mathbb{1}, \leq \rangle$ é um anelóide fracamente ordenado, então $\langle \mathrm{CR}, +, \cdot, (\mathbb{O},\mathbb{O}), (\mathbb{1},\mathbb{O}), \leq \rangle$ também é um anelóide fracamente ordenado.

A prova deste teorema pode ser encontrada em [KM79, KM81].

A.9 Vetóides

Definição A.9.1 Seja $\langle \mathrm{R}, +, \cdot, \mathbb{O}, \mathbb{1}, \leq \rangle$ um anelóide, $\langle \mathrm{V}, + \rangle$ um grupóide e

$$\cdot : \mathrm{R} \times \mathrm{V} \to \mathrm{V}$$

tal que

$$-\mathbf{a} = (-\mathbb{1}) \cdot \mathbf{a}, \; \forall \mathbf{a} \in \mathrm{V}$$

$\langle \mathrm{V}, \mathrm{R}, +, . \rangle$ é um *vetóide* sobre R ou um *R-vetóide* se:

P1$_{\mathbf{VTD}}$: **a+b=b+a**, $\forall$ **a,b** $\in$ V

P2$_{\mathbf{VTD}}$: Existe **o** $\in$ V tal que **a+o=o+a=a**, $\forall$ **a**$\in$ V

P3$_{\mathbf{VTD}}$: $a \cdot \mathbf{o} = \mathbf{o}$ e $\mathbb{0}\cdot$ **a=o** , $\forall a \in$ R, $\forall$**a** $\in$ V

P4$_{\mathbf{VTD}}$: $\mathbb{1}\cdot$ **a=a**, $\forall$**a** $\in$ V

P5$_{\mathbf{VTD}}$: $(-a \cdot \mathbf{a}) = (-a) \cdot \mathbf{a} = a \cdot (-\mathbf{a}), \forall a \in$ R, $\forall$**a** $\in$ V

P6$_{\mathbf{VTD}}$: $-$(**a+b**)=($-$**a**)+($-$**b**), $\forall$**a,b** $\in$ V

Um anelóide representa uma generalização de anel com elemento unidade, assim como um vetóide representa uma generalização de espaço vetorial. Tanto em anelóides quanto em vetóides não se assume a existência de elemento inverso.

A.10 Anelóides e Vetóides Completamente Ordenados

Conjuntos *consistentemente completos*, isto é, conjuntos onde todos seus subconjuntos limitados têm um maior e um menor elemento, podem sempre ser completados de tal forma que o menor e o maior elementos também satisfaçam propriedades algébricas e de ordem. Portanto, sempre que necessário, pode-se considerar um conjunto consistentemente completo como *completo*. O teorema a seguir justifica esta declaração no caso de anelóides. Para os vetóides existe teorema similar.

Teorema A.10.1 Seja $\langle$R$, +, \cdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ um anelóide ordenado (ou fracamente ordenado) onde R é consistentemente completo. Acrescentado-se a R um menor elemento $-p$ e um maior elemento $+p$ e as operações de adição, multiplicação e divisão são definidas como nas tabelas abaixo, então $\langle$R$\cup\{-p\}\cup\{+p\}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ é um anelóide completamente ordenado (ou um anelóide fracamente e completamente ordenado quando a divisão for definida).

	$b \in$R	$-p$	$+p$
$a \in$R	$a+b$	$-p$	$+p$
$-p$	$-p$	$-p$	$p-p$
$+p$	$+p$	$p-p$	$+p$

Figura A.1: Adição em um Anelóide

	$-p < b < \mathbb{0}$	$\mathbb{0} < b < +p$	$-p$	$-\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$+p$	$b \parallel \mathbb{0}$
$-p < a < \mathbb{0}$	ab	ab	$+p$	$-a$	$\mathbb{0}$	a	$-p$	ab
$\mathbb{0} < a < +p$	ab	ab	$-p$	$-a$	$\mathbb{0}$	a	$+p$	ab
$-p$	$+p$	$-p$	$+p$	$+p$	$\mathbb{0}$	$-p$	$-p$	$(-p)b$
$-\mathbb{1}$	$-b$	$-b$	$+p$	$\mathbb{1}$	$\mathbb{0}$	$-\mathbb{1}$	$-$p	$-$b
$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$
$\mathbb{1}$	b	b	$-p$	-$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$+p$	b
$+p$	$-p$	$+p$	$-p$	$-p$	$\mathbb{0}$	$+p$	$+p$	$(+p)b$
$a \parallel \mathbb{0}$	ab	ab	$a(-p)$	$-a$	$\mathbb{0}$	a	$a(+p)$	ab

Figura A.2: Multiplicação em um Anelóide

	$-p < b < \mathbb{0}$	$\mathbb{0} < b < +p$	$-p$	$\mathbb{1}$	$+p$	$b \parallel \mathbb{0}$
$-p < a < \mathbb{0}$	a/b	a/b	$\mathbb{0}$	a	$\mathbb{0}$	a/b
$\mathbb{0} < a < +p$	a/b	a/b	$\mathbb{0}$	a	$\mathbb{0}$	a/b
$-p$	$+p$	$-p$	$(-p)/(-p)$	$-p$	$(-p)/(+p)$	$(-p)/b$
$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$
$+p$	$-p$	$+p$	$(+p)/(-p)$	$+p$	$(+p)/(+p)$	$(+p)/b$
$a \parallel \mathbb{0}$	a/b	a/b	$a/(-p)$	a	$a/(+p)$	a/b

Figura A.3: Divisão em um Anelóides

A prova deste teorema pode ser encontrada em [KM79, KM81]. Tabelas similares podem ser construídas para vetóides.

A.11 Reticulados

Esta seção trata inicialmente de reticulados [Kul73, KM79, KM81, DP90]. Tais estruturas são usadas para a definição dos arredondamentos direcionados; estes arredondamentos, quando definidos sobre reticulados, têm propriedades de interesse para a definição do método horizontal da aritmética em computadores.

Definição A.11.1 Seja R um conjunto ordenado não-vazio, $\mathrm{X} \subseteq \mathrm{R}$ e $a, b \in \mathrm{R}$.

(a) b é o *supremo* de X em R, denotado por $\sup \mathrm{X}$, se $x \leq b$, $\forall x \in \mathrm{X}$ e se $c \in \mathrm{R}$ é tal que $x \leq c$, $\forall x \in \mathrm{X}$, então $b \leq c$.

(b) a é o *ínfimo* de X em R, denotado por $\inf \mathrm{X}$, se $a \leq x$, $\forall x \in \mathrm{X}$ e se $c \in \mathrm{R}$ é tal que $c \leq x$, $\forall x \in \mathrm{X}$, então $c \leq a$.

Então b ser o supremo de X em R significa que b é a menor das cotas superiores para X em R; de modo análogo, se a é o ínfimo para X em R, a é a maior das cotas inferiores para X em R [DP90, Lim76, KM79, KM81] .

Uma notação alternativa é $x \vee y$ em lugar de $\sup\{x, y\}$ e $x \wedge y$ em lugar de $\inf\{x, y\}$. De forma análoga, $\bigvee \mathrm{X}$ e $\bigwedge \mathrm{X}$ em lugar de $\sup \mathrm{X}$ e $\inf \mathrm{X}$. Se for necessário indicar em qual conjunto, R por exemplo, estão sendo tomados o supremo e o ínfimo, escreve-se, respectivamente, $\bigvee_R \mathrm{X}$ e $\bigwedge_R \mathrm{X}$.

Sejam L(X) e U(X), respectivamente, os conjuntos dos limites inferiores e superiores de X em R,

$$\mathrm{L(X)} = \{a \in \mathrm{R} \mid (\forall x \in \mathrm{X})\, a \leq x\}$$

$$\mathrm{U(X)} = \{b \in \mathrm{R} \mid (\forall x \in \mathrm{X})\, x \leq b\}$$

Definição A.11.2 Seja R um conjunto ordenado não-vazio.

(a) Se $x \vee y$ e $x \wedge y$ existem para todo $x, y \in \mathrm{R}$, então R é chamado um *reticulado*.

(b) Se para qualquer X⊆R não-vazio e limitado existem $\bigvee$X e $\bigwedge$X, então R é *consistentemente completo.*

(c) Se $\bigvee$X e $\bigwedge$X existem para todo X⊆R, então R é um *reticulado completo* ou *completamente ordenado.*

Seja R um conjunto ordenado. O maior elemento de R, se existe, é chamado elemento *topo* de R e é denotado por $\top$; dualmente, o elemento *bottom* de R é o menor elemento de R, sendo denotado por $\perp$. Em PR tem-se $\top$=R e $\perp = \emptyset$ [DP90].

Exemplo A.11.3 Sejam $\mathbb{N}$, $\mathbb{Q}$ e $\mathbb{R}$ os conjuntos dos números naturais, racionais e reais, respectivamente. $\mathbb{N}, \mathbb{Q}$ e $\mathbb{R}$ são reticulados com as ordens usuais, porém nenhum deles é reticulado completo. Todos falham com respeito ao elemento $\top$. A falha na completude de $\mathbb{Q}$ é mais fundamental de que em $\mathbb{R}$; em $\mathbb{Q}$ não apenas a falta dos elementos $\top$ e $\perp$ causa problemas; o conjunto $\{r \in \mathbb{Q} \mid r^2 < 2\}$ tem em $\mathbb{Q}$ limites superiores mas não um menor limite superior. Se $-\infty < x < y < +\infty$, então o intervalo fechado $[x, y]$ em $\mathbb{R}$ é um reticulado completo (completude de $\mathbb{R}$).

Exemplo A.11.4 Sejam $\langle \mathrm{R}_i, \leq_i \rangle$, $i = 1, \ldots, n$, reticulados completos e $\mathrm{R}=\mathrm{R}_1 \times \ldots \times \mathrm{R}_n = \{(a_1, \ldots, a_n) \mid a_i \in \mathrm{R}_i\}$. Dados $a, b \in$ R define-se

$$a \leq_{\mathrm{R}} b \Leftrightarrow a_i \leq_i a_i, \ \forall\ i = 1, ..., n.$$

Então $\langle \mathrm{R}, \leq_{\mathrm{R}} \rangle$ é um reticulado completo.

Exemplo A.11.5 Para qualquer conjunto R, o conjunto ordenado $\langle \mathrm{PR}, \subseteq \rangle$ é um reticulado completo no qual

$$\bigvee\{\mathrm{A}_i \mid i \in I\} = \bigcup_{i \in I} \mathrm{A}_i$$

$$\bigwedge\{\mathrm{A}_i \mid i \in I\} = \bigcap_{i \in I} \mathrm{A}_i$$

onde os $\mathrm{A}_i \subseteq$ R.

O teorema a seguir mostra que uma condição suficiente para um conjunto ordenado ser um reticulado completo é que qualquer um de seus subconjuntos tenha supremo ou ínfimo.

Teorema A.11.6 Seja R um conjunto ordenado tal que qualquer um de seus subconjuntos tenha ínfimo (ou supremo). Então R é um reticulado completo.

Demonstração. Seja X⊆R e $\mathrm{U(X)} = \{b \in \mathrm{R} \mid (\forall x \in \mathrm{X})\ x \leq b\}$. U(X)⊆R e por hipótese U(X) tem ínfimo. Será provado que U(X) também tem supremo. Seja u_0=inf U(X), logo

$$x \leq u_0, \ \forall x \in \mathrm{X} \tag{1}$$

Seja $t \in$ R tal que $x \leq t, \ \forall x \in$ X, isto é, t é uma outra cota superior para X. Logo $t \in$U(X) e

$$u_0 \leq t \tag{2}$$

pois u_0 é ínfimo de U(X).

Portanto, em (1) tem-se que u_0 é uma cota superior para X e em (2) tem-se que u_0 é a menor das cotas superiores de X, então pela definição A.11.1, $u_0 = \sup X$. Conclui-se então que X tem supremo e ínfimo o que implica que R é um reticulado completo. A prova para a existência de ínfimo na hipótese de que todo subconjunto tem supremo é feita de forma dual. ■

O teorema a seguir mostra como se obter um reticulado completo a partir de um conjunto ordenado consistentemente completo.

Teorema A.11.7 Seja R um conjunto ordenado consistentemente completo. Se se ajuntar a R um menor elemento $\perp$ e um maior elemento $\top$, então $R \cup \{\perp\} \cup \{\top\}$ é um reticulado completo.

Demonstração. Seja $X \subseteq R$. Se X é limitado então X tem supremo e ínfimo pelo fato de R ser consistentemente completo. Se X não é limitado, seja $X' = X \cup \{\perp\}$. Então $X' \subseteq R \cup \{\perp\} \cup \{\top\}$ e X' tem ínfimo, portanto usando o teorema A.11.6, X' também tem supremo e então $R \cup \{\perp\} \cup \{\top\}$ é um reticulado completo. Se $X = \emptyset$, então $\inf \emptyset = \top$ e pelo teorema A.11.6 também existe $\sup \emptyset = \perp$, o que torna $R \cup \{\perp\} \cup \{\top\}$ um reticulado completo. ■

Exemplo A.11.8 $\mathbb{R}$ é consistentemente completo. Ajuntando-se a $\mathbb{R}$ os conjuntos $\{-\infty\}$ e $\{+\infty\}$ tem-se o conjunto dos reais estendidos, que é um reticulado completo.

Seja $\langle R, \leq \rangle$ um reticulado e $X \subseteq R$. Portanto $\langle X, \leq \rangle$ é um conjunto ordenado com a ordem induzida de R; dados $x, y \in X$, $x \leq y$ em X se e só se $x \leq y$ em R. $\langle X, \leq \rangle$ também pode ser um reticulado.

Definição A.11.9 Seja $\langle R, \leq \rangle$ um conjunto ordenado e X um subconjunto de R.

(a) Se $\langle X, \leq \rangle$ é um reticulado, então X é chamado um *semireticulado*.

(b) Se $\forall a, b \in X$, $x \wedge_R y = x \wedge_X y$, então X é um *inf-semireticulado*.

(c) Se $\forall a, b \in X$, $x \vee_R y = x \vee_X y$, então X é um *sup-semireticulado*.

(d) Se $\forall a, b \in X$, $x \wedge_R y = x \wedge_X y$ e $x \vee_R y = x \vee_X y$, então X é um *subreticulado*.

Definição A.11.10 Seja $\langle R, \leq \rangle$ um reticulado completo e X um subconjunto de R.

(a) Se $\langle X, \leq \rangle$ também é um reticulado completo, então X é chamado um *semireticulado completo*.

(b) Se $\forall A \subseteq X$, $\bigwedge_R A = \bigwedge_X A$, então X é um *inf-semireticulado completo*.

(c) Se $\forall A \subseteq X$, $\bigvee_R A = \bigvee_X A$, então X é um *sup-semireticulado completo*.

(d) Se $\forall A \subseteq X$, $\bigwedge_R A = \bigwedge_X A$ e $\bigvee_R A = \bigvee_X A$, então X é um *subreticulado completo*.

Teorema A.11.11 Seja R um reticulado completo e $X \subseteq R$.

(a) X é um inf-semireticulado completo se e só se para todo $A \subseteq X$, $\bigwedge_R A \in X$.

(b) X é um sup-semireticulado completo se e só se para todo A$\subseteq$X, $\bigvee_{\mathrm{R}}$ A $\in$ X.

(c) X é um subreticulado completo se e só se para todo A$\subseteq$X, $\bigwedge_{\mathrm{R}}$ A $\in$ X e $\bigvee_{\mathrm{R}}$ A $\in$ X.

Demonstração.

(a) ($\Rightarrow$) Por hipótese (definição A.11.10 (b)),

$$\text{para todo A} \subseteq \text{X}, \bigwedge_{\mathrm{R}} \mathrm{A} = \bigwedge_{\mathrm{X}} \mathrm{A}$$

Mas $\bigwedge_{\mathrm{X}}$ A $\in$ X $\Rightarrow$ $\bigwedge_{\mathrm{R}}$ A $\in$ X.
($\Leftarrow$). Seja A$\subseteq$X e I=$\bigwedge_{\mathrm{R}}$ A. Portanto tem-se que para todo a $\in$A, I$\leq$ a. Então I é uma cota inferior para A e I$\in$X pois, por hipótese, $\bigwedge_{\mathrm{R}}$ A $\in$ X. Também,

$$\text{para todo } a \in \mathrm{A},\ x \leq a \Rightarrow x \leq \mathrm{I}, \text{ para todo } x \in \mathrm{X}.$$

Então I é a maior das cotas inferiores para A em X, logo, I=$\bigwedge_{\mathrm{X}}$ A e portanto

$$\forall \mathrm{A} \subseteq \mathrm{X}, \bigwedge_{\mathrm{R}} \mathrm{A} = \bigwedge_{\mathrm{X}} \mathrm{A}$$

Então X é um semi-reticulado completo.

(b) A prova é similar a de (a).

(c) Consequência de (a) e (b). ∎

Apêndice B

Aritmética Intervalar para Matrizes e Complexos

Neste apêndice é definida a artimética de exatidão máxima para para matrizes e complexos.

B.1 Matrizes Intervalares

Seja $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq \rangle$ um anelóide completamente ordenado (ou fracamente ordenado) e $\langle \mathrm{M}_n\mathrm{R}, +, \cdot, O, E, \leq \rangle$ o anelóide ordenado (fracamente ordenado) das matrizes sobre R, onde

$$O = \begin{pmatrix} \mathbb{0} & \mathbb{0} & \dots & \mathbb{0} \\ \mathbb{0} & \mathbb{0} & \dots & \mathbb{0} \\ \dots & \dots & \dots & \dots \\ \mathbb{0} & \mathbb{0} & \dots & \mathbb{0} \end{pmatrix}, E = \begin{pmatrix} \mathbb{1} & \mathbb{0} & \dots & \mathbb{0} \\ \mathbb{0} & \mathbb{1} & \dots & \mathbb{0} \\ \dots & \dots & \dots & \dots \\ \mathbb{0} & \mathbb{0} & \dots & \mathbb{1} \end{pmatrix}$$

Observações. Lembrando que,

(a) $\mathrm{M}_n\mathrm{R}$ significa matrizes quadradas sobre R.

(b) Se $\langle \mathrm{R}, \leq \rangle$ é um conjunto ordenado, $\mathrm{A} = (a_{ij})$, $\mathrm{B} = (b_{ij})$, uma relação de ordem, $\leq$, é definida em $\mathrm{M}_n\mathrm{R}$ por:

$\mathrm{A} \leq \mathrm{B} \Leftrightarrow a_{ij} \leq b_{ij},\ \forall i, j = 1, \dots, n.$

$\langle \mathrm{PM}_n\mathrm{R}, +, \cdot, \subseteq \rangle$ é um anelóide [KM79, KM81]. Seja $\mathrm{IM}_n\mathrm{R}$ o conjunto de todos os intervalos cujos limites, inferior e superior, são elementos de $\mathrm{M}_n\mathrm{R}$.

Exemplo B.1.1 $\mathrm{IM}_3\mathrm{I\!R}$ é o espaço de todos os intervalos cujos limites são matrizes de reais de dimensão 3; dado $\mathrm{A} \in \mathrm{IM}_3\mathrm{I\!R}$, A é da forma

$$\mathrm{A} = \left[\begin{pmatrix} a_{11}^{(1)} & a_{12}^{(1)} & a_{13}^{(1)} \\ a_{21}^{(1)} & a_{22}^{(1)} & a_{23}^{(1)} \\ a_{31}^{(1)} & a_{32}^{(1)} & a_{33}^{(1)} \end{pmatrix}, \begin{pmatrix} a_{11}^{(2)} & a_{12}^{(2)} & a_{13}^{(2)} \\ a_{21}^{(2)} & a_{22}^{(2)} & a_{23}^{(2)} \\ a_{31}^{(2)} & a_{32}^{(2)} & a_{33}^{(2)} \end{pmatrix} \right]$$

onde a_{ij} e b_{ij} são reais tais que $a_{ij}^{(1)} \leq a_{ij}^{(2)}$ para todo $i, j = 1, 2, 3$.

Seja $\overline{\mathrm{IM}_n\mathrm{R}} = \mathrm{IM}_n\mathrm{R} \cup \{\emptyset\}$.
Usando o teorema 3.3.5, $\langle \overline{\mathrm{IM}_n\mathrm{R}}, \subseteq \rangle$ é um *screen* simétrico superior de $\langle \mathrm{PM}_n\mathrm{R}, \subseteq \rangle$ e o arredondamento monótono direcionado para cima $\square : \mathrm{PM}_n\mathrm{R} \rightarrow \overline{\mathrm{IM}_n\mathrm{R}}$ é anti-simétrico. Propõe-se então o semimorfismo descrito a seguir.
Seja o arredondamento

$$\square : \mathrm{PM}_n\mathrm{R} \rightarrow \overline{\mathrm{IM}_n\mathrm{R}}$$

e para cada operação $* \in \{+, \cdot\}$ em $\mathrm{PM}_n\mathrm{R}$, tem-se $\boxast$, em $\mathrm{IM}_n\mathrm{R}$ tal que para todo A,B $\in \mathrm{PM}_n\mathrm{R}$,

(RG) $\quad \mathrm{A} \boxast \mathrm{B} = \square(\mathrm{A} * \mathrm{B}) = [\inf(\mathrm{A} * \mathrm{B}), \sup(\mathrm{A} * \mathrm{B})]$

onde $\square$ satisfaz

(R1) $\quad \square\mathrm{A} = \mathrm{A},\ \forall \mathrm{A} \in \overline{\mathrm{IM}_n\mathrm{R}}$
(R2) $\quad \mathrm{A} \subseteq \mathrm{B} \Rightarrow \square\mathrm{A} \subseteq \square\mathrm{B},\ \forall \mathrm{A},\mathrm{B} \in \mathrm{PM}_n\mathrm{R}$
(R3) $\quad \mathrm{A} \subseteq \square\mathrm{A},\ \forall \mathrm{A} \in \mathrm{PM}_n\mathrm{R}$
(R4) $\quad \square(-\mathrm{A}) = -\square\mathrm{A},\ \forall \mathrm{A} \in \mathrm{PM}_n\mathrm{R}$

Então pelo teorema 3.3.6, $\langle \mathrm{IM}_n\mathrm{R}, \boxplus, \boxdot, [O,O], [E,E], \leq, \subseteq \rangle$, com respeito à ordem $\leq$, é um anelóide completamente (fracamente) ordenado.

A questão agora é como definir explicitamente as operações aritméticas em $\mathrm{IM}_n\mathrm{R}$. Ainda pelo teorema 3.3.6, o resultado das operações aritméticas sempre é expresso em termos dos limites dos intervalos; no caso da adição ou subtração não há necessidade de se comparar operandos; com respeito à multiplicação e divisão, é imprescindível comparar operandos com $[O,O]$. Este problema é resolvido a seguir.

Seja $\mathrm{M}_n\mathrm{IR}$ o conjunto de todas as matrizes quadradas cujos elementos são intervalos sobre R.

Exemplo B.1.2 Supondo $\mathrm{M}_3\mathrm{IIR}$ e $\mathrm{A} \in \mathrm{M}_3\mathrm{IIR}$, então

$$\mathrm{A} = \begin{pmatrix} [a_{11}^{(1)}, a_{11}^{(2)}] & [a_{12}^{(1)}, a_{12}^{(2)}] & [a_{13}^{(1)}, a_{13}^{(2)}] \\ [a_{21}^{(1)}, a_{21}^{(2)}] & [a_{22}^{(1)}, a_{22}^{(2)}] & [a_{23}^{(1)}, a_{23}^{(2)}] \\ [a_{31}^{(1)}, a_{31}^{(2)}] & [a_{32}^{(1)}, a_{32}^{(2)}] & [a_{33}^{(1)}, a_{33}^{(2)}] \end{pmatrix}$$

onde $a_{ij}^{(1)}$ e $a_{ij}^{(2)}$ são números reais tais que para todo $i, j = 1, 2, 3$, $a_{ij}^{(1)} \leq a_{ij}^{(2)}$.

Define-se uma relação de ordem, $\leq$, e operações aritméticas de adição e multiplicação respectivamente por $+$ e $\cdot$ em $\mathrm{M}_n\mathrm{IR}$, através da relação de ordem e das operações aritméticas em IR, da seguinte forma:
Sejam $\mathrm{A}=(\mathrm{A}_{ij})$ e $\mathrm{B}=(\mathrm{B}_{ij}) \in \mathrm{M}_n\mathrm{IR}$

$$(\mathrm{A}_{ij}) \leq (\mathrm{B}_{ij}) \Leftrightarrow \mathrm{A}_{ij} \leq \mathrm{B}_{ij}, \forall i, j = 1, \ldots, n \qquad (1)$$

$$\mathrm{A} + \mathrm{B} = (\mathrm{A}_{ij} \boxplus \mathrm{B}_{ij}) \qquad (2)$$

$$\mathrm{A} \cdot \mathrm{B} = (\sum_{k=1}^{n} (\mathrm{A}_{ik} \boxdot \mathrm{B}_{kj})) \tag{3}$$

A_{ij} e B_{ij} são elementos de IR. Então em (1), no primeiro membro $\leq$ significa uma relação de ordem definida em M_nIR a partir da relação de ordem $\leq$ do segundo membro que é definida em IR. De forma similar, $+$ e $\cdot$ são operações aritméticas que estão sendo definidas em M_nIR a partir das operações $\boxplus$ e $\boxdot$ em IR. O símbolo $\sum$ representa uma soma em IR.

Exemplo B.1.3 Sejam

$$\mathrm{A} = \begin{pmatrix} [2,9] & [4,10] \\ [3,5] & [1,7] \end{pmatrix}, \mathrm{B} = \begin{pmatrix} [0,4] & [2,4] \\ [8,10] & [2,6] \end{pmatrix}$$

$$\mathrm{A} + \mathrm{B} = \begin{pmatrix} [2,9] & [4,10] \\ [3,5] & [1,7] \end{pmatrix} + \begin{pmatrix} [0,4] & [2,4] \\ [8,10] & [2,6] \end{pmatrix}$$

$$\mathrm{A} + \mathrm{B} = \begin{pmatrix} [2,9] \boxplus [0,4] & [4,10] \boxplus [2,4] \\ [3,5] \boxplus [8,10] & [1,7] \boxplus [2,6] \end{pmatrix}$$

$$\mathrm{A} + \mathrm{B} = \begin{pmatrix} [2,13] & [6,14] \\ [11,15] & [3,13] \end{pmatrix}$$

$$\mathrm{A} \cdot \mathrm{B} = \begin{pmatrix} [2,9] & [4,10] \\ [3,5] & [1,7] \end{pmatrix} \cdot \begin{pmatrix} [0,4] & [2,4] \\ [8,10] & [2,6] \end{pmatrix}$$

$$\mathrm{A} \cdot \mathrm{B} = \begin{pmatrix} [2,9] \boxdot [0,4] \boxplus [4,10] \boxdot [8,10] & [2,9] \boxdot [2,4] \boxplus [4,10] \boxdot [2,6] \\ [3,5] \boxdot [0,4] \boxplus [1,7] \boxdot [8,10] & [3,5] \boxdot [2,4] \boxplus [1,7] \boxdot [2,6] \end{pmatrix}$$

$$\mathrm{A} \cdot \mathrm{B} = \begin{pmatrix} [32,136] & [12,96] \\ [8,90] & [8,62] \end{pmatrix}$$

$$\begin{array}{lcrcrclclcccc} A \leq B & \Leftrightarrow & [2,9] & \leq & [0,4] & \Leftrightarrow & 2 & \leq & 0 & \text{e} & 9 & \leq & 4 & (F) \\ & & & \text{e} & & & & & & & & & \\ & & [4,10] & \leq & [2,4] & \Leftrightarrow & 4 & \leq & 2 & \text{e} & 10 & \leq & 4 & (F) \\ & & & \text{e} & & & & & & & & & \\ & & [3,5] & \leq & [8,10] & \Leftrightarrow & 3 & \leq & 8 & \text{e} & 5 & \leq & 10 & (V) \\ & & & \text{e} & & & & & & & & & \\ & & [1,7] & \leq & [2,6] & \Leftrightarrow & 1 & \leq & 2 & \text{e} & 7 & \leq & 6 & (F) \end{array}$$

Portanto não é verdade que A $\leq$ B.

Observação. É conveniente enfatizar que se A$\in$ M_nIR, A=$([a_{ij}^{(1)}, a_{ij}^{(2)}])$ e se A$\in$ IM_nR, então A=$[(a_{ij}^{(1)}), (a_{ij}^{(2)})]$.

Lema B.1.4 Seja $f : \mathrm{M}_n\mathrm{IR} \rightarrow \mathrm{IM}_n\mathrm{R}$
tal que $\forall$A $\in$ M_nIR,

$$f(\mathrm{A}) = f([a_{ij}^{(1)}, a_{ij}^{(2)}]) = [(a_{ij}^{(1)}), (a_{ij}^{(2)})].$$

Seja $\langle \mathrm{R}, +, \cdot, \leq\rangle$ um anelóide completamente e fracamente ordenado e o semimorfismo definido pelo arredondamento monótono direcionado para cima $\square : \mathrm{PR} \rightarrow \overline{\mathrm{IR}}$. Se

$$\sum_{k=1}^{n} \mathrm{A}_k \boxdot \mathrm{B}_k \subseteq \square(\sum_{k=1}^{n}(\mathrm{A}_k \cdot \mathrm{B}_k)),\ \forall \mathrm{A}_k, \mathrm{B}_k \in \mathrm{IR} \tag{4}$$

então f estabelece um isomorfismo entre os anelóides completamente e fracamente ordenados $\langle \mathrm{M}_n\mathrm{IR}, +, \cdot, \leq\rangle$ e $\langle \mathrm{IM}_n\mathrm{R}, \boxplus, \boxdot, \leq\rangle$, com respeito às operações algébricas e a relação de ordem.

Com respeito às operações aritméticas, este lema mostra que

$$f(\mathrm{A}) \boxplus f(\mathrm{B}) = f(\mathrm{A}+\mathrm{B})$$

e

$$f(\mathrm{A} \cdot \mathrm{B}) \subseteq f(\mathrm{A}) \boxdot f(\mathrm{B}).$$

O lema B.1.4 é válido sob a hipótese de (4) ser verdadeira. O lema a seguir mostra quando (4) é verdadeira.

Lema B.1.5 Seja $\langle \mathrm{R}, +, \cdot, \leq\rangle$ um anelóide completamente e totalmente ordenado e $\square : \mathrm{PR} \rightarrow \overline{\mathrm{IR}}$ o arredondamento monótono direcionado para cima. Então

$$\textstyle\sum_{k=1}^{n}(\mathrm{A}_k \boxdot \mathrm{B}_k) \subseteq \square(\sum_{k=1}^{n}(\mathrm{A}_k \cdot \mathrm{B}_k)),\ \forall \mathrm{A}_k, \mathrm{B}_k \in \mathrm{IR}.$$

Portanto dos lemas B.1.4 e B.1.5 e conclui-se que em um anelóide completamente e totalmente ordenado a função $f : \mathrm{M}_n\mathrm{IR} \rightarrow \mathrm{IM}_n\mathrm{R}$ estabelece um isomorfismo entre os anelóides completamente ordenados $\mathrm{M}_n\mathrm{IR}$ e $\mathrm{IM}_n\mathrm{R}$ com respeito às estruturas algébricas e de ordem. Isto significa que correspondentes elementos de $\langle \mathrm{M}_n\mathrm{IR}, +, \cdot, \leq\rangle$ e $\langle \mathrm{IM}_n\mathrm{R}, \boxplus, \boxdot, \leq\rangle$ podem ser identificados.

Qual o objetivo da definição da função f bem como do relacionamento entre os espaços $\langle \mathrm{M}_n\mathrm{IR}, +, \cdot, \leq\rangle$ e $\langle \mathrm{IM}_n\mathrm{R}, \boxplus, \boxdot, \leq\rangle$ através da função f? Se $\langle \mathrm{R}, +, \cdot, \leq\rangle$ é um anelóide totalmente ordenado então foram definidas fórmulas facilmente implementáveis para o anelóide $\langle \mathrm{IR}, \boxplus, \boxdot, [\mathbb{0},\mathbb{0}], [\mathbb{1},\mathbb{1}]\ \leq\rangle$. As operações $+$ e $\cdot$ para $\mathrm{M}_n\mathrm{IR}$, definidas em (2) e (3), são também, facilmente implementáveis. Porém como realizar a operação $\boxdot$ definida em $\mathrm{IM}_n\mathrm{R}$? As operações em $\mathrm{M}_n\mathrm{IR}$ são definidas a partir das em IR (que é uma forma vertical de definir uma operação), enquanto que as operações em $\mathrm{IM}_n\mathrm{R}$ são definidas por meio do semimorfismo $\square : \mathrm{PM}_n\mathrm{R} \rightarrow \overline{\mathrm{IM}_n\mathrm{R}}$ (definição horizontal da aritmética). O isomorfismo mostra que, nesse caso, ambos os métodos levam ao mesmo resultado.

B.2 Matrizes Intervalares em um Screen

Nesta seção é estudada a forma de realizar em computadores as operações aritméticas definidas em $\mathrm{IM}_n\mathrm{R}$.

Teorema B.2.1 Seja $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq\rangle$ um anelóide completamente e totalmente ordenado e $\langle \mathrm{S}, \leq\rangle$ um *screen* simétrico de $\langle \mathrm{R}, +, \cdot, \mathbb{0}, \mathbb{1}, \leq\rangle$. Seja o anelóide completamente ordenado $\langle \mathrm{M}_n\mathrm{R}, +, \cdot, O, E, \leq\rangle$ e os semimorfismos $\square : \mathrm{PM}_n\mathrm{R} \rightarrow \overline{\mathrm{IM}_n\mathrm{R}}$ e $\diamond : \overline{\mathrm{IM}_n\mathrm{R}} \rightarrow \overline{\mathrm{IM}_n\mathrm{S}}$. Então:

(a) Com respeito à $\subseteq$, $\mathrm{IM}_n\mathrm{S}$ é um anelóide *screen* superior monótono inclusamente ordenado de $\mathrm{IM}_n\mathrm{R}$;

(b) Com respeito a $\leq$, $\langle \mathrm{IM}_n\mathrm{S}, \diamondplus, \diamondcdot, \leq, \subseteq \rangle$ é um anelóide completamente ordenado. Os elementos neutros são $[O,O]$ e $[E,E]$.

Pelo teorema B.2.1, a forma de se olhar para $\mathrm{IM}_n\mathrm{R}$ é através de $\mathrm{IM}_n\mathrm{S}$, o conjunto de todos os intervalos cujos limites são matrizes com elementos em S. Porém, as operações em $\mathrm{IM}_n\mathrm{S}$ não são executáveis em computadores, portanto para que estas operações sejam expressas através de fórmulas computacionalmente executáveis será considerado o isomorfismo entre os anelóides $\langle \mathrm{M}_n\mathrm{IR}, +, \cdot, \leq \rangle$ e $\langle \mathrm{IM}_n\mathrm{R}, \boxplus, \boxdot, \leq \rangle$ como uma forma de reduzir as operações em $\mathrm{IM}_n\mathrm{S}$ às de $\mathrm{M}_n\mathrm{IR}$. Isto é visto a seguir.
Seja o isomorfismo definido a seguir,

$$f : \mathrm{M}_n\mathrm{IR} \to \mathrm{IM}_n\mathrm{R}$$

$$\forall \mathrm{A},\mathrm{B} \in \mathrm{M}_n\mathrm{IR},\ f\mathrm{A} \boxast f\mathrm{B} = f\,(\mathrm{A} * \mathrm{B}),\ \ * \in \{+, \cdot\} \tag{5}$$

Seja também $\Diamond : \overline{\mathrm{IR}} \to \overline{\mathrm{IS}}$. Utilizando o teorema 3.3.13, tem-se,

$$\Diamond : \mathrm{M}_n\mathrm{IR} \to \mathrm{M}_n\mathrm{IS}$$

$$\Diamond \mathrm{A} = (\Diamond \mathrm{A}_{ij}),\ \ \forall \mathrm{A} = (\mathrm{A}_{ij}) \in \mathrm{M}_n\mathrm{IR}$$

e as operações aritméticas em $\mathrm{M}_n\mathrm{IS}$ por meio deste arredondamento,

$$\mathrm{A} \diamondast \mathrm{B} = \Diamond(\mathrm{A} * \mathrm{B}),\ \ \forall \mathrm{A},\mathrm{B} \in \mathrm{M}_n\mathrm{IS},\ \ * \in \{+, \cdot\} \tag{6}$$

Considerando que $\mathrm{S} \subset \mathrm{R}$, $\mathrm{M}_n\mathrm{IR}$ e $\mathrm{IM}_n\mathrm{R}$ são isomorfos, $\mathrm{M}_n\mathrm{IS} \subset \mathrm{M}_n\mathrm{IR}$ e $\mathrm{IM}_n\mathrm{S} \subset \mathrm{IM}_n\mathrm{R}$ e que em (6) foi definido como operar elementos de $\mathrm{M}_n\mathrm{IS}$, é fácil ver que f também representa um isomorfismo entre os anelóides $\langle \mathrm{M}_n\mathrm{IS}, \diamondplus, \diamondcdot, \leq, \subseteq \rangle$ e $\langle \mathrm{IM}_n\mathrm{S}, \diamondplus, \diamondcdot, \leq, \subseteq \rangle$, isto é,

$$f : \mathrm{M}_n\mathrm{IS} \subset \mathrm{M}_n\mathrm{IR} \to \mathrm{IM}_n\mathrm{S} \subset \mathrm{IM}_n\mathrm{R}$$

onde a igualdade (5) também pode ser expressa como

$$f(\mathrm{A}) \diamondast f(\mathrm{B}) = f(\mathrm{A} \diamondast \mathrm{B}). \tag{7}$$

O isomorfismo (7) reduz as operações em $\mathrm{IM}_n\mathrm{S}$, que não são executáveis em um computador, às operações em $\mathrm{M}_n\mathrm{IS}$, que são executáveis, e que têm as seguintes propriedades,

$$\mathrm{A} \diamondplus \mathrm{B} = (\Diamond(\mathrm{A}_{ij} \boxplus \mathrm{B}_{ij})) = (\mathrm{A}_{ij} \diamondplus \mathrm{B}_{ij})$$

$$\mathrm{A} \diamondcdot\ \mathrm{B} = (\Diamond \sum_{k=1}^{n} (\mathrm{A}_{ik} \boxdot\ \mathrm{B}_{kj}))$$

A adição, componente a componente, pode ser realizada por meio da adição em IS e a multiplicação, por meio das regras de multiplicação e o produto escalar.

B.3 Aritmética Intervalar Complexa

Seja $\langle \mathrm{R}, \mathrm{N}, +, \cdot, /, \mathbb{0}, \mathbb{1}, \leq \rangle$, onde N é qualquer subconjunto de R que contém $\mathbb{0}$, um anelóide divisão completamente e totalmente ordenado e

$$\mathrm{CR} = \{(x, y) \mid x, y \in \mathrm{R}\}$$

Kulisch e Miranker [KM79, KM81] mostram que definindo a igualdade, =, relação de ordem, $\leq$, e as operações aritméticas $* \in \{+, \cdot, /\}$ de forma usual, $\langle \mathrm{CR}, \overline{\mathrm{N}}, +, \cdot, /, \leq \rangle$ com $\overline{\mathrm{N}} = \{\gamma \in \mathrm{CR} \mid \gamma = (c_1, c_2), c_1c_1 + c_2c_2 \in \mathrm{N}\}$ é um anelóide divisão completamente e fracamente ordenado com elementos $[\mathbb{0}, \mathbb{0}]$ e $[\mathbb{1}, \mathbb{1}]$ e que $\langle \mathrm{PCR}, \tilde{\mathrm{N}}, +, \cdot, / \rangle$ com $\tilde{\mathrm{N}} = \{\Phi \in \mathrm{PCR} \mid \Phi \cap \overline{\mathrm{N}} \neq \emptyset\}$ também é um anelóide divisão.
Seja ICR o conjunto de todos os intervalos sobre CR da forma

$$\Phi = [\varphi_1, \varphi_2] = \{\varphi \in \mathrm{CR} \mid \varphi_1, \varphi_2 \in \mathrm{CR},\ \varphi_1 \leq \varphi \leq \varphi_2\}$$

Exemplo B.3.1 Seja R=$\mathbb{R}$, CR=$\mathbb{C}$ e $\mathbb{IC}\mathbb{R}$. Então $\Phi = [1 + 5i, 2 + 6i]$ é um elemento de $\mathbb{IC}\mathbb{R}$.

Seja $\overline{\mathrm{ICR}} = \mathrm{ICR} \cup \{\emptyset\}$. Usando os teoremas 3.3.3 e 3.3.5, tem-se que $\langle \overline{\mathrm{ICR}}, \subseteq \rangle$ é um *screen* simétrico superior de $\langle \mathrm{PCR}, \subseteq \rangle$ e o arredondamento monótono direcionado para cima, $\square : \mathrm{PCR} \to \overline{\mathrm{ICR}}$ é anti-simétrico. Define-se então o seguinte semimorfismo.

Seja o arredondamento

$$\square : \mathrm{PCR} \to \overline{\mathrm{ICR}}$$

e para operação $* \in \{+, \cdot, /\}$ em PCR, tem-se $\boxed{*}$ em ICR tal que para todo $\Phi, \Psi \in \mathrm{ICR}$,

(**RG**) $\quad \Phi \boxed{*} \Psi = \square(\Phi * \Psi) = \square\{\varphi * \psi \mid \varphi \in \Phi \text{ e } \psi \in \Psi\}$

onde, quando $* = /$, tem-se que $\Psi \cap \tilde{\mathrm{N}} = \emptyset$.
$\square$ satisfaz,

(**R1**) $\quad \square \mathrm{A} = \mathrm{A}, \forall \mathrm{A} \in \mathrm{ICR}$
(**R2**) $\quad \mathrm{A} \subseteq \mathrm{B} \Rightarrow \square \mathrm{A} \subseteq \square \mathrm{B},\ \forall \mathrm{A}, \mathrm{B} \in \mathrm{ICR}$
(**R3**) $\quad \mathrm{A} \subseteq \square \mathrm{A},\ \forall \mathrm{A} \in \mathrm{ICR}$
(**R4**) $\quad \square(-\mathrm{A}) = -\square \mathrm{A}$

Sejam $\Phi = [\varphi_1, \varphi_2]$ e $\Psi = [\psi_1, \psi_2]$ elementos de ICR. Definindo uma relação de ordem em ICR por

$$\Phi \leq \Psi \Leftrightarrow \varphi_1 \leq \psi_1 \text{ e } \varphi_2 \leq \psi_2.$$

Então pelo teorema 3.3.6, $\langle \mathrm{ICR}, \mathrm{N}^*, \boxplus, \boxdot, \boxslash, \leq, \subseteq \rangle$ com $\mathrm{N}^* = \{\Phi \in \mathrm{ICR} \mid \Phi \cap \tilde{\mathrm{N}} = \emptyset\}$, é um anelóide divisão completamente e fracamente ordenado com respeito à $\leq$.

A questão agora é como definir explicitamente as operações aritméticas em ICR. Estas operações são definidas através de operações em PCR e portanto não são executáveis na prática. Para se obter fórmulas executáveis é imprescindível estudar a conexão entre as operações em ICR e um outro conjunto a este relacionado.

Seja

$$\mathrm{CIR} = \{(\mathrm{X},\mathrm{Y}) \mid \mathrm{X},\mathrm{Y} \in \mathrm{IR}\}$$

isto é, CIR é o conjunto de todos os complexos X+Yi onde X e Y são intervalos sobre R.

Exemplo B.3.2 Dados R=$\mathbb{R}$, CR=$\mathbb{C}$ e $\mathbb{C}$IR; então $\Phi = [2,3] + [5,9]i$ ou Φ=([2,3],[5,9]) é um elemento de $\mathbb{C}$IR.

Define-se uma igualdade, uma ordem e operações aritméticas em CIR através das respectivas relações definidas em IR da seguinte forma. Para todo $\Phi = (\mathrm{X}_1, \mathrm{X}_2)$ e $\Psi = (\mathrm{Y}_1, \mathrm{Y}_2)$ elementos de CIR tem-se que,

$$\Phi = \Psi \Leftrightarrow \mathrm{X}_1 = \mathrm{Y}_1 \text{ e } \mathrm{X}_2 = \mathrm{Y}_2$$

$$\Phi \leq \Psi \Leftrightarrow \mathrm{X}_1 \leq \mathrm{Y}_1 \text{ e } \mathrm{X}_2 \leq \mathrm{Y}_2$$

$$\Phi + \Psi = (\mathrm{X}_1 \boxplus \mathrm{Y}_1, \mathrm{X}_2 \boxplus \mathrm{Y}_2)$$

$$\Phi \cdot \Psi = (\mathrm{X}_1 \boxdot \mathrm{Y}_1 \boxminus \mathrm{X}_2 \boxdot \mathrm{Y}_2, \mathrm{X}_1 \boxdot \mathrm{Y}_2 \boxplus \mathrm{X}_2 \boxdot \mathrm{Y}_1)$$

$$\Phi/\Psi = ((\mathrm{X}_1 \boxdot \mathrm{Y}_1 \boxplus \mathrm{X}_2 \boxdot \mathrm{Y}_2) \boxslash (\mathrm{Y}_1 \boxdot \mathrm{Y}_1 \boxplus \mathrm{Y}_2 \boxdot \mathrm{Y}_2), (\mathrm{X}_2 \boxdot \mathrm{Y}_1 \boxminus \mathrm{X}_1 \boxdot \mathrm{Y}_2) \boxslash (\mathrm{Y}_1 \boxdot \mathrm{Y}_1 \boxplus \mathrm{Y}_2 \boxdot \mathrm{Y}_2)),$$

onde $\mathbb{O} \notin \mathrm{Y}_1, \mathbb{O} \notin \mathrm{Y}_2$.
Seja a função

$$g : \mathrm{CIR} \to \mathrm{ICR}$$

$$g([x_1, x_2], [y_1, y_2]) = [(x_1, y_1), (x_2, y_2)]$$

Por construção g é bijetiva, preserva a ordem e com respeito às operações aritméticas Kulisch e Miranker [KM79, KM81] mostram que

$$g(\Phi) \boxplus g(\Psi) = \mathrm{g}\ (\Phi + \Psi)$$

$$g(\Phi) \boxdot g(\Psi) = g\ (\Phi \cdot \Psi)$$

$$g(\Phi) \boxslash g(\Psi) \subseteq g\ (\Phi/\Psi)$$

Desde que os anelóides CIR e ICR são isomorfos, seus elementos correspondentes podem ser identificados. Este fato também possibilita definir uma relação de inclusão para os elementos $\Phi = (\mathrm{X}_1, \mathrm{X}_2), \Psi = (\mathrm{Y}_1, \mathrm{Y}_2) \in$ CIR da seguinte forma:

$$\Phi \subseteq \Psi \Leftrightarrow \mathrm{X}_1 \subseteq \mathrm{Y}_1 \text{ e } \mathrm{X}_2 \subseteq \mathrm{Y}_2.$$

B.4 Aritmética Intervalar Complexa em um Screen

Nesta seção é estudada a forma de realizar em computadores as operações aritméticas definidas em ICR.

Teorema B.4.1 Seja $\langle \mathrm{R}, +, \cdot, /, \mathbb{0}, \mathbb{1}, \leq \rangle$ um anelóide divisão completamente e totalmente ordenado e $\langle \mathrm{S}, \leq \rangle$ um *screen* simétrico de $\langle \mathrm{R}, +, \cdot, \leq \rangle$. Seja o anelóide divisão complexo $\langle \mathrm{CR}, +, \cdot, /, [\mathbb{0}, \mathbb{0}], [\mathbb{1}, \mathbb{0}], \leq \rangle$ e os semimorfismos $\Box : \mathrm{PCR} \to \overline{\mathrm{ICR}}$ e $\Diamond : \overline{\mathrm{ICR}} \to \overline{\mathrm{ICS}}$. Então:

(a) Com respeito à relação de ordem $\subseteq$, ICS é um anelóide divisão *screen* superior monótono inclusamente ordenado de ICR;

(b) Com respeito à $\leq$ tem-se que $\langle \mathrm{ICS}, \overline{\mathrm{N}}, \boxplus, \boxdot, \boxslash, [\mathbb{0}, \mathbb{0}], [\mathbb{1}, \mathbb{0}] \leq, \subseteq \rangle$, onde $\overline{N} = \{\mathrm{A} \in \mathrm{ICS} \mid (\mathbb{0}, \mathbb{0}) \in \mathrm{A}\}$, é um anelóide divisão completamente e fracamente ordenado.

As operações em ICS não são diretamente executáveis em um computador, portanto para que estas operações sejam expressas através de fórmulas computacionalmente executáveis será considerado o isomorfismo entre CIR e ICR. Este isomorfismo é definido por

$$g : \mathrm{CIR} \to \mathrm{ICR}$$

$$g(\Phi) \circledast g(\Psi) = \mathrm{g}(\Phi * \Psi), \ \forall \mathrm{A,B} \in \mathrm{CIR}, * \in \{+, \cdot\} \tag{8}$$

Seja o arredondamento

$$\Diamond : \mathrm{CIR} \to \mathrm{CIS}$$

$$\Diamond\Phi = (\Diamond \mathrm{X}_1, \Diamond \mathrm{X}_2), \ \forall \Phi = (\mathrm{X}_1, \mathrm{X}_2) \in \mathrm{CIR}$$

e as operações aritméticas definidas por meio deste arredondamento,

$$\Phi \circledast \Psi = \Diamond(\Phi * \Psi), \ \forall \Phi, \Psi \in \mathrm{CIS}, * \in \{+, \cdot\}$$

Considerando que S$\subset$R, CIR e ICR são isomorfos, CIS$\subset$CIR e ICS$\subset$ICR e que em (8) foi definido como operar elementos de CIS, é fácil ver que g também representa um isomorfismo entre os anelóides $\langle \mathrm{CIS}, \boxplus, \boxdot, \leq, \subseteq \rangle$ e $\langle \mathrm{ICS}, \boxplus, \boxdot, \leq, \subseteq \rangle$, isto é

$$g : \mathrm{CIS} \subset \mathrm{CIR} \to \mathrm{ICS} \subseteq \mathrm{ICR}$$

onde a igualdade (8) também pode ser expressa como

$$g(\Phi) \mathbin{\Diamond\!\!\!\!\!\ast\;} g(\Psi) = g(\Phi \mathbin{\Diamond\!\!\!\!\!\ast\;} \Psi) \tag{9}$$

O isomorfismo (9) reduz as operações em ICS (que não são executáveis em computadores) àquelas em CIS (que são executáveis em computadores) tal que:

$$\Phi \mathbin{\Diamond\!\!\!\!\!+\;} \Psi = (\mathrm{X}_1 \mathbin{\Diamond\!\!\!\!\!+\;} \mathrm{Y}_1, \mathrm{X}_2 \mathbin{\Diamond\!\!\!\!\!+\;} \mathrm{Y}_2)$$

$$\Phi \mathbin{\Diamond\!\!\!\!\!\cdot\;} \Psi = (\Diamond(\mathrm{X}_1 \boxdot \mathrm{Y}_1 \ , \boxminus \mathrm{X}_2 \boxdot \mathrm{X}_2), \Diamond(\mathrm{X}_1 \boxdot \mathrm{Y}_2 \boxplus \mathrm{X}_2 \boxdot \mathrm{Y}_1)).$$

A adição, componente a componente, pode ser realizada por meio da adição em IS e a multiplicação através do produto escalar.

Com respeito a matrizes e vetores intervalares complexos, bem como ao *screen* correspondente a cada um desses espaços, em linhas gerais o que é feito para a definição de uma aritmética de alta exatidão neles é conjugar os resultados vistos anteriormente.

Apêndice C

Números de Ponto Flutuante

Este apêndice refere-se à questão da representação dos números reais através de números de ponto flutuante. A seguir são mencionadas as principais características dos padrões para representação dos números de ponto flutuante, IEEE 754 e IEEE 854.

Todo número real x pode ser unicamente representado pela expansão b-ádica [KM79, KM81, Knu81]

$$x = *d_n d_{n-1} \ldots d_1 d_0 \cdot d_{-1} \ldots = * \sum_{i=n}^{-\infty} d_i b^i \tag{1}$$

onde,

$$* \in \{+, -\}, \;\; b \in \mathbb{N}, b > 1,$$
$$0 \leq d_i \leq b - 1, \;\; i = n(-1)(-\infty),$$
$$d_i \leq b - 2, \;\; \text{para uma quantidade infinita de índices } i.$$

Em (1) o ponto b-ádico pode ser mudado para qualquer posição desde que esta mudança seja convenientemente compensada. Se o ponto for mudado para a esquerda do primeiro dígito não nulo da expansão b-ádica do número x, através da multiplicação por uma correspondente potência de b, então tem-se o número x na forma *normalizada*. O número zero possui uma representação especial não normalizada.

A seguir uma explicação da necessidade da condição $d_i \leq b - 2$ para uma quantidade infinita de índices i.

$$0.3000 \cdots = 3 \cdot 10^{-1} + 0 \cdot 10^{-2} + \cdots = 3 \cdot 10^{-1} + \cdots + 0 \cdot 10^{-n} + \ldots$$
$$0.2999 \cdots = 2 \cdot 10^{-1} + 9 \cdot 10^{-2} + \cdots = 2 \cdot 10^{-1} + \cdots + 9 \cdot 10^{-n} + \ldots$$

Portanto as seqüências

$$s_{1_n} = 3 \cdot 10^{-1} + \cdots + 0 \cdot 10^{-n}$$
$$s_{2_n} = 2 \cdot 10^{-1} + \cdots + 9 \cdot 10^{-n}$$

são monótonas e limitadas. Então convergem, e convergem para 0.3. Como pode ser visto em s_{2_n}, $d_i \not\leq b - 2$ para uma quantidade infinita de índices i. Note que

$$s_{3_n} = 2 \cdot 10^{-1} + 8 \cdot 10^{-2} + \cdots + 8 \cdot 10^{-n}$$

converge para 0.29.

Seja R_b o conjunto de todos os x normalizados, mais o zero; em geral R_b não pode ser representado em computadores. Um subconjunto de R_b que é representável é definido a seguir.

Definição C.1 Um número real x é chamado um número de *ponto flutuante normalizado* [Ste74, Gol91, For77, KM81, Knu81] ou um número de *ponto flutuante* se

$$x = * \cdot d_1 d_2 \ldots d_l \cdot b^e \tag{2}$$

onde,

$$* \in \{+, -\},\ \ b \in \mathbb{N}, b > 1, \tag{3}$$

$$1 \leq d_1 \leq b - 1, \tag{4}$$

$$0 \leq d_i \leq b - 1,\ \ i = 2, \ldots, l \tag{5}$$

$$e_{min} \leq e \leq e_{max},\ \ e, e_{min}, e_{max} \quad \text{números inteiros.} \tag{6}$$

b é a *base* da representação, $*$ o sinal de x, $m = \cdot d_1 d_2 \ldots d_l$ é a *mantissa* e e é o *expoente*. A mantissa tem comprimento l. Representa-se o número zero unicamente por

$$0 = 0 \cdot 00 \ldots 0 \cdot b^{e_{min}}$$

$\mathrm{S}(b, l, e_{min}, e_{max})$ é um *sistema de ponto flutuante*, onde cada $x \in \mathrm{S}$, $x \neq 0$, satisfaz, (2),(3),(4),(5),(6). Uma característica de S é que,

$$0 \in \mathrm{S}$$

$$1 \in \mathrm{S}$$

$$x \in \mathrm{S} \Rightarrow -x \in \mathrm{S},\ \forall x \in \mathrm{S}$$

S é um conjunto finito. Tem exatamente $2(b-1)b^{l-1}(e_{max} - e_{min} + 1) + 1$ elementos, que só são igualmente espaçados entre sucessivas potências de b. Porque S é finito não há possibilidade de se representar o conjunto dos reais em detalhes. Como um modelo para $\mathbb{R}$, o conjunto S tem uma aritmética definida sobre ele. A questão é que esta aritmética não satisfaz propriedades básicas do ponto de vista da solução de problemas numéricos no conjunto dos reais. Supondo que x e y são números de ponto flutuante, então nem sempre $x + y$ ou $x \cdot y$ estão em S. A manipulação algébrica de fórmulas é baseada em algumas leis fundamentais que são válidas nos reais, mas não em S; [Knu81, Gol91, Ste74] mostram que, considerando as operações aritméticas de adição e multiplicação em S, respectivamente, $+$ e $\cdot$, são válidas (**T**) e não são válidas(**F**).

(**T**) $a + b = b + a,\ \forall a, b \in \mathrm{S}$
(**T**) $a \cdot b = b \cdot a,\ \forall a, b \in \mathrm{S}$
(**T**) $a + 0 = 0 + a = a,\ \forall a \in \mathrm{S}$
(**T**) $a \cdot 1 = 1 \cdot a = a,\ \forall a \in \mathrm{S}$
(**T**) $\forall a \in \mathrm{S},\ \exists(-a) \in \mathrm{S}$ tal que $a + (-a) = (-a) + a = 0$
(**F**) $(a + b) + c = a + (b + c),\ \forall a, b, c \in \mathrm{S}$
(**F**) $(a \cdot b) \cdot c = a \cdot (b \cdot c),\ \forall a, b, c \in \mathrm{S}$
(**F**) $a \cdot b = a \cdot c \Rightarrow b = c\ \forall a, b, c \in \mathrm{S},\ \ a \neq 0$
(**F**) $a \cdot (b + c) = (a \cdot b) + (a \cdot c),\ \forall a, b, c \in \mathrm{S}.$

C.1 Representação dos Números de Ponto Flutuante

Os primeiros computadores adotaram sistemas de representação de ponto flutuante com diferentes bases, tamanho da palavra, número de dígitos significativos, etc. Este fato ocasionava sérios problemas tais como dificuldade de raciocinar em torno de provas relacionadas com algoritmos que geravam números de ponto flutuante, porque os resultados aritméticos eram dependentes da máquina. Além disso, a ausência de um padrão que especificasse de modo detalhado as operações básicas e os formatos de dados acarretava a falta de portabilidade dos softwares.

O esforço para produzir um padrão para ponto flutuante originou o IEEE Standard for Binary Floating-Point Arithmetic [Cod88, Gol91, Ste81] e A Radix-Independent Standard for Floating-Point Arithmetic [Cod88].

Com respeito a ambos os padrões propostos tem-se que:

- IEEE 754: b=2; precisão simples ou dupla. A especificação do layout dos bits é de acordo com a precisão: Simples com 8 bits para o exponte, 23 para a mantissa e 1 bit para o sinal algébrico do número; Dupla com 11 bits para o exponte, 52 para a mantissa e 1 bit para o sinal algébrico do número.
- IEEE 854: b=2 ou b=10; não requer um valor particular para l; não especifica o *layout* dos bits.

Algumas características do padrão IEEE 754 são:

- *Base.* Desde que a mantissa sempre é normalizada e a base é 2, o bit mais significativo não precisa ser representado tendo-se o ganho de um bit (bit implícito).
- *Expoente.* É representado na forma polarizada; esta representação facilita comparações e evita o uso de um bit para o sinal antes dos expoentes.
- *Mantissa.* É representada na forma sinal/magnitude. 1 bit é reservado para o sinal e o restante para a magnitude do número.
- *Precisão.* São definidas as precisões simples, dupla, simples estendida e dupla estendida. Uma vantagem da precisão estendida, é a facilidade de dispor de mais dígitos no expoente e na mantissa.
- *Operações.* Além das aritméticas $(+, -, \cdot, /)$, estão incluídas: *remainder*, raiz quadrada, conversões entre os formatos de ponto flutuante, conversões entre formatos de ponto flutuantes e inteiros, conversão entre decimal e binário e comparações. Uma razão para especificar completamente os resultados das operações aritméticas é facilitar a portabilidade dos softwares. Uma vez que um algoritmo é provado como sendo correto em uma implementação do padrão IEEE, ele trabalhará corretamente em qualquer outra que também suporte o padrão. [KM86] sugerem que o produto interno seja uma operação precisamente especificada, através de semimorfismo, a ser incluída no padrão IEEE.
- *Quantidades Especiais.* O padrão IEEE especifica como valores especiais: ± 0, números *denormalized* e *unnormalized*, $\pm\infty$ e NaNs (não números) [Ste81, Cod88].

- *Exceções.* São exceções: overflow, underflow, divisão por zero, operação inválida e operação inexata. O tratamento das exceções pode ser realizado pelo hardware, de modo automático, ou pode ser gerado um *trap* para o sistema operacional que chama a rotina de software correspondente.

- *Arredondamentos.* Operações inexatas dão origem aos arredondamentos. O arredondamento *default* é para o número de máquina mais próximo, mas o padrão também requer que três outros arredondamentos sejam implementados: em direção ao 0, em direção a $+\infty$ (direcionado para cima) e em direção a $-\infty$ (direcionado para baixo).

Esses dois últimos arredondamentos e a representação de $\pm\infty$ viabilizam a implementação das operações aritméticas intervalares, ou mesmo a introdução do tipo de dado intervalo em algoritmos numéricos. Por exemplo, se a soma de dois números x e y vai gerar o intervalo $[z_1, z_2]$, z_1 é obtido arredondando-se $x + y$ em direção a $-\infty$ e z_2, em direção a $+\infty$. Kahan [Kah80] discute aspectos relacionados com aritmética intervalar de alguns padrões.