Álgebra booleana

Última revisão em 06 de abril de 2016

As funções lógicas podem ser formalizadas pela Álgebra Booleana. Como qualquer sistema álgebrico, a álgebra booleana considera um conjunto de elementos e operações definidas sobre esses elementos. O termo “booleana” é derivado do nome do matemático inglês George Boole (1815-1864), a quem é creditado a origem da álgebra booleana. A álgebra booleana é o resultado dos esforços de Boole para sistematizar o raciocínio lógico.

Neste documento veremos uma definição formal de álgebra booleana, que é baseada em um conjunto de axiomas (ou postulados). Veremos também algumas leis ou propriedades de álgebras booleanas e que todas essas leis podem ser derivadas algebricamente a partir dos postulados da definição. Vários exemplos de álgebras booleanas são listados. Dentre eles, merecem destaque a álgebra dos conjuntos e o cálculo proposicional.

Referências para esta parte do curso: [Hill and Peterson, 1981], [Garnier and Taylor, 1992], [Whitesitt, 1961] entre outros.

1 Definição axiomática de álgebra booleana

Seja uma sêxtupla $\langle A, +, \cdot, \bar{}, 0, 1\rangle$ na qual A é um conjunto, $+$ e $\cdot$ são operações binárias sobre A, $\bar{}$ é uma operação unária em A e 0 e 1 são dois elementos distintos em A. O sistema algébrico $\langle A, +, \cdot, \bar{}, 0, 1\rangle$ é uma **álgebra booleana** se os seguintes axiomas são satisfeitos:

A1. As operações $+$ e $\cdot$ são **comutativas**, ou seja, para todo x e y em A,

$$x + y = y + x \quad \text{e} \quad x \cdot y = y \cdot x$$

A2. Cada operação é **distributiva** sobre a outra, isto é, para todo x, y e z em A,

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad \text{e} \quad x + (y \cdot z) = (x + y) \cdot (x + z)$$

A3. Os elementos 0 e 1 são os **elementos identidades**, ou seja, para todo $x \in A$,

$$x + 0 = x \quad \text{e} \quad x \cdot 1 = x$$

A4. Todo elemento $x \in A$ possui um complemento, ou seja, existe um elemento $\overline{x}$ tal que

$$x + \overline{x} = 1 \quad \text{e} \quad x \cdot \overline{x} = 0\,.$$

Observação 1: Na literatura encontramos outras definições para álgebra booleana. Em geral, as definições incorporam um maior número de propriedades. Vale registrar que os postulados acima apresentados, elaborados por Huntington em 1904, correspondem a um conjunto minimal de postulados, isto é, nenhum deles pode ser derivado a partir dos demais. Mais ainda, é um conjunto completo no sentido de que qualquer outra propriedade de uma álgebra booleana pode ser derivada a partir desses postulados. Desta forma, qualquer sistema algébrico que satisfaz os 4 axiomas acima é uma álgebra Booleana. Mais adiante mostraremos como a propriedade associativa (frequentemente incorporada à definição de álgebra booleana) e várias outras podem ser derivadas a partir dos postulados acima.

Observação 2: Pode-se fazer um paralelo com a álgebra elementar dos números. Por exemplo, sobre o conjunto dos números reais, define-se as operações de adição, subtração, etc. Essas operações satisfazem alguma propriedades (por exemplo, a adição é comutativa). Enquanto na álgebra booleana temos a noção de complemento, na álgebra elementar temos a noção de oposto (em relação à adição) e de inverso (em relação à multiplicação).

2 Exemplos de álgebra booleana

Exemplo 1: O conjunto $B = \{0, 1\}$ para o qual definimos

$$\overline{1} = 0 \qquad \overline{0} = 1$$

$$1 \cdot 1 = 1 + 1 = 1 + 0 = 0 + 1 = 1$$

$$0 + 0 = 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$$

é uma álgebra booleana.

Os axiomas A1, A3 e A4 são satisfeitos por definição. Para verificar o axioma A2, dados três elementos quaisquer x, y e z em B, podemos construir uma tabela verdade para todas as possíveis combinações de valores para x, y e z. Vejamos, nas colunas indicadas com * na parte inferior da tabela, a validade da distributividade em relação a $\cdot$, ou seja, que $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

x	y	z	$(y+z)$	$x \cdot (y+z)$	$(x \cdot y)$	$(x \cdot z)$	$(x \cdot y) + (x \cdot z)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1
				*			*

Denotamos esta álgebra booleana por $\langle B, +, \cdot, ^-, 0, 1\rangle$. Esta é a álgebra que está por trás dos circuitos lógicos.

Exemplo 2: Dado um conjunto S, $\mathcal{P}(S)$ denota o conjunto das partes de S, isto é, $\mathcal{P}(S) = \{X : X \subseteq S\}$. Conforme já estamos familiarizados, as propriedades da álgebra de conjuntos equivalentes aos 4 postulados da definição de álgebra booleana são:

A1. $X \cup Y = Y \cup X \quad \text{e} \quad X \cap Y = Y \cap X$

A2. $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \quad \text{e} \quad X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

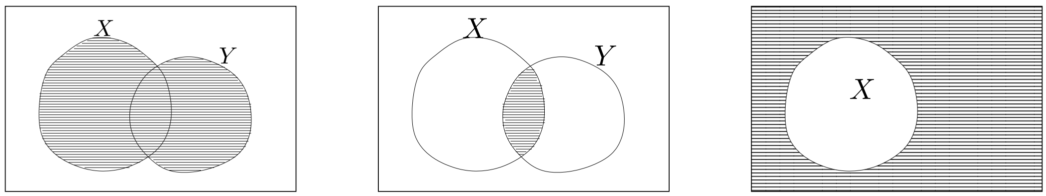
A3. $\emptyset \cup X = X \quad \text{e} \quad U \cap X = X$

A4. $X \cap X^c = \emptyset \quad \text{e} \quad X \cup X^c = U$

Então, $\langle \mathcal{P}(S), \cup, \cap, ^c, \emptyset, S\rangle$ é uma álgebra booleana. Dessas propriedades, a única que pode não ser trivial é a A2. Para se convencer da validade dessas proriedades, pode-se recorrer aos diagramas de Venn.

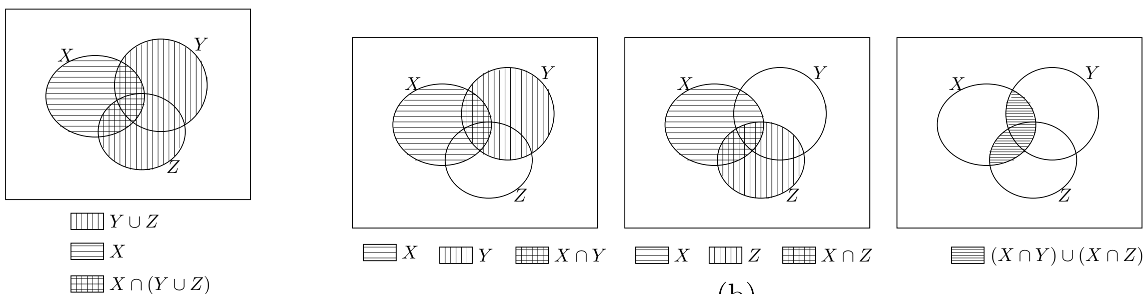
No diagrama de Venn o conjunto universo é representado por um retângulo, mais precisamente, pelos pontos interiores ao retângulo. Qualquer conjunto é desenhado como sendo uma curva fechada, inteiramente contida no retângulo. Pontos interiores à curva correspondem aos elementos do conjunto. No exemplo da figura 1, a união e interseção de dois conjuntos genéricos estão representadas pelas regiões hachuradas das figuras 1a e 1b, respectivamente. O complemento de um conjunto é representado no diagrama da figura 1c.

Como exemplo, vamos verificar a propriedade $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$. O conjunto $X \cap (Y \cup Z)$ corresponde à região hachurada pelas linhas verticais e pelas



(a) $X \cup Y$ (b) $X \cap Y$ (c) X^c

Figura 1: Diagramas de Venn (a) União de dois conjuntos. (b) Interseção de dois conjuntos. (c) Complemento de um conjunto.



(a) (b)

Figura 2: (a) $X \cap (Y \cup Z)$ e (b) $(X \cap Y) \cup (X \cap Z)$.

linhas horizontais na figura 2a. Esta coincide com a região hachurada no diagrama mais à direita da figura 2b, que representa o conjunto $(X \cap Y) \cup (X \cap Z)$.

Exemplo 3: O cálculo proposicional é um campo da lógica matemática que estuda proposições, ou seja, afirmações que ou são verdadeiras (V) ou são falsas (F), mas não ambas. As proposições podem ser conectadas usando-se os conectivos lógicos E, OU e NÃO, dando origem a novas proposições. Os conectivos lógicos podem ser representados pelos símbolos conforme tabela a seguir.

Conectivo	símbolo
E	$\wedge$
OU	$\vee$
NÃO	$\neg$

Supondo que x e y são duas proposições quaisquer, define-se essas operações conforme a tabela-verdade a seguir:

x	$\neg x$
F	V
V	F

x	y	$x \wedge y$
F	F	F
F	V	F
V	F	F
V	V	V

x	y	$x \vee y$
F	F	F
F	V	V
V	F	V
V	V	V

Qualquer semelhança com as operações lógicas vistas no contexto de circuitos lógicos não é mera coincidência. De fato, a lógica (ou cálculo) proposicional é uma álgebra booleana e ela tem uma correspondência um-para-um com $\langle B, +, \cdot, \bar{}, 0, 1\rangle$, visto acima, conforme apontado a seguir.

Lógica proposicional	álgebra booleana B
$\vee$	$+$
$\wedge$	$\cdot$
F	0
V	1
$\neg x$	$\overline{x}$

Como consequência, temos também a correspondência entre as tabelas-verdade das operações $\neg$, $\vee$, $\wedge$ com as tabelas-verdade das operações : $\bar{}$, $+$ e $\cdot$.

x	y	$\neg x$	$x \vee y$	$x \wedge y$
F	F	V	F	F
F	V	V	V	F
V	F	F	V	F
V	V	F	V	V

x	y	$\overline{x}$	$x + y$	$x \cdot y$
0	0	1	0	0
0	1	1	1	0
1	0	0	1	0
1	1	0	1	1

Exemplo 4: O conjunto $B^n = B \times B \times \ldots \times B$, com as operações $+$, $\cdot$ e $\bar{}$ herdadas de B e definidas, para quaisquer $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in B^n$, da seguinte forma

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

$$(x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) = (x_1 \cdot y_1, x_2 \cdot y_2, \ldots, x_n \cdot y_n)$$

$$\overline{(x_1, x_2, \ldots, x_n)} = (\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n)$$

é uma álgebra booleana. Verifique que de fato os 4 postulados são válidos.

3 Princípio da dualidade

Vimos que podemos escrever expressões envolvendo variáveis lógicas. Por exemplo, $a\,b\,c + a\,b\,\overline{c}$. Essa expressão pode ser manipulada algebricamente (por exemplo, $a\,b\,c + a\,b\,\overline{c} = a\,b\,(c + \overline{c}) = a\,b\,(1) = a\,b$). Se a cada derivação algébrica apenas alguma manipulação algébrica válida é aplicada, garante-se que a expressão final resultante é equivalente à expressão original (isto é, o valor de ambas é igual um ao outro para quaisquer atribuições de valores para as variáveis).

O princípio de dualidade da álgebra booleana afirma que cada expressão ou identidade algébrica dedutível a partir dos postulados em uma álgebra booleana continua válida se todas as ocorrências dos operadores + e · e os elementos identidade 0 e 1 são trocados um pelo outro.

De fato, isso faz sentido pois o dual de cada um dos axiomas é também um axioma. Observe:

$$\text{Axioma A1}\quad \begin{array}{ccccccc} x & \cdot & y & = & y & \cdot & x \\ & \downarrow & & & & \downarrow & \\ x & + & y & = & y & + & x \end{array}$$

$$\text{Axioma A2}\quad \begin{array}{ccccccccccccc} x & \cdot & (y & + & z) & = & (x & \cdot & y) & + & (x & \cdot & z) \\ & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \downarrow & \\ x & + & (y & \cdot & z) & = & (x & + & y) & \cdot & (x & + & z) \end{array}$$

$$\text{Axioma A3}\quad \begin{array}{ccccc} x & + & 0 & = & x \\ & \downarrow & \downarrow & & \\ x & \cdot & 1 & = & x \end{array}$$

$$\text{Axioma A4}\quad \begin{array}{ccccc} x & + & \overline{x} & = & 1 \\ & \downarrow & & & \downarrow \\ x & \cdot & \overline{x} & = & 0 \end{array}$$

Portanto, dada uma expressão E, ao se substituir sucessivamente subexpressões de E e das expressões derivadas de E por subexpressões equivalentes, obtém-se uma derivação que resulta em uma expressão equivalente a E. Se partirmos do dual da expressão original E e trocarmos todas as derivações realizadas a partir de E pelos correspondentes duais, obteremos uma expressão que é equivalente ao dual de E. Isto significa, em particular, que se conseguimos provar algebricamente que $E_1 = E_2$, automaticamente teremos a prova de que $dual(E_1) = dual(E_2)$.

4 Leis fundamentais da álgebra booleana

Desta parte em diante omitiremos o símbolo $\cdot$ na maioria das vezes; em vez de $x \cdot y$, escreveremos simplesmente xy. Suponha que $\langle A, +, \cdot, ^-, 0, 1\rangle$ é uma álgebra booleana. Então, os seguintes resultados são válidos.

[**Unicidade do 0 e 1**] Os elementos 0 e 1 são únicos.

PROVA: Sejam dois elementos zero, 0_1 e 0_2. Por A3, temos que para todo x_1 e x_2 em A,

$$x_1 + 0_1 = x_1 \quad \text{e} \quad x_2 + 0_2 = x_2$$

Logo, se tomarmos as igualdades para $x_1 = 0_2$ e $x_2 = 0_1$, temos que

$$0_2 + 0_1 = 0_2 \quad \text{e} \quad 0_1 + 0_2 = 0_1$$

Por A1 e a transitividade de $=$, resulta que $0_1 = 0_2$.

A unicidade de 1 pode ser provada usando o princípio da dualidade.

[**Idempotência**] Para todo elemento $x \in A$, $\quad x + x = x \;$ e $\quad xx = x$.

PROVA:

$$\begin{array}{rcll} x + x & = & (x+x)\cdot 1 & (A3) \\ & = & (x+x)(x+\overline{x}) & (A4) \\ & = & x + x\,\overline{x} & (A2) \\ & = & x + 0 & (A4) \\ & = & x & (A3) \end{array} \qquad \begin{array}{rcll} xx & = & x\,x + 0 & (A3) \\ & = & x\,x + x\,\overline{x} & (A4) \\ & = & x\,(x + \overline{x}) & (A2) \\ & = & x \cdot 1 & (A4) \\ & = & x & (A3) \end{array}$$

[**Identidade**] Para todo $x \in A$, $x + 1 = 1 \quad$ e $\quad x\,0 = 0$.

$$\begin{array}{rcll} x + 1 & = & 1 \cdot (x+1) & (A3) \\ & = & (x+\overline{x})(x+1) & (A4) \\ & = & x + \overline{x} \cdot 1 & (A2) \\ & = & x + \overline{x} & (A3) \\ & = & 1 & (A4) \end{array}$$

[**Complemento do um (zero)**] $\overline{1} = 0 \quad$ e $\quad \overline{0} = 1$.

$$\begin{aligned} \overline{1} &= \overline{1} \cdot 1 \quad (A3) \\ &= 0 \quad (A4) \end{aligned}$$

[**Absorção**] Para todo $x, y \in A$, $x + x\,y = x$ e $x\,(x + y) = x$.

$$\begin{aligned} x + xy &= x \cdot 1 + x\,y && (A3) \\ &= x\,(1 + y) && (A2) \\ &= x \cdot 1 && (Identidade) \\ &= x && (A3) \end{aligned}$$

[**Unicidade de $\overline{x}$**] O inverso de qualquer elemento $x \in A$ é único.

PROVA: Sejam $\overline{x}_1$ e $\overline{x}_2$ em A tais que

$$x + \overline{x}_1 = 1 \quad \text{e} \quad x + \overline{x}_2 = 1 \quad \text{e} \quad x\,\overline{x}_1 = 0 \quad \text{e} \quad x\,\overline{x}_2 = 0$$

Então, temos que

$$\begin{aligned} \overline{x}_2 &= 1 \cdot \overline{x}_2 && (A3) \\ &= (x + \overline{x}_1)\,\overline{x}_2 && \text{(hipótese)} \\ &= x\,\overline{x}_2 + \overline{x}_1\,\overline{x}_2 && (A2) \\ &= 0 + \overline{x}_1\,\overline{x}_2 && \text{(hipótese)} \\ &= x\,\overline{x}_1 + \overline{x}_1\,\overline{x}_2 && \text{(hipótese)} \\ &= (x + \overline{x}_2)\,\overline{x}_1 && (A2) \\ &= 1 \cdot \overline{x}_1 && \text{(hipótese)} \\ &= \overline{x}_1 && (A3) \end{aligned}$$

[**Involução**] Para todo $x \in A$, $\overline{\overline{x}} = x$.

PROVA: Seja $\overline{\overline{x}} = y$. Então, por A4 temos que $\overline{x}\,y = 0$ e $\overline{x} + y = 1$. Mas por A4, $\overline{x}\,x = 0$ e $\overline{x} + x = 1$. Por causa da unicidade do complemento, $\overline{\overline{x}} = y = x$.

[**Associatividade**] Para quaisquer $x, y, z \in A$, $x + (y + z) = (x + y) + z$ e $x(yz) = (xy)z$.

[**Lema**] Para quaisquer $x, y, z \in A$, $x[(x + y) + z] = [(x + y) + z]x = x$.

$$\begin{aligned} x[(x + y) + z] &= [(x + y) + z]x && (A1) \\ x[(x + y) + z] &= x(x + y) + xz && (A2) \\ &= x + xz && \text{(absorção)} \\ &= x && \text{(absorção)} \end{aligned}$$

Usando o lema acima, provaremos a propriedade associativa. Seja

$$
\begin{aligned}
Z &= [(x+y)+z][x+(y+z)] & \\
&= [(x+y)+z]x + [(x+y)+z](y+z) & (A2) \\
&= x + [(x+y)+z](y+z) & (lema) \\
&= x + \{[(x+y)+z]y + [(x+y)+z]z\} & (A2) \\
&= x + \{[(y+x)+z]y + [(x+y)+z]z\} & (A1) \\
&= x + \{y + [(x+y)+z]z\} & (lema) \\
&= x + (y+z) &
\end{aligned}
$$

De forma similar,

$$
\begin{aligned}
Z &= (x+y)[x+(y+z)] + z[x+(y+z)] & (A2) \\
&= (x+y)[x+(y+z)] + z & (lema) \\
&= \{x[x+(y+z)] + y[x+(y+z)]\} + z & (A2) \\
&= \{x[x+(y+z)] + y\} + z & (lema) \\
&= (x+y)+z & (lema)
\end{aligned}
$$

Logo, $x+(y+z) = (x+y)+z$

[<u>**Teorema de DeMorgan**</u>] Para quaisquer $x, y \in A$, $\overline{(x+y)} = \overline{x}\,\overline{y}$ e $\overline{x\,y} = \overline{x} + \overline{y}$.

Vamos mostrar que $(x+y) + \overline{x}\,\overline{y} = 1$ e que $(x+y)(\overline{x}\,\overline{y}) = 0$.

$$
\begin{aligned}
(x+y) + \overline{x}\,\overline{y} &= [(x+y)+\overline{x}][(x+y)+\overline{y}] & (A2) \\
&= [\overline{x}+(x+y)][\overline{y}+(x+y)] & (A1) \\
&= [(\overline{x}+x)+y)][x+(\overline{y}+y)] & (Associativa + A1) \\
&= 1 \cdot 1 & (A4 + Identidade) \\
&= 1 & (A3)
\end{aligned}
$$

$$
\begin{aligned}
(x+y) \cdot \overline{x}\,\overline{y} &= x(\overline{x}\,\overline{y}) + y(\overline{y}\,\overline{x}) & (A2 + A1) \\
&= (x\,\overline{x})\,\overline{y} + (y\,\overline{y})\,\overline{x} & (associativa) \\
&= 0 + 0 & (A4 + Identidade) \\
&= 0 & (A3)
\end{aligned}
$$

Portanto, pela unicidade do complemento, podemos concluir que $\overline{(x+y)} = \overline{x}\,\overline{y}$.

A igualdade dual pode ser demonstrada pelo princípio da dualidade, ou usando o fato de que as igualdades acima valem também para $\overline{x}$ e $\overline{y}$ no lugar de x e y. $\square$

5 Relações de Ordem Parciais

5.1 Conjuntos parcialmente ordenados (posets)

Seja A um conjunto não vazio. Uma **relação binária** R sobre A é um subconjunto de $A \times A$, isto é, $R \subseteq A \times A$. Se $(x, y) \in R$, denotamos a relação de x por y como sendo xRy (lê-se x-erre-y).

Relação de ordem parcial: Uma relação binária $\leq$ sobre A é uma **ordem parcial** se ela é

1. (reflexiva) $x \leq x$, para todo $x \in A$
2. (anti-simétrica) Se $x \leq y$ e $y \leq x$, então $x = y$, para todo $x, y \in A$
3. (transitiva) Se $x \leq y$ e $y \leq z$ então $x \leq z$, para todo $x, y, z \in A$

Se $\leq$ é uma ordem parcial em A, então a relação $\geq$ definida por, para quaisquer $x, y \in A$, $x \geq y$ se e somente se $y \leq x$, é também uma ordem parcial em A.

Observação: Apenas uma curiosidade: uma relação de equivalência é bem parecida com uma relação de ordem parcial. A diferença está na segunda propriedade: ordens parciais satisfazem anti-simetria, enquanto relações de equivalência satisfazem simetria (i.e., se $x \sim y$ então $y \sim x$, para todo $x, y \in A$).

Conjuntos parcialmente ordenados (poset): Um conjunto A munido de uma relação de ordem parcial $\leq$ é denominado um conjunto parcialmente ordenado (ou *poset*) e denotado por $(A, \leq)$. Se $(A, \leq)$ é um poset, então $(A, \geq)$ também é um poset.

Exemplo 1: A relação de ordem $\leq$ usual definida no conjunto dos números reais é uma ordem parcial (na verdade, ela é mais que uma ordem parcial; é uma **ordem total**, pois todos os elementos são comparáveis dois a dois). A relação $<$ não é uma ordem parcial pois ela não é reflexiva.

Exemplo 2: A relação de inclusão de conjuntos $\subseteq$ é uma ordem parcial.

Diagrama de Hasse: Escrevemos $x < y$ quando $x \leq y$ e $x \neq y$. Dado um poset $(A, \leq)$ e $x, y \in A$, dizemos que y cobre x se, e somente se, $x < y$ e não há outro elemento $z \in A$

tal que $x < z < y$. Um diagrama de Hasse do poset $(A, \leq)$ é uma representação gráfica onde vértices representam os elementos de A e dois elementos x e y são ligados por uma aresta se e somente se y cobre x. Em um diagrama de Hasse, os elementos menores (com relação a ordem parcial) são em geral desenhados abaixo dos elementos maiores.

Exemplo: O diagrama de Hasse do poset $(\{a, b, c\}, \subseteq)$ é mostrado na figura 3. Trata-se do cubo, visto no contexto de circuitos lógicos.

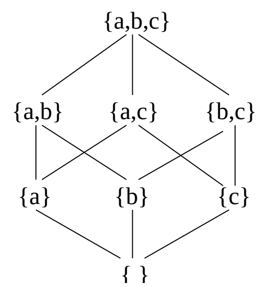


Figura 3: Diagrama de Hasse de $(\{a, b, c\}, \subseteq)$.

6 Relação de ordem e álgebra booleana

Seja $\langle A, +, \cdot, \bar{\ }, 0, 1\rangle$ uma álgebra booleana. Definimos uma relação binária $\leq$ em A da seguinte forma:

$$\forall x, y \in A, \quad x \leq y \ \text{ se e somente se } \ x + y = y \tag{1}$$

A relação $\leq$ definida pela equação 1 é uma relação de ordem parcial. De fato, a relação $\leq$ é (1) reflexiva pois pela lei de idempotência $(x + x = x)$ temos que $x \leq x$ para todo $x \in A$; é (2) anti-simétrica pois se $x \leq y$ e $y \leq x$, então $x + y = y$ e $y + x = x$ e, portanto, pela comutatividade de $+$, segue que $x = y$; e é (3) transitiva pois se $x \leq y$ e $y \leq z$, então

$$\begin{aligned} z &= y + z && \text{(pois } y \leq z\text{)} \\ &= (x + y) + z && \text{(pois } x \leq y\text{)} \\ &= x + (y + z) && \text{(associatividade de } +\text{)} \\ &= x + z && \text{(pois } y \leq z\text{)} \end{aligned}$$

Logo, $x \leq z$.

Referências

[Garnier and Taylor, 1992] Garnier, R. and Taylor, J. (1992). *Discrete Mathematics for New Technology*. Adam Hilger.

[Hill and Peterson, 1981] Hill, F. J. and Peterson, G. R. (1981). *Introduction to Switching Theory and Logical Design*. John Wiley, 3rd edition.

[Whitesitt, 1961] Whitesitt, J. E. (1961). *Boolean Algebra and its Applications*. Addison-Wesley.