Álgebra Booleana

Nesta parte 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. Todas essas leis podem ser derivadas algebricamente a partir dos postulados da definição.

Para as formalizações apresentadas aqui, procure associar os equivalentes vistos na parte de álgebra dos conjuntos. Recomenda-se também que o leitor faça o inverso: prestar atenção como os conceitos apresentados via álgebra de conjunto podem ser formalizados (tratados de forma abstrata).

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

1.1 Definição axiomática

Considere uma sêxtupla $\langle A, +, \cdot, ^{-}, 0, 1\rangle$ na qual A é um conjunto, $+$ e $\cdot$ são operações binárias sobre A, $^{-}$ é uma operação unária em A e 0 e 1 são dois elementos distintos em A. O sistema algébrico $\langle A, +, \cdot, ^{-}, 0, 1\rangle$ 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,

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

Observação: 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.

1.2 Exemplos de álgebra booleana

Exemplo 1: O conjunto $B = \{0, 1\}$ onde definimos

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

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

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

é uma álgebra booleana.

Os axiomas A1, A3 e A4 são satisfeitos por definição. Para verificar o axioma A2 podemos construir uma tabela verdade com todas as possíveis combinações de valores para x, y e z. Vejamos a validade da distributividade em relaçao 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 $\langle B, +, \cdot, \bar{}, 0, 1\rangle$. 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, $\mathcal{P}(S) = \{X : X \subseteq S\}$. Então, $\langle \mathcal{P}(S), \cup, \cap, ^c, \emptyset, S\rangle$ é uma álgebra booleana.

Como já vimos na parte de álgebra dos conjuntos, os equivalentes aos 4 postulados são:

A1. $X \cup Y = Y \cup X \quad$ e $\quad X \cap Y = Y \cap X$

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

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

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

Exemplo 3: A lógica (ou cálculo) proposicional é uma álgebra booleana. De fato, ela tem uma correspondência um-para-um com $\langle B, +, \cdot, \bar{}, 0, 1\rangle$, conforme mostrado a seguir:

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

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

1.3 Leis fundamentais da álgebra booleana

Princípio da dualidade: Cada expressão ou identidade algébrica dedutível a partir dos postulados em uma álgebra booleana continua válida se todas as ocorrências dos operadores $+$ e $\cdot$ e os elementos identidade 0 e 1 são trocados um pelo outro.

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

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

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

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

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

Assim, se na prova de uma proposição E trocarmos cada derivação pela sua dual obtemos uma outra prova (válida, pois axiomas são trocadas por axiomas). Esta nova prova é uma prova da dual de E.

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

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

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

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

Tome, em particular, $x_1 = 0_2$ e $x_2 = 0_1$. Assim temos

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

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:

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

[**Identidade**] Para todo $x \in A$, $x + 1 = 1 \quad$ e $\quad x0 = 0$.

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

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

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

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

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

[**Unicidade de $\overline{x}$**] O inverso de qualquer elemento $x \in A$ é único, isto é, se $x + y = 1$ e $x\,y = 0$ para algum $y \in A$, então $y = \overline{x}$.

PROVA: Por contradição. Suponha que existem dois elementos distintos $\overline{x}_1$ e $\overline{x}_2$ em A tais que

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

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

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

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

Usando o lema acima, provaremos a propriedade associativa. Seja

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

De forma similar,

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

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

[**Teorema de DeMorgan**] 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 $(x + y)(\overline{x}\,\overline{y}) = 0$.

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

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

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. $\square$

Note a similaridade destas propriedades com as propriedades dos conjuntos (e também com as da lógica proposicional). Enquanto lá fizemos uso dos diagramas de Venn e das tabelas-verdade, respectivamente, para nos convencermos da validade das propriedades, aqui as demonstrações são algébricas.

Exercícios:

1. Mostre que o conjunto B^n mais as operações definidas no exemplo 4 da página 3 é uma álgebra booleana.

2. Considere o conjunto dos números reais R, juntamente com as operações usuais de adição e multiplicação. Quais dos axiomas A1, A2, A3 não são satisfeitos ? É possível definir uma operação unária em R tal que o axioma A4 seja satisfeito ?

3. Seja $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$, ou seja, o conjunto de divisores de 30. Defina operações binárias $+$ e $\cdot$ e uma operação unária $\bar{}$ da seguinte forma: para quaiquer $a_1, a_2 \in A$,

   $$a_1 + a_2 = \text{o mínimo múltiplo comum entre } a_1 \text{ e } a_2$$

   $$a_1 \cdot a_2 = \text{o máximo divisor comum entre } a_1 \text{ e } a_2$$

   $$\overline{a}_1 = 30/a_1$$

   Quais são os elementos identidade com respeito a $+$ e $\cdot$? Mostre que A, com as três operações acima, é uma álgebra booleana.

4. Prove as seguintes igualdades

   a) $x + \overline{x}y = x + y$ (e sua dual $x(\overline{x} + y) = xy$)

   b) $x + y = \overline{\overline{x}\,\overline{y}}$ (e sua dual $xy = \overline{\overline{x} + \overline{y}}$)

   c) $(x + y)(x + \overline{y}) = x$ (e sua dual $xy + x\overline{y} = x$)

   d) (Teorema do consenso) $xy+yz+\overline{x}z = xy+\overline{x}z$ (ou o dual $(x+y)(y+z)(\overline{x}+z) = (x+y)(\overline{x}+z)$)

   e) $yx = zx$ e $y\overline{x} = z\overline{x}$ implica que $y = z$

   f) $(x + y + z)(x + y) = x + y$

5. Simplifique as seguintes expressões

   a) $y\overline{z}(\overline{z} + \overline{z}x) + (\overline{x} + \overline{y})(\overline{x}y + \overline{x}z)$

   b) $x + xyz + yz\overline{x} + wx + \overline{w}x + \overline{x}y$

6. Mostre que em qualquer álgebra booleana $\langle A, +, \cdot, ^-, 0, 1\rangle$, $x\,\overline{y} = 0$ se, e somente se, $x\,y = x$.

1.4 Relações de Ordem Parciais

1.4.1 Conjuntos parcialmente ordenados (posets)

Seja A um conjunto não vazio. Conforme visto anteriormente, 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 1.1.

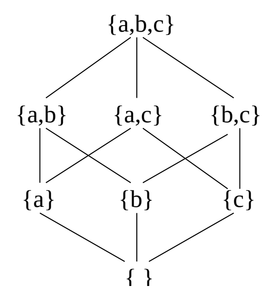


Figura 1.1: Diagrama de Hasse de $(\{a, b, c\}, \subseteq)$.

1.4.2 Elementos notáveis de um poset

Menor e maior elementos: Seja $(A, \leq)$ um poset.

- Chama-se **menor elemento** de A um elemento $0 \in A$ tal que $0 \leq x$ para todo $x \in A$ (também denotado $m(A)$).
- Chama-se **maior elemento** de A um elemento $1 \in A$ tal que $x \leq 1$ para todo $x \in A$ (também denotado $M(A)$).

Teorema: Em um poset $(A, \leq)$, se existe um menor elemento, ele é único. Similarmente, se existe um maior elemento, ele é único.

PROVA: Suponha que 0_1 e 0_2 são menores elementos de $(A, \leq)$. Então, teríamos $0_1 \leq 0_2$ (pois 0_1 é menor elemento) e $0_2 \leq 0_1$ (pois 0_2 é menor elemento). Pela propriedade anti-simétrica da relação $\leq$, concluímos que $0_1 = 0_2$. A unicidade do maior elemento segue de forma análoga. $\square$

Exemplo: Dado um conjunto não vazio S, no poset $(\mathcal{P}(S), \subseteq)$ o menor elemento é o $\emptyset$ (conjunto vazio) e o maior elemento é o S (conjunto universo).

Exemplo: No poset do diagrama abaixo, o maior elemento é a e não há um menor elemento.

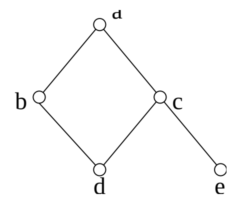


Figura 1.2: Diagrama de um poset.

Elementos minimais e maximais:

- Chama-se **elemento minimal** de A um elemento $a \in A$ tal que elemento algum de A precede estritamente a, isto é, para qualquer $x \in A$, se $x \leq a$ então $x = a$. O conjunto dos elementos minimais de A é denotado $min(A)$.
- Chama-se **elemento maximal** de A um elemento $a \in A$ tal que elemento algum de A sucede estritamente a, isto é, para qualquer $x \in A$, se $x \geq a$ então $x = a$. O conjunto dos elementos maximais de A é denotado $max(A)$.

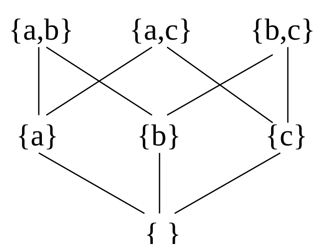
Exemplo: No poset da figura 1.2, os elementos minimais são d e e enquanto o único elemento maximal é a.

Teorema: Se 0 é o menor elemento de $(A, \leq)$, então 0 é o único elemento minimal de $(A, \leq)$.

PROVA: Seja 0 o menor elemento de A e suponha que $a \leq 0$ onde $a \in A$. Como 0 é o menor elemento em A, sabemos também que $0 \leq a$. Portanto, pela anti-simetria de $\leq$, temos que $a = 0$. Logo, 0 é minimal.

Suponha que x é um elemento minimal em A. Como 0 é o menor elemento, temos que $0 \leq x$. Por x ser minimal, temos $x = 0$ e, portanto, 0 é o único elemento minimal. □

Exemplo: Seja $S = \{a, b, c\}$ e considere o conjunto de todos os subconjuntos próprios de S, conforme ilustrado no diagrama abaixo.



Este conjunto tem três elementos maximais, $\{a, b\}$, $\{a, c\}$ e $\{b, c\}$. O menor elemento deste conjunto é $\{\}$ e, conforme teorema acima, é o único elemento minimal. O conjunto não possui maior elemento.

Limitantes inferiores e superiores; Ínfimo e supremo:

Seja $(A, \leq)$ um poset e seja $X \subset A$.

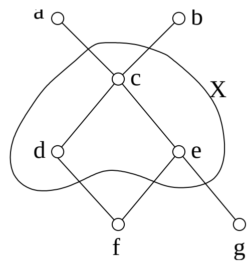
- Chama-se **limitante inferior** de X em A a todo elemento $a \in A$ tal que $a \leq x$ para todo $x \in X$. O conjunto dos limitantes inferiores de X em A é denotado por $li(X)$.

- Chama-se **limitante superior** de X em A a todo elemento $a \in A$ tal que $x \leq a$ para todo $x \in X$. O conjunto dos limitantes superiores de X em A é denotado por $ls(X)$.

- Chama-se **ínfimo** de X em A o maior elemento dos limitantes inferiores de X em A. O ínfimo de X é denotado $\bigwedge X$. O ínfimo de $\{x, y\}$ é denotado $x \wedge y$. O operador $\wedge$ é chamado *conjunção*.

- Chama-se **supremo** de X em A o menor elemento dos limitantes superiores de X em A. O supremo de X é denotado $\bigvee X$. O supremo de $\{x, y\}$ é denotado $x \vee y$. O operador $\vee$ é chamado *união*.

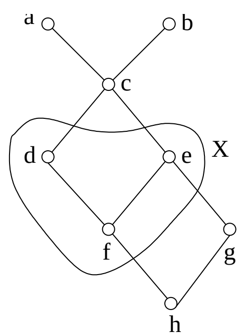
Exemplo:



Elementos minimais: $min(A) = \{f, g\}$
Menor elemento de A: não existe
Elementos maximais: $max(A) = \{a, b\}$
Maior elemento de A: não existe

$X = \{c, d, e\}$
Limitantes inferiores de X: $li(X) = \{f\}$
ínfimo de X: $\bigwedge X = f$
Limitantes superiores de X: $ls(X) = \{a, b, c\}$
Supremo de S: $\bigvee X = c$

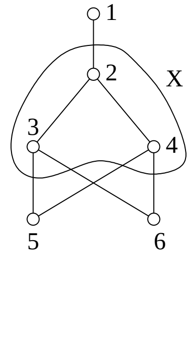
Exemplo:



Elementos minimais: $min(A) = \{h\}$
Menor elemento de A: $m(A) = h$
Elementos maximais: $max(A) = \{a, b\}$
Maior elemento de A: não existe

$X = \{d, e, f\}$
Limitantes inferiores de X: $li(X) = \{f, h\}$
ínfimo de X: $\bigwedge X = f$
Limitantes superiores de X: $ls(X) = \{a, b, c\}$
Supremo de S: $\bigvee X = c$

Exemplo:



Elementos minimais: $min(A) = \{5, 6\}$
Menor elemento de A: não existe
Elementos maximais: $max(A) = \{1\}$
Maior elemento de A: $M(A) = 1$

$X = \{2, 3, 4\}$
Limitantes inferiores de X: $li(X) = \{5, 6\}$
ínfimo de X: não existe
Limitantes superiores de X: $ls(X) = \{1, 2\}$
Supremo de S: $sup(X) = 2$

1.4.3 Reticulados

Um poset $(A, \leq)$ no qual cada par de elementos possui um ínfimo e um supremo em A (ou seja, para quaisquer $x, y \in A$, $x \wedge y$ e $x \vee y$ estão em A) é um **reticulado**.

Um reticulado $(A, \leq)$ é **completo** se todo subconjunto não vazio X de A possui um ínfimo e um supremo em A. Qualquer reticulado completo possui menor elemento 0 e maior elemento 1. Qualquer reticulado finito é completo.

Um reticulado $(A, \leq)$ é **distributivo** se as operações de união ($\vee$) e conjunção ($\wedge$) são distributivas, isto é, para quaisquer x, y e z em A,

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \text{e} \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

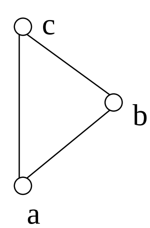
Um reticulado $(A, \leq)$, com menor elemento 0 e maior elemento 1, é **complementado** se todo elemento em A possui um complemento, isto é, para todo $x \in A$ existe $\overline{x}$ tal que $x \vee \overline{x} = 1$ e $x \wedge \overline{x} = 0$.

Teorema: Um reticulado $(A, \leq)$, distributivo e complementado, é uma álgebra booleana (também chamado de reticulado booleano).

> PROVA: Considere um reticulado distributivo e complementado $(A, \leq)$ com as operações de união $\vee$ e conjunção $\wedge$ como definidos acima, e complementação $\bar{\ }$. Claramente $\vee$ e $\wedge$ definem operações binárias em A. Sejam ainda 0 e 1 o menor e o maior elementos de $(A, \leq)$.
>
> Vamos verificar que os axiomas de Huntington são satisfeitos. As operações $\vee$ e $\wedge$ são comutativas por definição; são distributivas pois o reticulado é distributivo; o axioma 4 é satisfeito pois o reticulado é complementado, e o axioma 3 é satisfeito pois $x \vee 0 = x$ e $x \wedge 1 = x$ para qualquer $x \in A$. $\square$

Exercícios:

1. Mostre que a configuração abaixo não pode ocorrer no diagrama de Hasse de nenhum poset.



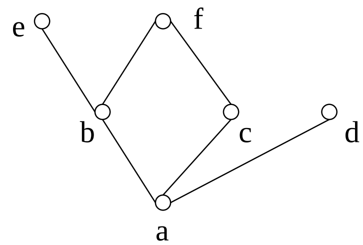
2. Seja R uma ordem parcial sobre A e seja $X \subseteq A$. Mostre que $S = R \cap (X \times X)$ é uma relação de ordem parcial (em outras palavras, qualquer subconjunto de um poset é também um poset).

3. Seja a relação de divisibilidade $|$ definida sobre os inteiros positivos da seguinte forma: para quaisquer x, y inteiros positivos, $x|y$ se, e somente se, x divide y.

   a) Mostre que $|$ é uma relação de ordem parcial

   b) Desenhe o diagram de Hasse de $\{1, 2, 3, 4, 6, 12\}$ com respeito à relação parcial $|$.

4. Liste os elementos da relação de ordem cujo diagrama de Hasse é o seguinte:



5. Mostre que se 1 é o maior elemento de $(A, \leq)$, então 1 é o único elemento maximal de $(A, \leq)$.

6. Mostre por indução que todo subconjunto finito de um reticulado tem um ínfimo e um supremo.

7. Sejam x, y elementos de uma álgebra booleana $\langle A, +, \cdot, ^-, 0, 1\rangle$. Mostre que os elementos $x + y$ e xy são respectivamente o supremo e o ínfimo de $\{x, y\}$.

1.5 Relação de ordem e álgebra booleana

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

$$\forall x, y \in A, \quad x \leq y \;\text{ se e somente se }\; x + y = y \tag{1.1}$$

A relação $\leq$ definida pela equação 1.1 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

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

Logo, $x \leq z$.

1.5.1 Toda álgebra booleana é um reticulado

Teorema: Sejam x, y elementos de uma álgebra booleana $\langle A, +, \cdot, ^-, 0, 1\rangle$. Então os elementos $x + y$ e xy são respectivamente o supremo e o ínfimo de $\{x, y\}$.

Teorema: Toda álgebra booleana $\langle A, +, \cdot, ^-, 0, 1\rangle$ é um reticulado.

PROVA: Qualquer subconjunto $\{x, y\}$ de A tem supremo $x + y$ e ínfimo xy (teorema anterior). Logo $\langle A, +, \cdot, ^-, 0, 1\rangle$ é um reticulado. $\square$

1.5.2 Átomos

Um **átomo** de uma álgebra booleana $\langle A, +, \cdot, ^-, 0, 1\rangle$ é um elemento não nulo x que não pode ser expresso na forma $x = y + z$ com $y \neq x$ e $z \neq x$.

Exemplo 1: Os átomos de $\langle \mathcal{P}(S), \cup, \cap, ^c, \emptyset, S\rangle$ são todos os conjuntos unitários.

Exemplo 2: A álgebra booleana relativa ao conjunto B^n de todas as n-uplas binárias tem como átomos as n-uplas com exatamente uma coordenada igual a 1.

Teorema: Um elemento não nulo x de uma álgebra booleana $\langle A, +, \cdot, ^-, 0, 1\rangle$ é um **átomo** se e somente se não há elemento y em A tal que $0 < y < x$.

PROVA:

(se x é um átomo então não há elemento y em A tal que $0 < y < x$) Suponha que x é um átomo e que $y < x$. Então, $x = x\,1 = (y+x)\cdot(y+\overline{y}) = y+(x\,\overline{y})$. Como x é um átomo, então ou $y = x$ ou $(x\,\overline{y}) = x$. Como $x \neq y$ por hipótese, então $(x\,\overline{y}) = x$. Consequentemente $y = x\,y = (x\,\overline{y})\,y = x\,(\overline{y}\,y) = x\,0 = 0$.

(se não há elemento y em A tal que $0 < y < x$ então x é um átomo) Agora suponha que não há elemento y em A tal que $0 < y < x$ e (suponha por absurdo) que x não é um átomo. Então, $x = y + z$ para y e z diferentes de x e, como $y \leq y + z = x$, temos que $y < x$. Além disso, $y = 0$ (pois caso contrário teríamos $0 < y$, uma contradição). Logo, $x = 0 + z = z \neq x$ (absurdo). $\square$

Teorema: Seja $\langle A, +, \cdot, ^-, 0, 1\rangle$ uma álgebra booleana finita com conjunto de átomos $\{a_1, a_2, \ldots, a_n\}$. Cada elemento não nulo x de A pode ser escrito como o supremo de um conjunto de átomos

$$x = a_{i_1} + a_{i_2} + \cdots + a_{i_k}\,.$$

Mais ainda, tal expressão é única, a menos da ordem dos átomos.

PROVA: A demonstração é por contradição. Suponha que existem elementos que não são expressos como supremo de átomos. Seja x um desses elementos. Então como x não é atomo, temos que $x = y + z$ para algum $y < x$ e $z < x$, e mais ainda, pelo menos y ou z não são átomos. Supondo que y não é átomo, temos que ele é supremo de dois elementos menores que ele, dos quais pelo menos um não é átomo. Assim, há uma seqüência de elementos não-átomos $x_0 = x > x_1 = y > x_2 > \ldots$. Mas, como A é finito, haverão índices k e m, com $k < m$ tal que $x_k = x_m$. Pela transitividade de $<$ em $x_k > x_{k+1} > \ldots > x_m$ segue que $x_k > x_m$, contradizendo $x_k = x_m$. Portanto, podemos concluir que todos os elementos não-nulos em A podem ser expressos como supremo de átomos.

Para mostrar a unicidade, primeiro devemos mostrar que

$$x = \bigvee\{a \in A : a \text{ é átomo e } a \leq x\} \tag{1.2}$$

isto é, x pode ser expresso como o supremo de todos os átomos menores ou igual a ele. (A demonstração fica como exercício).

Agora, suponha que $x = a_{i_1} + a_{i_2} + \cdots + a_{i_k}$ é uma expressão de x como supremo de átomos. Então temos que $a_{i_j} \leq x$, e, portanto, $a_{i_j} \in \{a \in A : a \text{ é átomo}, a \leq x\}$. Agora, seja a um átomo tal que $a \in \{a \in A : a \text{ é átomo e } a \leq x\}$. Então, como a é átomo e $a \leq x$,

$$0 \neq a = a\,x = a\,(a_{i_1} + a_{i_2} + \cdots + a_{i_k}) = a\,a_{i_1} + a\,a_{i_2} + \cdots + a\,a_{i_k}$$

Pelo menos um $a\,a_{i_j}$ precisa ser diferente de zero. Logo, $a\,a_{i_j} = a = a_{i_j}$ uma vez que ambos são átomos. Ou seja, a é um dos átomos em $\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\}$. $\square$

1.5.3 Isomorfismo de álgebras booleanas

Uma função bijetora ϕ entre duas álgebras booleanas $\langle A_1, +_1, \cdot_1, \bar{}_1, 0_1, 1_1 \rangle$ e $\langle A_2, +_2, \cdot_2, \bar{}_2, 0_2, 1_2 \rangle$ que satisfaz, para todo $x, y \in A_1$,

1) $\phi(x +_1 y) = \phi(x) +_2 \phi(y)$, $\phi(x \cdot_1 y) = \phi(x) \cdot_2 \phi(y)$ e $\phi(\overline{x}) = \overline{\phi(x)}$, e

2) $\phi(0_1) = 0_2$ e $\phi(1_1) = 1_2$

é um **isomorfismo** de álgebra booleana.

Duas álgebras booleanas são isomorfas se existe um isomorfismo entre elas.

Teorema: Sejam duas álgebras booleanas finitas com o mesmo número de átomos e sejam $\{a_1, a_2, \ldots, a_n\}$ e $\{b_1, b_2, \ldots, b_n\}$ respectivamente os seus conjuntos de átomos. Então, existe um isomorfismo ϕ entre eles tal que $\phi(a_i) = b_i$, para todo $i \in \{1, 2, \ldots, n\}$.

Teorema: Qualquer álgebra booleana finita com n átomos é isomorfa à álgebra booleana $\langle \mathcal{P}(S), \cup, \cap, {}^c, \emptyset, S \rangle$ onde S é um conjunto com n elementos.

1.6 Resumo via um exemplo

Os principais conceitos vistos nesta seção são sumarizados através da especialização para a álgebra booleana $\langle \mathcal{P}(S), \cup, \cap, ^c, \emptyset, S \rangle$.

- A seguinte relação binária é definida em $\mathcal{P}(S)$:

$$\forall X, Y \in \mathcal{P}(S), \quad X \subseteq Y \Longleftrightarrow X \cup Y = Y$$

- a relação $\subseteq$ é uma ordem parcial. Logo, $(\mathcal{P}(S), \subseteq)$ é um poset
- o maior elemento de $\mathcal{P}(S)$ é S
- o menor elemento de $\mathcal{P}(S)$ é $\emptyset$
- o supremo de dois conjuntos $X, Y \in \mathcal{P}(S)$ é dado por $X \cup Y$
- o ínfimo de dois conjuntos $X, Y \in \mathcal{P}(S)$ é dado por $X \cap Y$
- $(\mathcal{P}(S), \subseteq)$ é um reticulado booleano (distributivo e complementado)
- os átomos de $\langle \mathcal{P}(S), \cup, \cap, ^c, \emptyset, S \rangle$ são os conjuntos unitários.
- qualquer elemento de $\mathcal{P}(S)$ pode ser expresso como união de conjuntos unitários.

Exercícios:

1. Mostre que em qualquer álgebra booleana, $x + y = y$ se, e somente se, $xy = x$. Expresse essa relação na álgebra dos conjuntos.

2. Mostre que em uma álgebra booleana $\langle A, +, \cdot, \bar{}, 0, 1\rangle$, se $x \leq y$ então $x + y = y$ e $x\,y = x$, para todo $x, y \in A$.

3. Mostre que em uma álgebra booleana $\langle A, +, \cdot, \bar{}, 0, 1\rangle$, se $y \leq z$ então $x\,y \leq x\,z$ e $x + y \leq x + z$ para todo $x \in A$.

4. Mostre que em qualquer álgebra booleana $\langle A, +, \cdot, \bar{}, 0, 1\rangle$

   a) $xy \leq x \leq x + y$, para todo x e y em A,

   b) $0 \leq x \leq 1$, para todo x em A.

5. Seja $\langle A, +, \cdot, \bar{}, 0, 1\rangle$ uma álgebra booleana finita com conjunto de átomos $\{a_1, a_2, \ldots, a_n\}$. Sabendo que cada elemento não nulo x de A pode ser escrito como o supremo de um conjunto de átomos
$$x = a_{i_1} + a_{i_2} + \cdots + a_{i_k}$$
   mostre que, mais especificamente,
$$x = \bigvee\{a \in A : a \text{ é átomo e } a \leq x\}$$
   isto é, x é o supremo de todos os átomos menores ou igual a ele.

   Dica: Comece expressando 1 como um supremo de átomos e use o fato de que $x = x\,1$.

Referências Bibliográficas

[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.

Última revisão em 7 de março de 2007.