Resolução da Lista 5 da disciplina de Matemática Discreta

Feita por Guilherme de Abreu Barreto[1]

1. Álgebras booleanas

1.

a.$(a' + b')c$;

b. $bc + ca = c(a + b)$. Forma dual: $c' + a'b'$;

c. $a + b' + c'$;

d. $ab(b + c') = abb + abc' = (ab) + (ab)c' = ab$. Forma dual: $a' + b'$;

e. $(a' + b')(b' + c')(c' + a')$;

2.

A algebra booleana está definida nos seguintes termos:

- Existe um conjunto (no caso, B) contendo pelo menos dois elementos ditos **especiais**:
  - o elemento nulo aditivo (no caso, 0);
  - o elemento nulo multiplicativo (no caso, 1);
- Existem duas operações binárias (que relacionam dois elementos):
  - Adição (no caso, $+$) e
  - Multiplicação (no caso, $*$).
- Existe uma operação unária que associa cada elemento $x \in B$ a um elemento $x' \in B$ denominado seu complemento.
  - No caso, a operação é denotada pelo sinal $'$ e os elementos complementares entre si são a com f, b com e, c com d, 0 com 1.

Fica demonstrada a relação de $\mathscr{B}$ com a álgebra booleana.

3.

a. Para qualquer $a \in D_N$ tem-se:

- $a + 1 = mmc(a, 1) = a$;
- $a * N = mdc(a, N)$, como $a \leq N$, $N \mid a$ então $mdc(a, N) = a$.

b,c e d. Uma sêxtupla de elementos constitui uma álgebra booleana se cinco propriedades são satisfeitas, demonstradas à seguir, $\forall a, b, c \in \mathbb{N} - \{1, 0\}$:

P1. Comutatividade

• $a + b = mmc(a, b) = mmc(b, a) = b + a$;

• $a * b = mdc(a, b) = mdc(b, a) = b * a$;

P2. Associatividade

• $(a + b) + c = mmc(mmc(a, b), c) = mmc(a, mmc(b, c)) = a + (b + c)$;
• $(a * b) * c = mdc(mdc(a, b), c) = mdc(a, mdc(b, c)) = (a * b) * c$

P3. Distributividade

• $a + (b * c) = mmc(a, mdc(b, c)) = mdc(mmc(a, b), mmc(a, c)) = (a + b) * (a + c)$;
• $a * (b + c) = mdc(a, mmc(b, c)) = mmc(mdc(a, b), mdc(a, c)) = (a * b) + (a * c)$;

Prova

Quaisquer números $a, b \in \mathbb{N}$ tais que $a, b > 1$ podem ser escritos como produtos de potências dos mesmos n números primos p, ainda que por diferentes expoentes (k e l)[2]:

$$a = \prod_{i=1}^{n} p_i^{k_i} \qquad b = \prod_{i=1}^{n} p_i^{l_i}$$

Assim, as expressões $mmc(a, b)$ e $mdc(a, b)$ podem ser descritas enquanto uma decomposição de números primos[3] da seguinte maneira:

$$mmc(a, b) = p_1^{\max(k_1, l_1)} p_2^{\max(k_2, l_2)} \dots p_n^{\max(k_n, l_n)} = \prod_{i=1}^{n} p_i^{\max(k_i, l_i)}$$

$$mdc(a, b) = p_1^{\min(k_1, l_1)} p_2^{\min(k_2, l_2)} \dots p_n^{\min(k_n, l_n)} = \prod_{i=1}^{n} p_i^{\min(k_i, l_i)}$$

Onde $max(a, b)$ e $min(a, b)$ tratam-se das funções $\mathbb{N}^2 \to \mathbb{N}$ que escolhem o maior e o menor valor entre aqueles fornecidos, respectivamente.

Lema: As operações de máximo e mínimo são distributivas entre si.

Procederemos por exaustão. Temos 6 casos a considerar:

- $a \leq b \leq c$
  - $\max(a, \min(b, c)) = \max(a, b) = b$
    $\min(\max(a, b), \max(a, c)) = \min(b, c) = b$
  - $\min(a, \max(b, c)) = \min(a, c) = a$
    $\max(min(a, b), \min(a, c)) = \max(a, a) = a$
- $a \leq c \leq b$
  - $\max(a, min(b, c)) = \max(a, c) = c$
    $\min(\max(a, b), \max(a, c)) = \min(b, c) = c$
  - $\min(a, \max(b, c)) = \min(a, b) = a$
    $\max(\min(a, b), \min(a, c)) = \max(a, a) = a$
- $b \leq a \leq c$
  - $\max(a, \min(b, c)) = \max(a, b) = a$
    $\min(\max(a, b), \max(a, c)) = \min(a, c) = a$
  - $\min(a, \max(b, c)) = \min(a, c) = a$
    $\max(\min(a, b), \min(a, c)) = \max(b, a) = a$
- $b \leq c \leq a$
  - $\max(a, \min(b, c)) = \max(a, c) = a$
    $\min(\max(a, b), \max(a, c)) = \min(a, a) = a$
  - $\min(a, \max(b, c)) = \min(a, c) = c$
    $\max(\min(a, b), \min(a, c)) = \max(b, c) = c$
- $c \leq a \leq b$
  - $\max(a, \min(b, c)) = \max(a, c) = a$
    $\min(\max(a, b), \max(a, c)) = \min(b, a) = a$
  - $\min(a, \max(b, c)) = \min(a, b) = a$
    $\max(\min(a, b), \min(a, c)) = \max(a, c) = a$
- $c \leq b \leq a$

- $\max(a, \min(b, c)) = \max(a, c) = a$
  $\min(\max(a, b), \max(a, c)) = \min(a, a) = a$

- $\max(a, \min(b, c)) = \max(a, c) = a$
  $\min(\max(a, b), \max(a, c)) = \min(a, a) = a$

Corolário: As operações de mmc e mdc são distributivas entre si.

$$mmc(a, mdc(b, c)) = \prod_{i=1}^{n} p_i^{\max(k_i, \min(l_i, m_i))} = \prod_{i=1}^{n} p_i^{\min(\max(k_i, l_i), \max(k_i, m_i))}$$
$$= mdc(mmc(a, b), mmc(a, c))$$

$$mdc(a, mmc(b, c)) = \prod_{i=1}^{n} p_i^{\min(k_i, \max(l_i, m_i))} = \prod_{i=1}^{n} p_i^{\max(\min(k_i, l_i), \min(k_i, m_i))}$$
$$= mmc(mdc(a, b), mdc(a, c))$$

P4. Identidade

- $a + 1 = mmc(a, 1) = a$
- $a * N = mdc(a, N) = a$

P5. Complementariedade

- $a + a' = mmc(a, N/a) = N$, se $N/a \nmid a$
- $a * a' = mdc(a, N/a) = 1$, se $N/a \nmid a$

Assim, a $\mathscr{B} = \langle D_N, +, *, ', 1, N \rangle$ tal qual definida pelo enunciado **pode** constituir uma álgebra booleana, a depender do valor $N \in \mathbb{N}$. Analisemos os casos apresentados: D_{70}, D_{15} e D_18. Nestes três as propriedades **P1** à **P4** se sustentam, mas a propriedade **P5** apresenta divergência:

D_{15} :

a	a'	$mmc(a, a')$	$mdc(a, a')$
1	15	15	1
3	5	15	1
5	3	15	1
15	1	15	1

D_{70} :

a	a'	$mmc(a, a')$	$mdc(a, a')$
1	70	70	1
2	35	70	1
5	14	70	1
7	10	70	1
10	7	70	1
14	5	70	1
35	2	70	1
70	1	70	1

D_{18} :

a	a'	$mmc(a, a')$	$mdc(a, a')$
1	18	18	1
2	9	18	1
3	6	**6**	**3**
6	3	**6**	**3**
9	2	18	1
18	1	18	1

Destes três conjuntos, apenas os dois primeiros conjuntos satisfazem a definição de álgebra booleana. ■

e. Prosseguiremos em nossa demonstração por contradição. Por hipótese, D_N constitui uma algebra booleana e possui a propriedade de complementariedade $p * p' = mdc(p, N/p) = 1$, onde $1 < p < N$. Também, $N \mid p$ e $N \mid p^2$. Assim,

$$\begin{cases} N = p \cdot p' \\ N = p^2 \cdot (p^2)' \end{cases} \therefore p' = (p^2)' \cdot p$$

E portanto, $p * p' = mdc(p, p') = mdc(p, (p^2)' \cdot p) = p$, chegamos à uma contradição. Logo, não é possível D_N constituir uma álgebra booleana se esta contêm tanto a p e p^2. ■

4.

a. Usando as definições das operações $*$,$+$ e $'$ obtemos os seguintes resultados quando os valores de a, b e c são 0 ou 1:

Para $ab + c = (a + c)(b + c)$:

a	b	c	ab	$ab + c$
0	0	0	0	**0**
0	0	1	0	**1**
0	1	0	0	**0**
0	1	1	0	**1**
1	0	0	0	**0**
1	0	1	0	**1**
1	1	0	1	**1**
1	1	1	1	**1**

a	b	c	$(a + c)$	$(b + c)$	$(a + c)(b + c)$
0	0	0	0	0	**0**
0	0	1	1	1	**1**
0	1	0	0	1	**0**
0	1	1	1	1	**1**
1	0	0	1	0	**0**
1	0	1	1	1	**1**
1	1	0	1	1	**1**
1	1	1	1	1	**1**

Para $(a + b)c = ac + bc$:

a	b	c	$(a + b)$	$(a + b)c$
0	0	0	0	**0**
0	0	1	0	**0**
0	1	0	1	**0**
0	1	1	1	**1**
1	0	0	1	**0**
1	0	1	1	**1**
1	1	0	1	**0**
1	1	1	1	**1**

a	b	c	ac	bc	$ac + bc$
0	0	0	0	0	**0**
0	0	1	0	0	**0**
0	1	0	0	0	**0**
0	1	1	0	1	**1**
1	0	0	0	0	**0**
1	0	1	1	0	**1**
1	1	0	0	0	**0**
1	1	1	1	1	**1**

b.

a	b	$a + b$	ab	$a'b'$	$(a + b)'$
0	0	0	0	**1**	**1**
0	1	1	0	**0**	**0**
1	0	1	0	**0**	**0**
1	1	1	1	**0**	**0**

a	b	ab	$(ab)'$	$a' + b'$
0	0	0	**1**	**1**
0	1	0	**1**	**1**
1	0	0	**1**	**1**
1	1	1	**0**	**0**

5.

a. $a + a'b = (a + a')(a + b) = 1(a + b) = a + b$

b. $a + ab + b = (a + ab) + b = a + b$

c. $a + b(a + c) = a + ba + bc = (a + ba) + bc = a + bc = (a + b)(a + c)$

d. $a + b + a'b'c = a + (b + a')\cancel{(b + b')}(b + c) = a + b + a'c =$
$b + \cancel{(a + a')}(a + c) = a + b + c$

---

1. nUSP: 12543033; Turma 04 ↩
2. **Expression for Integers as Powers of Same Primes**. Disponível em: https://proofwiki.org/wiki/Expression_for_Integers_as_Powers_of_Same_Primes. Acesso em: 28 nov. 2021. ↩
3. **GCD and LCM from Prime Decomposition**. Disponível em: https://proofwiki.org/wiki/GCD_and_LCM_from_Prime_Decomposition. Acesso em: 28 nov. 2021. ↩
4. **Boolean algebra**. Disponível em: https://en.wikipedia.org/wiki/Boolean_algebra#Duality_principle. Acesso em: 28 nov. 2021. ↩