INE0003

Fundamentos de Matemática Discreta para a Computação

Prof. Daniel S. Freitas

UFSC - CTC - INE

6 - RELAÇÕES DE ORDENAMENTO

6.1) Conjuntos parcialmente ordenados (posets)

6.2) Extremos de posets

6.3) Reticulados

6.4) Álgebras Booleanas Finitas

6.5) Funções Booleanas

RETICULADOS $(P(S), \subseteq)$

- Vamos restringir nossa atenção aos reticulados do tipo $(P(S), \subseteq)$, onde S é um conjunto finito.
  - Muitas propriedades que não valem para reticulados em geral.
  - Por isto, são mais fáceis de trabalhar
  - Têm papel importante em muitas aplicações na Ciência da Computação:
    - construção de representações lógicas para os circuitos do computador
    - estudo de cifradores simétricos, na Criptografia

Reticulados $(P(S), \subseteq)$

- **Teorema**: Sejam $S_1 = \{x_1, x_2..., x_n\}$ e $S_2 = \{y_1, y_2..., y_n\}$ dois conjuntos finitos quaisquer com n elementos.
  - Então os reticulados $(P(S_1), \subseteq)$ e $(P(S_2), \subseteq)$ são isomórficos
    - ou seja, seus diagramas de Hasse são idênticos

- **Prova**: arranjar os conjuntos e definir a seguinte f:

$$\begin{array}{lcccc} S_1\text{:} & x_1 & x_2 & \ldots & x_n \\ & \updownarrow & \updownarrow & & \updownarrow \\ S_2\text{:} & y_1 & y_2 & \ldots & y_n \end{array}$$

$$S_1\text{:}\ x_1\ \overbrace{x_2\ x_3\ x_4}^{\text{subconj. } A} \ldots x_n$$

$$S_2\text{:}\ y_1\ \underbrace{y_2\ y_3\ y_4}_{\text{subconj. } f(A)} \ldots y_n$$

RETICULADOS $(P(S), \subseteq)$

- **Prova (cont.)**:
  - $f(A)$: elementos de S_2 que correspondem aos elementos de A
    - f: bijeção de subconjuntos de S_1 para subconjuntos de S_2
    - além disto, se A e B são subconjuntos quaisquer de S_1:

$$A \subseteq B \quad \Leftrightarrow \quad f(A) \subseteq f(B)$$

  - Logo, os reticulados $(P(S_1), \subseteq)$ e $(P(S_2), \subseteq)$ são isomórficos.

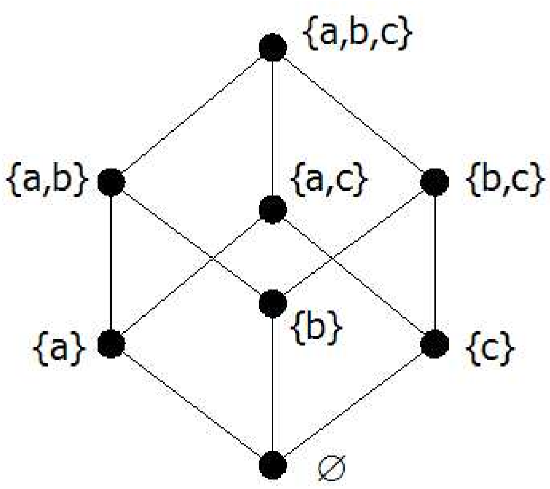
$\square$

RETICULADOS $(P(S), \subseteq)$

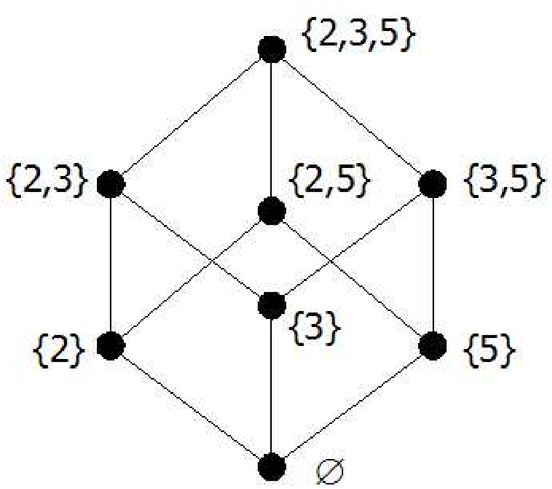
- Logo: a condição de poset do reticulado $(P(S), \subseteq)$ é determinada pelo número $|S|$ e não depende da natureza dos elementos de S.

- **Exemplo**: Sejam os posets:

$(P(S), \subseteq)$, $S = \{a, b, c\}$:



$(P(T), \subseteq)$, $T = \{2, 3, 5\}$:



RETICULADOS $(P(S), \subseteq)$

- Note que os 2 reticulados são isomórficos, sendo um possível isomorfismo $f : P(S) \to P(T)$ dado por:

$$f(\{a\}) = \{2\}$$

$$f(\{b\}) = \{3\}$$

$$f(\{c\}) = \{5\}$$

$$f(\{a, b\}) = \{2, 3\}$$

$$f(\{b, c\}) = \{3, 5\}$$

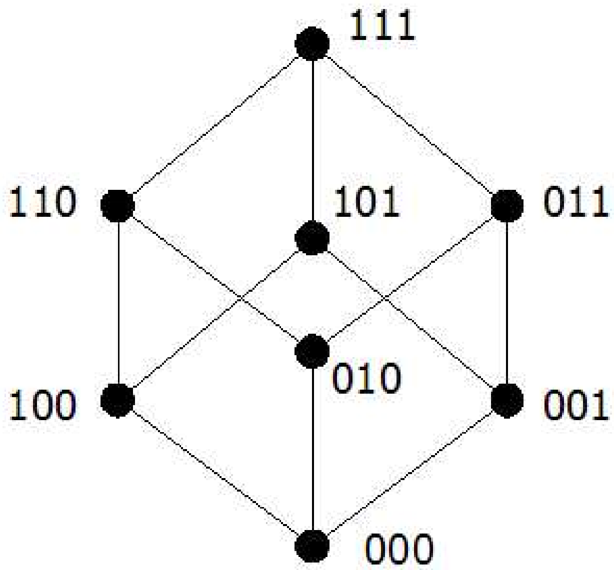
$$f(\{a, c\}) = \{2, 5\}$$

$$f(\{a, b, c\}) = \{2, 3, 5\}$$

RETICULADOS $(P(S), \subseteq)$

- Conclusão: para cada $n = 0, 1, 2, \ldots$, há apenas um tipo de reticulado com a forma $(P(S), \subseteq)$
  - o qual depende apenas de n (e não de S)
  - e tem 2^n elementos (= nro de possíveis subconjuntos de S).

- Pode-se, portanto, tomar um diagrama de Hasse genérico para $(P(S), \subseteq)$ e rotulá-lo assim:



RETICULADOS $(P(S), \subseteq)$

- Rotulando desta forma, este diagrama serve para descrever os 2 reticulados anteriores.
  - Melhor: para descrever um reticulado $(P(S), \subseteq)$ originado de qualquer conjunto S com 3 elementos.

- Se o diagrama de Hasse do reticulado correspondente a um conjunto com n elementos é rotulado desta forma (seqüências de 0s e 1s de comprimento n), o reticulado resultante é chamado de B_n.

PROPRIEDADES DO ORDENAMENTO PARCIAL EM B_n

- Sejam 2 elementos de B_n: $x = a_1 a_2 \ldots a_n$ e $y = b_1 b_2 \ldots b_n$.
- Então:
  - $x \leq y$ se e somente se $a_k \leq b_k$ para $k = 1, 2, \ldots, n$
  - $x \wedge y = c_1 c_2 \ldots c_n$, onde $c_k = min\{a_k, b_k\}$
  - $x \vee y = d_1 d_2 \ldots d_n$, onde $d_k = max\{a_k, b_k\}$
  - o complemento de x é dado por $x' = z_1 z_2 \ldots z_n$, onde:

$$\begin{cases} z_k = 1 & \text{se } x_k = 0 \\ z_k = 0 & \text{se } x_k = 1 \end{cases}$$

PROPRIEDADES DO ORDENAMENTO PARCIAL EM B_n

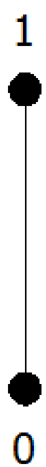
- Estas afirmações podem ser confirmadas pela observação de que $(B_n, \leq)$ é isomórfico a $(P(S), \subseteq)$:
  - $x, y \in B_n$ correspondem a subconjuntos A e B de S
  - então:
    - $x \leq y$ corresponde a $A \subseteq B$
    - $x \wedge y$ corresponde a $A \cap B$
    - $x \vee y$ corresponde a $A \cup B$
    - x' corresponde a $\overline{A}$

RETICULADOS B_n

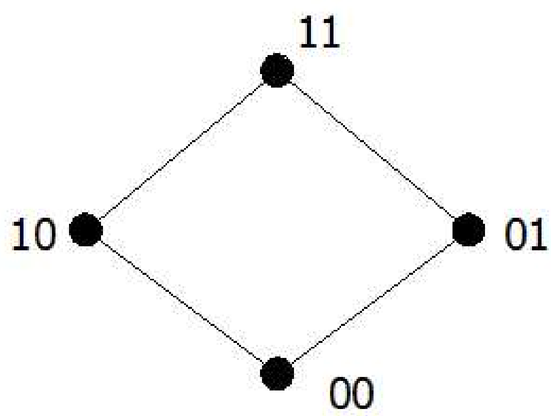
- Diagramas de Hasse dos reticulados B_0, B_1, B_2 e B_3:

n=0: •

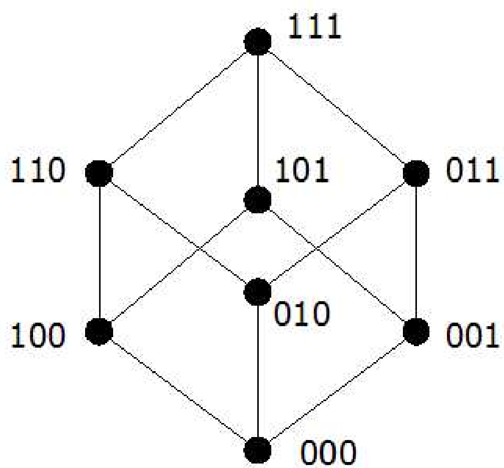
n=1:



n=2:



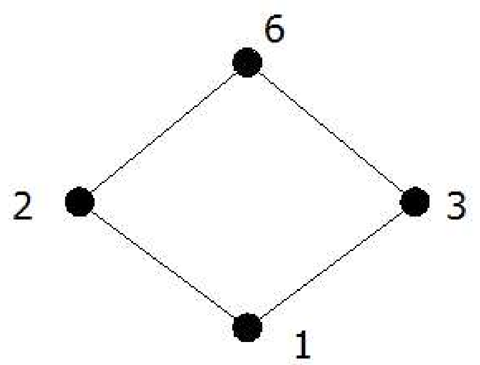
n=3:

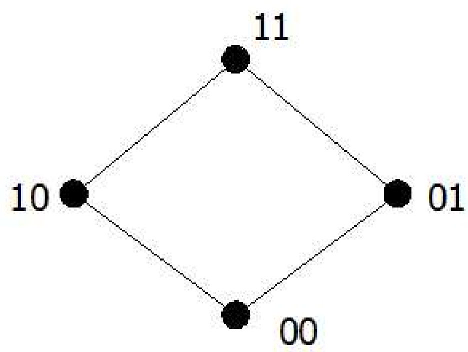


Reticulados B_n

- Todo reticulado $(P(S), \subseteq)$ é isomórfico com B_n, onde $n =\mid S \mid$.
- Outros reticulados também podem ser isomórficos com algum B_n.
  - Possuindo todas as propriedades especiais que o B_n possui.
- **Exemplo**: D_6 (divisores de 6, ordem parcial de divisibilidade).
  - Isomorfismo $f : D_6 \to B_2$ dado por:

$$f(1) = 00 \qquad f(2) = 10 \qquad f(3) = 01 \qquad f(6) = 11$$





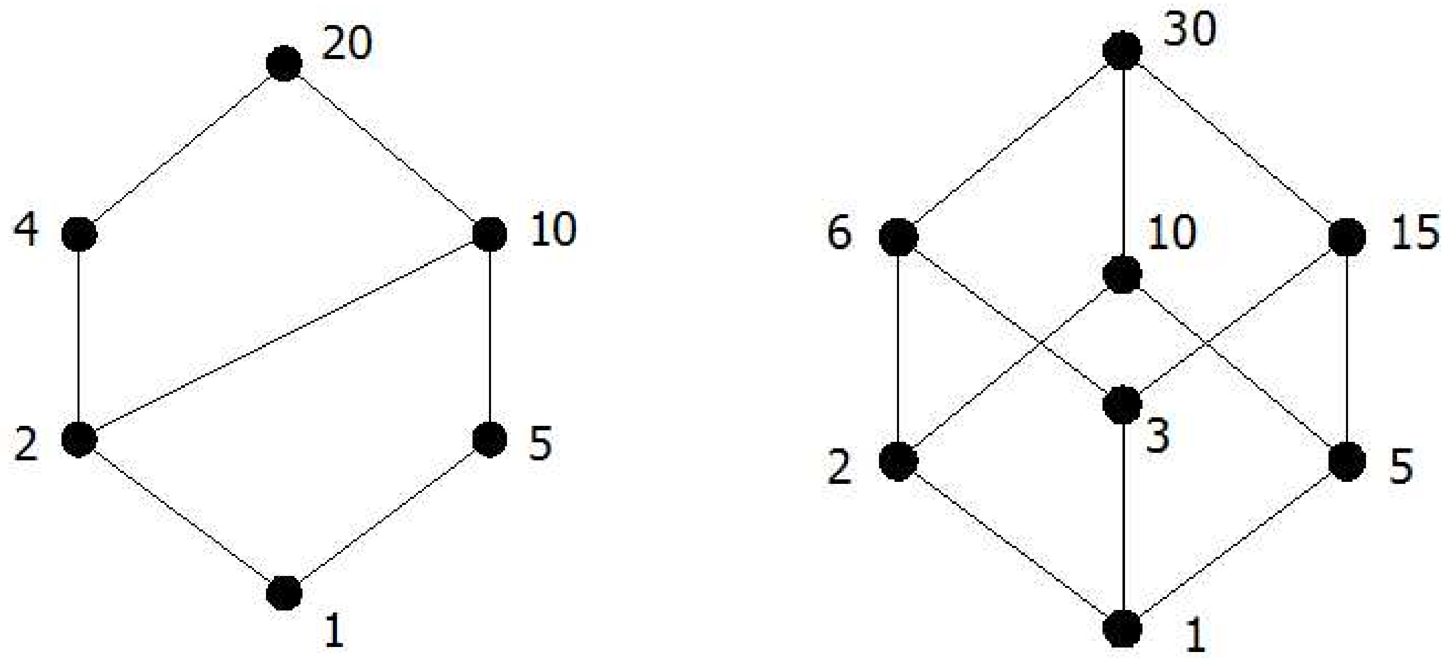
ÁLGEBRAS BOOLEANAS

- Em geral: um reticulado finito é chamado de **Álgebra Booleana** se ele for isomórfico com algum B_n.

- Portanto:
  - todo B_n é uma Álgebra Booleana
  - assim como todo reticulado $(P(S), \subseteq)$.

Álgebras Booleanas

- **Exemplo**: reticulados D_{20} e D_{30} (divisores de 20 e 30, ordem parcial de divisibilidade):



ÁLGEBRAS BOOLEANAS

- **Exemplo (cont.)**:
  - D_{20} tem 6 elementos:
    - $6 \neq 2^n$
    - D_{20} não é uma Álgebra Booleana
  - Já o poset D_{30} tem 8 elementos:
    - $8 = 2^3 \quad \Rightarrow$ chance de ser Álgebra Booleana
    - note que D_{30} é isómórfico com B_3
      - com isomorfismo $f : D_{30} \to B_3$ dado por:

$$f(1) = 000 \qquad f(2) = 100 \qquad f(3) = 010 \qquad f(5) = 001$$

$$f(6) = 110 \qquad f(10) = 101 \qquad f(15) = 011 \qquad f(30) = 111$$

    - portanto, D_{30} é uma Álgebra Booleana. $\square$

ÁLGEBRAS BOOLEANAS

- CONCLUSÃO:
  - Se um reticulado L não contém 2^n elementos, sabemos que L não pode ser uma Álgebra Booleana.
  - Se $\mid L \mid = 2^n$, então L pode ou não ser uma Álgebra Booleana.
  - Se L for pequeno, pode-se tentar comparar o seu diagrama de Hasse com o de B_n
    - no entanto, esta técnica pode não ser prática se L for grande
      - aí tenta-se construir diretamente um isomorfismo com B_n ou com $(P(S), \subseteq)$

ÁLGEBRAS BOOLEANAS GRANDES

- Para ver se um dado reticulado D_n (n grande) é Álgebra Booleana:
- **Teorema**: Seja $n = p_1 p_2 \ldots p_k$ onde os p_i são primos distintos. Então D_n é uma Álgebra booleana.
- **Prova**:
  - Seja $S = \{p_1, p_2, \ldots, p_k\}$.
  - Todo divisor de n deve ser da forma a_T, onde:
    - a_T é o produto dos primos em algum subconjunto T de S (nota: $a_\emptyset = 1$)
  - Aí, se V e T são subconjuntos de S:
    - $V \subseteq T$ se e somente se $a_V \mid a_T$
    - $a_{V \cap T} = a_V \wedge a_T$ (= $MDC(a_V, a_T)$)
    - $a_{V \cup T} = a_V \vee a_T$ (= $MMC(a_V, a_T)$)
  - Logo, $f : P(S) \rightarrow D_n$, dada por $f(T) = a_T$, é um isomorfismo de $P(S)$ para D_n
  - Então, como $(P(S), \subseteq)$ é uma Álgebra Booleana, D_n também o é. $\square$

Álgebras Booleanas grandes

- **Exemplo**:

$210 = 2.3.5.7 \quad \Rightarrow \quad D_{210}$ é Álgebra Booleana

$66 = 2.3.11 \quad \Rightarrow \quad D_{66}$ é Álgebra Booleana

$646 = 2.17.19 \quad \Rightarrow \quad D_{646}$ é Álgebra Booleana

ÁLGEBRAS BOOLEANAS GRANDES

- Outros casos de reticulados L grandes:
  - tentar mostrar que L não é uma Álgebra Booleana
    - mostrando que o ordenamento parcial de L não apresenta as propriedades necessárias.

- Exemplo: uma Álg. Booleana é sempre isomórfica com algum B_n e, portanto, com algum reticulado $(P(S), \subseteq)$.
  - Logo, se o reticulado L for uma Álgebra Booleana:
    - ele deverá ser limitado (deverá possuir LUB e GLB)
    - cada um dos seus elementos deverá possuir um complemento
  - Ou seja, para que L seja reticulado:
    - L deverá ter um maior elemento **I** ($\Leftrightarrow S$) e um menor elemento **O** ($\Leftrightarrow \emptyset$)
    - todo elemento x de L deverá ter um complemento x'

ÁLGEBRAS BOOLEANAS

- O Princípio da Correspondência entre posets ajuda a estabelecer propriedades das Álgebras Booleanas.

- **Teorema** (REGRA DA SUBSTITUIÇÃO):

  Toda fórmula que envolve $\cup$ e $\cap$, ou que vale para subconjuntos arbitrários de um conjunto S, continuará a valer para elementos arbitrários de uma Álgebra Booleana L se:

  - $\cap$ for substituído por $\wedge$
  - $\cup$ for substituído por $\vee$

ÁLGEBRAS BOOLEANAS

- **Exemplo**: Se x, y e z são elementos de uma Álgebra Booleana qualquer L, valem:

  (a) $(x')' = x$ $\longrightarrow$ involução

  (b) $(x \wedge y)' = x' \vee y'$ $\longrightarrow$ 1a. lei de De Morgan

  (c) $(x \vee y)' = x' \wedge y'$ $\longrightarrow$ 2a. lei de De Morgan

- Isto vale para Álgebras booleanas, pois sabemos que as fórmulas:

  (a') $\overline{\overline{(A)}} = A$

  (b') $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

  (c') $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$

  - valem para subconjuntos arbitrários A e B de um conjunto S.

PROPRIEDADES DAS ÁLGEBRAS BOOLEANAS $(L, \leq)$

- De maneira similar, podemos listar outras propriedades que devem valer em qualquer Álgebra Booleana em conseqüência da regra de substituição.

- Na tabela a seguir:
  - x, y e z são elementos arbitrários em L
  - A, B e C são subconjuntos arbitrários de S
  - **I** e **O** denotam o maior e o menor elemento de L, respectivamente.

Propriedades das Álgebras Booleanas $(L, \leq)$ (1/2)

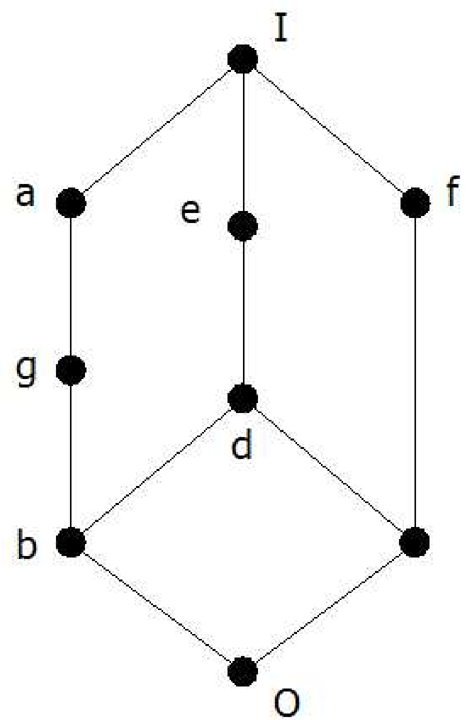
Algumas propriedades básicas de uma Álgebra Booleana $(L, \leq)$	Propriedade correspondente para subconjuntos de um conjunto S
1) $x \leq y$ se e somente se $x \vee y = y$	1') $A \subseteq B$ se e somente se $A \cup B = B$
2) $x \leq y$ se e somente se $x \wedge y = x$	2') $A \subseteq B$ se e somente se $A \cap B = A$
3) (a) $x \vee x = x$ (b) $x \wedge x = x$	3') (a) $A \cup A = A$ (b) $A \cap A = A$
4) (a) $x \vee y = y \vee x$ (b) $x \wedge y = y \wedge x$	4') (a) $A \cup B = B \cup A$ (b) $A \cap B = B \cap A$
5) (a) $x \vee (y \vee z) = (x \vee y) \vee z$ (b) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$	5') (a) $A \cup (B \cup C) = (A \cup B) \cup C$ (b) $A \cap (B \cap C) = (A \cap B) \cap C$
6) (a) $x \vee (x \wedge y) = x$ (b) $x \wedge (x \vee y) = x$	6') (a) $A \cup (A \cap B) = A$ (b) $A \cap (A \cup B) = A$
7) **O** $\leq x \leq$ **I**, $\forall x \in L$	7') $\emptyset \subseteq A \subseteq S, \ \forall A \in P(S)$
8) (a) $x \vee$ **O** $= x$ (b) $x \wedge$ **O** $=$ **O**	8') (a) $A \cup \emptyset = A$ (b) $A \cap \emptyset = \emptyset$

PROPRIEDADES DAS ÁLGEBRAS BOOLEANAS $(L, \leq)$ (2/2)

Algumas propriedades básicas de uma Álgebra Booleana $(L, \leq)$	Propriedade correspondente para subconjuntos de um conjunto S
9) (a) $x \vee \mathbf{I} = \mathbf{I}$ (b) $x \wedge \mathbf{I} = x$	9') (a) $A \cup S = S$ (b) $A \cap S = A$
10) (a) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ (b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$	10') (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
11) Todo elemento x tem um único (a) $x \vee x' = \mathbf{I}$ (b) $x \wedge x' = \mathbf{O}$	11') Todo elemento A tem um único (a) $A \cup \overline{A} = S$ (b) $A \cap \overline{A} = \emptyset$
12) (a) $\mathbf{O}' = \mathbf{I}$ (b) $\mathbf{I}' = \mathbf{O}$	12') (a) $\overline{\emptyset} = S$ (b) $\overline{S} = \emptyset$
13) $(x')' = x$	13') $\overline{\overline{A}} = A$
14) (a) $(x \wedge y)' = x' \vee y'$ (b) $(x \vee y)' = x' \wedge y'$	14') (a) $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (b) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

PROPRIEDADES DAS ÁLGEBRAS BOOLEANAS $(L, \leq)$

- Talvez seja possível mostrar que um reticulado L não é Álgebra Booleana mostrando que ele não possui alguma propriedade básica.
- **Exemplo**: Mostre que o reticulado abaixo não é Álgebra Booleana:



PROPRIEDADES DAS ÁLGEBRAS BOOLEANAS $(L, \leq)$

- **Exemplo (cont.)**:
  - Os elementos a e g são ambos complementos de c
    - ou seja, ambos satisfazem as propriedades 11(a) e 11(b) com respeito ao elemento c.
  - Mas a propriedade estabelece que tal elemento deve ser único em qualquer Álgebra booleana.
  - Logo, o reticulado dado não é uma Álgebra booleana. $\square$

PROPRIEDADES DAS ÁLGEBRAS BOOLEANAS $(L, \leq)$

- **Exemplo**: Mostre que se $p^2 \mid n$, onde p é um primo, então D_n não é uma Álgebra Booleana.
  - suponha que $p^2 \mid n$
    - então $n = p^2.q$
  - mas p também é divisor de n, de modo que $p \in D_n$
  - se D_n é uma Álg. Booleana, p deve ter um complemento p'
    - de modo que $MDC(p, p') = 1$ e $MMC(p, p') = n$
    - daí temos que $p.p' = n$
    - de modo que $p' = n/p = p.q$
  - mas isto significa que $MDC(p, p.q)$ teria que ser 1 (!!)
  - Logo, D_n não pode ser uma Álg. Booleana. $\square$

PROPRIEDADES DAS ÁLGEBRAS BOOLEANAS $(L, \leq)$

- Na verdade, de acordo com um teorema já visto,
  - "Seja $n = p_1p_2 \ldots p_k$ onde os p_i são primos distintos. Então D_n é uma Álgebra booleana".
- concluímos que:
  - D_n é uma Álgebra Booleana se e somente se nenhum primo divide n mais do que uma vez.
- **Exemplo**: $40 = 2^3.5$ e $125 = 3.5^2$
  - Então: nem D_{40} nem D_{125} podem ser Álgebras Booleanas.

ÁLGEBRAS BOOLEANAS

- Final deste item.
- Dica: fazer exercícios sobre Álgebras Booleanas...