Álgebras Booleanas finitas

Gustavo Zambonin

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística
INE5601 — Fundamentos Matemáticos da Informática

gustavo.zambonin@posgrad.ufsc.br

Contexto

- Reticulados
  - *Poset* onde qualquer par de elementos tem supremo e ínfimo
  - Representado também como estrutura algébrica

Contexto

- Reticulados
  - *Poset* onde qualquer par de elementos tem supremo e ínfimo
  - Representado também como estrutura algébrica
- Isomorfismo entre reticulados
  - Função bijetora que mapeia elementos entre dois reticulados

Contexto

- Reticulados
  - *Poset* onde qualquer par de elementos tem supremo e ínfimo
  - Representado também como estrutura algébrica
- Isomorfismo entre reticulados
  - Função bijetora que mapeia elementos entre dois reticulados
- Tipos de reticulados
  - Limitado, complementado, distributivo

Contexto

- Reticulados
  - *Poset* onde qualquer par de elementos tem supremo e ínfimo
  - Representado também como estrutura algébrica
- Isomorfismo entre reticulados
  - Função bijetora que mapeia elementos entre dois reticulados
- Tipos de reticulados
  - Limitado, complementado, distributivo
  - Mapa de reticulados

Exemplos práticos

- Cálculo proposicional pode ser demonstrado logicamente equivalente a uma expressão Booleana

Exemplos práticos

- Cálculo proposicional pode ser demonstrado logicamente equivalente a uma expressão Booleana
- Modelagem de circuitos em engenharia elétrica, para representar estados de alta e baixa tensão
  - Criação de portas lógicas (AND, OR, NAND, NOR, XOR, XNOR)

Exemplos práticos

- Cálculo proposicional pode ser demonstrado logicamente equivalente a uma expressão Booleana
- Modelagem de circuitos em engenharia elétrica, para representar estados de alta e baixa tensão
  - Criação de portas lógicas (AND, OR, NAND, NOR, XOR, XNOR)
- Construção de caixas de substituição em criptografia simétrica, com funções Booleanas

Exemplos práticos

- Cálculo proposicional pode ser demonstrado logicamente equivalente a uma expressão Booleana
- Modelagem de circuitos em engenharia elétrica, para representar estados de alta e baixa tensão
  - Criação de portas lógicas (AND, OR, NAND, NOR, XOR, XNOR)
- Construção de caixas de substituição em criptografia simétrica, com funções Booleanas
- Ideia geral: formalismo para descrever operações lógicas

Reticulados de conjuntos sob inclusão

- Considere um *poset* $(\mathcal{P}(S), \subseteq)$, onde S é finito
  - $\forall t_1, t_2 \in \mathcal{P}(S)$,
    $\inf(\{t_1, t_2\}) = t_1 \cap t_2, \quad \sup(\{t_1, t_2\}) = t_1 \cup t_2$

Reticulados de conjuntos sob inclusão

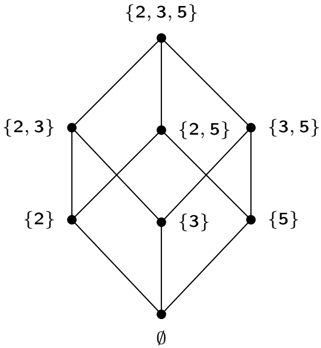
- Considere um *poset* $(\mathcal{P}(S), \subseteq)$, onde S é finito
  - $\forall t_1, t_2 \in \mathcal{P}(S)$,
    $\inf(\{t_1, t_2\}) = t_1 \cap t_2, \quad \sup(\{t_1, t_2\}) = t_1 \cup t_2$
- Tome $S_1 = \{x_1, \ldots, x_n\}, S_2 = \{y_1, \ldots, y_n\}$
  - Existe um isomorfismo f que mapeia
    $x_i \to y_i, i \in \{1, \ldots, n\}$
  - Para quaisquer subconjuntos $A, B \subseteq S$, então
    $A \subseteq B \Leftrightarrow f(A) \subseteq f(B)$

Reticulados de conjuntos sob inclusão

- Considere um *poset* $(\mathcal{P}(S), \subseteq)$, onde S é finito
  - $\forall t_1, t_2 \in \mathcal{P}(S)$,
    $\inf(\{t_1, t_2\}) = t_1 \cap t_2, \quad \sup(\{t_1, t_2\}) = t_1 \cup t_2$
- Tome $S_1 = \{x_1, \ldots, x_n\}, S_2 = \{y_1, \ldots, y_n\}$
  - Existe um isomorfismo f que mapeia
    $x_i \rightarrow y_i, i \in \{1, \ldots, n\}$
  - Para quaisquer subconjuntos $A, B \subseteq S$, então
    $A \subseteq B \Leftrightarrow f(A) \subseteq f(B)$
- Então, $(\mathcal{P}(S_1), \subseteq)$ e $(\mathcal{P}(S_2), \subseteq)$ são isomórficos

Exemplo

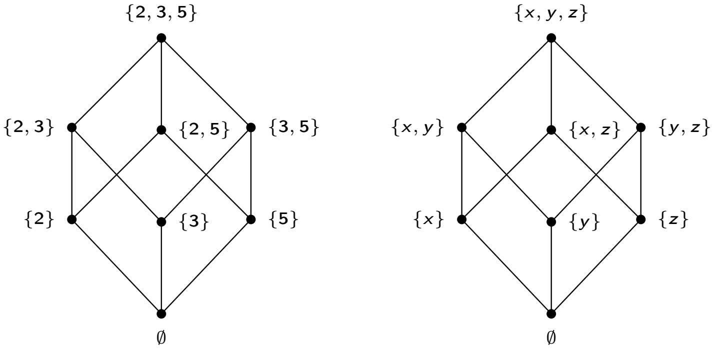
Isomorfismo entre reticulados



- Seja $S_1 = \{2,3,5\}, S_2 = \{x,y,z\}$, então $n = 3$

Exemplo

Isomorfismo entre reticulados



- Seja $S_1 = \{2, 3, 5\}, S_2 = \{x, y, z\}$, então $n = 3$
- $f : S_1 \to S_2$
  $f(\emptyset) = \emptyset,\ f(\{2\}) = \{x\},\ f(\{3\}) = \{y\},\ \ldots$

Reticulado $(\mathcal{P}(S), \subseteq)$ genérico

- Portanto, $(\mathcal{P}(S), \subseteq)$ independe de S
- Reticulado determinado apenas por $n = |S|$
  - O número de elementos do reticulado sempre será da forma $|\mathcal{P}(S)| = 2^n$

Reticulado $(\mathcal{P}(S), \subseteq)$ genérico

- Portanto, $(\mathcal{P}(S), \subseteq)$ independe de S
- Reticulado determinado apenas por $n = |S|$
  - O número de elementos do reticulado sempre será da forma $|\mathcal{P}(S)| = 2^n$
- É possível construir um reticulado genérico, composto de n-tuplas de 0 e 1, chamado B_n
  - 0 denota a ausência do elemento no subconjunto, e 1 a presença

Ordenamento em B_n

- Tome $x = x_1x_2\dots x_n, y = y_1y_2\dots y_n \in B_n$ quaisquer

Ordenamento em B_n

- Tome $x = x_1 x_2 \ldots x_n, y = y_1 y_2 \ldots y_n \in B_n$ quaisquer
  - Ordenação "lexicográfica":
    $x \preccurlyeq y \Leftrightarrow a_k \preccurlyeq b_k, k \in \{1, \ldots, n\}$

Ordenamento em B_n

- Tome $x = x_1x_2\ldots x_n, y = y_1y_2\ldots y_n \in B_n$ quaisquer
  - Ordenação "lexicográfica":
    $x \preccurlyeq y \Leftrightarrow a_k \preccurlyeq b_k, k \in \{1,\ldots,n\}$
  - $x \wedge y = s_1s_2\ldots s_n, \quad s_k = \min\left(a_k, b_k\right)$

Ordenamento em B_n

- Tome $x = x_1 x_2 \dots x_n, y = y_1 y_2 \dots y_n \in B_n$ quaisquer
  - Ordenação "lexicográfica":
    $x \preccurlyeq y \Leftrightarrow a_k \preccurlyeq b_k, k \in \{1, \dots, n\}$
  - $x \wedge y = s_1 s_2 \dots s_n, \quad s_k = \min(a_k, b_k)$
  - $x \vee y = z_1 z_2 \dots z_n, \quad z_k = \max(a_k, b_k)$

Ordenamento em B_n

- Tome $x = x_1 x_2 \ldots x_n, y = y_1 y_2 \ldots y_n \in B_n$ quaisquer
  - Ordenação "lexicográfica":
    $x \preccurlyeq y \Leftrightarrow a_k \preccurlyeq b_k, k \in \{1, \ldots, n\}$
  - $x \wedge y = s_1 s_2 \ldots s_n, \quad s_k = \min(a_k, b_k)$
  - $x \vee y = z_1 z_2 \ldots z_n, \quad z_k = \max(a_k, b_k)$
  - Complemento: se $z_k = 1, z'_k = 0$ e vice-versa

Ordenamento em B_n

- Tome $x = x_1x_2 \ldots x_n, y = y_1y_2 \ldots y_n \in B_n$ quaisquer
  - Ordenação "lexicográfica":
    $x \preccurlyeq y \Leftrightarrow a_k \preccurlyeq b_k, k \in \{1, \ldots, n\}$
  - $x \wedge y = s_1s_2 \ldots s_n, \quad s_k = \min(a_k, b_k)$
  - $x \vee y = z_1z_2 \ldots z_n, \quad z_k = \max(a_k, b_k)$
  - Complemento: se $z_k = 1, z_k' = 0$ e vice-versa
- Note que $(B_n, \preccurlyeq)$ é isomórfico a $(\mathcal{P}(S), \subseteq)$

Ordenamento em B_n

- Então, existe uma correspondência entre reticulados sob conjuntos e B_n, da seguinte forma
- Para quaisquer subconjuntos $A, B \in \mathcal{P}(S)$

Ordenamento em B_n

- Então, existe uma correspondência entre reticulados sob conjuntos e B_n, da seguinte forma
- Para quaisquer subconjuntos $A, B \in \mathcal{P}(S)$
  - $x \preccurlyeq y \Leftrightarrow A \subseteq B$

Ordenamento em B_n

- Então, existe uma correspondência entre reticulados sob conjuntos e B_n, da seguinte forma
- Para quaisquer subconjuntos $A, B \in \mathcal{P}(S)$
  - $x \preccurlyeq y \Leftrightarrow A \subseteq B$
  - $x \wedge y \Leftrightarrow A \cap B$

Ordenamento em B_n

- Então, existe uma correspondência entre reticulados sob conjuntos e B_n, da seguinte forma
- Para quaisquer subconjuntos $A, B \in \mathcal{P}(S)$
  - $x \preccurlyeq y \Leftrightarrow A \subseteq B$
  - $x \wedge y \Leftrightarrow A \cap B$
  - $x \vee y \Leftrightarrow A \cup B$

Ordenamento em B_n

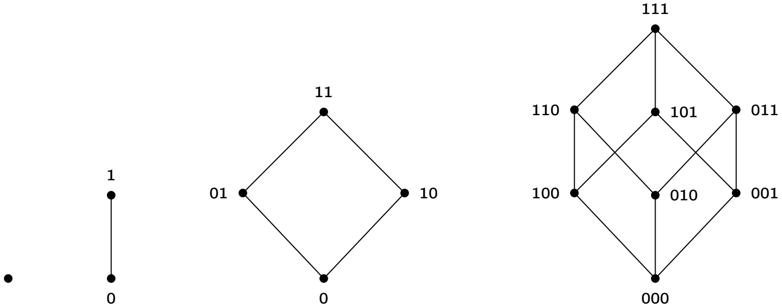
- Então, existe uma correspondência entre reticulados sob conjuntos e B_n, da seguinte forma
- Para quaisquer subconjuntos $A, B \in \mathcal{P}(S)$
  - $x \preccurlyeq y \Leftrightarrow A \subseteq B$
  - $x \wedge y \Leftrightarrow A \cap B$
  - $x \vee y \Leftrightarrow A \cup B$
  - $x' \Leftrightarrow \overline{A}$

Álgebras Booleanas finitas

- Um reticulado complementado distributivo é chamado de **álgebra Booleana**
- De maneira equivalente, um reticulado finito isomórfico a B_n é uma álgebra Booleana
- Note que é possível representar quaisquer reticulados $(\mathcal{P}(S), \subseteq)$ como $B_{|S|}$
  - Ou seja, todo reticulado isomórfico a $(\mathcal{P}(S), \subseteq)$ também é uma álgebra Booleana

Exemplo

Álgebras Booleanas finitas



- Álgebras Booleanas mais simples: B_0, B_1, B_2, B_3
- Número de elementos: $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8$

Outros reticulados isomórficos a B_n

- Reticulados que não são da forma $(\mathcal{P}(S), \subseteq)$ também podem ser álgebras Booleanas

Outros reticulados isomórficos a B_n

- Reticulados que não são da forma $(\mathcal{P}(S), \subseteq)$ também podem ser álgebras Booleanas
- Considere o reticulado D_n, onde S é composto pelos divisores de n e a relação parcial é de divisibilidade
  - $D_{30} = (\{1, 2, 3, 5, 6, 10, 15, 30\}, |)$

Outros reticulados isomórficos a B_n

- Reticulados que não são da forma $(\mathcal{P}(S), \subseteq)$ também podem ser álgebras Booleanas
- Considere o reticulado D_n, onde S é composto pelos divisores de n e a relação parcial é de divisibilidade
  - $D_{30} = (\{1, 2, 3, 5, 6, 10, 15, 30\}, |)$
- Observe que D_{30} é isomórfico a B_3

Outros reticulados isomórficos a B_n

- Reticulados que não são da forma $(\mathcal{P}(S), \subseteq)$ também podem ser álgebras Booleanas
- Considere o reticulado D_n, onde S é composto pelos divisores de n e a relação parcial é de divisibilidade
  - $D_{30} = (\{1, 2, 3, 5, 6, 10, 15, 30\}, |)$
- Observe que D_{30} é isomórfico a B_3
  - $f(1) = 000, f(2) = 100, f(3) = 010, f(5) = 001, f(6) = 110, f(10) = 101, f(15) = 011, f(30) = 111$

Determinação de álgebras Booleanas

- Todo reticulado que não tenha 2^n elementos não pode ser uma álgebra Booleana

Determinação de álgebras Booleanas

- Todo reticulado que não tenha 2^n elementos não pode ser uma álgebra Booleana
- Um reticulado com 2^n elementos é uma condição necessária, mas não suficiente

Determinação de álgebras Booleanas

- Todo reticulado que não tenha 2^n elementos não pode ser uma álgebra Booleana
- Um reticulado com 2^n elementos é uma condição necessária, mas não suficiente
  - É necessário demonstrar o isomorfismo com B_n ou $(\mathcal{P}(S), \subseteq)$
  - Comparar o diagrama de Hasse é possível para conjuntos pequenos

Determinação de álgebras Booleanas

- Todo reticulado não limitado não será álgebra Booleana

Determinação de álgebras Booleanas

- Todo reticulado não limitado não será álgebra Booleana
- Todo elemento deverá ter um único complemento

Determinação de álgebras Booleanas

- Todo reticulado não limitado não será álgebra Booleana
- Todo elemento deverá ter um único complemento
- O reticulado D_p, onde $p = p_1 \times p_2 \times \cdots \times p_k$, com $p_1 \neq p_2 \neq \cdots \neq p_k$, é álgebra Booleana?
  - $S = (\{p_1, \ldots, p_k\})$, então $D_p = (S, |)$

Determinação de álgebras Booleanas

- Todo reticulado não limitado não será álgebra Booleana
- Todo elemento deverá ter um único complemento
- O reticulado D_p, onde $p = p_1 \times p_2 \times \cdots \times p_k$, com $p_1 \neq p_2 \neq \cdots \neq p_k$, é álgebra Booleana?
  - $S = (\{p_1, \ldots, p_k\})$, então $D_p = (S, |)$
  - Note que existe um isomorfismo f, de modo que $\forall T \in \mathcal{P}(S),\ f(T) = t_1 \ldots t_k$

Determinação de álgebras Booleanas

- Todo reticulado não limitado não será álgebra Booleana
- Todo elemento deverá ter um único complemento
- O reticulado D_p, onde $p = p_1 \times p_2 \times \cdots \times p_k$, com $p_1 \neq p_2 \neq \cdots \neq p_k$, é álgebra Booleana?
  - $S = (\{p_1, \ldots, p_k\})$, então $D_p = (S, |)$
  - Note que existe um isomorfismo f, de modo que $\forall T \in \mathcal{P}(S),\ f(T) = t_1 \ldots t_k$
  - Portanto, D_p é uma álgebra Booleana

Identidades axiomáticas de álgebras Booleanas

- Defina uma álgebra Booleana como $(S, \vee, \wedge, \neg, \bot, \top)$
  - Ou seja, um conjunto finito S, operações binárias de junção e encontro, operação unária de complemento, elementos mínimo e máximo

Identidades axiomáticas de álgebras Booleanas

- Defina uma álgebra Booleana como $(S, \vee, \wedge, \neg, \bot, \top)$
  - Ou seja, um conjunto finito S, operações binárias de junção e encontro, operação unária de complemento, elementos mínimo e máximo
- Então, as leis abaixo são verdade
  - Associatividade, comutatividade, absorção, identidade, distributividade, complementação

Identidades axiomáticas de álgebras Booleanas

- Defina uma álgebra Booleana como $(S, \vee, \wedge, \neg, \perp, \top)$
  - Ou seja, um conjunto finito S, operações binárias de junção e encontro, operação unária de complemento, elementos mínimo e máximo
- Então, as leis abaixo são verdade
  - Associatividade, comutatividade, absorção, identidade, distributividade, complementação
- Note que estes axiomas são derivados das definições de reticulado limitado, distributivo e complementado

Identidades axiomáticas de álgebras Booleanas

- Outras três propriedades podem ser derivadas
- Para elementos quaisquer x, y de uma álgebra Booleana

Identidades axiomáticas de álgebras Booleanas

- Outras três propriedades podem ser derivadas
- Para elementos quaisquer x, y de uma álgebra Booleana
  - $\neg(\neg x) = x$ (lei da involução)

Identidades axiomáticas de álgebras Booleanas

- Outras três propriedades podem ser derivadas
- Para elementos quaisquer x, y de uma álgebra Booleana
  - $\neg(\neg x) = x$ (lei da involução)
  - $\neg(x \wedge y) = \neg x \vee \neg y$ (lei de De Morgan I)
  - $\neg(x \vee y) = \neg x \wedge \neg y$ (lei de De Morgan II)

Identidades axiomáticas de álgebras Booleanas

- Outras três propriedades podem ser derivadas
- Para elementos quaisquer x, y de uma álgebra Booleana
  - $\neg(\neg x) = x$ (lei da involução)
  - $\neg(x \wedge y) = \neg x \vee \neg y$ (lei de De Morgan I)
  - $\neg(x \vee y) = \neg x \wedge \neg y$ (lei de De Morgan II)
- Assim como em conjuntos, pois para S qualquer e $A, B \subseteq S$ quaisquer
  - $\overline{(\overline{A})}, \quad \overline{(A \cap B)} = \overline{A} \cup \overline{B}, \quad \overline{(A \cup B)} = \overline{A} \cap \overline{B}$

Material de estudo

Kolman, B., Busby, R., and Ross, S. (1999).
Discrete Mathematical Structures.
4th edition.

Rosen, K. H. (2011).
Discrete Mathematics and Its Applications.
7th edition.

- Kolman: leitura das páginas 217-223 (especialmente p. 222) e resolução dos exercícios 1-21
- Rosen: leitura das páginas 811-817 e resolução dos exercícios 1-4, 24-28