Notas de aula de MAC0329 – Álgebra Booleana e Aplicações

Nina S. T. Hirata
Depto. de Ciência da Computação – IME / USP

Este texto é uma referência-base para o curso de MAC0329 (Álgebra Booleana e Aplicações). No entanto, ele não constitui um livro-texto, no sentido de que muitas informações aparecem de forma suscinta, sem o apronfudamento desejável, e também porque ele pode conter alguns erros e talvez algumas omissões (não propositais). O material presente aqui deve ser comlementado com a leitura das referências indicadas, bem como através da resolução dos exercícios propostos.

Página da disciplina: `www.vision.ime.usp.br/~nina/cursos/mac0329-03/`

Conteúdo programado para o curso (2003)

Álgebra dos conjuntos
Cálculo proposicional
Álgebra Booleana - definição axiomática
Teoria de chaveamentos e aplicações em projeto lógico de circuitos digitais
Minimização de expressões booleanas
Circuitos combinacionais
Circuitos seqüenciais
Aplicações em processamento de imagens binárias (se sobrar tempo)
Álgebra de reticulados (se sobrar tempo)

Objetivos do curso

Este curso objetiva ensinar o que é algebra booleana, mostrar alguns exemplos de álgebra booleana, mostrar com quais problemas práticos ela se relaciona (principalmente projeto lógico de circutos digitais), mostrar de que forma ou por que a formalização teórica é util, e proporcionar oportunidades para o aluno exercitar a manipulação axiomática da álgebra.

Alguns termos / nomes

- **Álgebra**. Um ramo da matemática no qual operações aritméticas e relações são generalizadas através do uso de símbolos alfabéticos para representar números ou membros desconhecidos do conjunto de números.

  Qualquer cálculo abstrato, uma linguagem formal na qual as funções e operações podem ser definidas e suas propriedades estudadas. Exemplos : teoria dos conjuntos, álgebra da lógica.

- **Álgebra booleana** Sistema algébrico desenvolvido por George Boole para sistematizar o tratamento da lógica. Esse sistema permitiu que as relações lógicas fossem estudadas formalmente, sem as confusões e ambiguidades de uma linguagem natural.

- **Álgebra dos reticulados** Uma estrutura algébrica baseada em relação de ordens parciais que engloba a álgebra booleana como um caso particular.

- **George Boole** (1815-1864). Ver
  `http://www-history.mcs.st-andrews.ac.uk/history/References/Boole.html`

1 Álgebra dos conjuntos

A álgebra dos conjuntos é um exemplo de álgebra booleana que intuitivamente é relativamente simples de ser entendida. Por esta razão, ela será introduzida antes da introdução formal de álgebra booleana, com o objetivo de ajudar o entendimento de uma definição formal a ser apresentada mais adiante no curso.

Referências para esta parte do curso: capítulos 1 a 6 de [Filho, 1980], capítulo 2 de [Mendelson, 1977], capítulo 1 de [Whitesitt, 1961], capítulo sobre **conjuntos** de qualquer livro sobre Matemática Discreta (Discrete Mathematics) [Ross and Wright, 1992, Garnier and Taylor, 1992].

Conjuntos e elementos

Conjuntos são coleções de objetos, denominados elementos[1]

Exemplos de conjuntos

O conjunto de todos os números inteiros, o conjunto de todos os alunos de MAC0329 do semestre corrente, o conjunto de todos os seres humanos vivos atualmente, o conjunto de todos os números reais maiores que zero e menores que 1, o conjunto de todos os jogadores da seleção brasileira de futebol, o conjunto de todas as letras do alfabeto romano, etc.

Notação

Conjuntos serão representados por letras maiúsculas: A, B, C, S, etc. Elementos de um conjunto serão representados por letras minúsculas: a, b, x, y, etc.

Em geral podemos especificar um conjunto descrevendo os elementos, ou então enumerando os elementos, como nos seguintes exemplos:

$$\{x \in Z : x \text{ é par}\}$$

$$\{verde, amarelo, azul, branco\}$$

Conjuntos universo e vazio

Dois conjuntos especiais são o **conjunto universo**, isto é, o conjunto de todos os objetos em questão, e o **conjunto vazio**, isto é, o conjunto que não contém nenhum elemento. Os conjuntos universo e vazio são denotados, respectivamente, por U e $\emptyset$.

Conjunto unitário

Em álgebra de conjuntos, os objetos de interesse são os conjuntos e não os elementos que o formam. Assim, as operações devem ser definidas sobre ou entre conjuntos, mas nunca sobre elementos isolados. Para tratar elementos, devemos considerar conjuntos unitários. Por exemplo, se a é um elemento de U então $\{a\}$ denota o **conjunto unitário** que contém apenas um único elemento.

[1]Não é objetivo fazermos uma definição formal de conjunto. Por ora utilizaremos a noção intuitiva que nós temos (temos mesmo?)

Relação elemento $\times$ conjunto

Se um elemento x **pertence** a um conjunto A, escrevemos $x \in A$. Diremos, alternativamente, que x é **membro** de A. Se x não pertence ao conjunto A, escrevemos $x \notin A$.

Relação conjunto $\times$ conjunto

Um conjunto A é **igual** a um conjunto B, denotado $A = B$, se eles contém exatamente os mesmos elementos. Se não forem iguais, eles são **diferentes**, denotado $A \neq B$.

Um conjunto A está **contido** num conjunto B se todos os elementos de A pertencem também ao conjunto B. Escrevemos $A \subseteq B$ e dizemos também que A é um **subconjunto** de B. Se, além disso, B possui pelo menos um elemento que não pertence a A, então dizemos que A está **propriamente contido** em B, ou que A é subconjunto próprio de B, e denotamos $A \subset B$.

Propriedades da relação $\subseteq$

A relação de inclusão de conjuntos $\subseteq$ obedece às seguintes propriedades. Para quaisquer X, Y e Z,

- I1. (reflexiva) $X \subseteq X$
- I2. (transitiva) $X \subseteq Y$ e $Y \subseteq Z \Longrightarrow X \subseteq Z$
- I3. (anti-simétrica) $X \subseteq Y$ e $Y \subseteq X \Longrightarrow X = Y$
- I4.
  - (a) $\emptyset \subseteq X$
  - (b) $X \subseteq U$

Conjunto potência (power set) ou conjunto das partes de um conjunto

Dado um conjunto A, o **conjunto potência de** A é denotado por $\mathcal{P}(A)$ e definido por $\mathcal{P}(A) = \{X \subseteq U : X \subseteq A\}$, ou seja, $\mathcal{P}(A)$ é o conjunto de todos os subconjuntos de A.

Exercício: Mostre que se A contém n elementos então $\mathcal{P}(A)$ contém 2^n elementos.

Prova: Para $n = 0$ o resultado é óbvio. Suponha $n > 0$. Na escolha de um subconjunto X de A, existem duas possibilidades para cada elemento $x \in A$: ou $x \in X$ ou $x \notin X$. Como o fato de x estar ou não em X independe do fato de qualquer outro elemento y de A estar ou não em X, então existem 2^n formas de se escolher um subconjunto de A.

Exercício: Seja $A = \{a, b, c\}$. Liste todos os elementos de $\mathcal{P}(A)$.

Complemento, união e interseção

O **complemento** de um conjunto X, denotado X^c, consiste de todos os elementos em U que não estão em X, ou seja, $X^c = \{x \in U : x \notin X\}$.

Conjuntos podem ser combinados para gerar outros conjuntos. Para isso, podemos considerar duas regras (operações) que definem formas pelas quais conjuntos podem ser combinados: a **união** e a **interseção**.

Dados dois conjuntos X e Y quaisquer, a **união** de X e Y é denotada $X \cup Y$ e definida como sendo o conjunto de elementos que pertencem ou a X, ou a Y ou a ambos, ou seja, $X \cup Y = \{x \in U : x \in X \text{ ou } x \in Y\}$. A **interseção** de X e Y é denotada $X \cap Y$ e definida como sendo o conjunto de elementos que pertencem tanto a X como a Y, ou seja, $X \cap Y = \{x \in U : x \in X \text{ e } x \in Y\}$.

Se $X \cap Y = \emptyset$ então dizemos que X e Y são disjuntos.

Exemplos:

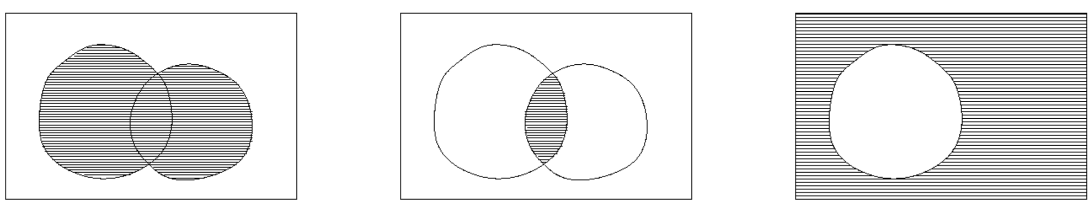
$\{1,2,3\} \cup \{2,4,6\} = \{1,2,3,4,6\}$ $\{1,2,3\} \cap \{2,4,6\} = \{2\}$

$\{a\} \cup \{b\} = \{a,b\}$ $\{a\} \cap \{b\} = \emptyset$

Diagramas de Venn

Os diagramas de Venn são úteis para reforçar a noção intuitiva sobre conjuntos, principalmente para analisar relações entre os conjuntos e também seus membros. Para demonstrar propriedades dos conjuntos, uma prova estritamente algébrica seria necessária. No entanto, para entender uma propriedade e, mais do que isso, para nos convencermos de sua validade, os diagramas de Venn são bastante úteis.

No diagrama de Venn o conjunto universo é representado por um retângulo, isto é, 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. 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.



(a) (b) (c)

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

Exercício: Seja x um elemento no conjunto universal e X e Y dois conjuntos quaisquer. Mostre que x é membro de apenas um dos conjuntos $X \cap Y$, $X \cap Y^c$, $X^c \cap Y$ e $X^c \cap Y^c$.

Dica: Desenhe o diagrama de Venn e argumente.

Leis fundamentais

Dados conjuntos X, Y, Z quaisquer, utilize diagramas de Venn para convencer-se da validade das seguintes leis.

- L1. Comutativa

- (a) $X \cap Y = Y \cap X$
- (b) $X \cup Y = Y \cup X$

- L2. Associativa
  - (a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$
  - (b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$
- L3. Distributiva
  - (a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
  - (b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$
- L4. Idempotência
  - (a) $X \cap X = X$
  - (b) $X \cup X = X$
- L5. Absorção
  - (a) $X \cap (X \cup Y) = X$
  - (b) $X \cup (X \cap Y) = X$
- L6. Complementação
  - (a) $X \cap X^c = \emptyset$
  - (b) $X \cup X^c = U$
- L7. Complementação dupla
  - $(X^c)^c = X$
- L8. De Morgan
  - (a) $(X \cap Y)^c = X^c \cup Y^c$
  - (b) $(X \cup Y)^c = X^c \cap Y^c$
- L9. Operações com $\emptyset$ e U
  - (a) (Elemento neutro) $U \cap X = X$ e $\emptyset \cup X = X$
  - (b) $\emptyset \cap X = \emptyset$ e $U \cup X = U$
  - (c) $\emptyset^c = U$ e $U^c = \emptyset$

As igualdades das leis acima podem ser mostradas via uso de diagramas de Venn, ou mostrando que o conjunto do lado esquerdo está contido no do lado direito e vice-versa, ou ainda via transformações lógicas (ver exemplo mais adiante).

Note que $X \cup Y = (X^c \cap Y^c)^c$. Isto implica que o operador $\cup$ poderia ser dispensado. Maiores detalhes sobre isso serão vistos oportunamente. Enquanto isso, vale a pena mencionarmos que embora não necessário, o uso dos três operadores é conveniente.

Algumas leis são semelhantes aos da álgebra dos números. No entanto, na álgebra dos conjuntos não existem, como na álgebra usual, expressões do tipo $2X$ ou X^2 e algumas leis como as de número 3b, 4 e 5 não são válidas na álgebra dos números.

Observe também que a maior parte das leis aparece aos pares. Iremos ver mais adiante que isso está ligado ao princípio da dualidade.

Exercício: Prove ou mostre via diagramas de Venn a validade das leis L3, L5 e L8 acima.

Como exemplo, vamos mostrar a validade da lei L3(a), isto é, $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$. Primeiramente pelo diagrama de Venn, o conjunto $X \cap (Y \cup Z)$ corresponde à região hachurada por linhas verticais e horizontais na figura 2a. Esta coincide com a região hachurada no diagrama mais a direita da figura 2b, que representa o conjunto $(X \cap Y) \cup (X \cap Z)$.

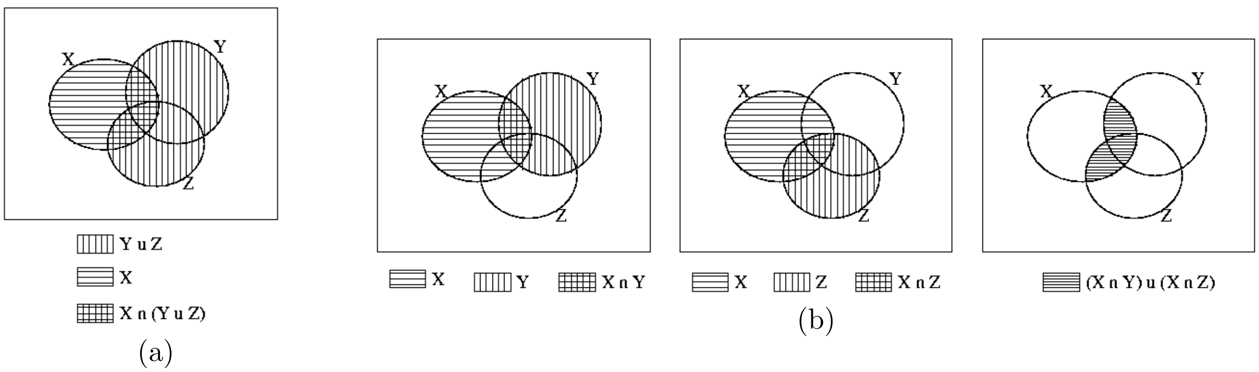


Figura 2: (a) $X \cap (Y \cup Z)$. (b) $(X \cap Y) \cup (X \cap Z)$.

Vamos mostrar que $X \cap (Y \cup Z) \subseteq (X \cap Y) \cup (X \cap Z)$ e que $(X \cap Y) \cup (X \cap Z) \subseteq X \cap (Y \cup Z)$. Considere $x \in X \cap (Y \cup Z)$. Então $x \in X$. Além disso, $x \in Y \cup Z$. Isso significa que ou $x \in Y$, e neste caso $x \in X \cap Y$, ou $x \in Z$, e neste caso $x \in X \cap Z$. Logo, $x \in (X \cap Y) \cup (X \cap Z)$.

Por outro lado, considere $y \in (X \cap Y) \cup (X \cap Z)$. Então, ou $y \in (X \cap Y)$ ou $y \in (X \cap Z)$. Se $y \in (X \cap Y)$, então $y \in X$ e $y \in Y$, o que implica que $y \in Y \cup Z$ e portanto, $y \in X \cap (Y \cup Z)$. De forma similar, se $y \in (X \cap Z)$, então $y \in X$ e $y \in Z$, de modo que $y \in Y \cup Z$ e portanto, $y \in X \cap (Y \cup Z)$.

Algebricamente,

$$
\begin{aligned}
X \cap (Y \cup Z) &= \{x : x \in X \text{ e } x \in Y \cup Z\} \\
&= \{x : x \in X \text{ e } (x \in Y \text{ ou } x \in Z)\} \\
&= \{x : (x \in X \text{ e } x \in Y) \text{ ou } (x \in X \text{ e } x \in Z)\} \\
&= \{x : x \in X \cap Y \text{ ou } x \in X \cap Z\} \\
&= (X \cap Y) \cup (X \cap Z)
\end{aligned}
$$

Exercício: A seguintes generalizações das leis de De Morgan são válidas ? Explique sua resposta.

$$(A_1 \cup A_2 \cup \cdots \cup A_n)^c = A_1^c \cap A_2^c \cap \cdots \cap A_n^c$$

$$(A_1 \cap A_2 \cap \cdots \cap A_n)^c = A_1^c \cup A_2^c \cup \cdots \cup A_n^c$$

<u>Exercício</u>: Desenhe a relação $X \subseteq Y$ num diagrama de Venn. Quais igualdades envolvendo os conjuntos X e Y são verdadeiras quando $X \subseteq Y$? Liste pelo menos três.

Outras propriedades

Para quaisquer conjuntos X, Y e Z, as seguintes propriedades são verdadeiras:

- P1(a) $X \cap Y \subseteq X$ e $X \cap Y \subseteq Y$
- P1(b) $X \subseteq X \cup Y$ e $Y \subseteq X \cup Y$
- P2(a) $X \cap Y = X$ sse $X \subseteq Y$
- P2(b) $X \cup Y = Y$ sse $X \subseteq Y$
- P3(a) $X = Y$ sse ($X \subseteq Y$ e $Y \subseteq X$)
- P3(b) $X = Y$ sse $X^c = Y^c$

<u>Exercício</u>: Mostre que $A \cap (A \cup B) = A$.

Por P1(b), sabemos que $A \subseteq A \cup B$. Mas então, por P2(a) $A \subseteq A \cup B$ implica que $A \cap (A \cup B) = A$.

<u>Exercício</u>: Dados dois conjuntos X e Y a **diferença** deles é definida por $X \setminus Y = \{x \in U : x \in X \text{ e } x \notin Y\}$ e a **diferença simétrica** entre eles é definida por $X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$. Expresse estes conjuntos em termos das operações de complementação, união e interseção (deduza a partir do diagrama de Venn).

Obs.: Na presença dos operadores $\cup$, $\cap$ e ^{c}, não há necessidade dos operadores $\setminus$ e Δ. No entanto, estes operadores podem ser práticos.

Simplificação de expressões

> As operações $\cup$, $\cap$ e ^{c} podem ser utilizadas para combinar conjuntos de várias formas. A combinação pode ser representada por uma expressão que descreve como os conjuntos foram combinados. Assim como a combinação de conjuntos resulta em um conjunto, uma expressão que descreve uma combinação de conjuntos representa um conjunto (aquele que resulta após as combinações serem executadas).
>
> Como vimos no caso de algumas leis, existem diferentes formas para se expressar um mesmo conjunto. Por exemplo, vimos que $X = X \cup X$. Ou ainda, $(X \cup Y)^c = X^c \cap Y^c$. Assim sendo, surge a possibilidade de estudarmos diferentes formas de expressão de conjuntos. Expressões podem ser expandidas, fatoradas, simplificadas aplicando-se as leis fundamentais.

Exemplo: Mostramos a simplificação da expressão $[(A \cap B) \cup (A \cap B^c)] \cap (A^c \cup B)$.

$$\begin{aligned}
[(A \cap B) \cup (A \cap B^c)] \cap (A^c \cup B) &= [A \cap (B \cup B^c)] \cap (A^c \cup B) \\
&= (A \cap U) \cap (A^c \cup B) \\
&= A \cap (A^c \cup B) \\
&= (A \cap A^c) \cup (A \cap B) \\
&= \emptyset \cup (A \cap B) \\
&= A \cap B
\end{aligned}$$

Exercício: Simplifique as seguintes expressões:
a) $(A \cap B^c)^c \cup (B \cap C)$
b) $[(A \cup B) \cap (A \cup B^c)] \cap (A \cup B)$
c) $(A \cap B \cap C) \cup (A \cap B \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B \cap C^c)$
d) $(A \cup B) \cap (A \cup B^c) \cap (A^c \cup B)$

Exercício: Verifique se as seguintes igualdades / afirmações são válidas. Justifique (pode ser via diagrama de Venn) ou mostre um contra-exemplo
a) $(A \cap B) \cup B = B$
b) $(A \cap C) \cap (B \cup C) = A \cap C$
c) Se $A \cup B = A \cup C$ então $B = C$
d) $A \cap (B \cup C) = (A \cap B) \cup C$
e) $A \cup B = (A^c \cap B^c)^c$
f) $(A \cup B^c) \cap (A^c \cup B) \cap (A^c \cup B^c) = A^c \cup B^c$
g) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$
h) $A \cap B = A \setminus (A \setminus B)$
i) $X \setminus X = \emptyset$
j) $X \setminus \emptyset = X$
k) $\emptyset \setminus X = \emptyset$
l) $(X \setminus Y) \setminus Z = X \setminus (Y \cup Z)$
m) $(X \setminus Y) \setminus Z = (X \setminus Z) \setminus Y$
n) $X \setminus Y = X \cap Y^c$
o) $(A \setminus B)^c = B \cup A^c$
p) $(A \setminus B) \cap C = (A \cap C) \setminus B$
q) $X \Delta X = \emptyset$
r) $X \Delta Y = Y \Delta X$
s) $X \Delta \emptyset = X$
t) $X \Delta Y = (X \cap Y^c) \cup (X^c \cap Y)$
u) $X \cap (Y \Delta Z) = (X \cap Y) \Delta (X \cap Z)$
v) $X \cup (Y \Delta Z) = (X \cup Y) \Delta (X \cup Z)$
x) Se $A \subseteq B$ e $A \subseteq C$ então $A \subseteq B \cap C$

Produto cartesiano

Sejam A e B dois conjuntos não vazios. O produto cartesiano de A e B, denotado $A \times B$, é o conjunto de todos os pares ordenados (x, y) tais que o primeiro elemento x pertence a A e o segundo elemento y pertence a B.

$$A \times B = \{(x, y) : x \in A \text{ e } y \in B\}$$

Generalizando, dados n conjuntos A_1, A_2,..., A_n, o produto cartesiano destes n conjuntos é dado por

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1 \text{ e } a_2 \in A_2 \text{ e } \ldots \text{ e } a_n \in A_n\}$$

Quando $A_i = A_j$ para quaisquer i e j, denota-se o produto cartesiano acima também por A^n.

<u>Exercício</u>: Seja $B = \{0, 1\}$. Liste todos os elementos do produto cartesiano $B \times B \times B$.

Relações binárias e funções

Sejam A e B dois conjuntos não vazios. Uma relação binária R sobre A e B é um subconjunto de $A \times B$, isto é, $R \subseteq A \times B$.

Dizemos que y é correspondente de x pela relação R se $(x, y) \in R$, e denotamos xRy (lê-se x-erre-y).

Uma relação binária $f \subseteq A \times B$ é uma função de A em B se para todo $x \in A$ existe um único $y \in B$ tal que $(x, y) \in f$. A função é denotada $f : A \to B$ e em vez de xfy denotamos $f(x) = y$.

<u>Exercício</u>: Explique o que são funções sobrejetoras, injetoras e bijetoras.

Resumo da seção

Nesta seção foram abordados os seguintes conceitos / tópicos :

- Conjuntos, elementos e relação de pertinência
- Conjuntos universo e vazio, subconjuntos, e inclusão e igualdade de conjuntos
- Propriedades da relação de inclusão
- Operações sobre conjuntos (união, interseção e complementação)
- As leis fundamentais
- Diagrama de Venn
- Expressão, equivalência e simplificação de expressões
- Produto cartesiano, relações binárias e funções

Referências

[Filho, 1980] Filho, E. A. (1980). *Teoria Elementar dos Conjuntos*. Livraria Nobel S.A., São Paulo.

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

[Mendelson, 1977] Mendelson, E. (1977). *Álgebra Booleana e Circuitos de Chaveamento*. Mcgraw-Hill.

[Ross and Wright, 1992] Ross, K. A. and Wright, C. R. B. (1992). *Discrete Mathematics*. Prentice Hall, 3rd edition.

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