Specification	BA	
Sorts	B	
Constants	$0, 1 \ : \ \mathrm{B}$	
	$\bar{} \ : \ \mathrm{B} \to \mathrm{B}$	
	$+, \cdot \ : \ \mathrm{B} \to \mathrm{B} \to \mathrm{B}$	
Axioms		
Commutativity	$xy = yx$	$x + y = y + x$
Assocativity	$(xy)z = x(yz)$	$(x + y) + z = x + (y + z)$
Distributivity	$x(y + z) = xy + xz$	$x + yz = (x + y)(x + z)$
Identity	$x1 = x$	$x + 0 = x$
Complement	$x\bar{x} = 0$	$x + \bar{x} = 1$

Figure 3: Specification BA

5 Boolean Algebra

Boolean Algebra is a theory that originated with the work of George Boole (Laws of Thought, 1854). Boole's goal was an axiomatization of the logical operations conjunction, disjunction and negation. As it turned out, Boole's axioms are also satisfied by the set operations intersection, union and complement. Historically, Boole's work was the first investigation of abstract algebras, and it preceded Cantor's invention of set theory.

5.1 The Specification

Our starting point is the specification BA in Figure 3, which employs the following constants:

$$0, 1 : B$$

$$\bar{} : B \to B \qquad \text{negation}$$

$$+, \cdot : B \to B \to B \qquad \text{disjunction, conjunction}$$

For $+$ and $\cdot$ we use infix notation, where $\cdot$ takes precedence over $+$. We also write st for $s \cdot t$, which gives us $x + yz = x + (y \cdot z) = (+)x((\cdot)yz)$. This somewhat daring notation will work fine as long as all variables have type B, which usually will be the case.

The models of BA are known as **Boolean Algebras**. The **two-valued Boolean algebra** $\mathcal{T}$ is the structure that interprets the sort B as $\mathbb{B} = \{0, 1\}$, the constants

0 and 1 as their names suggest, the functional constant $\bar{}$ as negation, and $+$ and $\cdot$ as disjunction and conjunction. It is easy to see that $\mathcal{T}$ is a proper model of BA.

We now come to the models of BA that interpret the functional constants as set operations. To obtain such a model, we start from any set X. Now we interpret the sort B as the set of all subsets of X (the power set of X). The basic constants 0 and 1 are interpreted as $\emptyset$ and X. The functional constants $\bar{}$, $+$, and $\cdot$ are interpreted as the set operations complement with respect to X, union and intersection. The verification that the thus obtained structure $\mathcal{P}_X$ is a model of BA is not difficult. The Boolean algebras $\mathcal{P}_X$ are known as **power set algebras**.

Exercise 5.1 How would you prove BA $\nvdash 0 = 1$?

The symmetric presentation of the axioms of BA in Figure 3 exhibits a prominent duality of BA:

Proposition 5.2 The substitution $\delta = \{0{:=}1,\ 1{:=}0,\ +{:=}\cdot,\ \cdot{:=}+\}$ is a duality of BA that satisfies $\mathbf{S}\delta(\mathrm{BA}) = \mathrm{BA}$ and $\mathbf{S}\delta(\mathbf{S}\delta s) = s$.

We will use the notation $\hat{s} := \mathbf{S}\delta s$ and call $\hat{s}$ the **dual** of s. For equations, the duals $\hat{e}$ are defined analogously. Observe, that BA contains e if and only if it contains $\hat{e}$.

A **Boolean variable** is a variable of type B. A **Boolean parameter** is a constant of type B that are different from 0, 1. In this chapter, we adopt the following conventions:

- x, y, z denote Boolean variables.
- a, b, c denote Boolean parameters.

The set BT of **Boolean terms** is defined recursively as follows:

$$s \in BT \subseteq Ter \ ::= \ x \ | \ a \ | \ 0 \ | \ 1 \ | \ \bar{s} \ | \ s+s \ | \ s \cdot s$$

A **Boolean equation** is an equation $s = t$ where s and t are Boolean terms. Note that every axiom of BA is a Boolean equation. A **tautology** is a Boolean equation that is deducible from BA (i.e., BA $\vdash e$). Two Boolean terms s, t are **equivalent** if $s = t$ is a tautology.

Eventually, we will prove that

$$\mathrm{BA} \vDash e \iff \mathrm{BA} \vdash e \iff \mathcal{B} \vDash e$$

holds for every Boolean equation e and every proper model $\mathcal{B}$ of BA. This surprising result says that BA axiomatizes exactly those Boolean equations that are valid in any non-trivial power set algebra, and also exactly those Boolean equations that are valid in the two-valued Boolean algebra $\mathcal{T}$. Since $\mathcal{T}$ is finite (i.e.,

Algebraic Specifications

BA is a typical example of an algebraic specification. Algebraic specifications make only restricted use of functional types. They have limited expressivity and enjoy special properties. We define algebraic specifications as follows.

An **algebraic constant** is a constant whose type has the form

$$C_1 \to \cdots \to C_n \to C$$

where $n \geq 0$ and $C_1, \ldots, C_n$ and C are sorts. In other words, an algebraic constant is a constant that doesn't take functional arguments. An **algebraic variable** is a variable with a non-functional type (i.e., a sort). The set of **algebraic terms** is defined recursively:

1. Every algebraic variable is an algebraic term.
2. If $c : C_1 \to \cdots \to C_n \to C$ is an algebraic constant and $s_1 : C_1, \ldots, s_n : C_n$ are algebraic terms, then $cs_1 \ldots s_n$ is an algebraic term.

An **algebraic equation** is an equation $s = t$ where s and t are algebraic terms. An **algebraic specification** is a specification whose axioms are algebraic.

only two values for Boolean variables), the equivalences also provide us with an algorithm that decides $\mathrm{BA} \vDash e$ and $\mathrm{BA} \vdash e$.

A famous result of Boolean Algebra is Stone's Representation Theorem (1936), which says that every finite Boolean algebra is isomorphic to a power set algebra, and that every infinite Boolean algebra is isomorphic to a subalgebra of a power set algebra.

Exercise 5.3 Is there a Boolean algebra with 7 elements?

The specification BA is not minimal. In J. Eldon Whitesitt's *Boolean Algebra and its applications* (Addison Wesley, 1961) you will find a proof that the assocativity axioms are deductive consequences of the other axioms.

There exist many equivalent specifications of Boolean Algebra. Here is one due to Huntington and Robbins (1933) that consists of only four axioms:

$$\begin{aligned} x + y &= y + x \\ (x + y) + z &= x + (y + z) \\ xy &= \overline{\bar{x} + \bar{y}} \\ (x + y)(x + \bar{y}) &= x \end{aligned}$$

Idempotence	$xx = x$	$x + x = x$
Dominance	$0x = 0$	$1 + x = 1$
Absorption	$x(x + y) = x$	$x + xy = x$
Negation	$\bar{1} = 0$	$\bar{0} = 1$
de Morgan	$\overline{xy} = \bar{x} + \bar{y}$	$\overline{x + y} = \bar{x}\bar{y}$
Resolution	$xy + \bar{x}z = xy + \bar{x}z + yz$	$(x + y)(\bar{x} + z) = (x + y)(\bar{x} + z)(y + z)$
Involution	$\bar{\bar{x}} = x$	

Figure 4: Some useful tautologies

Let's call this specification HR. It's easy to see that BA $\vdash$ HR (see next section). However, it took until 1996 that William McCune could prove the other direction HR $\vdash$ BA with the help of an automated theorem prover. From this we learn that deciding whether two specifications are equivalent can be extremely difficult.

You will find lots of interesting information about Boolean algebras in the Web (start with Wickipedia).

5.2 Boolean Laws

The more tautologies one knows the easier it becomes to deduce new tautologies. Figure 4 collects some useful tautologies that together with the axioms in Figure 3 form a collection of equations we call **Boolean laws**.

This section will show you how the tautologies in Figure 4 can be deduced from the axioms of BA. This way you get familiar with the deductive structure of BA. We start with a conversion proof for BA $\vdash xx = x$:

$$\begin{aligned} xx &= xx + 0 && \text{Identity} \\ &= xx + x\bar{x} && \text{Complement} \\ &= x(x + \bar{x}) && \text{Distributivity} \\ &= x1 && \text{Complement} \\ &= x && \text{Identity} \end{aligned}$$

The proof uses the Commutativity and Assocativity tacitly and mentions the use of the other axioms explicitly. By duality (Proposition 4.15), the proof also shows that $x + x = x$ is a tautology (since $x + x = x$ is the dual of $xx = x$).

Exercise 5.4 Show that Dominance, Absorption, and Resolution are deducible from BA. We offer the following hints:

a) To show $0x = 0$, start with $0x = 0x + 0$, then use complements.

b) To show $x = x(x + y)$, start with $x = x + 0$, then use Dominance and Distributivity.
c) To show $xy + \bar{x}z = xy + \bar{x}z + yz$, start from left and use Absorption in the form of $x = x(x + y)$ and $\bar{x} = \bar{x}(\bar{x} + y)$, then use Idempotence and Complement.

Proposition 5.5 BA, $0{=}1 \vdash x{=}y$

Proof Follows with Identity and Dominance. ∎

The proposition implies that no proper Boolean Algebra equates 0 and 1.

To prove that Negation, de Morgan, and Involution are tautologies, we will employ a notion of deductive equivalence:

$$E \overset{\text{BA}}{\vdash\dashv} E' \;:\Longleftrightarrow\; \text{BA} \cup E \vdash E' \;\wedge\; \text{BA} \cup E' \vdash E \qquad \textbf{deductive equivalence in } \text{BA}$$

Proposition 5.6 (Uniqueness of Complements (UoC))
$ab = 0,\; a + b = 1 \;\overset{\text{BA}}{\vdash\dashv}\; \bar{a} = b$

The proposition is formulated with a notational convenience that omits the curly braces in the official formulation $\{ab = 0,\; a + b = 1\} \overset{\text{BA}}{\vdash\dashv} \{\bar{a} = b\}$.

Exercise 5.7 Find a proof for UoC.

With UoC, we can prove BA $\vdash \bar{s} = t$ by proving BA $\vdash st = 0$ and BA $\vdash s + t = 1$ (by Stability, Proposition 4.13). Thus to prove that the involution law $\bar{\bar{x}} = x$ is a tautology it suffices to show that $\bar{x}x = 0$ and $\bar{x} + x = 1$ are tautologies. This can be done with the complement laws.

Exercise 5.8 Prove that Negation and de Morgan are tautologies (see Figure 4).

Proposition 5.9 (Zero-One (0-1)) If s is a Boolean term that contains neither Boolean variables nor Boolean parameters, then BA $\vdash s = 0$ or BA $\vdash s = 1$.

Proof By induction on $|s|$ with Negation, Identity, Dominance and Commutativity. ∎

We arrange the following notations:

$s \to t$	$\rightsquigarrow$	$\bar{s} + t$	**implication**
$s \leftrightarrow t$	$\rightsquigarrow$	$(s \to t)(t \to s)$	**equivalence**

Note that $\leftrightarrow$ describes the identity function for $\mathbb{B}$ if we take the two-valued Boolean algebra $\mathcal{T}$ as interpretation. To save parentheses, we employ the operator precedence $\cdot \succ + \succ \to \succ \leftrightarrow$.

Equation Systems

We can see $\{ab = 0,\ a + b = 1\}$ as an *equation system* where the parameters a and b take the role of *unknowns*. Because of their generative nature, variables are not suited as unknowns if more than one equation is involved.

A deductive equivalence $E \overset{\mathrm{BA}}{\vdash\dashv} E'$ tells us that the equation systems E and E' have the same solutions for the parameters in a given Boolean algebra. UoC tells us that the system $\{ab = 0,\ a + b = 1\}$ has the same solutions as $\{\bar{a} = b\}$. The equivalences (a) and (c) of Exercise 5.11 give us a method that allows us to transform a finite Boolean equation system E into a single term s such that $E \overset{\mathrm{BA}}{\vdash\dashv} \{s = 1\}$.

Exercise 5.10 Show that the following equations are tautologies:

a) $1 \to x = x, \quad x \to 0 = \bar{x}$

b) $0 \to x = 1, \quad x \to 1 = 1$

c) $x \to x = 1$ reflexivity

d) $x \to y = \bar{y} \to \bar{x}$ contraposition

e) $x = \bar{x} \to 0$ contradiction

f) $xy \to z = x \to y \to z$ Schönfinkel

g) $x + y = (x \to y) \to y$

h) $x \leftrightarrow y = xy + \bar{x}\bar{y}$

Exercise 5.11 Prove the following deductive equivalences. You may use all Boolean laws.

a) $a = 1,\ b = 1 \ \overset{\mathrm{BA}}{\vdash\dashv}\ ab = 1$

b) $a \to b = 1 \ \overset{\mathrm{BA}}{\vdash\dashv}\ a = ab$

c) $a \leftrightarrow b = 1 \ \overset{\mathrm{BA}}{\vdash\dashv}\ a = b$

Equivalences (a) and (c) state interesting properties of Boolean algebras. They say that in a Boolean algebra an equation $s = t$ is equivalent to the "normalized" equation $s \leftrightarrow t = 1$, and that two normalized equations $s = 1$ and $t = 1$ can be combined into the normalized equation $s \cdot t = 1$.