A hierarchy of algebras for Boolean subsets

Walter Guttmann, Bernhard Möller

Angaben zur Veröffentlichung / Publication details:

Guttmann, Walter, and Bernhard Möller. 2020. "A hierarchy of algebras for Boolean subsets." *Lecture Notes in Computer Science* 12062: 152–68. https://doi.org/10.1007/978-3-030-43520-2_10.

A Hierarchy of Algebras for Boolean Subsets

Walter Guttmann[1] and Bernhard Möller[2]

[1] Department of Computer Science and Software Engineering,
University of Canterbury, Christchurch, New Zealand
walter.guttmann@canterbury.ac.nz
[2] Institut für Informatik, Universität Augsburg, Augsburg, Germany
bernhard.moeller@informatik.uni-augsburg.de

Abstract. We present a collection of axiom systems for the construction of Boolean subalgebras of larger overall algebras. The subalgebras are defined as the range of a complement-like operation on a semilattice. This technique has been used, for example, with the antidomain operation, dynamic negation and Stone algebras. We present a common ground for these constructions based on a new equational axiomatisation of Boolean algebras. All results are formally proved in Isabelle/HOL.

1 Introduction

Boolean algebras abound in formal approaches to program semantics as well as algorithm derivation and verification. Often such an algebra arises as a subalgebra of some overall algebra for the problem at hand. There are various methods of defining a Boolean substructure, for example, introducing a special type or sort for the subalgebra and then stipulating one of the standard Boolean algebra axiom sets for it. However, the extra type may get into the way of automatic verification with tools that only support a single sort. Then the Boolean sort has to be simulated by a characterising predicate, and many otherwise equational formulas need to be enriched by a premise involving that predicate. This complicates specifications and may hamper efficient automatic treatment.

Therefore a different approach has been studied: enrich the algebra with a special operation leading into the intended subalgebra and add sufficiently many axioms to guarantee that the range of that operation has a Boolean structure. Examples for this are the antidomain operation in idempotent (left) semirings [10–12], dynamic negation [21], the operation yielding tests in [17, 19], and the pseudocomplement operation in Stone algebras [13, 16, 18].

The axiomatisations in these examples are all similar since they follow the same goal. The aim of the present paper is to exhibit a ground pattern for them and so allow a more unified treatment. For instance, the common structure of the seemingly disparate topics of Stone algebras and antidomain semirings is exhibited. To this end we first propose a succinct yet understandable set of axioms for Boolean algebras. Imposing these on the range of the complement operation, we develop a hierarchy of algebras with a Boolean subalgebra and further structure overall. The hierarchy ultimately specialises to antidomain semirings and Stone algebras.

The contributions of this paper are as follows:

- Formally verified proofs of Byrne's axiomatisations of Boolean algebras in Sections 4.1 and 4.2.
- A new and formally verified axiomatisation of Boolean algebras, which is equational and based on join and complement, in Section 4.3.
- A hierarchy of algebras each with a subset that forms a Boolean algebra and successively stronger assumptions for the overall set in Section 6. Stone algebras arise as a specialisation of this hierarchy in Section 7. One of the algebras corresponds to antidomain semirings as shown in Section 8.

All results have been formally verified in Isabelle/HOL [31]. Due to their extent the proofs are omitted in this paper. They can be found in the Isabelle/HOL theory file at http://www.csse.canterbury.ac.nz/walter.guttmann/algebra/.

In Sections 3 and 4 we review various axiomatisations of Boolean algebras from the literature and present a new equational one tailored to our needs. Section 5 adapts this for the above-mentioned construction of Boolean subalgebras of larger overall algebras. In Section 6 we add successively stronger assumptions to the overall algebra. Sections 7 and 8 show how Stone algebras and antidomain semirings fit into this hierarchy.

2 Related Work

Boolean algebras have been extensively studied in the literature. In the following we discuss a selection of related works.

Some approaches build Boolean algebras on a hierarchy of more basic algebraic structures, for example, as complemented distributive lattices [2]. Other approaches are based on fewer operations and axioms, and introduce further operations of Boolean algebras by definitions. For example, one of Huntington's axiomatisations uses just the operations of join and complement with three equational axioms [22].

Huntington postulates that join is associative and commutative, but the third axiom is quite complex and not handy for manual proofs. There have been attempts to replace this axiom. Byrne [5] substitutes an equivalence, as detailed in Section 4, and also combines associativity and commutativity into one equational axiom. A related axiomatisation was proposed by Frink [14]. A later axiomatisation based on join and complement [28] uses the following two equations:

$$\overline{(\overline{x} \sqcup y)} \sqcup x = x \qquad \overline{(\overline{x} \sqcup y)} \sqcup (z \sqcup y) = y \sqcup (z \sqcup x)$$

Here again the second axiom is not easy to explain. A single-equation axiomatisation in terms of the Sheffer stroke or NAND operation | was given in [27]:

$$(x|((y|x)|x))|(y|(z|x)) = y$$

However, it seems too complex for practical purposes.

In Section 4.3 we present an axiomatisation in which we try to strike a balance between simplicity/understandability and small number of axioms.

Axioms for domain and antidomain in idempotent semirings and weaker semiring structures have been studied, for example, in [9–12]. Axioms for these operations in semigroups and monoids have been studied, for example, in [7, 23].

3 Boolean Algebras

In this section we present Huntington's axioms for Boolean algebras and discuss how Boolean algebras are implemented in Isabelle/HOL.

3.1 Huntington's Axioms

Huntington gave the following axiomatisation of Boolean algebras [22]. It is based only on join and complement.

Definition 1. *A* Boolean algebra *is a set $S \neq \emptyset$ with a binary operation $\sqcup$ and a unary operation $\overline{}$ such that, for all $x, y, z \in S$,*

$$\begin{aligned} x \sqcup (y \sqcup z) &= (x \sqcup y) \sqcup z \\ x \sqcup y &= y \sqcup x \\ x &= \overline{\overline{x} \sqcup y} \sqcup \overline{\overline{x} \sqcup \overline{y}} \end{aligned}$$

The operation $\sqcup$ is called join and the operation $\overline{}$ is called complement. In a Boolean algebra, $x \sqcup \overline{x} = y \sqcup \overline{y}$ for all $x, y \in S$. Hence the order $\sqsubseteq$, the strict order $\sqsubset$, the meet operation $\sqcap$, the difference $-$, the greatest element $\top$ and the least element $\bot$ can be defined as follows.

Definition 2. *An* extended Boolean algebra *is a Boolean algebra S with relations $\sqsubseteq$ and $\sqsubset$, binary operations $\sqcap$ and $-$, and constants $\top$ and $\bot$ such that, for all $x, y \in S$,*

$$\begin{array}{lll} x \sqsubseteq y \Leftrightarrow x \sqcup y = y & \qquad x \sqcap y = \overline{\overline{x} \sqcup \overline{y}} & \qquad \top = x \sqcup \overline{x} \\ x \sqsubset y \Leftrightarrow x \sqsubseteq y \wedge \neg(y \sqsubseteq x) & \qquad x - y = \overline{\overline{x} \sqcup y} & \qquad \bot = \overline{\top} \end{array}$$

3.2 Boolean Algebras in Isabelle/HOL

We explain the hierarchy of orders and lattices in Isabelle/HOL up to Boolean algebras. These structures are implemented as type classes, which offer means to group operations and axioms, arrange them in hierarchies, dynamically inherit results, and exhibit multiple instances [20]. Every class has a single type parameter, which can be instantiated with a HOL type. Types in HOL must not be empty.

A *partial order* $\sqsubseteq$ on a set $S \neq \emptyset$ is a reflexive, transitive and antisymmetric relation on S with associated strict order $\sqsubset$. This means, for all $x, y, z \in S$:

$$\begin{aligned} x &\sqsubseteq x \\ x \sqsubseteq y \wedge y \sqsubseteq z &\Rightarrow x \sqsubseteq z \\ x \sqsubseteq y \wedge y \sqsubseteq x &\Rightarrow x = y \\ x \sqsubset y &\Leftrightarrow x \sqsubseteq y \wedge \neg(y \sqsubseteq x) \end{aligned}$$

A *lattice* is a set S partially ordered by $\sqsubseteq$ where any two elements $x, y \in S$ have a least upper bound or join $x \sqcup y$ and a greatest lower bound or meet $x \sqcap y$. This means, for all $x, y, z \in S$:

$$\begin{aligned} x &\sqsubseteq x \sqcup y & x \sqcap y &\sqsubseteq x \\ y &\sqsubseteq x \sqcup y & x \sqcap y &\sqsubseteq y \\ x \sqsubseteq z \wedge y \sqsubseteq z \Rightarrow x \sqcup y &\sqsubseteq z & z \sqsubseteq x \wedge z \sqsubseteq y \Rightarrow z &\sqsubseteq x \sqcap y \end{aligned}$$

A *bounded lattice* is a lattice S with a least element $\bot$ and a greatest element $\top$. This means, for all $x \in S$:

$$\bot \sqsubseteq x \qquad\qquad x \sqsubseteq \top$$

A lattice S is *distributive* if the following axiom holds for all $x, y, z \in S$:

$$x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$$

A *Boolean algebra* is a bounded distributive lattice S with a complement $\overline{}$ and a difference $-$ satisfying, for all $x, y \in S$:

$$\begin{aligned} x \sqcup \overline{x} &= \top \\ x \sqcap \overline{x} &= \bot \\ x - y &= x \sqcap \overline{y} \end{aligned}$$

The above axiomatisation is equivalent to the extended Boolean algebras based on Huntington's axioms. This has been proved in Isabelle/HOL in [33], which also shows the equivalence to Robbins algebras and to an axiomatisation basing the lattice structure on $\sqcup$ and $\sqcap$ rather than $\sqsubseteq$.

Next we describe Stone algebras. Previous work extended the Isabelle/HOL hierarchy by various pseudocomplemented algebras [18]. Their place is between bounded (distributive) lattices and Boolean algebras.

A *(distributive) p-algebra* is a bounded (distributive) lattice S with a unary pseudocomplement $\overline{}$ satisfying, for all $x, y \in S$:

$$x \sqcap y = \bot \Leftrightarrow x \sqsubseteq \overline{y}$$

A *Stone algebra* is a distributive p-algebra S satisfying the following equation for all $x \in S$:

$$\overline{x} \sqcup \overline{\overline{x}} = \top$$

An *extended Stone algebra* adds to a Stone algebra S a difference $-$ satisfying, for all $x, y \in S$:

$$x - y = x \sqcap \overline{y}$$

To simplify comparisons, we provide this and similar extensions of algebras to obtain the signature $(S, \sqsubseteq, \sqsubset, \sqcup, \sqcap, -, ^{-}, \bot, \top)$ used by Isabelle/HOL. Adding the axiom $x = \overline{\overline{x}}$ to extended Stone algebras gives extended Boolean algebras.

4 Alternative Axiomatisations of Boolean Algebras

In this section we consider three axiomatisations of Boolean algebras, which are based only on join and complement, as are Huntington's axioms. The first two are from the literature and the third is new. A motivation for these versions is that the axioms are easier to understand than Huntington's third axiom.

4.1 Lee Byrne's Formulation A

The following axiomatisation is from [5, Formulation A]; see also [14]. It replaces Huntington's third axiom with an equivalence. The formulas in the equivalence express $y \sqsubseteq x$ in two different ways, noting that $z \sqcup \overline{z}$ represents $\top$.

Theorem 3. *The structure* $(S, \sqcup, ^{-})$ *is a Boolean algebra if and only if, for all* $x, y, z \in S$,

$$\begin{gathered} x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z \\ x \sqcup y = y \sqcup x \\ x \sqcup \overline{y} = z \sqcup \overline{z} \Leftrightarrow x \sqcup y = x \end{gathered} \qquad \square$$

4.2 Lee Byrne's Formulation B

The following axiomatisation is from [5, Formulation B]. It combines associativity and commutativity into one axiom.

Theorem 4. *The structure* $(S, \sqcup, ^{-})$ *is a Boolean algebra if and only if, for all* $x, y, z \in S$,

$$\begin{gathered} (x \sqcup y) \sqcup z = (y \sqcup z) \sqcup x \\ x \sqcup \overline{y} = z \sqcup \overline{z} \Leftrightarrow x \sqcup y = x \end{gathered} \qquad \square$$

4.3 An Equational Axiomatisation Based on Semilattices

The following new axiomatisation is based on semilattices, that is, sets with an associative, commutative and idempotent $\sqcup$ operation. We add the double complement rule and that $\top$ is unique. The final axiom is similar to the logical statement $P \vee Q = P \vee (\neg P \wedge Q)$. The dual of the final axiom is used in [1] for an axiomatisation of pseudocomplemented semilattices.

Theorem 5. *The structure* $(S, \sqcup, {}^{-})$ *is a Boolean algebra if and only if, for all* $x, y, z \in S$,

$$\begin{aligned} x \sqcup (y \sqcup z) &= (x \sqcup y) \sqcup z \\ x \sqcup y &= y \sqcup x \\ x \sqcup x &= x \\ \overline{\overline{x}} &= x \\ x \sqcup \overline{x} &= y \sqcup \overline{y} \\ x \sqcup \overline{\overline{x} \sqcup y} &= x \sqcup \overline{y} \end{aligned} \qquad \square$$

This axiomatisation is equational with few and simple axioms, which is useful for both manual and automated proofs. Counterexamples generated by Nitpick [4] witness that the axioms are independent of each other. The smallest counterexample for independence of associativity the tool found has 16 elements.

5 Subset Boolean Algebras

In a number of situations a subset of the elements under consideration forms a Boolean algebra, whereas a more general structure is desired for the overall set. An example is that of Kleene algebras with tests [24] where the overall structure forms a Kleene algebra (with operations for join, composition and iteration) and a designated subset of tests forms a Boolean algebra (in which meet coincides with composition). In computation models, elements of the Kleene algebra model state changes while tests model conditions on states. Another example is that of weighted graphs [18] where the overall structure forms a Stone relation algebra and a subset forms a relation algebra. It uses the well-known fact that the elements of a Stone algebra satisfying $x = \overline{\overline{x}}$ form a Boolean subalgebra [16]. Elements of the Stone relation algebra model graphs with edge weights while elements of the Boolean subset model unweighted graphs. In both examples it is convenient to have a single-sorted structure, where the Boolean algebra axioms hold only for a subset of elements of the overall algebra.

In the remainder of this paper we study axiomatisations describing the common structure underlying these situations. Our most general setting, taken from [19], is a set S with a subset $S' \subseteq S$ of elements that forms a Boolean algebra. We axiomatise that Boolean algebra structure using the $\sqcup$ and ${}^{-}$ operations. To obtain a single-sorted structure in Isabelle/HOL these operations are introduced on the overall set S, however their axioms are restricted to the subset S'.

This first building block B_0 in our hierarchy of structures results by applying Huntington's axioms [22] to the range S' of operation ${}^{-}$, which serves as complement on the range. It provides a Boolean algebra structure on S' without imposing any further constraints on the overall set. Building block B_0 is used as a reference in the subsequent development and to prove results to be inherited by further, more special structures. Results that hold in Boolean algebras can be stated for the subset S' by using elements from the range of ${}^{-}$ instead of arbitrary elements; they are derived in the order used by [25].

Given a set S with a unary operation $^-$ we write $S' = \{\overline{x} \mid x \in S\}$ for the range of $^-$. The first three equations are Huntington's axioms for Boolean algebras applied to the range of $^-$. The last equation states that S' is closed under $\sqcup$. Note that the behaviour of the operations on elements in $S \setminus S'$ is left unspecified by the axioms.

Definition 6. *A* B_0-algebra *is a set $S \neq \emptyset$ with a binary operation $\sqcup$ and a unary operation $^-$ such that, for all $x, y, z \in S$,*

$$
\begin{aligned}
\overline{x} \sqcup (\overline{y} \sqcup \overline{z}) &= (\overline{x} \sqcup \overline{y}) \sqcup \overline{z} \\
\overline{x} \sqcup \overline{y} &= \overline{y} \sqcup \overline{x} \\
\overline{x} &= \overline{\overline{\overline{x}} \sqcup \overline{y}} \sqcup \overline{\overline{\overline{x}} \sqcup \overline{\overline{y}}} \\
\overline{x} \sqcup \overline{y} &= \overline{\overline{\overline{x} \sqcup \overline{y}}}
\end{aligned}
$$

The remaining operations of Boolean algebras can be defined in terms of $\sqcup$ and $^-$ on S'.

Definition 7. *An* extended B_0-algebra *is a B_0-algebra S with relations $\sqsubseteq$ and $\sqsubset$, binary operations $\sqcap$ and $-$, and constants $\top$ and $\bot$ such that, for all $x, y \in S$,*

$$
\begin{array}{lll}
\overline{x} \sqsubseteq \overline{y} \Leftrightarrow \overline{x} \sqcup \overline{y} = \overline{y} & \qquad \overline{x} \sqcap \overline{y} = \overline{\overline{\overline{x}} \sqcup \overline{\overline{y}}} & \qquad \top = \overline{x} \sqcup \overline{\overline{x}} \\
\overline{x} \sqsubset \overline{y} \Leftrightarrow \overline{x} \sqsubseteq \overline{y} \wedge \neg(\overline{y} \sqsubseteq \overline{x}) & \qquad \overline{x} - \overline{y} = \overline{\overline{\overline{x}} \sqcup \overline{y}} & \qquad \bot = \overline{\top}
\end{array}
$$

The following result confirms that we obtain the desired Boolean algebra structure on S'.

Theorem 8.
1. *Let $(S, \sqcup, ^-)$ be a B_0-algebra. Then $(S', \sqcup, ^-)$ is a Boolean algebra.*
2. *Let $(S, \sqsubseteq, \sqsubset, \sqcup, \sqcap, -, ^-, \bot, \top)$ be an extended B_0-algebra.*
   Then $(S', \sqsubseteq, \sqsubset, \sqcup, \sqcap, -, ^-, \bot, \top)$ is an extended Boolean algebra. □

Structural results about extended algebras, such as part 2 of Theorem 8, enable the use of existing Isabelle/HOL theories for Boolean algebras.

6 Subset Boolean Algebras with Additional Structure

We now discuss axioms that make the range of $^-$ a Boolean algebra, but add further properties that are common to the intended models. In these models, the unary operation can be a complement, a pseudocomplement or the antidomain operation. For simplicity, we mostly call $^-$ the 'complement'.

We first look at structures based only on join and complement, and then add axioms for the remaining operations of Boolean algebras. In the intended models, the operation $\sqcap$, which is the meet on the range of the operation $^-$, can be the meet in the overall algebra or the composition operation of a (left) semiring. For simplicity, we mostly call $\sqcap$ the 'meet'.

6.1 Assumptions Derived from the New Axiomatisation

The axioms of building block B_1 are based on the ones in Section 4.3. We follow the idea of applying the Boolean algebra axioms to the range of the operation $^-$, but we only do this where necessary for the intended models. For example, the intended models have a semilattice structure on the overall algebra, not just on the Boolean subset. In contrast, the double complement axiom only applies to the subset, not to the overall algebra.

Definition 9. *A* B_1-algebra *is a set $S \neq \emptyset$ with a binary operation $\sqcup$ and a unary operation $^-$ such that, for all $x, y, z \in S$,*

$$\begin{aligned} x \sqcup (y \sqcup z) &= (x \sqcup y) \sqcup z \\ x \sqcup y &= y \sqcup x \\ x \sqcup x &= x \\ \overline{\overline{\overline{x}}} &= \overline{x} \\ \overline{x \sqcup \overline{x}} &= \overline{y \sqcup \overline{y}} \\ \overline{x} \sqcup \overline{\overline{x} \sqcup y} &= \overline{x} \sqcup \overline{y} \end{aligned}$$

Using a similar approach, the remaining operations of Boolean algebras are introduced as follows.

Definition 10. *An* extended B_1-algebra *is a B_1-algebra S with relations $\sqsubseteq$ and $\sqsubset$, binary operations $\sqcap$ and $-$, and constants $\top$ and $\bot$ such that, for all $x, y \in S$,*

$$\begin{array}{lll} x \sqsubseteq y \Leftrightarrow x \sqcup y = y & \overline{x} \sqcap \overline{y} = \overline{\overline{\overline{x}} \sqcup \overline{\overline{y}}} & \bot = \overline{x \sqcup \overline{x}} \\ x \sqsubset y \Leftrightarrow x \sqsubseteq y \wedge \neg(y \sqsubseteq x) & \overline{x} - \overline{y} = \overline{\overline{\overline{x}} \sqcup \overline{y}} & \top = \overline{\bot} \end{array}$$

The following result shows that B_1-algebras specialise B_0-algebras. Hence we again obtain the Boolean algebra structure on S'.

Theorem 11.

1. *Every B_1-algebra is a B_0-algebra.*
2. *Every extended B_1-algebra is an extended B_0-algebra.* □

6.2 Stronger Assumptions Based on Join and Complement

In building block B_2 we add axioms covering further properties common to structures with antidomain or (pseudo)complement. In particular, they allow us to derive that $^-$ is antitone and satisfies one of De Morgan's laws in the overall algebra. Moreover, double complement distributes over $\sqcup$ in the overall algebra.

Definition 12. *A* B_2-algebra *is a set* $S \neq \emptyset$ *with a binary operation* $\sqcup$ *and a unary operation* $^{-}$ *such that, for all* $x, y, z \in S$*,*

$$\begin{aligned} x \sqcup (y \sqcup z) &= (x \sqcup y) \sqcup z \\ x \sqcup y &= y \sqcup x \\ x \sqcup x &= x \\ x \sqcup \overline{y \sqcup \overline{y}} &= x \\ \overline{x \sqcup y} &= \overline{\overline{\overline{x}} \sqcup \overline{\overline{y}}} \\ \overline{x} \sqcup \overline{\overline{x} \sqcup y} &= \overline{x} \sqcup \overline{y} \end{aligned}$$

An extended B_2-algebra is obtained from this by adding the operations and axioms given in Definition 10. The following result shows consequences.

Theorem 13.
1. *Every (extended)* B_2*-algebra is an (extended)* B_1*-algebra.*
2. *Let* S *be a* B_2*-algebra. Then, for all* $x, y \in S$*,*

$$\overline{x \sqcup y} \sqcup \overline{x \sqcup \overline{y}} = \overline{x} \qquad \overline{\overline{x \sqcup y}} = \overline{\overline{x}} \sqcup \overline{\overline{y}}$$
$$\overline{\overline{x} \sqcup \overline{y}} \sqcup \overline{\overline{x} \sqcup y} = \overline{\overline{x}}$$

3. *Let* S *be an extended* B_2*-algebra. Then, for all* $x, y \in S$*,*

$$x \sqsubseteq y \Rightarrow \overline{y} \sqsubseteq \overline{x} \qquad \overline{x \sqcup y} = \overline{x} \sqcap \overline{y}$$
$$x \sqsubseteq y \Rightarrow \overline{\overline{x}} \sqsubseteq \overline{\overline{y}} \qquad \square$$

6.3 Axioms for Meet

In building block B_3 we add axioms of $\sqcap$ covering further properties common to the antidomain and pseudocomplement instances. We omit the left distributivity rule and the right zero rule as they do not hold in some models. For the same reason, the operation $\sqcap$ does not have to be commutative.

To simplify comparison with the antidomain model we supply a translation table for the operations and relations, where $+$, $\cdot$, 0 and 1 are operations known from semirings, a stands for antidomain and d for domain:

extended B_0-algebra	antidomain model
$\sqcup$	$+$
$\sqcap$	$\cdot$
$^{-}$	a
$^{=}$	d
$\bot$	0
$\top$	1
$\sqsubseteq$	$\leq$
$\sqsubset$	$<$

We frequently write xy instead of $x \cdot y$. The additional equations in the following definition are just translations of the formulas on the left and not part of the axiomatisation. We translate results similarly in the remainder of this paper.

Definition 14. *An* extended B_3-algebra *is an extended B_2-algebra S such that, for all $x, y, z \in S$,*

$$\begin{aligned}
x \sqcap (y \sqcap z) &= (x \sqcap y) \sqcap z & x(yz) &= (xy)z \\
(x \sqcup y) \sqcap z &= (x \sqcap z) \sqcup (y \sqcap z) & (x + y)z &= (xz) + (yz) \\
\overline{x} \sqcap x &= \bot & a(x)x &= 0 \\
\top \sqcap x &= x & 1x &= x \\
\overline{x \sqcap \overline{\overline{y}}} &= \overline{x \sqcap y} & a(x \cdot d(y)) &= a(xy)
\end{aligned}$$

The following result gives derived properties of $\sqcap$.

Theorem 15. *Let S be an extended B_3-algebra. Then, for all $x, y, z \in S$,*

$$\begin{aligned}
x \sqsubseteq y \Rightarrow x \sqcap z &\sqsubseteq y \sqcap z & x \le y &\Rightarrow xz \le yz \\
\bot \sqcap x &= \bot & 0x &= 0 \\
\overline{\overline{x}} \sqcap x &= x & d(x)x &= x \\
\overline{\overline{\overline{x} \sqcap y}} &= \overline{x} \sqcap \overline{\overline{y}} & d(a(x)y) &= a(x)d(y) \\
\overline{\overline{\overline{\overline{x}} \sqcap y}} &= \overline{\overline{x}} \sqcap \overline{\overline{y}} & d(d(x)y) &= d(x)d(y)
\end{aligned}$$

□

Counterexamples generated by Nitpick witness that

$$\begin{aligned}
x \sqcap \top &= x & x1 &= x \\
x \sqcap y &= y \sqcap x & xy &= yx \\
x \sqsubseteq y \Rightarrow z \sqcap x &\sqsubseteq z \sqcap y & x \le y &\Rightarrow zx \le zy
\end{aligned}$$

do not hold for some extended B_3-algebra S and some $x, y, z \in S$. Hence our axiomatisation also covers structures weaker than idempotent left semirings (where the first and third of these properties are required).

6.4 Stronger Assumptions for Meet

The following axioms of building block B_4 also hold in the pseudocomplement and antidomain models, but follow from the axioms of B_5-algebras introduced below.

Definition 16. *An* extended B_4-algebra *is an extended B_3-algebra S such that, for all $x, y, z \in S$,*

$$\begin{aligned}
x \sqcap \top &= x & x1 &= x \\
x \sqsubseteq y \Rightarrow z \sqcap x &\sqsubseteq z \sqcap y & x \le y &\Rightarrow zx \le zy
\end{aligned}$$

Counterexamples generated by Nitpick witness that

$$\begin{aligned}
x \sqcup \top &= \top & x + 1 &= 1 \\
x \sqcap \bot &= \bot & x0 &= 0 \\
x \sqcap (y \sqcup z) &= (x \sqcap z) \sqcup (y \sqcap z) & x(y + z) &= (xz) + (yz) \\
x \sqcap y = \bot &\Leftrightarrow x \sqsubseteq \overline{y} & xy = 0 &\Leftrightarrow x \le a(y)
\end{aligned}$$

do not hold for some extended B_4-algebra S and some $x, y, z \in S$.

We will come back to B_4-algebras when we study the antidomain model in more detail in Section 8.

7 Subset Boolean Algebras in Stone Algebras

In building block B_5 we specialise $\sqcap$ to meet and $^-$ to pseudocomplement.

Definition 17. *An* extended B_5-algebra *is an extended B_3-algebra S such that, for all $x, y \in S$,*

$$\begin{aligned} x \sqcap y &= y \sqcap x \\ x \sqcap (x \sqcup y) &= x \end{aligned}$$

The following result shows that B_5-algebras correspond to Stone algebras. Parts 2 and 3 do not combine to an equivalence because the difference operation $-$ is axiomatised only on S' in B_5-algebras but on S in Stone algebras.

Theorem 18.
1. *Every extended B_5-algebra is an extended B_4-algebra.*
2. *Every extended B_5-algebra is a Stone algebra.*
3. *Every extended Stone algebra is an extended B_5-algebra.* □

8 Antidomain Semirings

In this section we study the connection to antidomain semirings, which, in particular, are semilattices. We show that they correspond to extended B_4-algebras. We start by introducing idempotent left semirings (IL-semirings).

Definition 19. *An* IL-semiring *is a set $S \neq \emptyset$ with relations $\sqsubseteq$ and $\sqsubset$, binary operations $\sqcup$ and $\sqcap$, and constants $\top$ and $\bot$ such that, for all $x, y, z \in S$,*

$$\begin{array}{ccc}
x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z & x \sqsubseteq y \Leftrightarrow x \sqcup y = y & x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z \\
x \sqcup y = y \sqcup x & x \sqsubset y \Leftrightarrow x \sqsubseteq y \wedge \neg(y \sqsubseteq x) & \top \sqcap x = x \\
x \sqcup x = x & x \sqsubseteq y \Rightarrow z \sqcap x \sqsubseteq z \sqcap y & x \sqcap \top = x \\
x \sqcup \bot = x & (x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z) & \bot \sqcap x = \bot
\end{array}$$

$$\begin{array}{ccc}
x + (y + z) = (x + y) + z & x \leq y \Leftrightarrow x + y = y & x(yz) = (xy)z \\
x + y = y + x & x < y \Leftrightarrow x \leq y \wedge \neg(y \leq x) & 1x = x \\
x + x = x & x \leq y \Rightarrow zx \leq zy & x1 = x \\
x + 0 = x & (x + y)z = (xz) + (yz) & 0x = 0
\end{array}$$

An IL-semiring S is partially ordered by $\sqsubseteq$.

We now introduce the notion of tests, using semiring notation for ease of reference. Our presentation follows [29]. Tests algebraically represent conditions in programs and can be used to construct conditionals, while-loops, assertions and related statements. All these statements have in common that they check if a condition is satisfied in the current state, but this check does not modify the state. A condition p acts as an identity on states that satisfy p, so it is reasonable to model it algebraically by an element below 1 which represents 'do nothing'.

In an IL-semiring a *test* is an element p that has a *complement* q relative to 1, that is, $p + q = 1$ and $p \cdot q = 0 = q \cdot p$. In particular, 0 and 1 are tests. By the requirement $p + q = 1$ every test is a *sub-identity*, that is, satisfies $p \leq 1$. The set of all tests of an IL-semiring S is denoted by $\mathit{test}(S)$. It is not hard to show that a complement of p is unique if it exists; we will denote it by $\neg p$.

Next we introduce an abstract domain operation d that assigns to a semiring element, which represents a set of transitions from states to states, the test that describes precisely its possible starting states.

As a motivation, consider the IL-semiring of binary relations over a set M, with union as $+$, relational composition as $\cdot$, the identity relation as 1 and the empty relation as 0. Then the domain $d(R)$ of a binary relation $R \subseteq M \times M$ is the set $\{u \in M \mid \exists v \in M : (u, v) \in R\}$. In the semiring setting, this set should be represented as a test in the IL-semiring of binary relations, that is, as the sub-identity $d(R) = \{(u, u) \in M \times M \mid \exists v \in M : (u, v) \in R\}$.

Abstracting from the relational IL-semiring to a general one, we arrive at the following definitions [8, 29]. A *left prepredomain semiring* is an IL-semiring S with an additional *prepredomain operation* $d : S \to \mathit{test}(S)$ satisfying

$$x \leq d(x) \cdot x \tag{d1}$$

for all $x \in S$. We call d a *predomain operation* if additionally

$$d(p \cdot x) \leq p \tag{d2}$$

for all $x \in S$ and $p \in \mathit{test}(S)$. Finally, a predomain operation d is called a *domain operation* if it satisfies the *locality* axiom

$$d(x \cdot d(y)) \leq d(x \cdot y) \tag{d3}$$

for all $x, y \in S$. See [9] for axioms (d1), (d2) and (d3) in idempotent semirings.

In IL-semirings, axioms (d1), (d2) and (d3) are independent of each other. However, (d1) and (d3) together with the assumption $d(0) = 0$ imply (d2). Moreover, having a predomain operation d implies that d is surjective and $\mathit{test}(S)$ forms a Boolean algebra [29, Theorem 2.4.6 items 1 and 8]. Predomain is studied since in a number of cases it already suffices for the purpose at hand. For example, the algebraic soundness proof of Hoare logic in [30] does not need (d3); that axiom is only used in the proof of relative completeness of the logic. Therefore we give an antidomain analogue of (d2) below.

Technically, by referring to $\mathit{test}(S)$ the above axioms have a 'two-sorted' flavour. So there have been approaches [10–12] to give a different axiomatisation in terms of a combination of d and $\neg$, namely the *antidomain operation* $a(x) = \neg d(x)$, and to leave $\mathit{test}(S)$ unmentioned in the axioms. Originally there were three axioms for antidomain corresponding roughly to the test property, (d1) and (d3). In the present paper we also discuss the role of a further axiom corresponding to (d2); here we can show that the original antidomain axioms imply that without an additional assumption corresponding to $d(0) = 0$.

To do this we first introduce *preantidomain* in PPA-semirings, *preantidomain* in PA-semirings and *antidomain* in A-semirings, and afterwards relate them to our general treatment of sets with a Boolean subset.

We start with preantidomain using axioms that correspond to (d1) and the test property. These are axioms (BD1) and (BD3) of [11]. In the antidomain model, $d(x) = a(a(x))$.

Definition 20. *A* PPA-semiring *is an IL-semiring S with a unary operation $^-$ such that, for all $x \in S$,*

$$\begin{array}{lr} \overline{x} \sqcap x = \bot & a(x)x = 0 \\ \overline{x} \sqcup \overline{\overline{x}} = \top & a(x) + d(x) = 1 \end{array}$$

It is somewhat unexpected that the simple PPA-semiring axioms already imply a rich set of consequences shown in the following result. Many of them are concerned with how tests interact with each other and general elements under meet/composition.

Theorem 21. *Let S be a PPA-semiring. Then, for all $x, y \in S$,*

$$\begin{array}{cccc} \overline{\bot} = \top & \overline{\overline{\overline{x}}} = \overline{x} & x \sqsubseteq \overline{\overline{x}} \sqcap x & \overline{\overline{x}} \sqsubseteq \overline{\overline{y}} \Rightarrow \overline{y} \sqsubseteq \overline{x} \\ \overline{\top} = \bot & \overline{x} \sqcap \overline{\overline{x}} = \bot & \overline{x} \sqcap \overline{y} = \overline{y} \sqcap \overline{x} & \overline{x} \sqsubseteq \overline{y} \Rightarrow \overline{x} \sqcap y = \bot \\ a(0) = 1 & a(d(x)) = a(x) & x \leq d(x)x & d(x) \leq d(y) \Rightarrow a(y) \leq a(x) \\ a(1) = 0 & a(x)d(x) = 0 & a(x)a(y) = a(y)a(x) & a(x) \leq a(y) \Rightarrow a(x)y = 0 \end{array} \square$$

To obtain preantidomain we add an axiom that corresponds to (d2). This axiom facilitates the import/export of composition with a test under a domain.

Definition 22. *A* PA-semiring *is a PPA-semiring S such that, for all $x, y \in S$,*

$$\overline{\overline{x}} \sqsubseteq \overline{\overline{x} \sqcap y} \qquad\qquad d(x) \leq a(a(x)y)$$

Consequences of this additional axiom are given in the following result. They are mostly concerned with the (anti)domain of joins and the (anti)domain of meets/compositions where the first component is a test.

Theorem 23. *Let S be a PA-semiring. Then, for all $x, y \in S$,*

$$\begin{array}{ccc} \overline{x} \sqcap \overline{y} = \overline{x \sqcup y} & \overline{\overline{\overline{\overline{x}} \sqcap y}} \sqsubseteq \overline{\overline{x}} & x \sqsubseteq y \Rightarrow \overline{y} \sqsubseteq \overline{x} \\ \overline{\overline{x \sqcup y}} = \overline{\overline{x}} \sqcup \overline{\overline{y}} & \overline{x \sqcap \overline{\overline{y}}} \sqsubseteq \overline{x \sqcap y} & \overline{x} \sqsubseteq \overline{y} \Leftrightarrow \overline{x} \sqcap y = \bot \\ \overline{x} \sqcup \overline{y} = \overline{\overline{\overline{x}} \sqcap \overline{\overline{y}}} & \overline{\overline{\overline{x} \sqcap y}} = \overline{x} \sqcap \overline{\overline{y}} & \\ a(x)a(y) = a(x + y) & d(d(x)y) \leq d(x) & x \leq y \Rightarrow a(y) \leq a(x) \\ d(x + y) = d(x) + d(y) & a(x \cdot d(y)) \leq a(xy) & a(x) \leq a(y) \Leftrightarrow a(x)y = 0 \\ a(x) + a(y) = a(d(x)d(y)) & d(a(x)y) = a(x)d(y) & \end{array} \square$$

To obtain antidomain, we finally add a version of (d3), called (BD2) in [11]. This axiom is concerned with the (anti)domain of meets/compositions where the second component is a test. In the terminology of [10], an A-semiring is an idempotent pre-semiring with 1 and δ that satisfies the basic Boolean domain axioms (BD1), (BD2) and (BD3).

Definition 24. *An* A-semiring *is a PPA-semiring S such that, for all $x, y \in S$,*

$$\overline{x \sqcap y} \sqsubseteq \overline{x \sqcap \overline{\overline{y}}} \qquad\qquad a(xy) \leq a(x \cdot d(y))$$

An A-algebra *is an A-semiring with a binary operation $-$ defined, for all $x, y \in S$, by*

$$\overline{x} - \overline{y} = \overline{\overline{\overline{x}} \sqcup \overline{y}}$$

Note that A-semirings are based on PPA-semirings. However, by the following result they form PA-semirings. Previous work has shown that (d2) follows if S is an A-semiring where $\sqcap$ distributes over $\sqcup$ and has $\bot$ as a zero (that is, a semiring not just an IL-semiring) [11]. Moreover, using results in [10] one can show that (d2) and the PA-semiring axiom follow also when only an IL-semiring is assumed. The result also locates A-algebras in our hierarchy of algebras.

Theorem 25.
1. *Every PA-semiring is a B_2-algebra.*
2. *Every A-semiring is a PA-semiring.*
3. *Every Stone algebra is an A-semiring.*
4. *S is an A-algebra if and only if S is an extended B_4-algebra.* □

Theorems 18 and 25 imply that every extended Stone algebra is an A-algebra.

9 Conclusion

We have presented a hierarchy of axiom systems as a common basis for approaches to induce a Boolean subalgebra in a larger overall algebra as the range of a complement-like operation. Except for the most basic axiomatisation, which imposes no extra structure beyond the Boolean subalgebra, the axioms assume that the overall algebra is a semilattice. The hierarchy has shed new light on the interconnections between several such approaches. The axioms are simple and perspicuous when translated into formulas of the respective theories. All of our axioms are (or can be written as) equations and hence well suited to mechanical support.

In situations which require a Boolean subalgebra our hierarchy offers a number of choices for axiom systems verified in Isabelle/HOL. Basing an axiomatisation on one of them eliminates the need to prove the intended Boolean laws for the substructure.

Working with Boolean algebras involves a choice about which operations to include in the signature and which to derive by definition. For example, [25] includes join and complement in the signature and derives meet, $\bot$ and $\top$, whereas

[15] includes all of these in the signature. The standard type-class implementation of Boolean algebras in Isabelle/HOL has parameters for all of these operations, a binary difference and the orders $\sqsubseteq$ and $\sqsubset$. The separate treatment of extended structures in this paper reflects this.

Proving results such as Theorem 23 is typically highly automated in Isabelle/HOL using the built-in Sledgehammer tool [3, 32]. It filters relevant lemmas, calls fully automated external theorem provers (such as E, Spass, Vampire) and SMT solvers (such as CVC4, Z3) and reconstructs proofs within Isabelle/HOL to avoid trusting external software. In several cases, Prover9 [26] was able to find a proof where the tools called by Sledgehammer failed. Since Prover9 is not integrated with Sledgehammer, we wrote a program that transforms the output generated by Prover9 to an Isabelle/HOL proof. The translation currently works for a limited range of proofs but could form the basis of an integration into Sledgehammer. Such an extension would be beneficial because Prover9 performs well for algebraic applications [6].

Acknowledgement. We thank Andreas Zelend and the anonymous referees for their helpful comments.

References

1. Balbes, R., Horn, A.: Stone lattices. Duke Mathematical Journal **37**(3), 537–545 (1970)
2. Birkhoff, G.: Lattice Theory, Colloquium Publications, vol. XXV. American Mathematical Society, third edn. (1967)
3. Blanchette, J.C., Böhme, S., Paulson, L.C.: Extending Sledgehammer with SMT solvers. In: Bjørner, N., Sofronie-Stokkermans, V. (eds.) CADE 2011. LNCS, vol. 6803, pp. 116–130. Springer (2011)
4. Blanchette, J.C., Nipkow, T.: Nitpick: A counterexample generator for higher-order logic based on a relational model finder. In: Kaufmann, M., Paulson, L.C. (eds.) ITP 2010. LNCS, vol. 6172, pp. 131–146. Springer (2010)
5. Byrne, L.: Two brief formulations of Boolean algebra. Bulletin of the American Mathematical Society **52**(4), 269–272 (1946)
6. Dang, H.H., Höfner, P.: First-order theorem prover evaluation w.r.t. relation- and Kleene algebra. In: Berghammer, R., Möller, B., Struth, G. (eds.) PhD Programme at RelMiCS10/AKA5. pp. 48–52. Report 2008-04, Institut für Informatik, Universität Augsburg (2008)
7. Desharnais, J., Jipsen, P., Struth, G.: Domain and antidomain semigroups. In: Berghammer, R., Jaoua, A.M., Möller, B. (eds.) RelMiCS/AKA 2009. LNCS, vol. 5827, pp. 73–87. Springer (2009)
8. Desharnais, J., Möller, B.: Fuzzifying modal algebra. In: Höfner, P., Jipsen, P., Kahl, W., Müller, M.E. (eds.) RAMiCS 2014. LNCS, vol. 8428, pp. 395–411. Springer (2014)
9. Desharnais, J., Möller, B., Struth, G.: Kleene algebra with domain. ACM Transactions on Computational Logic **7**(4), 798–833 (2006)
10. Desharnais, J., Struth, G.: Domain axioms for a family of near-semirings. In: Meseguer, J., Roşu, G. (eds.) AMAST 2008. LNCS, vol. 5140, pp. 330–345. Springer (2008)

11. Desharnais, J., Struth, G.: Modal semirings revisited. In: Audebaud, P., Paulin-Mohring, C. (eds.) MPC 2008. LNCS, vol. 5133, pp. 360–387. Springer (2008)
12. Desharnais, J., Struth, G.: Internal axioms for domain semirings. Sci. Comput. Program. **76**(3), 181–203 (2011)
13. Frink, O.: Pseudo-complements in semi-lattices. Duke Mathematical Journal **29**(4), 505–514 (1962)
14. Frink, Jr., O.: Representations of Boolean algebras. Bulletin of the American Mathematical Society **47**(10), 755–756 (1941)
15. Givant, S., Halmos, P.: Introduction to Boolean Algebras. Springer (2009)
16. Grätzer, G.: Lattice Theory: First Concepts and Distributive Lattices. W. H. Freeman and Co. (1971)
17. Guttmann, W.: Algebras for iteration and infinite computations. Acta Inf. **49**(5), 343–359 (2012)
18. Guttmann, W.: Verifying minimum spanning tree algorithms with Stone relation algebras. Journal of Logical and Algebraic Methods in Programming **101**, 132–150 (2018)
19. Guttmann, W., Struth, G., Weber, T.: Automating algebraic methods in Isabelle. In: Qin, S., Qiu, Z. (eds.) ICFEM 2011. LNCS, vol. 6991, pp. 617–632. Springer (2011)
20. Haftmann, F., Wenzel, M.: Constructive type classes in Isabelle. In: Altenkirch, T., McBride, C. (eds.) TYPES 2006. LNCS, vol. 4502, pp. 160–174. Springer (2007)
21. Hollenberg, M.: An equational axiomatization of dynamic negation and relational composition. Journal of Logic, Language, and Information **6**(4), 381–401 (1997)
22. Huntington, E.V.: Boolean algebra. A correction. Transactions of the American Mathematical Society **35**(2), 557–558 (1933)
23. Jackson, M., Stokes, T.: Semilattice pseudo-complements on semigroups. Communications in Algebra **32**(8), 2895–2918 (2004)
24. Kozen, D.: Kleene algebra with tests. ACM Trans. Progr. Lang. Syst. **19**(3), 427–443 (1997)
25. Maddux, R.D.: Relation-algebraic semantics. Theor. Comput. Sci. **160**(1–2), 1–85 (1996)
26. McCune, W.: Prover9 and Mace4 (2005–2010), accessed 16 January 2020 at https://www.cs.unm.edu/~mccune/prover9/
27. McCune, W., Veroff, R., Fitelson, B., Harris, K., Feist, A., Wos, L.: Short single axioms for Boolean algebra. Journal of Automated Reasoning **29**(1), 1–16 (2002)
28. Meredith, C.A., Prior, A.N.: Equational logic. Notre Dame Journal of Formal Logic **9**(3), 212–226 (1968)
29. Möller, B., Desharnais, J.: Basics of modal semirings and of Kleene/omega algebras. Report 2019-03, Institut für Informatik, Universität Augsburg (2019)
30. Möller, B., Struth, G.: Algebras of modal operators and partial correctness. Theor. Comput. Sci. **351**(2), 221–239 (2006)
31. Nipkow, T., Paulson, L.C., Wenzel, M.: Isabelle/HOL: A Proof Assistant for Higher-Order Logic, LNCS, vol. 2283. Springer (2002)
32. Paulson, L.C., Blanchette, J.C.: Three years of experience with Sledgehammer, a practical link between automatic and interactive theorem provers. In: Sutcliffe, G., Ternovska, E., Schulz, S. (eds.) Proceedings of the 8th International Workshop on the Implementation of Logics. pp. 3–13 (2010)
33. Wampler-Doty, M.: A complete proof of the Robbins conjecture. Archive of Formal Proofs (2016, first version 2010)