

The representation of Boolean algebras in the spotlight of a proof checker^{*}

Rodica Ceterchi¹, Eugenio G. Omodeo², Alexandru I. Tomescu³

¹ Facultatea de Matematică și Informatică, Universitatea din București
email: rceterchi@gmail.com

² Dipartimento di Matematica e Geoscienze, Università di Trieste,
Via Valerio 12/1, I-34127 – Trieste, Italy
email: eomodeo@units.it

³ Helsinki Institute for Information Technology HIIT,
Department of Computer Science, University of Helsinki,
P.O. 68 (Gustaf Hällströmin katu 2b), FI-00014 – Helsinki, Finland
email: tomescu@cs.helsinki.fi

Abstract. We report on a proof-checked version of Stone’s result on the representability of Boolean algebras via the clopen sets of a totally disconnected compact Hausdorff space. Our experiment is based on a proof verifier based on set theory, whose usability can in its turn benefit from fully formalized proofs of representation theorems akin to the one discussed in this note.

Key words: Theory-based automated reasoning; proof checking; Referee aka *ÆtnaNova*; Boolean rings; Boolean algebras; Stone spaces.

“Boolean algebras have an almost embarrassingly rich structure.” [7, p. 10]

Introduction

This paper reports on a formally verified proof of Stone’s celebrated results [20,21,22] on the representability of Boolean algebras as fields of sets, carried out along the lines found in [4, pp. 41–43] by means of Jacob T. Schwartz’s proof-checker *Referee*, aka *ÆtnaNova*, to be simply called ‘Ref’ for brevity in the ongoing. The proof of Zorn’s lemma, formalized much earlier (cf. [19, Chapter 7]) and previously exploited in the compactness proof for classical propositional logic [16], played again a crucial role in our present scenario.

A website reporting on our experiment is at <http://www2.units.it/eomodeo/StoneReprScenario.html>. In its final form, the script-file supporting it and leading from first principles to the topological version of Stone’s result, comprises 42 definitions and proves 210 theorems altogether, organized in 19 **THEORIES**, including the background **THEORY Set.theory**. Its processing takes about 25 seconds.

^{*} Work partially supported by the INdAM/GNCS 2013 project “*Specifica e verifica di algoritmi tramite strumenti basati sulla teoria degli insiemi*” and by the Academy of Finland under grant 250345 (CoECGR)

1 Boolean algebras and rings

A ring is said to be **BOOLEAN** when every one of its elements is self-inverse w.r.t. addition and idempotent w.r.t. multiplication:

$$\begin{aligned} X + X &= \mathbf{0}, \\ X \cdot X &= X. \end{aligned}$$

The former of these laws makes it superfluous to postulate the commutativity of addition (for, it implies it); the latter implies the commutativity of multiplication. When endowed with multiplicative identity, $\mathbf{1}$, a Boolean ring is called a Boolean algebra. (To avoid trivialities, we will require that $\mathbf{0} \neq \mathbf{1}$).

An aspect of the richness of Boolean rings is that the relation

$$X \leq Y \leftrightarrow_{\text{Def}} X \cdot Y = X$$

is a partial order, in which every pair X, Y of elements has greatest common lower bound $X \sqcap Y = X \cdot Y$ and least common upper bound $X \sqcup Y = X \cdot Y + X + Y$. In this ordering $\mathbf{0}$ acts as the minimum and—when present— $\mathbf{1}$ acts as the maximum. Historically, Boolean algebras were first studied as lattices endowed with peculiar properties (namely, distributivity and complementedness).⁴ The salient operations, from this viewpoint, were $\sqcap, \sqcup, \overline{}$; the algebraic kinship with the rings of numbers remained unnoticed for quite a while (cf.[9, p. 208]).

From the ring-based point of view—the one which will prevail in these pages—the complementation operation turns out to be: $\overline{X} =_{\text{Def}} \mathbf{1} + X$.

$\begin{aligned} X \in \mathcal{B} &\rightarrow \overline{X} \in \mathcal{B} \ \& \ \overline{\overline{X}} = X \ \& \ \overline{1_{\mathcal{B}}} = 0_{\mathcal{B}} \ \& \ \overline{0_{\mathcal{B}}} = 1_{\mathcal{B}} \\ \{X, Y\} \subseteq \mathcal{B} &\rightarrow \overline{X} + X = 1_{\mathcal{B}} \ \& \ Y \cdot X + Y \cdot \overline{X} = Y \ \& \ (Y \cdot X) \cdot (Y \cdot \overline{X}) = 0_{\mathcal{B}} \\ \{X, Y\} \subseteq \mathcal{B} &\rightarrow \overline{X + Y} = X \cdot Y + \overline{X} \cdot \overline{Y} \\ X \in \mathcal{B} &\rightarrow \overline{X} \neq X \ \& \ (X \notin \{0_{\mathcal{B}}, 1_{\mathcal{B}}\}) \rightarrow \overline{X} \in \mathcal{B} \setminus \{0_{\mathcal{B}}, 1_{\mathcal{B}}\} \\ \{X, Y\} \subseteq \mathcal{B} &\rightarrow (X \cdot Y = 1_{\mathcal{B}} \rightarrow X = 1_{\mathcal{B}} \ \& \ Y = 1_{\mathcal{B}}) \\ \{U, V, X, Y\} \subseteq \mathcal{B} &\rightarrow U \cdot \overline{X} + V \cdot \overline{Y} = (U \cdot \overline{X} + V \cdot \overline{Y}) \cdot \overline{X \cdot Y} \end{aligned}$

Fig. 1. A few derived Boolean laws

⁴ From the lattice-based point of view, the simplest available characterization of the structure ‘Boolean algebra’ is the one proposed by Herbert Robbins, ca. 1933 (cfr. [12,10]). Ignoring the construct \sqcap , which can be introduced by way of shortening notation, the Robbins laws are:

$$X \sqcup Y = Y \sqcup X, \quad X \sqcup (Y \sqcup Z) = (X \sqcup Y) \sqcup Z, \quad \overline{\overline{X \sqcup Y \sqcup X \sqcup Y}} = X.$$

2 Fields of sets

Starting with a non-void set S , let us construct the following families of sets:⁵

- $\mathcal{P}(S) =_{\text{Def}} \{x : x \subseteq S\}$, the family of *all* subsets of S ;
- $\mathcal{F}(S) =_{\text{Def}} \{x \subseteq S \mid |x| \in \mathbb{N}\}$, the family of all *finite subsets* of S ;
- $\mathcal{B}(S) =_{\text{Def}} \mathcal{F}(S) \cup \{S \setminus x : x \in \mathcal{F}(S)\}$, the family formed by those subsets of S each of which is either finite or has a *finite complement* (relative to S).

If S is finite, $\mathcal{P}(S) = \mathcal{F}(S) = \mathcal{B}(S)$ holds; otherwise, we get three families.

To get Boolean rings out of these, it suffices to define:

$$\begin{aligned} X \cdot Y &=_{\text{Def}} X \cap Y && (\textit{intersection}), \\ X + Y &=_{\text{Def}} (X \cup Y) \setminus (X \cap Y) && (\textit{symmetric difference}). \end{aligned}$$

One readily sees that $\mathcal{P}(S)$ and $\mathcal{B}(S)$ thus become Boolean algebras, whose additive identity, $\mathbf{0}$, and multiplicative identity, $\mathbf{1}$, are \emptyset and S ; as for $\mathcal{F}(S)$, it lacks $\mathbf{1}$ when S is infinite.

By generalizing the case of $\mathcal{P}(S)$ and $\mathcal{B}(S)$, one calls **FIELD OF SETS** any family \mathcal{B} which

- is closed under the operations of intersection and symmetric difference;
- has $\bigcup \mathcal{B}$ among its members, viz., owns a maximum w.r.t. set inclusion;
- differs from $\{\emptyset\}$.

This clearly is an instance of a Boolean algebra. How general? A renowned theorem by Marshall H. Stone [20] gives us the answer:

Every Boolean algebra is isomorphic to a field of sets.

This field is not always of the form $\mathcal{P}(S)$ (this holds only for particular Boolean algebras, among which the ones whose underlying domain is finite⁶): in fact it is trivial that the field $\mathcal{B}(\mathbb{N})$, whose cardinality equals the one of \mathbb{N} , cannot be isomorphic to $\mathcal{P}(S)$ for any S .⁷

3 Stone spaces

We define a **BASE OF A TOPOLOGICAL SPACE** to be a pair (\mathcal{X}, β) such that: **(i)** $\mathcal{X} \neq \emptyset$; **(ii)** $\beta \subseteq \mathcal{P}(\mathcal{X})$; **(iii)** β enjoys, w.r.t. dyadic intersection, \cap , and to monadic union, \bigcup , the following closure properties:

⁵ We designate by $|X|$ the cardinality of a set X and by \mathbb{N} the set $\{0, 1, 2, \dots\}$ of all natural numbers (which is, in its turn, a cardinal number—the first infinite one).

⁶ More generally, the Boolean algebras which are isomorphic to $\mathcal{P}(S)$ for some S are the ones which are *completely distributive*; [2, pp. 221–222] credits this result to Alfred Tarski.

⁷ Indeed, $|\mathcal{P}(S)| \in \mathbb{N}$ (i.e., $|\mathcal{P}(S)|$ is smaller than the cardinal number \mathbb{N}) when $|S| \in \mathbb{N}$; whereas $|\mathcal{P}(S)|$ exceeds \mathbb{N} —because $|\mathcal{P}(S)|$ exceeds $|S|$ —when S is infinite.

- 1) $\bigcup \beta = \mathcal{X}$,
- 2) $(A \in \beta \ \& \ B \in \beta) \rightarrow (A \cap B) \subseteq \bigcup \{c \in \beta \mid c \subseteq (A \cap B)\}$.

The TOPOLOGICAL SPACE generated by such a base is, by definition, the pair (\mathcal{X}, τ) where

$$\tau = \{\bigcup a : a \subseteq \beta\}.$$

A topological space hence is a pair (\mathcal{X}, τ) such that: **(i)** $\mathcal{X} \neq \emptyset$; **(ii)** $\tau \subseteq \mathcal{P}(\mathcal{X})$; **(iii)** τ enjoys, w.r.t. dyadic intersection, \cap , and to monadic union, \bigcup , the following closure properties:

- $\mathcal{X} \in \tau$,
- $A, B \in \tau \rightarrow (A \cap B) \subseteq \bigcup \{c \in \tau \mid c \subseteq (A \cap B)\}$,
- $\mathcal{A} \in \mathcal{F}(\tau) \rightarrow \bigcup \mathcal{A} \in \tau$,

whence it plainly follows that $A, B \in \tau \rightarrow A \cap B \in \tau$ and, more generally, that $\mathcal{A} \in \mathcal{F}(\tau) \rightarrow \bigcap \mathcal{A} \in \tau$, under the proviso that the intersection $\bigcap \emptyset$ equals \mathcal{X} .

The OPEN and the CLOSED sets of such a space are, respectively, the members of τ and their complements $\mathcal{X} \setminus A$ (with $A \in \tau$). A subset of \mathcal{X} which is open and closed is called a CLOPEN set: examples are \emptyset and \mathcal{X} . It is apparent that clopen sets form a *field of sets*.

A topological space is said to be

- a HAUSDORFF SPACE if: for every pair of *distinct* members $p, q \in \mathcal{X}$, there exist *disjoint* open sets $P, Q \subseteq \mathcal{X}$ such that $p \in P, q \in Q$;⁸
- COMPACT if: every family of open sets whose union is \mathcal{X} includes a finite subfamily whose union is \mathcal{X} .

One calls STONE SPACE any topological space which, in addition to enjoying the two properties just stated, also

- owns a BASE—namely a $\beta \subseteq \tau$ such that every open set is the union of a subfamily of β —entirely formed by clopen sets.

By relying on these concepts, one enhances the claim of Stone's theorem as follows (cf. [21,22]):

Every Boolean algebra is isomorphic to a field of sets consisting of the clopen sets of a Stone space.

In sight of the proof of this theorem, it is worthwhile to recall another way of stating the compactness property, dual to the one proposed above:

A topological space (\mathcal{X}, τ) is compact if and only if every (non-void) family \mathcal{C} of closed sets whose intersection $\bigcap \mathcal{C}$ is void has some finite subfamily whose intersection is void: $\mathcal{F} \subseteq \mathcal{C}, |\mathcal{F}| \in \mathbb{N} \setminus \{0\}, \bigcap \mathcal{F} = \emptyset$.

⁸ This definition implies that in a Hausdorff space every singleton subset of \mathcal{X} is closed.

4 Boolean ideals and their maximal enlargements

The study of an abstract algebraic structure forcibly leads one to investigate the associated homomorphisms. In the Boolean case at hand, to move resolutely in the direction that best suits our purposes, we will just consider those homomorphisms which translate the operations of a Boolean algebra (the homomorphism's domain) into the set-operations \cap, Δ of intersection and symmetric difference. The images of such a homomorphism will hence form a field of sets; particularly worth of consideration, among the homomorphisms of interest, are the ones whose values form the special field $\mathbf{2} = (\{\emptyset, \{0\}\}, \cap, \Delta, \{0\}, \emptyset)$.

Let us refer by $\mathbb{B} = (\mathcal{B}, \cdot, +, 1_{\mathcal{B}}, 0_{\mathcal{B}})$ to a Boolean algebra which, tacitly, will act as domain of the homomorphisms that will enter into play. A homomorphism of \mathbb{B} into $\mathbf{2}$ is fully characterized by either one of the two subsets of the underlying domain \mathcal{B} which are counter-images, respectively, of $0 = \emptyset$ and of $1 = \{0\}$. Not all subsets of \mathcal{B} can play the role of counter-images of the minimum via a Boolean homomorphism; let us hence figure out which conditions a set must meet in order to qualify for such a role. In investigations of this nature, algebraists tend to focus on the counter-images of the minimum, the so-called *ideals*, or 'kernels'; logicians, on the opposite, tend to focus on the counter-images of the maximum, the so-called *filters*, or 'shells'. We will conform to the algebraic habit; moreover, since we must concentrate mainly on homomorphisms into $\mathbf{2}$, we will tribute special attention to ideals which are *maximal* w.r.t. to set inclusion.

Definition 1. An IDEAL is a subset of the underlying domain \mathcal{B} which is closed with respect to addition, as well as to multiplication of its elements by elements of \mathcal{B} , and which is not one of the (exceedingly trivial) sets $\emptyset, \{0_{\mathcal{B}}\}, \mathcal{B}$.

Three theorems about ideals play a crucial role in the proof of Stone's results:

- a) Every element x of \mathcal{B} which is neither $1_{\mathcal{B}}$ nor $0_{\mathcal{B}}$ belongs to at least one ideal: the least such ideal, named a PRINCIPAL IDEAL, is simply formed by the multiples of x . It hence follows, save in the case when $\mathcal{B} = \{0_{\mathcal{B}}, 1_{\mathcal{B}}\}$, that there is at least one ideal.
- b) To each ideal I and each $x \neq 1_{\mathcal{B}}$ not belonging to I , there corresponds an ideal $J \supseteq I$ one of whose elements is \bar{x} : this is $\{a \cdot \bar{x} + y : a \in \mathcal{B}, y \in I\}$.
- c) Every ideal I is included in an ideal which is maximal w.r.t. \subseteq .

Checking the first two of these is very plain; the third can be proved by means of Zorn's lemma, after observing that every chain of ideals is closed w.r.t. union.

5 1st Stone's representation theorem

Let us recall first the algebraic version of Stone's theorem:

Theorem 1 (Stone's algebraic representation). Every Boolean algebra

$$\mathbb{B} = (\mathcal{B}, \cdot, +, 1_{\mathcal{B}}, 0_{\mathcal{B}})$$

is isomorphic to a field \mathbb{H} of sets whose underlying domain is included in $\mathcal{P}(\mathcal{H})$, where \mathcal{H} is the set of all homomorphisms from \mathbb{B} into $\mathbf{2}$.

Proof. Associate with each $x \in \mathcal{B}$ the set \widetilde{x} of those homomorphisms in \mathcal{H} which send x to $\{\emptyset\}$; thus, clearly, $\widetilde{0_{\mathcal{B}}} = \emptyset$ and $\widetilde{1_{\mathcal{B}}} = \mathcal{H}$. Moreover $\widetilde{x \cdot y} = \widetilde{x} \cap \widetilde{y}$ holds: in fact, when h is a homomorphism, $h(x \cdot y) = h(x) \cap h(y)$ equals $\{\emptyset\}$ if and only if $h(x) = h(y) = \{\emptyset\}$, i.e. iff $h \in \widetilde{x} \cap \widetilde{y}$. By an analogous argument, $h(x + y) = h(x) \Delta h(y)$ and $\widetilde{x + y} = \widetilde{x} \Delta \widetilde{y}$. Take \mathbb{H} to be the image-set of the function $x \mapsto \widetilde{x}$.

In order to see the injectivity of this function, consider the difference $e_0 = x_0 + x_0 \cdot x_1$ between two elements $x_0, x_1 \in \mathcal{B}$ such that $x_0 \cdot x_1 \neq x_0$ (whence $e_0 \neq 0_{\mathcal{B}}$). We will show that there is an $h \in \mathcal{H}$ sending e_0 to $1_{\mathcal{B}}$; accordingly, since $1_{\mathcal{B}} = h(e_0) = h(x_0 + x_0 \cdot x_1) = h(x_0) \Delta (h(x_0) \cap h(x_1))$, we will have $h(x_0) = \{\emptyset\}$, $h(x_1) = \emptyset$, and therefore $h \in \widetilde{x_0} \setminus \widetilde{x_1}$ as desired. We readily get the sought h if $\mathcal{B} = \{0_{\mathcal{B}}, 1_{\mathcal{B}}\}$; otherwise we pick a $y_0 \in \mathcal{B} \setminus \{0_{\mathcal{B}}, 1_{\mathcal{B}}\}$, choosing $y_0 = e_0$ if $e_0 \neq 1_{\mathcal{B}}$. This y_0 belongs to a principal ideal and hence to a maximal ideal M , and it is plain that the opposite $h = 1 - \chi_M$ of the characteristic function of M , manifestly a homomorphism from \mathbb{B} to $\mathbf{2}$, does to our case. \dashv

Call SET-REPRESENTATION of the algebra \mathbb{B} the field of sets just built. We will see next that this \mathbb{H} generates a very peculiar topology on \mathcal{H} .

6 2nd Stone's representation theorem

We are now ready for the topological version of Stone's theorem:

Theorem 2 (Stone's topological representation). *The field of sets by which we have represented a Boolean algebra \mathbb{B} is the base—as well as the family of all clopen sets—of a topology on the set \mathcal{H} of all homomorphisms from \mathbb{B} into $\mathbf{2}$. Once endowed with such a topology, \mathcal{H} turns out to be a Stone space.*

Proof. To see that \mathbb{H} (constructed as in the preceding proof) is the base of a topology on \mathcal{H} , we can directly check that $\mathbb{H} \subseteq \mathcal{P}(\mathcal{H})$ and $\bigcup \mathbb{H} = \mathcal{H} \neq \emptyset$ hold, and that $\bigcap F$ belongs to \mathbb{H} for every finite non-void subset F of \mathbb{H} . Indeed, \mathbb{H} is the image-set of an injective function $x \mapsto \widetilde{x}$ from \mathcal{B} into $\mathcal{P}(\mathcal{H})$, where \mathcal{B} is at least doubleton; hence, readily, $\mathcal{H} \neq \emptyset$, $\mathbb{H} \subseteq \mathcal{P}(\mathcal{H})$, and $\bigcup \mathbb{H} \subseteq \mathcal{H}$ hold. The last inclusion is in fact an equality, because \mathcal{H} , which is $\widetilde{1_{\mathcal{B}}}$, belongs to \mathbb{H} . Then we get that \mathbb{H} is closed under intersection through the remark, made above, that $\widetilde{x} \cap \widetilde{y} = \widetilde{x \cdot y}$.

Knowing, at this point, that \mathbb{H} qualifies as the base for a topology on \mathcal{H} , let us notice that all sets in \mathbb{H} are clopen in the topology τ generated by it: in fact, since $\mathcal{H} \setminus \widetilde{x} = \mathcal{H} \Delta \widetilde{x} = \widetilde{1_{\mathcal{B}}} \Delta \widetilde{x} = \widetilde{1_{\mathcal{B}} + x}$, the complement of a set in the base belongs to the base in its turn. This remark readily gives us that (\mathcal{H}, τ) is a Hausdorff space. In fact, when $f, g \in \mathcal{H}$ differ, there is an $x \in \mathcal{B}$ such that $f(x) = 1 \leftrightarrow g(x) \neq 1$; thus, since $\mathcal{H} \setminus \widetilde{x} = \widetilde{\widetilde{x}}$, we can find sets $u, v \in \tau$ such that $f \in u$, $g \in v$, and $u \cap v = \emptyset$, by also insisting that $\{u, v\} = \{\widetilde{\widetilde{x}}, \widetilde{\widetilde{x}}\}$.

It remains to be shown that the space is compact, which will also yield that every clopen set of τ belongs to \mathbb{H} .⁹ One easily sees that the closed sets in τ are: \mathcal{H} and all intersections of non-void subsets of $\{\tilde{x} : x \in \mathcal{B}\}$; compactness will hence readily follow if we manage to show that whenever $\emptyset \neq \mathcal{O} \subseteq \mathbb{H}$ and $\bigcap \mathcal{O} = \emptyset$ hold, there is an $\mathcal{F} \subseteq \mathcal{O}$ such that $|\mathcal{F}| \in \mathbb{N} \setminus \{0\}$ and $\bigcap \mathcal{F} = \emptyset$. Equivalently, assuming that $\emptyset \neq \mathcal{O} \subseteq \mathbb{H}$ and that $\bigcap \mathcal{F} \neq \emptyset$ holds for every finite non-void subset \mathcal{F} of \mathcal{O} , we will show that $\bigcap \mathcal{O} \neq \emptyset$.

Notice that the subset

$$\mathcal{B}_0 =_{\text{def}} \left\{ x : \mathcal{F} \subseteq \mathcal{O} \mid |\mathcal{F}| \in \mathbb{N} \setminus \{0\} \ \& \ \tilde{x} = \bigcap \mathcal{F} \right\} \cup \{1_{\mathcal{B}}\}$$

of \mathcal{B} meets the conditions:

- 1) $x \cdot y \in \mathcal{B}_0$ for all $x, y \in \mathcal{B}_0$,
- 2) $0_{\mathcal{B}} \notin \mathcal{B}_0 \not\subseteq \{1_{\mathcal{B}}\}$,

implying that $\{a \cdot \bar{x} : a \in \mathcal{B}, x \in \mathcal{B}_0\}$ is an ideal of \mathbb{B} . By enlarging this into a maximal ideal, we get the kernel of a homomorphism h sending all complements of el'ts of \mathcal{B}_0 to \emptyset , hence sending all elements of \mathcal{B}_0 to $\{\emptyset\}$. Thus, $h \in \bigcap \mathcal{O}$. \dashv

7 Formalization of Stone's representation theorems in Ref

This section offers glimpses of our formal development of Stone's result on the representability of Boolean algebras via the clopen sets of a totally disconnected, compact Hausdorff space. In carrying out this task, we relied on a proof checker: Ref. Our experiment culminated in a rather elaborate series of mathematical claims, shown not in this section, but in the appendix.

Organization and rationale of our automated proof assistant are extensively discussed in [19]; but so far, due to the short time elapsed from its implementation, Ref is not widely known. Hence, putting aside our report on our experiment for a moment, we devote a quick subsection to introducing Ref itself.

7.1 Brief presentation of the proof-checking framework

Ref is a proof assistant for mathematics based on a variant of Zermelo-Fraenkel set theory, which is "hardwired" in Ref's proof-checking abilities. From the user Ref receives script files, called *scenarios*, consisting of successive definitions, theorems, and auxiliary commands, which it either certifies as constituting a valid sequence or rejects as defective. In the case of rejection, the verifier attempts to pinpoint the troublesome locations within a scenario, so that errors can be

⁹ To derive from compactness that $\bigcup \mathcal{O} \in \mathbb{H}$ holds when $\mathcal{O} \subseteq \mathbb{H}$ and $\bigcup \mathcal{O}$ is closed, we argue as follows. Assuming, w.l.o.g., that $\emptyset \neq \mathcal{O}$, since $\emptyset = (\bigcup \mathcal{O}) \cap (\mathcal{H} \setminus \bigcup \mathcal{O}) = (\bigcup \mathcal{O}) \cap \bigcap \{\mathcal{H} \setminus u : u \in \mathcal{O}\}$ is the intersection of a family of closed sets, we can pick an \mathcal{F} such that $\emptyset \neq \mathcal{F} \subseteq \mathcal{O}$, $|\mathcal{F}| \in \mathbb{N}$, and $(\bigcup \mathcal{O}) \cap \bigcap \{\mathcal{H} \setminus u : u \in \mathcal{F}\} = \emptyset$. Thus $\bigcup \mathcal{O} = \bigcap \{\mathcal{H} \setminus u : u \in \mathcal{F}\} \in \mathbb{H}$, because \mathbb{H} is closed relative to complementation and to finite intersection.

located and repaired. Step timings are produced even for correct proofs, to help the user in spotting places where appropriate modifications could speed up proof processing.

The bulk of the text normally submitted to the verifier consists of *theorems and proofs*. Some theorems (and their proofs) are enclosed within so-called **THEORYS**, whose external conclusions are justified by these internal theorems. This lets scenarios be subdivided into modules, which increases the readability and supports proof reuse.

Many theorems are not enclosed within a user-defined **THEORY**; when this happens, they belong on their own right to the underlying “big” **THEORY** identified by the name `Set_theory`.

Of all relationships treated within `Set_theory`, the most fundamental is *membership*, \in , which is supposed to be well founded in the sense that no infinite sequence x_0, x_1, x_2, \dots of sets can satisfy $x_{i+1} \in x_i$ for every i . The well foundedness of \in is witnessed by the built-in *arbitrary selection* operator, **arb**, meeting the conditions $\mathbf{arb}(x) \in x$ and $\mathbf{arb}(x) \cap x = \emptyset$ for every set x other than the null set \emptyset (about which the equality $\mathbf{arb}(\emptyset) = \emptyset$ is assumed).

At their simplest *definitions* are merely abbreviations which concentrate attention on interesting constructs by assigning them names which shorten their syntactic form (an example of this kind is the definition of finitude that we will soon meet). Beyond this simple level, Ref offers a primitive scheme of \in -recursive definition legitimized by the well foundedness of \in and illustrated, e.g., by the following specification:

$$\boxed{\text{DEF : [Join singletons] } \mathbf{filum}(X) =_{\text{Def}} \{X\} \cup \mathbf{arb}(\{\mathbf{filum}(y) : y \in X \mid X = \{y\}\})}$$

(This collects together into $\mathbf{filum}(X)$ all elements of the finitely many singletons “spreading”—in a quite definite sense—from $\{X\}$.)

This example also shows the availability, in the formal language of Ref, of perspicuous *set-formers* such as $\{\mathbf{filum}(y) : y \in X \mid X = \{y\}\}$. Just in order to see a few other set-formers at work, consider the following shorthand definitions:

$$\begin{aligned} \bigcup Y &=_{\text{Def}} \{z : x \in Y, z \in x\}, \\ \mathbf{edges}(V, E) &=_{\text{Def}} \{\{x, y\} : x \in V, y \in V \mid x \neq y\} \cap E, \\ \mathbf{Connected}(E) &\leftrightarrow_{\text{Def}} \{\mathbf{b} : \mathbf{b} \subseteq E \mid \bigcup \mathbf{b} \cap \bigcup (E \setminus \mathbf{b}) = \emptyset\} \subseteq \{\emptyset, E\}. \end{aligned}$$

A very small Ref scenario, consisting of one definition (involving yet another set-former) and two theorems with their proofs, is shown in Fig. 2. As one sees there, each inference step in a Ref proof has two components, separated by the ‘ \Rightarrow ’ sign: on the right of which a logical statement (sometimes hidden behind one of the keywords **AUTO**, **QED**) appears; while, on the left, there is a justification of the statement, namely an indication of which inference method enables its derivation from the preceding part of the proof.

Last but not least, Ref supports proof reuse through a construct named **THEORY**, essentially a second-order form of Skolemization. Fig. 3 shows the interface of a specific **THEORY**, named `finite_image`, which has two input parameters: s_0 , a

DEF \mathcal{P} : [Family of all subsets of a given set] $\mathcal{P}S =_{\text{Def}} \{x : x \subseteq S\}$

THM pow_0 : [No set equals its own powerset] $(X \supseteq Y \leftrightarrow Y \in \mathcal{P}X) \ \& \ X \neq \mathcal{P}X$. PROOF:

```

Suppose_not( $x_0, y_0$ )  $\Rightarrow$  AUTO
Use_def( $\mathcal{P}x_0$ )  $\Rightarrow$  AUTO
Suppose  $\Rightarrow$   $x_0 = \mathcal{P}x_0$ 
ELEM  $\Rightarrow$   $\text{Stat}0 : x_0 \notin \{y : y \subseteq x_0\}$ 
 $\langle x_0 \rangle \hookrightarrow \text{Stat}0 \Rightarrow$  false; Discharge  $\Rightarrow$  AUTO
EQUAL  $\Rightarrow$   $\text{Stat}1 : x_0 \supseteq y_0 \neq y_0 \in \{y : y \subseteq x_0\}$ 
Suppose  $\Rightarrow$   $\text{Stat}2 : y_0 \in \{y : y \subseteq x_0\}$ 
 $\langle y_1 \rangle \hookrightarrow \text{Stat}2(\text{Stat}1\star) \Rightarrow$  false; Discharge  $\Rightarrow$   $\text{Stat}3 : y_0 \notin \{y : y \subseteq x_0\}$ 
 $\langle y_0 \rangle \hookrightarrow \text{Stat}3(\text{Stat}1\star) \Rightarrow$  false; Discharge  $\Rightarrow$  QED

```

THM pow_1 : [Monotonicity of powerset] $S \supseteq X \rightarrow \mathcal{P}X \cup \{\emptyset, X\} \subseteq \mathcal{P}S$. PROOF:

```

Suppose_not( $s_0, x_0$ )  $\Rightarrow$  AUTO
Set_monot  $\Rightarrow$   $\{x : x \subseteq x_0\} \subseteq \{x : x \subseteq s_0\}$ 
Use_def( $\mathcal{P}$ )  $\Rightarrow$   $\text{Stat}1 : \emptyset \notin \{x : x \subseteq s_0\} \vee x_0 \notin \{x : x \subseteq s_0\}$ 
 $\langle \emptyset, x_0 \rangle \hookrightarrow \text{Stat}1 \Rightarrow$  false; Discharge  $\Rightarrow$  QED

```

THM pow_2 : [Powerset of null set and of singletons] $\mathcal{P}\emptyset = \{\emptyset\}$ &

$\mathcal{P}\{X\} = \{\emptyset, \{X\}\}$. PROOF:

```

Suppose_not( $x_0$ )  $\Rightarrow$  AUTO
Suppose  $\Rightarrow$   $\mathcal{P}\emptyset \neq \{\emptyset\}$ 
 $\langle \emptyset, \emptyset \rangle \hookrightarrow \text{Tp}ow_1 \Rightarrow$   $\text{Stat}0 : \mathcal{P}\emptyset \not\subseteq \{\emptyset\}$ 
 $\langle y_0 \rangle \hookrightarrow \text{Stat}0(\text{Stat}0\star) \Rightarrow$   $\text{Stat}1 : y_0 \in \mathcal{P}\emptyset \ \& \ y_0 \notin \{\emptyset\}$ 
 $\langle \emptyset, y_0 \rangle \hookrightarrow \text{Tp}ow_0(\text{Stat}1\star) \Rightarrow$  false; Discharge  $\Rightarrow$   $\mathcal{P}\{x_0\} \neq \{\emptyset, \{x_0\}\}$ 
 $\langle \{x_0\}, \{x_0\} \rangle \hookrightarrow \text{Tp}ow_1 \Rightarrow$   $\text{Stat}2 : \mathcal{P}\{x_0\} \not\subseteq \{\emptyset, \{x_0\}\}$ 
 $\langle y_1 \rangle \hookrightarrow \text{Stat}2 \Rightarrow$   $\text{Stat}3 : y_1 \in \mathcal{P}\{x_0\} \ \& \ y_1 \notin \{\emptyset, \{x_0\}\}$ 
 $\langle \{x_0\}, y_1 \rangle \hookrightarrow \text{Tp}ow_0(\text{Stat}3\star) \Rightarrow$  false; Discharge  $\Rightarrow$  QED

```

Fig. 2. Tiny sample of a Ref scenario

finite set, and g , a global function. Inside `finite_image`, from the assumed finiteness of s_0 the user has derived that $\{g(x) : x \in s_0\}$ is a finite set; moreover, (s)he has defined the output parameter f_\emptyset so as to insure that f_\emptyset be an \subseteq -minimal subset of s_0 such that f_\emptyset and s_0 are sent by g to the same image.

```

THEORY finite_image ( $s_0, g(X)$ )
  Finite( $s_0$ )
 $\Rightarrow$  ( $f_\emptyset$ )
  Finite( $\{g(x) : x \in s_0\}$ )
   $f_\emptyset \subseteq s_0 \ \& \ \langle \forall t \subseteq f_\emptyset \mid g(t) = g(s_0) \leftrightarrow t = f_\emptyset \rangle$ 
END finite_image

```

Fig. 3. Interface of a THEORY specifying an induction principle

7.2 Excerpts from our proof scenario of Stone's theorems

As a warm-up exercise, we developed with the assistance of Ref the **THEORY** `pord` displayed in Fig. 4, showing that every partially ordered set is isomorphic to a family of sets partially ordered by inclusion. The assumptions of `pord` state that `Le` must be a partial ordering of `dd`. By sending each element x of `dd` to the set consisting of those elements of `dd` which are smaller than or equal to x , we get an order monomorphism between (dd, Le) and $(\mathcal{P}(dd), \subseteq)$: whose name '`polsoΘ`', as indicated by the subscript Θ , is specified—along with its definition—inside the **THEORY**.

```

THEORY pord(dd, Le(U, V))
  ⟨∀x, y | {x, y} ⊆ dd → (Le(x, y) & Le(y, x) ↔ x = y)⟩
  ⟨∀x, y, z | {x, y, z} ⊆ dd → Le(x, y) & Le(y, z) → Le(x, z)⟩
⇒ (polsoΘ)
  polsoΘ = { [x, {v ∈ dd | Le(v, x)}] : x ∈ dd }
  ⟨∀x | x ∈ dd → Le(x, x) & polsoΘ | x = {v ∈ dd | Le(v, x)}⟩
  ⟨∀x, y | {x, y} ⊆ dd → (Le(x, y) ↔ polsoΘ | x ⊆ polsoΘ | y)⟩
  1-1(polsoΘ) & domain(polsoΘ) = dd
END pord

```

Fig. 4. Interface of a representation **THEORY** about partial orderings

Our next step consisted in developing a theory of Boolean rings:

```

THEORY booleanRing(bb, ·, ÷)
  bb ≠ ∅
  ⟨∀x, y | {x, y} ⊆ bb → x · y ∈ bb⟩
  ⟨∀x, y | {x, y} ⊆ bb → x ÷ y ∈ bb⟩
  ⟨∀x, y, z | {x, y, z} ⊆ bb → x · (y · z) = (x · y) · z⟩
  ⟨∀x, y, z | {x, y, z} ⊆ bb → x ÷ (y ÷ z) = (x ÷ y) ÷ z⟩
  ⟨∀x, y, z | {x, y, z} ⊆ bb → (x ÷ y) · z = z · y ÷ z · x⟩
  ⟨∀x, y | {x, y} ⊆ bb → x ÷ x = y ÷ y⟩
  ⟨∀x, y | {x, y} ⊆ bb → x ÷ (y ÷ x) = y⟩
  ⟨∀x | x ∈ bb → x · x = x⟩
⇒ (zzΘ)
  zzΘ = arb(bb) ÷ arb(bb)
  ⟨∀x | (x ∈ bb → x ÷ x = zzΘ & x ÷ zzΘ = x & zzΘ ÷ x = x) & zzΘ ∈ bb⟩
  ⟨∀x, y | x, y ∈ bb → x ÷ y = y ÷ x⟩
  ⟨∀x, y | x, y ∈ bb → x · y = y · x⟩
  ⟨∀x | x ∈ bb → zzΘ · x = zzΘ⟩
  ⟨∀u, v | {u, v} ⊆ bb & u · v = u & v · u = v → u = v⟩
END booleanRing

```

Here zz_{\emptyset} designates the additive identity. Notice, among the internally derived claims, the commutativity laws.

Due to its entirely algebraic character, this **THEORY** could have been developed somewhat more easily with an autonomous theorem prover oriented to the treatment of equality: as announced in [6, Sec. 3], we plan to implement interfaces between Ref and outer automated proof assistants.

Our next **THEORY**, presupposing the definition of symmetric difference, shows that rings of sets match the assumptions of the **THEORY** `booleanRing`:

THEORY `protoBoolean(dd)`

$\emptyset \neq \bigcup dd$

$\langle \forall x, y \mid \{x, y\} \subseteq dd \rightarrow x \cap y \in dd \rangle$

$\langle \forall x, y \mid \{x, y\} \subseteq dd \rightarrow x \Delta y \in dd \rangle$

\Rightarrow

$dd \neq \emptyset$

$\langle \forall x \in dd, y \in dd, z \in dd \mid x \cap (y \cap z) = (x \cap y) \cap z \rangle$

$\langle \forall x \in dd, y \in dd, z \in dd \mid x \Delta (y \Delta z) = (x \Delta y) \Delta z \rangle$

$\langle \forall x \in dd, y \in dd, z \in dd \mid (x \Delta y) \cap z = z \cap y \Delta z \cap x \rangle$

$\langle \forall x \in dd, y \in dd \mid x \Delta x = y \Delta y \rangle$

$\langle \forall x \in dd, y \in dd \mid x \Delta (y \Delta x) = y \rangle$

$\langle \forall x \in dd \mid x \cap x = x \rangle$

END `protoBoolean`

Two claims, proved inside the background **THEORY**, namely `Set_theory`, and presupposing the definition of \mathcal{P} , show that the family of all subsets, and the one of all finite and cofinite subsets, of a non-void set constitute instances of `protoBoolean`:

THM . $W \neq \emptyset \ \& \ \{X, Y\} \subseteq \mathcal{P}W \rightarrow \{X \cap Y, X \Delta Y\} \subseteq \mathcal{P}W \ \& \ \bigcup(\mathcal{P}W) \neq \emptyset$,

THM . $W \neq \emptyset \ \& \ D = \{s \subseteq W \mid \text{Finite}(s) \vee \text{Finite}(W \setminus s)\} \ \& \ \{X, Y\} \subseteq D \rightarrow$
 $\{X \cap Y, X \Delta Y\} \subseteq D \ \& \ \bigcup D \neq \emptyset$.

Another **THEORY**, akin to the preceding one, introduces a slightly more specific algebraic variety than the one treated by `protoBoolean`:

THEORY `archoBoolean(dd)`

$\emptyset \neq \bigcup dd$

$\langle \forall x, y, z \mid \{x, y\} \subseteq dd \ \& \ z \subseteq x \cup y \rightarrow z \in dd \rangle$

\Rightarrow

$\langle \forall x, y \mid \{x, y\} \subseteq dd \rightarrow x \cap y \in dd \rangle$

$\langle \forall x, y \mid \{x, y\} \subseteq dd \rightarrow x \Delta y \in dd \rangle$

$dd \neq \emptyset$

END `archoBoolean`

After switching back to the background `Set_theory` level, one proves that there are fields of sets which are instances of `protoBoolean` but are not instances

of `archoBoolean`. Indeed, the collection of all finite and cofinite subsets of an infinite set is not closed with respect to inclusion.

$$\text{THM . } \neg\text{Finite}(W) \ \& \ D = \{s \subseteq W \mid \text{Finite}(s) \vee \text{Finite}(W \setminus s)\} \rightarrow \\ W \in D \ \& \ \langle \exists z \subseteq W \mid z \notin D \rangle.$$

Surprisingly enough, it is unnecessary to resort to a theory of cardinals of any sophistication in order to get the result just cited: the distinction between *finite* sets and sets which are not finite more than suffices for that purpose, where the following definition applies:

$$\text{DEF : [Finitude] Finite(F) } \leftrightarrow_{\text{Def}} \langle \forall g \in \mathcal{P}(\mathcal{P}F) \setminus \{\emptyset\}, \exists m \mid g \cap \mathcal{P}m = \{m\} \rangle$$

Last but not least, we developed the `THEORY booleanAlgebra` whose interface is shown in the Appendix.

Conclusions and future work

Proof-verification can highly benefit from representation theorems of the kind illustrated by Stone’s results on Boolean algebras. On the human side, such results disclose new insights by shedding light on a discipline from unusual angles; on the technological side, they enable the transfer of proof methods from one realm of mathematics to another.

Examples of this can be found in various recent proofs concerning *connected claw-free graphs*:¹⁰ thanks to a convenient choice on how to represent those graphs, Milanič and Tomescu [13] proved with relative ease two classical propositions, namely that any such graph owns a near-perfect matching and has a Hamiltonian cycle in its square; a proof of the somewhat deeper theorem [8] that all connected claw-free graphs have a *vertex-pancyclic* square was also attained cheaply through the same representation [23]. Specifically, the facilitation stems from transferring those results to the special class of the *membership digraphs*, whose set of vertices is a hereditarily finite set and whose arcs precisely reflect the membership relation between vertices. Under this change of perspective, a fully formal reconstruction of the first two results became affordable and, once carried out, was certified correct with the `Ref` proof-checker [15,17,18].

This motivated us in undertaking the formal development, with `Ref`, of proofs of various representation theorems (see also [1]). An envisaged continuation of the present work will be in the direction of MV-algebras (cf. [14,5,3,11]).

¹⁰ A graph is said to be *claw-free* if no induced subgraph of its is isomorphic to the graph, called *the claw*: $K_{1,3} = (\{w, x, y, z\}, \{\{y, x\}, \{y, z\}, \{y, w\}\})$.

References

1. P. Calligaris, E. G. Omodeo, and A. I. Tomescu. A proof-checking experiment on representing graphs as membership digraphs. In D. Cantone and M. Nicolosi Asmundo, editors, *CILC 2013: Italian Conference on Computational Logic*, volume 1068 <http://ceur-ws.org/Vol-1068/>, ISSN 1613-0073, pages 227–233. CEUR Workshop Proceedings, Sept. 2013.
2. Paul Moritz Cohn. *Universal Algebra*. Harper and Row, 1965.
3. E. J. Dubuc and Y. A. Poveda. Representation theory of MV-algebras. *Ann. Pure Appl. Logic*, 161(8):1024–1046, 2010.
4. Nelson Dunford and Jacob T. Schwartz. *Linear Operators, Part I General Theory*. Interscience Publishers, 1958.
5. A. Dvurečenskij. Pseudo MV-algebras are intervals in ℓ -groups. *J. Austral. Math. Soc.*, 72:427–425, 2002.
6. Andrea Formisano and Eugenio G. Omodeo. Theory-specific automated reasoning. In Agostino Dovier and Enrico Pontelli, editors, *A 25-Year Perspective on Logic Programming: Achievements of the Italian Association for Logic Programming, GULP*, volume 6125 of *Lecture Notes in Computer Science*, pages 37–63. Springer, 2010.
7. Paul R. Halmos. *Algebraic Logic*. AMS Chelsea Publishing, Providence, Rhode Island, 1962.
8. George Hendry and Walter Vogler. The square of a connected $S(K_{1,3})$ -free graph is vertex pancyclic. *Journal of Graph Theory*, 9(4):535–537, 1985.
9. Nathan Jacobson. *Lectures in Abstract Algebra, Vol.1 – Basic Concepts*. D. Van Nostrand, New York, 1951.
10. G. Kolata. With major math proof, brute computers show flash of reasoning power. *The New York Times*, Dec. 10, 1996.
11. M. Konig. Gödel Łukasiewicz logic. *LP&S – Logic and Philosophy of Science*, VIII(1):119–142, 2010.
12. W. W. McCune. Solution of the Robbins problem. *J. of Automated Reasoning*, 19(3):263–276, 1997.
13. M. Milanič and A. I. Tomescu. Set graphs. I. Hereditarily finite sets and extensional acyclic orientations. *Discrete Applied Mathematics*, 161(4-5):677–690, 2013.
14. D. Mundici. Interpretation of af c^* -algebras in Łukasiewicz sentential calculus. *J. Funct. Anal.*, 65:15–63, 1986.
15. E. G. Omodeo. The Ref proof-checker and its “common shared scenario”. In Martin Davis and Ed Schonberg, editors, *From Linear Operators to Computational Biology: Essays in Memory of Jacob T. Schwartz*, pages 121–131. Springer, 2012.
16. E. G. Omodeo and A. I. Tomescu. Using Ætнанova to formally prove that the Davis-Putnam satisfiability test is correct. *Le Matematiche*, 63(1):85–105, 2008.
17. E. G. Omodeo and A. I. Tomescu. Appendix: Claw-free graphs as sets. In Martin Davis and Ed Schonberg, editors, *From Linear Operators to Computational Biology: Essays in Memory of Jacob T. Schwartz*, pages 131–167. Springer, 2012.
18. E. G. Omodeo and A. I. Tomescu. Set graphs. III. Proof Pearl: Claw-free graphs mirrored into transitive hereditarily finite sets. *J. Autom. Reason.*, 52(1):1–29, 2014.
19. J.T. Schwartz, D. Cantone, and E.G. Omodeo. *Computational Logic and Set Theory - Applying Formalized Logic to Analysis*. Springer, 2011.
20. Marshall H. Stone. The theory of representations for Boolean algebras. *Transactions of the American Mathematical Society*, 40:37–111, 1936.

21. Marshall H. Stone. Applications of the theory of Boolean rings to general topology. *Transactions of the American Mathematical Society*, 41:375–481, 1937.
22. Marshall H. Stone. The representation of Boolean algebras. *Bulletin of the American Mathematical Society*, 44(Part 1):807–816, 1938.
23. Alexandru I. Tomescu. A simpler proof for vertex-pancyclicity of squares of connected claw-free graphs. *Discrete Mathematics*, 312(15):2388–2391, 2012.

A The main theory in our scenario on Boolean algebras

THEORY booleanAlgebra($\mathcal{B}, \cdot, \div, 1_{\mathcal{B}}$)

$$\begin{aligned}
& 1_{\mathcal{B}} \in \mathcal{B} \\
& 1_{\mathcal{B}} \neq 1_{\mathcal{B}} \div 1_{\mathcal{B}} \\
& \langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \rightarrow x \cdot y \in \mathcal{B} \rangle \\
& \langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \rightarrow x \div y \in \mathcal{B} \rangle \\
& \langle \forall x, y, z \mid \{x, y, z\} \subseteq \mathcal{B} \rightarrow x \cdot (y \cdot z) = (x \cdot y) \cdot z \rangle \\
& \langle \forall x, y, z \mid \{x, y, z\} \subseteq \mathcal{B} \rightarrow x \div (y \div z) = (x \div y) \div z \rangle \\
& \langle \forall x, y, z \mid \{x, y, z\} \subseteq \mathcal{B} \rightarrow (x \div y) \cdot z = z \cdot y \div z \cdot x \rangle \\
& \langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \rightarrow x \div x = y \div y \rangle \\
& \langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \rightarrow x \div (y \div x) = y \rangle \\
& \langle \forall x \mid x \in \mathcal{B} \rightarrow x \cdot x = x \rangle \\
& \langle \forall x \mid x \in \mathcal{B} \rightarrow 1_{\mathcal{B}} \cdot x = x \rangle \\
\Rightarrow & (0_{\theta}, (\bar{\quad})_{\theta}, \text{Ideal}_{\theta}, \text{BooHom}_{\theta}, \mathcal{H}_{\theta}, \varphi_{\theta}) \\
& 0_{\theta} = \text{arb}(\mathcal{B}) \div \text{arb}(\mathcal{B}) \\
& \langle \forall x \mid (x \in \mathcal{B} \rightarrow x \div x = 0_{\theta} \ \& \ x \div 0_{\theta} = x \ \& \ 0_{\theta} \div x = x) \ \& \ 0_{\theta} \in \mathcal{B} \rangle \\
& \langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \rightarrow x \div y = y \div x \rangle \\
& \langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \rightarrow x \cdot y = y \cdot x \rangle \\
& \langle \forall u, v \mid \{u, v\} \subseteq \mathcal{B} \ \& \ u \cdot v = u \ \& \ v \cdot u = v \rightarrow u = v \rangle \\
& \langle \forall x \mid x \in \mathcal{B} \rightarrow (\bar{x})_{\theta} = 1_{\mathcal{B}} \div x \rangle \\
& \langle \forall x \mid (x \in \mathcal{B} \rightarrow (\bar{x})_{\theta} \in \mathcal{B} \ \& \ (\overline{(\bar{x})_{\theta}})_{\theta} = x) \ \& \ (\overline{1_{\mathcal{B}}})_{\theta} = 0_{\theta} \ \& \ (\overline{0_{\theta}})_{\theta} = 1_{\mathcal{B}} \rangle \\
& \langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \rightarrow (\bar{x})_{\theta} \div x = 1_{\mathcal{B}} \ \& \ y \cdot x \div y \cdot (\bar{x})_{\theta} = y \ \& \ y \cdot x \cdot (y \cdot (\bar{x})_{\theta}) = 0_{\theta} \rangle \\
& \langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \rightarrow (\overline{x \div y})_{\theta} = x \cdot y \div (\bar{x})_{\theta} \cdot (\bar{y})_{\theta} \rangle \\
& \langle \forall x \mid x \in \mathcal{B} \rightarrow (\bar{x})_{\theta} \neq x \ \& \ (x \notin \{0_{\theta}, 1_{\mathcal{B}}\} \rightarrow (\bar{x})_{\theta} \in \mathcal{B} \setminus \{0_{\theta}, 1_{\mathcal{B}}\}) \rangle \\
& \langle \forall u, v \mid \{u, v\} \subseteq \mathcal{B} \ \& \ u \cdot v = 1_{\mathcal{B}} \rightarrow u = 1_{\mathcal{B}} \ \& \ v = 1_{\mathcal{B}} \rangle \\
& \langle \forall u, v, x, y \mid \{u, v, x, y\} \subseteq \mathcal{B} \rightarrow u \cdot (\bar{x})_{\theta} \div v \cdot (\bar{y})_{\theta} = (u \cdot (\bar{x})_{\theta} \div v \cdot (\bar{y})_{\theta}) \cdot (\overline{x \cdot y})_{\theta} \rangle \\
& \langle \forall i \mid \text{Ideal}_{\theta}(i) \leftrightarrow \{x \div y : x \in i, y \in i\} \subseteq i \ \& \ \{x \cdot y : x \in \mathcal{B}, y \in i\} \subseteq i \ \& \ i \subseteq \mathcal{B} \setminus \{1_{\mathcal{B}}\} \ \& \ i \not\subseteq \{0_{\theta}\} \rangle \\
& \langle \forall i, x, y \mid \text{Ideal}_{\theta}(i) \ \& \ \{x, y\} \subseteq i \rightarrow x \div y \in i \rangle \\
& \langle \forall i \mid \text{Ideal}_{\theta}(i) \rightarrow 0_{\theta} \in i \ \& \ (x \in i \ \& \ y \in \mathcal{B} \rightarrow x \cdot y, y \cdot x \in i \ \& \ (\bar{x})_{\theta} \notin i) \ \& \ 1_{\mathcal{B}} \notin i \rangle \\
& \langle \forall i \mid \text{Ideal}_{\theta}(i) \rightarrow \langle \exists m \mid i \subseteq m \ \& \ \langle \forall j \mid \text{Ideal}_{\theta}(j) \ \& \ m \subseteq j \leftrightarrow j = m \rangle \rangle \rangle \\
& \langle \forall b \mid b \subseteq \mathcal{B} \setminus \{0_{\theta}\} \ \& \ \{x \cdot y : x \in b, y \in b\} \subseteq b \ \& \ b \not\subseteq \{1_{\mathcal{B}}\} \rightarrow \text{Ideal}_{\theta}(\{a \cdot (\bar{x})_{\theta} : a \in \mathcal{B}, x \in b\}) \rangle \\
& \langle \forall x \mid x \in \mathcal{B} \setminus \{0_{\theta}, 1_{\mathcal{B}}\} \rightarrow \text{Ideal}_{\theta}(\{a \cdot x : a \in \mathcal{B}\}) \ \& \ x \in \{a \cdot x : a \in \mathcal{B}\} \rangle \\
& \langle \forall h \mid \text{BooHom}_{\theta}(h) \leftrightarrow \text{Svm}(h) \ \& \ \text{domain}(h) = \mathcal{B} \ \& \ h \upharpoonright 1_{\mathcal{B}} = \bigcup \text{range}(h) \ \& \ h \upharpoonright 1_{\mathcal{B}} \neq h \upharpoonright 0_{\theta} \ \& \\
& \quad \langle \forall x \in \mathcal{B}, y \in \mathcal{B} \mid h \upharpoonright (x \cdot y) = h \upharpoonright x \cap h \upharpoonright y \ \& \ h \upharpoonright (x \div y) = h \upharpoonright x \Delta h \upharpoonright y \rangle \rangle
\end{aligned}$$

$$\begin{aligned}
\mathcal{H}_\theta &= \{h \subseteq \mathcal{B} \times 2 \mid \text{BooHom}_\theta(h)\} \\
&\langle \forall h \mid h \in \mathcal{H}_\theta \rightarrow h \upharpoonright 0_\theta = \emptyset \ \& \ h \upharpoonright 1_\mathcal{B} = 1 \rangle \\
&\langle \forall h \mid h \in \mathcal{H}_\theta \ \& \ \{x, y\} \subseteq \mathcal{B} \ \& \ h \upharpoonright (x \div x \cdot y) = 1 \ \& \ h \upharpoonright y = \emptyset \rightarrow h \upharpoonright x = 1 \rangle \\
&\langle \forall i, x \mid \text{Ideal}_\theta(i) \ \& \ x \in \mathcal{B} \ \& \ (\bar{x})_\theta \notin i \rightarrow \langle \exists j \mid \text{Ideal}_\theta(j) \ \& \ i \cup \{x\} \subseteq j \rangle \rangle \\
&\langle \forall x, m \mid x \notin m \ \& \ x \in \mathcal{B} \ \& \ \langle \forall j \mid \text{Ideal}_\theta(j) \ \& \ m \subseteq j \leftrightarrow j = m \rangle \rightarrow (\bar{x})_\theta \in m \rangle \\
&\langle \forall m \mid \langle \forall j \mid \text{Ideal}_\theta(j) \ \& \ m \subseteq j \leftrightarrow j = m \rangle \rightarrow \{[x, \text{if } x \in m \text{ then } \emptyset \text{ else } 1 \text{ fi}] : x \in \mathcal{B}\} \in \mathcal{H}_\theta \rangle \\
\mathcal{B} &\subseteq \{0_\theta, 1_\mathcal{B}\} \rightarrow \{[0_\theta, \emptyset], [1_\mathcal{B}, 1]\} \in \mathcal{H}_\theta \\
&\langle \forall x \in \mathcal{B} \setminus \{0_\theta\} \mid \{h \in \mathcal{H}_\theta \mid h \upharpoonright x = 1\} \neq \emptyset \rangle \ \& \ \mathcal{H}_\theta \neq \emptyset \\
\varphi_\theta &= \{[b, \{h \in \mathcal{H}_\theta \mid h \upharpoonright b = 1\}] : b \in \mathcal{B}\} \\
&\langle \forall x \in \mathcal{B} \mid \varphi_\theta \upharpoonright x = \{h \in \mathcal{H}_\theta \mid h \upharpoonright x = 1\} \rangle \\
&\langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \rightarrow \varphi_\theta \upharpoonright (x \cdot y) = \varphi_\theta \upharpoonright x \cap \varphi_\theta \upharpoonright y \ \& \ \varphi_\theta \upharpoonright (x \div y) = \varphi_\theta \upharpoonright x \Delta \varphi_\theta \upharpoonright y \rangle \\
&\langle \forall x, y \mid \{x, y\} \subseteq \mathcal{B} \ \& \ x \cdot y \neq x \rightarrow \varphi_\theta \upharpoonright x \neq \varphi_\theta \upharpoonright y \rangle \\
\mathcal{H}_\theta &= \bigcup \text{range}(\varphi_\theta) \ \& \ \varphi_\theta \upharpoonright 0_\theta = \emptyset \ \& \ \varphi_\theta \upharpoonright 1_\mathcal{B} \neq \varphi_\theta \upharpoonright 0_\theta \ \& \ \varphi_\theta \upharpoonright 1_\mathcal{B} = \mathcal{H}_\theta \\
&\langle \forall x \in \mathcal{B} \mid \varphi_\theta \upharpoonright (\bar{x})_\theta = \mathcal{H}_\theta \setminus \varphi_\theta \upharpoonright x \rangle \\
1-1(\varphi_\theta) \ \& \ \text{domain}(\varphi_\theta) &= \mathcal{B} \\
\text{BooHom}_\theta(\varphi_\theta) & \\
\text{range}(\varphi_\theta) &\subseteq \{x : x \subseteq \mathcal{H}_\theta\} \ \& \ \emptyset \in \text{range}(\varphi_\theta) \ \& \ \mathcal{H}_\theta \in \text{range}(\varphi_\theta) \\
&\langle \forall u \in \text{range}(\varphi_\theta) \mid \mathcal{H}_\theta \setminus u \in \text{range}(\varphi_\theta) \rangle \\
&\langle \forall f, g \mid \{f, g\} \subseteq \mathcal{H}_\theta \ \& \ f \neq g \rightarrow \langle \exists u \in \text{range}(\varphi_\theta), v \in \text{range}(\varphi_\theta) \mid f \in u \ \& \ g \in v \ \& \ u \cap v = \emptyset \rangle \rangle \\
&\langle \forall f \subseteq \text{range}(\varphi_\theta) \mid f \neq \emptyset \ \& \ \text{Finite}(f) \rightarrow \bigcap f \in \text{range}(\varphi_\theta) \rangle \\
&\langle \forall k \subseteq \text{range}(\varphi_\theta) \mid k \neq \emptyset \ \& \ \bigcap k = \emptyset \rightarrow \langle \exists f \subseteq k \mid f \neq \emptyset \ \& \ \text{Finite}(f) \rightarrow \bigcap f = \emptyset \rangle \rangle
\end{aligned}$$

END booleanAlgebra