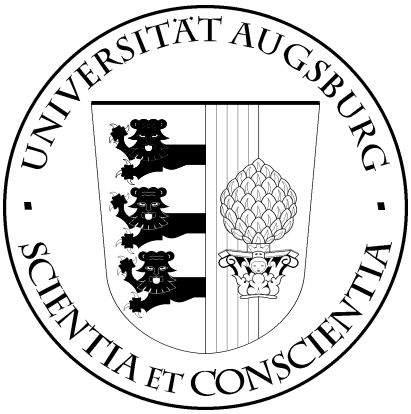
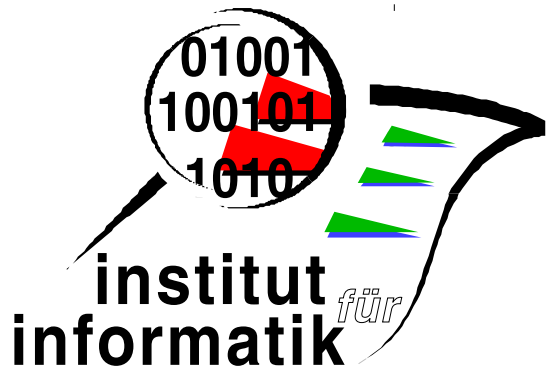
Universität Augsburg



A Calculus for Set-Based Program Development
Part I: Mathematical Foundations

Georg Struth

Report 2003-15 September 2003



Institut für Informatik
D-86135 Augsburg

A Calculus for Set-Based Program Development Part I: Mathematical Foundations

Georg Struth

Institut für Informatik, Universität Augsburg
Universitätsstr. 14, D-86135 Augsburg, Germany
Tel:+49-821-598-3109, Fax:+49-821-598-2274,
struth@informatik.uni-augsburg.de

Abstract We propose an algebraic core calculus for naive or intuitive set theory. We reconstruct a fragment of set theory via atomic distributive lattices. Semantically, atomic distributive lattices extend boolean reasoning about sets by element-wise reasoning; the ontological commitment to a universal set is avoided. Operationally, reasoning with atomic distributive lattices yields abstract, concise, elegant proofs for sets from a few elementary principles. We also present an algebraic treatment of extensionality in terms of a lattice congruence. Our results are particularly suited for automated proof search in set theory. Main application is the proof support for set-based program development methods like B or Z.

Keywords Naive set theory, set-based program development, lattice theory, sectional complements, extensionality, atomicity.

1 Introduction

Intuitive or naive set theory is both an official mathematical ontology and a universal mathematical tool. In computer science, it is the basis of popular and successful formal methods like Z [21] or B [1]. But the quality of formal proof support for mathematics in general and of a formal method in particular crucially depends not only on its flexibility and comprehensiveness for specifications, but also on its degree of automation for reasoning. Therefore, the integration of intuitive set-theoretic reasoning into efficient focused automated deduction systems is an important question, both for mechanizing mathematics and for enhancing industrial strength formal hardware and software development. We believe that it has so far not sufficiently been answered: There are a few systems that implement axiomatic set theory (e.g. [9,20,18,19]), but these are either interactive or designed for foundations rather than for applications as automated formal methods. At the operational side, Hines [13] proposes a resolution calculus for restricted reasoning with some set-theoretic operations, but the problems of characterizing the corresponding fragment of set theory and of proving completeness of his calculus are now open for more than a decade. So the apparent lack of

answer to the above question indicates an interesting and challenging gap both in the field of formal methods and in automated deduction.

Here, we develop the mathematical foundations of an operational core calculus for intuitive set theory as used in formal methods that is intended to close this gap. In [22], we integrate this calculus into a focused resolution-based automated proof-search procedure. This solves the longstanding open problem related to [13].

Unlike the usual logical approaches, our core calculus is purely algebraic. It is the calculus of atomic distributive lattices (ADL). Appropriateness of ADL for intuitive set theory follows from the representation theorem for this class. Accordingly, every atomic distributive lattice can be isomorphically embedded into a field of sets; the zero of the lattice represented by the empty set, join and meet by union and intersection, the lattice order by set inclusion. But reasoning with ADL differs from boolean reasoning about sets: The ontological commitment to a universal set is avoided since there need not be a maximal element. Set-difference can nevertheless be expressed since ADL has unique sectional complements. It is even more important that ADL supports element-wise reasoning: elements of sets are in one-to-one correspondence with singleton sets, which represent atoms. Using techniques from the representation theorem we also show that atomicity of the lattice captures precisely extensionality of the set theory. Moreover, we reconstruct extensionality algebraically in terms of a lattice congruence. This is of independent interest, since it introduces a notion of *observational equivalence* for non-atomic and therefore intensional lattices or sets.

Our approach shares the usual benefits of other algebraic calculi for reasoning about hardware or software (c.f. [7,14,15,5]): Economy of axioms, support of abstract, concise, elegant calculations from few elementary principles and relation to standard algebraic decision procedures. It is therefore particularly suited for automation.

The remainder of this text is organized as follows. In Section 2 we speculate about the merits of algebraic approaches to formal methods. Section 3 introduces and discusses some postulates for a core calculus for intuitive set theory. Section 4 revisits some basic notions of lattice theory. Section 5 discusses the notion of complement, in particular sectional complement, for lattices; Section 6 presents some of their useful calculatory laws. Section 7 and Section 8 introduce the notions of atoms and atomicity in lattices. Section 9 discusses the correspondence between atomicity and extensionality in set theory. Section 10 presents some meta-theorems about atomic distributive lattices; representability and closure under direct products. Section 11 briefly sketches the relation between atomic distributive lattices and boolean rings. Section 12 draws a conclusion.

2 The Point of Algebra

The quality of formal proof support for mathematics in general and for hardware or software development in particular crucially depends on the combination of simple readable specifications with powerful proof search. Complex problems

usually require man-machine interaction. Therefore, specifications and proofs should be formally and informally rigorous. They should be both feasible for a machine and simple, natural and understandable for a human. This requirement is far from straightforward. Humans prefer to use informal and semantical arguments that are often not accessible for machines. They reason in terms of pictures, diagrams and similar models or using methods like abstraction or analogy. They concentrate on creative aspects and are often sketchy or even silent about routine parts. They are usually better trained with algebraic or arithmetic reasoning than with logical arguments and the manipulation of quantifiers. Machines, in contrast, drastically outperform a human with combinatorial and symbolic search, syntactic manipulations or the evaluation of huge data sets. An ideal formal method should integrate these complementary strengths.

For a smooth man-machine interaction, the expressive and computational power of a formal method should be well-balanced. On the one hand, it should provide simple intuitive formalisms that support a human's development of specifications and proofs in the intended area of application. On the other hand, it should provide powerful algorithms to verify or even decide arising proof obligations with a machine. These two requirements are in opposition. Deduction should however be replaced by computation as far as possible in order to minimize human interaction in favor of automation. In an ideal formal method, a human should focus entirely on the creative parts and outlines of proofs; the routine work should be left to the machine.

A key for achieving these requirements even for complex problem domains is abstraction. This idea is fundamental also to other areas. Abstracting from the individual behavior of particles to collective phenomena, for instance, gives rise to the laws of thermodynamics. Abstracting from coordinates yields elegant categorical formalizations in differential geometry. Abstracting from variables leads to concise and elegant programs and correctness proofs in functional programming. In all these cases, abstraction establishes simple principles, often algebraic laws, that rule the abstract behavior of a system. The structural complexity is hidden in bridge lemmas that connect the different levels of abstraction

As our example of interest, consider set theory. In the usual axiomatic approach, this is the logical theory of the $\in$-relation. It is appropriate for foundational purposes like the reduction of mathematics to a minimal ontological basis. But mathematical practice and software engineering tasks require an operational approach to sets. And a considerable part of operational set-theoretic reasoning takes place at a higher level of abstraction. It is entirely algebraic, using notions like set-inclusion, set-union or set-intersection and properties like laws of order, distributivity, complementation or monotonicity. Examples for bridge laws between the foundational logical and the operational algebraic layer are for instance the definition of set-inclusion $a \subseteq b$ by $\forall x.x \in a \Rightarrow x \in b$ or the definition of relational composition $R \cdot S$ by $\{(x,y) : \exists z.(x,z) \in R \wedge (z,y) \in S\}$. Here, the abstraction leads in particular to the elimination of quantification. This enables the replacement of deduction by computation. The verification of an existential sentence or the falsification of a universal sentence requires a witness for the

quantified variable; a rather creative task which may be circumvented at the abstract algebraic level. Conversely, for machine reasoning, the transition from the algebraic to the logical level is in general not desirable, since the problem structure may be destroyed and in the extreme case, simple algebraic calculations may be turned into complex logical deductions.

Abstraction is also a main mechanism in formal methods like Z or B. The B method, for instance, uses four layers of abstraction: A layer of first-order logic on which a typed set theory is built as a second layer. A set calculus as a third layer on top of the set theory and a relational calculus as a fourth layer on top of the set calculus. But experience shows that the quality of specifications and proofs with these methods usually increases proportionally with abstraction: The better they are, the less they are logical, the more they are algebraic. The development of libraries of algebraic laws, usually in terms of bridge lemmas, is therefore an important issue in this area. Hundreds of pages in Abrial's book on B [1] are devoted to this task. But the logic-based approach hides the natural algebraic hierarchy among these laws.

So why not turn to a leaner method which avoids the lower logic-based levels as far as possible and where reasoning focuses on the more abstract algebraic ones? This algebraic turn might lead to several improvements. First, an increase in the economy of axioms and the structure of libraries of lemmas. Second, support of standard algebraic concepts, proof techniques and decision procedures. Third, commitment of users to a more abstract and concise algebraic or arithmetic style of specification and analysis, which is also more in the tradition of mathematics and engineering than logic. It therefore supports the replacement of deduction by computation, may yield a better balance between expressive and computational power and enables both formally and informally rigorous specifications and proofs. Concretely, we plan an algebraic set calculus in combination with a modal Kleene algebra [5] at the level of the relational calculus. The latter subsumes many traditional programming logics like Hoare logic, propositional dynamic logic or temporal logics. This combination opens the way for integrating powerful proof search methods into state of the art set-based program development methods.

Here, we only consider the mathematical foundations of a core calculus for intuitive set theory. Thus we restrict ourselves to the consideration of formal and informal rigor. Evidence that expressive and computational power is well-balanced and that deduction can be to a large extent replaced by computation is given in [22]. More theoretical foundations will be provided in further papers. The full integration of our calculus into an industrial strength formal method is intended on the long run.

3 Postulates for a Core Calculus

But what are minimal requirements for an algebraic core calculus for intuitive set theory as used in everydays mathematics and in formal methods? We propose the following five postulates.

Postulate 1 *The core calculus should model the empty set.*

This requirement implies that there is at least one set. It needs no further explanation.

Postulate 2 *The core calculus should support boolean reasoning, but avoid an ontological commitment to a universal set.*

In particular, we would like to reason about set-union, set-intersection, set-equality, set-inclusion and set-complementation or set-difference. Laws for these operations and relations should yield elementary principles for building new sets from given ones. Depending on the context, there should not be a universal set. In [22] we present simplification techniques for set-theoretic expressions that are based on the axiom that there is no universal set. In other contexts, however, it may be desirable to add such a set.

Postulate 3 *The core calculus should support element-wise reasoning.*

Element-wise reasoning is not automatically available in a boolean world. Elements of sets are of course in one-to-one correspondence with singleton sets. To enrich the ontology if necessary, such elements can be assumed as so-called urelements. Singleton sets or urelements can of course not be described by the above-mentioned operations.

Postulate 4 *The core calculus should reflect extensionality of the corresponding set theory.*

Extensionality means that every set is completely determined by the behavior of its elements. In particular, two sets are equal, if they are built from the same elements. Extensionality is one of the most important properties both of axiomatic and intuitive set theories. Operationally, extensionality is often used for presenting a witness for a certain property, for instance, that one set is not included in another one.

The fifth postulate is a placeholder for adding further postulates by need.

Postulate 5 *The core calculus should be open to admit further set-theoretic entities and properties.*

The core calculus should allow the integration of, for instance, infinite sets, induction and comprehension principles, ordered pairs and elementary data-structures like numbers, lists or trees. It should also provide means to rule out the well-known paradoxes.

The following sections are devoted to the development of an algebra that satisfies these postulates.

4 Lattices

This section introduces some basic notions from lattice theory. More information can be found, for instance, in the textbooks [2,16,4,12]. Here and in the remaining

sections, we always add examples which show that sets are among the models of lattices. Consequently, we can do with sets at most what we can do with lattices. Moreover, according to the representation theorems for the classes of lattices we consider (c.f. 10), we can do with sets (and the respective operations) at least what we can do with lattices. The reader should keep this in mind to follow our arguments.

A structure $(A, \leq)$ is a *quasiordered set* (a *quoset*), if A is a set and $\leq$ a reflexive transitive relation on A. Accordingly, $\leq$ is called a *quasiordering*. Antisymmetric quasiorderings are called *partial orderings* and the associated structures are called *posets*. A *join semilattice* is a poset A closed under least upper bounds or joins (denoted by $\sqcup$) for all pairs of elements. Formally, for all $a, b, c \in A$,

$$a \leq c \wedge b \leq c \Leftrightarrow a \sqcup b \leq c. \tag{1}$$

A *meet semilattice* is defined dually as a quoset closed under greatest lower bound or meets (denoted by $\sqcap$) for all pairs of elements. Formally, for all $a, b, c \in A$,

$$c \leq a \wedge c \leq b \Leftrightarrow c \leq a \sqcap b. \tag{2}$$

The *dual* of a statement about lattices is obtained by interchanging joins and meets and converting the ordering. A *lattice* is both a join and a meet semilattice. It is *distributive*, if

$$a \sqcap (b \sqcup c) \leq (a \sqcap b) \sqcup (a \sqcap c)$$

holds for all $a, b, c \in A$ or its dual and therewith both. We denote the minimal and the maximal elements with respect to $\leq$ of a lattice, if they exist, by 0 and 1. A lattice with 0 and 1 is called *bounded*. Formally, for all $a \in L$,

$$0 \leq a, \tag{3}$$

$$a \leq 1. \tag{4}$$

The class of lattices is denoted by L, the class of distributive lattices by DL. If K is a class of lattices, then K_0 denotes the subclass that has a zero, K_1 the subclass that has a one and K_{01} the subclass that is bounded.

We consider lattices as orderings. Alternatively, the class can also be axiomatized equationally. The translation between the two classes is given by

$$a \leq b \Leftrightarrow a \sqcup b = b \Leftrightarrow a \sqcap b = a. \tag{5}$$

In the equational definition, joins and meets are associative, commutative, idempotent ($a \sqcap a = a = a \sqcup a$) and absorptive ($a \sqcup (a \sqcap b) = a = a \sqcap (a \sqcup b)$) operations. Experience shows that order-based reasoning with lattices is more natural than equational reasoning. By (5) we need not distinguish between equations and inequalities. We will therefore use the term *equation* freely for both expressions.

Let P_1 and P_2 be posets. A mapping $h : P_1 \to P_2$ is *monotone*, iff $a \leq b$ in P_1 implies $h(a) \leq h(b)$ in P_2. A monotone mapping is an *order-embedding*, iff $h(a) \leq h(b)$ in P_2 implies $a \leq b$ in P_1, that is h is also injective. An *order-isomorphism* is a surjective order-embedding.

Let $L_1, L_2 \in \mathsf{L}$. A mapping $h : L_1 \to L_2$ is a *join-morphism*, iff $h(a \sqcup b) = h(a) \sqcup h(b)$ for all $a, b \in L_1$, that is h *preserves joins*. It is a *meet-morphism*, iff $h(a \sqcap b) = h(a) \sqcap h(b)$ for all $a, b \in L_1$, that is h *preserves meets*. A *lattice-homomorphism* (or *homomorphism*, more briefly) is both a join- and a meet-morhphism. For bounded lattices, we also require $h(0) = 0$ and $h(1) = 1$. An injective lattice homomorphism is called a *(lattice-)embedding*, a surjective lattice embedding a *(lattice-)isomorphism*.

Note that $h(a) \sqcup h(b) \leq h(a \sqcup b)$ and $h(a \sqcap b) \leq h(a) \sqcap h(b)$ hold whenever h is monotone. Moreover all homomorphisms are monotone, but not conversely.

It is easy to show that the operations of join and meet are monotone in both arguments.

The following lemma characterizes distributive lattices (c.f. [2]).

Lemma 1. *A lattice is distributive iff it has no sublattice isomorphic to a pentagon or a diamond from Figure 1.*

Example 1.

(i) A family of subsets of some set is called *ring of sets*, if it closed under (set-theoretic) union and intersection. Every ring of sets is a distributive lattice. A finite lattice is distributive iff it is isomorphic to a ring of sets. If the ring of sets contains the empty set, then this element is the zero of the corresponding lattice.

(ii) Every chain (for example the chain of natural numbers) is a distributive lattice.

(iii) The lattices in Figure 1 are not distributive.

pentagon diamond

Figure1.

Using distributive lattices with zero, we have thus achieved Postulate 1 and part of Postulate 2: We are able to reason algebraically about the empty set and about unions and intersections of sets.

5 Complements

For our intended application in mechanized intuitive set theory and in set-based formal methods, in accordance with Postulate 2, we would like to be able to reason also about set complements or set difference, but avoid the ontological commitment to a universal set. Therefore we abstain from plain boolean algebra and replace the well-known boolean complement by the much less popular sectional complements, that may generally exist in lattices with a zero, but without a unit. Sectional complements are usually not studied in detail in textbook. We therefore present their most important properties and outline a calculus.

Let $L \in \mathsf{L}_{01}$. A *complement* of an element a of L is an element b of L such that $a \sqcup b = 1$ and $a \sqcap b = 0$. L is *complemented*, if every element has a complement. A *boolean lattice* is a complemented distributive lattice. The class of boolean lattices is denoted by BL.

We are also interested in lattices with a weaker notion of complementation. Let $L \in \mathsf{L}$ and let $a, b \in L$. We define the *interval*

$$[a, b] = \{c \in L : a \leq c \leq b\}.$$

Every interval in a lattice is a sublattice. Let $c \in [a, b]$. x is a *relative complement* of c in $[a, b]$, if $c \sqcap x = a$ and $c \sqcup x = b$. L is *relatively complemented*, if every $a \in L$ has a relative complement in every interval containing it. This is the case iff every sublattice $[a, b]$ of L is complemented. L is *sectionally complemented*, if $L \in \mathsf{L}_0$ and every sublattice $[0, a]$ is complemented. We write $L|a$ for the sublattice $[0, a]$ of L. A relatively complemented distributive lattice is usually called a *generalized boolean lattice*.

Let K be a class of lattices. Then K^{rc} denotes the relatively complemented, K^{sc} the sectionally complemented and K^{c} the complemented subclass. The class of generalized boolean lattices is denoted by GBL.

Lemma 2. *The following elements are uniquely defined (provided they exist).*

(i) All relative complements in DL.
(ii) All sectional complements in DL_0.
(iii) All complements in DL_{01}.

Proof. (ad i) Let b_1 and b_2 be relative complements of a in the interval $[c, d]$. We calculate

$$b_1 = b_1 \sqcup c = b_1 \sqcup (a \sqcap b_2) = (b_1 \sqcup a) \sqcap (b_1 \sqcup b_2) = d \sqcap (b_1 \sqcup b_2) = b_1 \sqcup b_2 \leq b_2.$$

The proof of $b_2 \leq b_1$ is similar.

(ad ii) Similar to the proof of (i).

(ad iii) Similar to the proof of (ii). □

In DL_0, the sectional complement of a in $[0, a \sqcup b]$ is denoted by $b - a$. In particular, when $a \leq b$, then $b - a$ is the sectional complement of a in $[0, b]$. In DL_{01}, the complement of a is denoted by a'. Obviously,

$$a' = 1 - a. \tag{6}$$

Lemma 3.

(i) If $L \in \mathsf{DL}_{01}$ and a' is the complement of $a \in L$, then $b - a = a' \sqcap (a \sqcup b)$.
(ii) If $L \in \mathsf{DL}_{01}$, a' is the complement of $a \in L$ and $a \in [b, c]$, then $(a' \sqcap a) \sqcup c$ is the relative complement of a in $[b, c]$.
(iii) If $L \in \mathsf{DL}_0$, $c - a$ is the sectional complement of a in $[0, c]$ and $a \in [b, c]$, then $(c - a) \sqcup b$ is relative complement of a in $[b, c]$.

The proof is by simple computations.

Lemma 4.

(i) $\mathsf{L}_0^{rc} \subsetneq \mathsf{L}^{sc}$, $\mathsf{L}_1^{sc} \subsetneq \mathsf{L}^{c}$.
(ii) $\mathsf{BL} \subseteq \mathsf{DL}^{sc} \subseteq \mathsf{GBL}$.
(iii) $\mathsf{GBL}_0 = \mathsf{DL}^{sc}$, $\mathsf{GBL}_{01} = \mathsf{BL}$.

Proof. (ad i) The inclusions are straightforward. Examples for strictness can be found in [12], p. 49.
(ad ii) Immediate from Lemma 3.
(ad iii) Immediate from (i) and (ii). □

By Lemma 4 (iii), the notion of complementation to be used in DL depends on the ontological commitments, the presuppositions on the existence of zero and one. In Section 8 we will see that sectional complementation is very natural for atomic distributive lattices. Also in the context of sets and Postulate 2 of Section 3, sectional completeness are natural and appropriate. As we have pointed out, the empty set corresponds to the zero, but we would like to avoid assuming the existence of a one, that is a set of all sets. Moreover, Lemma 4 (iii) shows that the extension of $\mathsf{DL}^{\mathrm{sc}}$ to BL is conservative. We will see that all our constructions work already in $\mathsf{DL}^{\mathrm{sc}}$.

Lemma 5. *A lattice is distributive, iff all relative complements are unique.*

Proof. The only if direction follows from Lemma 2 (i).
Every non-distributive lattices has, by Lemma 1, a sublattice isomorphic with a pentagon or a diamond. Both have an element with multiple complements. Thus the lattice has multiple relative complements. □

Example 2.

(i) In a ring of sets, $s_1 - s_2$ denotes set-difference, that is $s_1 - s_2$ is the set of all elements of s_1 that are not elements of s_2. Let s_3 be that set. We verify the defining conditions of sectional complements, that is $s_3 \cup s_2 = s_1 \cup s_2$ and $s_3 \cap s_2 = \emptyset$.

$$\begin{aligned} a \in (s_3 \cup s_2) &\Leftrightarrow a \in s_3 \vee a \in s_2 \\ &\Leftrightarrow (a \in s_1 \wedge a \notin s_2) \vee a \in s_2 \\ &\Leftrightarrow (a \in s_1 \vee a \in s_2) \wedge (a \notin s_2 \vee a \in s_2) \\ &\Leftrightarrow a \in s_1 \vee a \in s_2 \\ &\Leftrightarrow a \in (s_1 \cup s_2). \end{aligned}$$

$$\begin{aligned} a \in (s_3 \cap s_2) &\Leftrightarrow a \in s_3 \wedge a \in s_2 \\ &\Leftrightarrow a \in s_1 \wedge a \notin s_2 \wedge a \in s_2 \\ &\Leftrightarrow a \in \emptyset. \end{aligned}$$

(ii) A family of subsets of some set is called *field of sets*, if it closed under (set-theoretic) union and intersection and set difference. Every field of sets is a boolean lattice.

6 Computing with Complements

Besides their defining laws, three kinds of rules are important for computing with complements in boolean lattices: simplification rules, de Morgan rules and shunting rules. In this section, we first derive generalizations of these rules for sectionally complemented lattices. We then show that the standard de Morgan rules and shunting rules for boolean lattices arise as corollaries. The computations of this sections are interesting for two reasons. First, they can be used for abstract algebraic reasoning with sets in the context of set-based program development. Second, we will need them for the proof search procedures in [22].

The following lemma is a key for the computations that follow.

Lemma 6. *Let $L \in \mathsf{GBL}_0$. Then for all $a, b, c \in L$,*

$$a = b - c \Leftrightarrow a \sqcup c = b \sqcup c \wedge a \sqcap c = 0. \tag{7}$$

This is immediate from the definition and uniqueness of differences.

The following two lemmas collect some rewrite rules for sectional complements, when read from left to right. We group them with respect to similarity. Some of these laws appear already in [12,6]. The first set of identities is mainly auxiliary for proving those of later lemmas.

Lemma 7. *Let $L \in \mathsf{GBL}_0$. For all $a, b \in L$,*

$$(a - b) \sqcup b = a \sqcup b, \tag{8}$$
$$(a - b) \sqcap b = 0, \tag{9}$$
$$a \sqcap (a - b) = a - b, \tag{10}$$
$$a \sqcup (a - b) = a. \tag{11}$$

Proof. (ad (8)) Immediate from (7).

(ad (9)) Immediate from (7).

(ad (10)) By Lemma 6 we must show

$$(a \sqcap (a - b)) \sqcap b = 0,$$
$$(a \sqcap (a - b)) \sqcup b = a \sqcup b.$$

The first equality follows from (9), the second inequality follows from (8).

(ad (11)) Using (10) and the absorption law for lattices, we calculate

$$a \sqcup (a - b) = a \sqcup (a \sqcap (a - b)) = a.$$

□

In particular, (10) is very useful in the form $a - b \leq a$. The next lemma simplifies nested sectional complements.

Lemma 8. *Let $L \in \mathsf{GBL}_0$. For all $a, b, c \in L$,*

$$a - a = 0, \tag{12}$$
$$a - (b - c) = (a - b) \sqcup (a \sqcap c), \tag{13}$$
$$a - (a - b) = a \sqcap b. \tag{14}$$

Proof. (ad (12)) $a - a = a \sqcap (a - a) = 0$ by (10).

(ad (13)) By Lemma 6 we must show

$$((a - b) \sqcup (a \sqcap c)) \sqcap (b - c) = 0,$$
$$((a - b) \sqcup (a \sqcap c)) \sqcup (b - c) = a \sqcup (b - c).$$

For the first inequality,

$$\begin{aligned} ((a - b) \sqcup (a \sqcap c)) \sqcap (b - c) &= ((a - b) \sqcap (b - c)) \sqcup ((a \sqcap c) \sqcap (b - c)) \\ &\leq ((a - b) \sqcap b) \sqcup 0 \\ &= 0 \end{aligned}$$

by (11) and (9). For the second inequality,

$$\begin{aligned} ((a - b) \sqcup (a \sqcap c)) \sqcup (b - c) &= ((a - b) \sqcup (b - c) \sqcup a) \sqcap ((a - b) \sqcup (b - c) \sqcup c) \\ &= (a \sqcup (b - c)) \sqcap ((a - b) \sqcup b \sqcup c) \\ &= (a \sqcup (b - c)) \sqcap (a \sqcup b \sqcup c) \\ &= a \sqcup (b - c) \end{aligned}$$

using (8) and (11).

(ad (14)) A special case of (13). □

The first two identities in the next lemma state generalized de Morgan laws.

Lemma 9. *Let $L \in \mathsf{GBL}_0$. For all $a, b, c \in L$,*

$$a - (b \sqcap c) = (a - b) \sqcup (a - c), \tag{15}$$
$$a - (b \sqcup c) = (a - b) \sqcap (a - c), \tag{16}$$
$$(a \sqcap b) - c = (a - c) \sqcap (b - c), \tag{17}$$
$$(a \sqcup b) - c = (a - c) \sqcup (b - c). \tag{18}$$

Proof. (ad (15)) By Lemma 6 we must show

$$((a - b) \sqcup (a - c)) \sqcap b \sqcap c = 0,$$
$$((a - b) \sqcup (a - c)) \sqcup (b \sqcap c) = a \sqcup (b \sqcap c).$$

The first equality follows from (9). For the second equality,

$$\begin{aligned}((a-b)\sqcup(a-c))\sqcup(b\sqcap c) &= ((a-b)\sqcup(a-c)\sqcup b)\sqcap((a-b)\sqcup(a-c)\sqcup c)\\ &= (a\sqcup b\sqcup(a-c))\sqcap(a\sqcup c\sqcup(a-b))\\ &= (a\sqcup b)\sqcap(a\sqcup c)\\ &= a\sqcup(b\sqcap c)\end{aligned}$$

using (8) and (11).

(ad (16)) By Lemma 6 we must show

$$\begin{aligned}(a-b)\sqcap(a-c)\sqcap(b\sqcup c) &= 0,\\ ((a-b)\sqcap(a-c))\sqcup b\sqcup c &= a\sqcup b\sqcup c.\end{aligned}$$

The first equality follows from (9). For the second equality,

$$\begin{aligned}((a-b)\sqcap(a-c))\sqcup b\sqcup c &= ((a-b)\sqcup b\sqcup c)\sqcap((a-c)\sqcup b\sqcup c)\\ &= a\sqcup b\sqcup c\end{aligned}$$

using (8).

(ad (17)) By Lemma 6 we must show

$$\begin{aligned}(a-c)\sqcap(b-c)\sqcap c &= 0,\\ ((a-c)\sqcap(b-c))\sqcup c &= (a\sqcap b)\sqcup c.\end{aligned}$$

$$\begin{aligned}((a-c)\sqcap(a-c))\sqcup c &= ((a-c)\sqcup c)\sqcap(b-c)\sqcup c)\\ &= (a\sqcup c)\sqcap(b\sqcup c)\\ &= (a\sqcap b)\sqcup c\end{aligned}$$

using (8).

(ad (18)) By Lemma 6 we must show

$$\begin{aligned}((a-c)\sqcup(b-c))\sqcap c &= 0,\\ (a-c)\sqcup(a-c)\sqcup c &= a\sqcup b\sqcup c.\end{aligned}$$

The first equality follows from (9), the second one from (8). □

The rules (15)–(18) can also be read as follows. (15) and (16) show that the mapping $\lambda x.a-x$ is anticonjunctive and antidisjunctive. (17) and (18) show that the mapping $\lambda x.x-c$ is conjunctive and disjunctive.

The standard de Morgan laws of boolean lattices are recovered by setting $a=1$ and using $s'=1-s$ in (15) and (16).

The disjunctivity and antidisjunctivity laws immediately imply monotonicity and antimonotonicity laws for sectional complements.

Lemma 10. *Let $L \in \mathsf{GBL}_0$. For all $a, b, c \in L$,*

$$a \leq b \Rightarrow a - c \leq b - c, \tag{19}$$
$$a \leq b \Rightarrow c - b \leq c - a. \tag{20}$$

Proof. (ad (19)) By (18) and the assumption,

$$(a - c) \sqcup (b - c) = (a \sqcup b) - c = b - c.$$

Hence $a - c \leq b - c$.

(ad (20)) By (15) and the assumption,

$$(c - a) \sqcup (c - b) = c - (a \sqcap b) = c - a.$$

Hence $c - b \leq c - a$. □

The standard monotonicity law for complements is recovered by setting $c = 1$ and using $s' = 1 - s$ in (20).

We now prove generalized shunting rules for sectional complements.

Lemma 11. *Let $L \in \mathsf{GBL}_0$. For all $a, b, c, d \in L$,*

$$a - b \leq c \Leftrightarrow a \leq b \sqcup c, \tag{21}$$
$$a \sqcap (c - b) \leq d \Leftrightarrow a \sqcap c \leq b \sqcup d, \tag{22}$$
$$a \leq (c - b) \sqcup d \Leftrightarrow a \leq c \sqcup d \wedge a \sqcap b \leq d, \tag{23}$$
$$a \leq c - b \Leftrightarrow a \leq c \wedge a \sqcap b \leq 0. \tag{24}$$

Proof. (ad (21)) Let $a - b \leq c$. By (8) and the assumption

$$a \leq a \sqcup b = b \sqcup (a - b) \leq b \sqcup c.$$

Let $a \leq b \sqcup c$. By (19), (18), (12), (10) and the assumption,

$$a - b \leq (b \sqcup c) - b = (b - b) \sqcup (c - b) = c - b = c \sqcap (c - b) \leq c.$$

(ad (22)) Let $a \sqcap (b - c) \leq d$. By (8),

$$a \sqcap c \leq a \sqcap (c \sqcup b) = a \sqcap (b \sqcup (c - b) = (a \sqcap b) \sqcup (a \sqcap (c - b)) \leq b \sqcup d.$$

Let $a \sqcap c \leq b \sqcup d$. By (10) and (9),

$$\begin{aligned} a \sqcap (c - b) &= a \sqcap c \sqcap (c - b) \\ &\leq (b \sqcup d) \sqcap (c - b) \\ &= (b \sqcap (c - b) \sqcup (d \sqcap (c - b)) \\ &= d \sqcap (c - b) \\ &\leq d. \end{aligned}$$

(ad (23)) Let $a \leq (c - b) \sqcup d$. Then

$$a \leq (c - b) \sqcup d = (c \sqcap (c - b)) \sqcup d \leq c \sqcup d$$

by (10) and

$$a \sqcap b \leq ((c - b) \sqcup d) \sqcap b = ((c - b) \sqcap b) \sqcup (b \sqcap d) = b \sqcap d \leq d$$

by (9).

Let $a \leq c \sqcup d$ and $a \sqcap b \leq d$. Then by (8)

$$\begin{aligned} a &= a \sqcap (c \sqcup d) \\ &\leq a \sqcap (b \sqcup c \sqcup d) \\ &= a \sqcap (b \sqcup (c - b) \sqcup d) \\ &= (a \sqcap b) \sqcup (a \sqcap ((c - b) \sqcup d)] \\ &= a \sqcap ((c - b) \sqcup d) \\ &= (c - b) \sqcup d, \end{aligned}$$

(ad (24)) Let $d = 0$ in (23). □

The standard shunting rules for complements are recovered by setting $c = 1$ and using $s' = 1 - s$ in (22) and (23).

The laws (21) and (23) are of particular interest. (21) is a Galois connection with lower adjoint $\lambda x.x - b$ and upper adjoint $\lambda x.b \sqcup x$. See [8] for an introduction to Galois connections. The computational interest of Galois connections is that they can be used as theorem generators. In particular, lower adjoints of Galois connections commute with all existing suprema, whereas upper adjoints commute with all existing infima. Moreover, both adjoints are monotonic. This immediately implies that the disjunctivity and monotonicity laws (18) and (19) hold. Moreover, the lower and upper adjoints of a Galois connection satisfy the cancellation laws

$$a \leq b \sqcup (a - b), \tag{25}$$

$$(b \sqcup c) - b \leq c. \tag{26}$$

(25) and (26) are weak forms of (8) and (18), respectively. Note however, that (21) alone does not completely characterize sectional complementation.

(23) is very similar to (7). It states that $c - b$ is the greatest solution in x of the equation $x \sqcap b \leq 0$ with "boundary condition" $x \leq c$. In absence of the boundary condition this reduces to the definition of a pseudo-complement as used, for instance, in Heyting algebra [2]. Again, (23) alone does not completely characterize sectional complementation.

The final lemma of this section generalizes the following well-known fact from boolean lattices.

$$a = b \Leftrightarrow (a \sqcap b') \sqcup (b \sqcap a') = 0.$$

Lemma 12. *Let $L \in \mathsf{GBL}_0$. For all $a, b \in L$,*

$$a = b \Leftrightarrow (a \sqcap (a - b)) \sqcup (b \sqcap (b - a)) = 0. \tag{27}$$

Proof. Let $a = b$. Then, by (12),

$$(a \sqcap (a - b)) \sqcup (b \sqcap (b - a)) = a \sqcap (a - a) = a \sqcap 0 = 0.$$

Let $(a \sqcap (a - b)) \sqcup (b \sqcap (b - a)) = 0$. Then

$$\begin{aligned} a &= a \sqcap (a \sqcup b) \sqcap (a \sqcup b) \\ &= a \sqcap (a \sqcup (b - a)) \sqcap (b \sqcup (a - b)) \\ &= a \sqcap ((a \sqcap b) \sqcup (a \sqcap (a - b)) \sqcup (b \sqcap (b - a)) \sqcup ((a - b) \sqcap (b - b))) \\ &= a \sqcap ((a \sqcap b) \sqcup 0 \sqcup ((a - b) \sqcap (b - b))) \\ &= (a \sqcap b) \sqcup (a \sqcap (a - b) \sqcap (b - a)) \\ &= a \sqcap b, \end{aligned}$$

by (8) and (9). Hence $a \leq b$. The proof of $b \leq a$ is similar. □

As a result of this section, we have now fulfilled Postulate 1 and Postulate 2 of Section 3 with computational laws for sectional complements or set difference that generalize those of the boolean complements.

7 Atoms

We now turn to Postulate 3 of Section 3, the integration of element-wise (or point-wise) reasoning into our core calculus for intuitive set theory. This goes beyond boolean reasoning, which only allows reasoning about set-inclusion. Lattice theory, however, offers an entity corresponding to that of an element of a set. This is the concept of an *atom*. In this and the following section, we do not only recall the well-known facts about atoms in lattices. We develop specific laws for calculating in the respective structures. These laws are in particular appropriate for the proof-search procedures in [22].

Let $(P, \leq)$ be a poset with 0 and let $a, b \in P$. b *covers* a, iff $a < b$ and $a \leq c \leq b$ implies $c = a$ or $c = b$ for all $c \in P$. An *atom* is a cover of 0. We denote the set of atoms of P by $A(P)$.

Lemma 13. *Let P be a poset with 0. $\alpha \in A(P)$, iff $\alpha \not\leq 0$ holds and $b \leq \alpha$ implies $\alpha \leq b$ or $b \leq 0$ for all $b \in P$.*

Lemma 14. *Let $\in \mathsf{L}_0$. An element $a \in L$ is an atom, iff $a \not\leq 0$ and, for all $b \in L$,*

$$a \leq b \vee a \sqcap b \leq 0. \tag{28}$$

Proof. We first show that the conditions of Lemma 13 imply (28).

Let a be an atom and $a \leq b \not\leq 0$. Then $a \not\leq 0$ and by Lemma 13, $a \sqcap b \leq a$ implies $a \leq a \sqcap b$ and therefore $a \leq b$.

Let a be an atom and $a \not\leq b$. Then $a \not\leq a \sqcap b$ and $a \sqcap b \leq a$ hold, thus $a \sqcap b \leq 0$ by Lemma 13.

We now show that (28) and $a \not\leq 0$ imply the conditions of Lemma 13.

Let $a \not\leq 0$, $b \leq a$ and $a \not\leq b$. Then $a \sqcap b \leq 0$ by (28) and therefore $b = b \sqcap b \leq a \sqcap b \leq 0$.

Let $a \not\leq 0$, $b \leq a$ and $b \not\leq 0$. Then $b \sqcap a \not\leq 0$ and $a \leq b$ by (28) □

Let $L \in \mathsf{L}_0$. An element $c \in L$, $c \neq 0$, is *join-irreducible*, if for all $a, b \in L$,

$$c = a \sqcup b \Rightarrow c = a \vee c = b. \tag{29}$$

We denote the set of all join-irreducible elements of L by $J(L)$.

Lemma 15. *Let $L \in \mathsf{DL}_0$. Then $c \in J(L)$, iff $c \neq 0$ and for all $a, b \in L$.*

$$c \leq a \sqcup b \Rightarrow c \leq a \vee c \leq b. \tag{30}$$

Proof. Let $c \in J(L)$ and let $c \leq a \sqcup b$. Thus $c = c \sqcap (a \sqcup b) = (c \sqcap a) \sqcup (c \sqcap b)$ and therefore $c = c \sqcap a$ or $c = c \sqcap b$ by join-irreducibility. Consequently, $c \leq a$ or $c \leq b$.

Let $c = a \sqcup b$. Then $a \sqcup b \leq c$ and $c \leq a \sqcup b$. The first inequality implies that $a \leq c$ and $b \leq c$. The second inequality and the assumption imply that $c \leq a$ or $c \leq b$. Thus both together imply that $c = a$ or $c = b$. □

Lemma 16. *Let $L \in \mathsf{L}_0$.*

(i) $A(L) \subseteq J(L)$.
(ii) $J(L) \subseteq A(L)$, *if* $L \in \mathsf{GBL}_0$.
(iii) Let $L \in \mathsf{GBL}_0$. Then $\alpha \in A(L)$ iff, for all $a, b \in L$,

$$\alpha \not\leq 0, \tag{31}$$

$$\alpha \leq a \sqcup b \Leftrightarrow \alpha \leq a \vee \alpha \leq b. \tag{32}$$

Proof. (ad i) By reductio ad absurdum, let α be an atom, let $\alpha \not\leq a$ and $\alpha \not\leq b$ and let $\alpha = a \sqcup b$. Then $\alpha \sqcap a < a$ and $\alpha \sqcap b < b$, which can only be the case, if $a = b = 0$. Then $\alpha = 0 \sqcup 0 = 0$, a contradiction to atomicity.

(ad ii) Let $a \in J(L)$ and $b \leq a$. We show that $b = a$ or $b = 0$ by Lemma 13. By Lemma 4 (iii), we consider sectional complements. Using (8), we obtain

$$a = (a \sqcup b) \sqcap a = (b \sqcup (a - b)) \sqcap a = b \sqcup (a \sqcap (a - b)),$$

thus $b = a$ or $a = a \sqcap (a - b) = (a - b)$ by join-irreducibility and (10). Then $b = a \sqcap b \leq (a - b) \sqcap b = 0$ by the assumption $b \leq a$ and (9).

(ad iii) This is immediate from Lemma 13, Lemma 15, (i) and (ii). □

The following properties are helpful as rewrite rules for eliminating certain negative inequalities.

Lemma 17. *Let $L \in \mathsf{L}_0$. For all $\alpha, \beta \in A(L)$ and $a, b \in L$,*

$$\alpha \not\leq b \Leftrightarrow \alpha \sqcap b \leq 0, \tag{33}$$

$$\alpha \sqcap \beta \not\leq 0 \Leftrightarrow \alpha = \beta, \tag{34}$$

$$\alpha \sqcap a \leq b \Leftrightarrow \alpha \sqcap a \leq 0 \vee \alpha \leq b, \tag{35}$$

$$\alpha \sqcap a \not\leq b \Leftrightarrow \alpha \sqcap b \leq 0. \tag{36}$$

Proof. (ad (33)) Let $\alpha \not\leq b$. Then $\alpha \sqcap b \neq \alpha$ by definition of $\leq$. Thus $\alpha \sqcap b = 0$, since $\alpha \sqcap b$ must be smaller than α and α covers 0.

Let $\alpha \sqcap b \neq 0$. Then $\alpha \sqcap b \leq \alpha$ by definition, hence $\alpha \sqcap b = \alpha$, since α covers 0. Thus $\alpha \leq b$.

(ad (34)) Obvious.

(ad (35)) Let $\alpha \sqcap a \leq 0$ or $\alpha \leq b$. In both cases, obviously, $\alpha \sqcap a \leq b$ holds.

Let $\alpha \sqcap a \leq b$ and let $\alpha \sqcap a \not\leq 0$. Then $\alpha \leq a$ by (33) and consequently

$$\alpha = \alpha \sqcap \alpha \leq \alpha \sqcap a \leq b.$$

Let $\alpha \sqcap s \leq t$ and let $\alpha \not\leq t$. Then $\alpha \sqcap t \leq 0$ by (33) and

$$\alpha \sqcap s = \alpha \sqcap \alpha \sqcap s \leq \alpha \sqcap t \leq 0.$$

(ad (36)) Immediate from (35). □

The following lemma yields a helpful visualization of join-irreducible elements in Hasse diagrams of finite lattices.

Lemma 18. *An element of a finite lattice is join-irreducible, iff it has precisely one lower cover.*

Example 3.

(i) In a field of sets, the atoms are precisely the singleton sets.

(ii) In the chain of natural numbers, all elements are join-irreducible. 0 is the only atom.

(iii) Consider the boolean lattice L_n generated by $a_1, \ldots, a_n$. L_n is finite. Every element $c_1 \sqcap \ldots \sqcap c_n$, where c_i is one of a_i and a_i', is an atom of L_n. Using the distributivity laws, every element $s \in L_n$ is equivalent to a term t which is a join of meets of a_i and a_i'. If the join contains at least two elements, then t has at least two lower covers, hence t is not join-irreducible. If the join contains only one element, then $t = c_1 \sqcap \ldots \sqcap c_k$, where c_i is one of a_i and a_i' and $k \leq n$. If $k = n$, then t is an atom, hence join-irreducible. If $k < n$, then $t \sqcap a_{k+1}$ and $t \sqcap a_{k+1}'$ are lower covers of t. Thus t is not join-irreducible. Thus the join-irreducible elements of L_n are precisely the atoms.

8 Atomicity

In the previous section we have seen that atoms are appropriate for simulating element-wise reasoning in lattices. In this section, we look for conditions that guarantee that a lattice has enough atoms for this kind of reasoning.

We now give two definitions of atomicity for a lattice. These are the two standard notions as used in textbooks. A lattice $L \in \mathsf{L}_0$ is *preatomic*, if for each non-zero $a \in L$ there exists an $\alpha \in A(L)$ such that $\alpha \leq a$. L is *atomic*, if for each non-zero $a \in L$ there is a nonempty subset T of $A(L)$ such that $a = \bigsqcup T$. For a class K of lattices, the subclass of preatomic lattices is denoted by pAK and the class of atomic lattices by AK.

We also define a mapping $\eta : L \to 2^{A(l)}$ that associates with each element $a \in L$ the set of atoms below it.

$$\eta(a) = \{\alpha \in A(L) : \alpha \leq a\}. \tag{37}$$

L is *η-stable*, iff $a = \bigsqcup \eta(a)$ holds for all $a \in L$. In particular, η preserves atoms, that is $\eta(\alpha) = \alpha$ for all $\alpha \in A(L)$.

Lemma 19. *Let $L \in \mathsf{L}_0$.*

(i) η is monotone.
(ii) η is a meet-homomorphism.
(iii) η is a join-homomorphism (thus a homomorphism), if $L \in \mathsf{DL}$.
(iv) There is a non-distributive lattice[1], where η is not a join-homomorphism.

Proof. (ad i) Let $a \leq b$. Then $\alpha \leq a$ implies $\alpha \leq b$ for all $\alpha \in A(L)$, hence $\eta(a) \subseteq \eta(b)$.

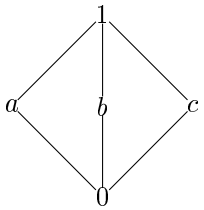
(ad ii)

$$\begin{aligned} \alpha \in \eta(a \sqcap b) &\Leftrightarrow \alpha \leq a \sqcap b \\ &\Leftrightarrow \alpha \leq a \wedge \alpha \leq b \\ &\Leftrightarrow \alpha \in \eta(a) \wedge \alpha \in \eta(b) \\ &\Leftrightarrow \alpha \in \eta(a) \cap \eta(b). \end{aligned}$$

Moreover, $\eta(0) = \{\alpha \in A(L) : \alpha \leq 0\} = \emptyset$.

(ad iii) By Lemma 16 (iii), $\alpha \leq a \sqcup b \Leftrightarrow \alpha \leq a \wedge \alpha \leq b$ holds in DL_0 for every atom α. Then the proof goes through like that in (ii).

(ad iv) Consider again the diamond D, which is non-distributive.



[1] even modular and complemented

Obviously, $A(D) = \{a, b, c\}$. Moreover,

$$\eta(a \sqcup b) = \eta(1) = \{a, b, c\} \neq \{a, b\} = \{a\} \cup \{b\} = \eta(a) \cup \eta(b).$$

□

Lemma 20. *A lattice (with at least two elements) is preatomic, if η is injective.*

Proof. Let L be a lattice with at least two elements. Then $A(L) \neq \emptyset$, since these elements have different images under η by injectivity. Moreover, $0 \in L$, since the definition of atoms presupposes a zero. Since $\eta(0) = \emptyset$, $\eta(a)$ must, for all $a \neq 0$, contain at least one atom. Thus L is preatomic. □

We now give an alternative characterization of atomicity. $L \in \mathsf{L}_0$ is *extensional*, if for all $a, b \in L$,

$$\forall \alpha \in A(L).(\alpha \leq a \Rightarrow \alpha \leq b) \Rightarrow a \leq b. \tag{38}$$

The meaning of extensionality is further discussed in Section 9.

Lemma 21. *$L \in \mathsf{L}_0$ is extensional iff for all $a, b \in L$,*

$$a \not\leq b \Rightarrow \exists.\alpha \in A(L).(\alpha \leq a \wedge \alpha \sqcap b \leq 0). \tag{atomic}$$

Proof.

$$a \not\leq b \Rightarrow \exists \alpha \in A(L)(\alpha \leq a \wedge \alpha \not\leq b)) \Leftrightarrow \exists \alpha \in A(L)(\alpha \leq a \wedge \alpha \sqcap b \leq 0).$$

The last step uses lemma 17. □

Note that the converse implications to (38) and (atomic) hold a forteriori in atomic lattices. We therefore often use the corresponding bi-implications without further mentioning.

Proposition 1. *Let $L \in \mathsf{L}_0$ with at least two elements. The following statements are equivalent.*

(i) $L \in \mathsf{AL}$.
(ii) L *is* η*-stable.*
(iii) $\eta(a) \leq \eta(b) \Rightarrow a \leq b$ *for all* $a, b \in L$.
(iv) η *is injective.*
(v) L *is extensional.*

Proof. (i) implies (ii). Let $L \in \mathsf{AL}$ and let $a \in L$. Then $a = \bigsqcup T$ for some non-empty $T \subseteq A(L)$. Consequently, $\alpha \leq a$ for all $\alpha \in T$, hence $T \subseteq \eta(a)$ and $\bigsqcup T \leq \bigsqcup \eta(a)$. This yields $a \leq \bigsqcup \eta(a)$. Since $\bigsqcup \eta(a) \leq a$ by definition, we have $a = \bigsqcup \eta(a)$ and therefore η-stability.

(ii) implies (i). Let $T = \eta(a)$.

(ii) implies (iii). $\eta(a) \subseteq \eta(b)$ implies $\bigsqcup \eta(a) \leq \bigsqcup \eta(b)$ and therefore $a \leq b$. Note that the infinite joins exist by definition of η-stability.

(iii) implies (ii) Monotonicity of η and (iii) yield

$$a \leq b \Leftrightarrow \eta(a) \subseteq \eta(b) \tag{39}$$

for all $a, b \in L$ and consequently

$$a = b \Leftrightarrow \eta(a) = \eta(b). \tag{40}$$

Moreover, $\eta(a)$ and $\eta(b)$ are non-empty, since by lemma 20, L is preatomic.

We now show that a is a least upper bound of $\eta(a)$. Since η is an embedding of L into some subsemilattice of $2^{A(L)}$ (η is a meet-homomorphism), we can carry out the proof entirely on the set-side. Obviously, a is an upper bound of $\eta(a)$. To show that it is a least upper bound, assume, by reductio ad absurdum, another upper bound b of $\eta(a)$ such that $a \not\leq b$. Thus $\eta(a) \not\subseteq \eta(b)$ by (39) and by boolean reasoning $\eta(a) \cap (A(L) - \eta(b)) \neq \emptyset$. So there is some atom $\alpha \in \eta(a) \cap (A(L) - \eta(b))$. Consequently, $\alpha \in \eta(a)$ and $\alpha \in A(L) - \eta(b)$, hence on the one hand $\alpha \notin \eta(b)$. On the other hand, $\alpha \in \eta(a)$ implies $\alpha \in \eta(b)$, a contradiction.

(iii) implies (iv). Obvious.

(iv) implies (iii). Let η be injective, that is $\eta(a) = \eta(b) \Rightarrow a = b$. Thus

$$\begin{aligned} \eta(a) \leq \eta(b) &\Leftrightarrow \eta(a) = \eta(a) \cap \eta(b) \\ &\Leftrightarrow \eta(a) = \eta(a \sqcap b) \\ &\Rightarrow a = a \sqcap b \\ &\Leftrightarrow a \leq b. \end{aligned}$$

This uses the fact that η is a meet-homomorphism.

(iii) equivalent to (v). Using (39), we calculate

$$a \leq b \Leftrightarrow \eta(a) \subseteq \eta(b) \Leftrightarrow \forall \alpha \in A(L).(\alpha \leq a \Rightarrow \alpha \leq b) \tag{41}$$

□

Note that the chain of reasoning from atomicity to extensionality is rather simple. Intuitively, if a lattice is atomic, then there are enough points for boiling down every lattice element as a join of atoms. Thus this element is completely determined by these atoms and therefore extensional. The converse direction requires a deeper argument.

(38) and (atomic) are important for normal form computations in the context of the proof-search procedures in [22]. In particular, (atomic) is crucial here. Its operational impact is the replacement of negative inequalities by positive ones. The existential quantifier can be handled by skolemization. We can thus circumvent using the second-order definition of atomicity.

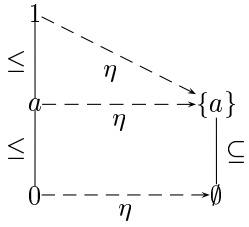
Lemma 22.

(i) $\mathsf{AL} \subseteq \mathsf{pAL}$.
(ii) There is a (finite) distributive preatomic, but not atomic lattice.
(iii) $L \in \mathsf{pAL}^{sc}$ *implies* L *is* η*-stable, hence* $\mathsf{pAL}^{sc} \subseteq \mathsf{AL}$.

(iv) $L \in \mathsf{pABL}$ *implies* L *is* η*-stable, hence* $\mathsf{pABL} \subseteq \mathsf{ABL}$.

Proof. (ad i) By Proposition 1, atomicity implies that the lattice is η-stable. By Lemma 20, η-stability implies preatomicity.

(ad ii) Consider the distributive preatomic lattice $0 \leq a \leq 1$.



The mapping $\eta = \{0 \mapsto \emptyset, a \mapsto \{a\}, 1 \mapsto \{a\}\}$ is clearly not injective and $1 \neq \bigsqcup\{a\} = a$.

(ad iii) Like in the proof of Proposition 1, we show that a is a least upper bound of $\eta(a)$. It is an upper bound by definition. We proceed by reductio ad absurdum. Let b be another upper bound of $\eta(a)$ in L such that $a \not\leq b$. Then $a \sqcap b < a$, but still $\bigsqcup \eta(a) \leq a \sqcap b$. Let c be a sectional complement of $a \sqcap b$ in $[0, a]$. $c \neq 0$, since $a \sqcap b < a$. By weak atomicity there is some $\alpha \in A(L)$ with $\alpha \leq c$. Since $c \in [0, a]$, we have that $\alpha \leq a$ and $\alpha \in \eta(a)$. Therefore $\alpha \leq a \sqcap b$ and in particular $\alpha \leq b$. This yields $\alpha \leq b \sqcap c = 0$, a contradiction to the definition of atoms. η-stability is equivalent to atomicity by Proposition 1.

(ad iv) By Lemma 4, every boolean lattice is sectionally complemented. Then the result follows from (iii). □

The following lemma shows an interesting connection between atomicity and complementation. In a sense, atoms induce sectional complements. This is only natural, since in an atomic lattice, all kinds of complements can be constructed from atoms. Atomicity guarantees that there are enough points for these constructions.

Lemma 23. $\mathsf{ADL} \subseteq \mathsf{GBL}_0$. *For* $L \in \mathsf{ADL}$ *and* $a, b \in L$, $b - a = \bigsqcup(\eta(b) - \eta(a))$.

Proof. First, we show that $a \sqcap (b - a) = 0$. Since $\eta(a)$ and $\eta(b) - \eta(a)$ are disjoint, the suprema of these sets are also disjoint. This holds, since in an atomic lattice, $a \sqcap b \neq 0$ iff $\alpha \leq a$ and $\alpha \leq b$ for some atom α, whence the set of atoms cannot be disjoint. Therefore $a \sqcap (b - a) \leq 0$.

Now we show that $b \sqcup (a - b) = a \sqcup b$. We calculate

$$\begin{aligned} b \sqcup (a - b) &= (\bigsqcup \eta(b)) \sqcup (\bigsqcup(\eta(a) - \eta(b))) \\ &= \bigsqcup(\eta(b) \cup (\eta(a) - \eta(b))) \\ &= \bigsqcup(\eta(a) \cup \eta(b)) \\ &= \bigsqcup \eta(a) \sqcup \bigsqcup \eta(b) \\ &= a \sqcup b \end{aligned}$$

Thus $b - a$ is a sectional complement of b with respect to a. By distributivity of the lattice, the complement is unique (Lemma 2 (ii)). □

Consequently, we can use (32) instead of (28) as a defining property in ADL. But (32) is computationally more pleasant than (28), in particular, for our proof-search procedures in [22].

We now give yet an alternative characterization of atomicity.

Lemma 24. *$L \in$ BL is atomic iff $A(L)$ is a partition of 1, that is $1 = \bigsqcup A(L)$.*

Proof. Let $L \in$ ABL. Then $1 = \bigsqcup \eta(1) = \bigsqcup A(L)$.

Let $1 = \bigsqcup A(L)$. Then

$$\begin{aligned} a &= a \sqcap 1 \\ &= a \sqcap \bigsqcup A(L) \\ &= \bigsqcup\{b \in L : b = a \sqcap \alpha \text{ for some } \alpha \in A(L)\} \\ &= \bigsqcup\{\beta \in A(L) : \beta \leq a\} \\ &= \bigsqcup \eta(a). \end{aligned}$$

Hence $L \in$ ABL. □

Example 4.

(i) The set of all subsets of some set is an atomic boolean lattice.

(ii) Let A be an infinite set. Define the congruence $\sim$ on 2^A by $a \sim b$ iff a and b identical up to finitely many elements. Then $L = 2^A/\sim$ is a boolean lattice. Its 0 is the set of finite subsets of 2^A. L is atomless. To see this, note that every nontrivial element of L contains an infinite subset of a of A. Like every infinite set, a can be partitioned in two infinite subsets a' and a''. Obviously, $a' \not\sim 0$, since a' is infinite and $a' \not\sim a$, since a'', the difference of a' and a is infinite. Moreover, $a' \subseteq a$, such that a is not an atom.

(iii) In Example 2 (i) we have shown, that in a field of sets, $s_1 - s_2$ denotes the set of all elements of s_1 that are not in s_2. The proof was based on set theory and used the epsilon relation. We now give an algebraic reconstruction in ADL. First, we replace every statement of the form $a \in s$ by $\alpha_a \leq s$. Then, it remains to show that $\alpha \leq s_1 - s_2$ iff $\alpha \leq s_1 \wedge \alpha \not\leq s_2$. This follows immediately from (24) and (33).

We have now seen that atomic distributive lattices are structures that satisfy our Postulates 1, 2 and 3 for a core calculus for intuitive set theory. The requirement of atomicity may impose the existence of some infinite joins, namely those that determine some elements high up in a lattice. This however does not imply the existence of arbitrary joins, since not even the existence of arbitrary joins of atoms is required.

9 Extensionality

In this section we consider Postulate 4, the modeling of extensionality in lattice theory. For $L \in \mathsf{GBL}_0$, consider again the extensionality property

$$a \leq b \Leftrightarrow \forall \alpha.(\alpha \leq a \Rightarrow \alpha \leq b), \tag{38}$$

for all $a, b \in L$. The right-hand side induces a relation $\preceq$ defined by

$$a \preceq b \Leftrightarrow \forall \alpha \in A(L).(\alpha \leq a \Rightarrow \alpha \leq b), \tag{42}$$

for all $a, b \in L$. We also define $\sim = \preceq \cap \succeq$, whence

$$a \sim b \Leftrightarrow \forall \alpha \in A(L).(\alpha \leq a \Leftrightarrow \alpha \leq b), \tag{43}$$

for all $a, b \in L$.

Lemma 25. *Let $L \in \mathsf{GBL}_0$.*

(i) The relation $\prec$ is a precongruence on L.
(ii) The relation $\sim$ is a congruence on L.

Proof. (ad i) Let $a \preceq b$, that is $\alpha \leq a \Rightarrow \alpha \leq b$.
We show that $a \sqcup c \preceq b \sqcup c$.

$$\alpha \leq a \sqcup c \Leftrightarrow \alpha \leq a \vee \alpha \leq c \Rightarrow \alpha \leq b \vee \alpha \leq c \Leftrightarrow \alpha \leq b \sqcup c.$$

The first step uses (32). We now show that $a \sqcap c \preceq b \sqcap c$.

$$\alpha \leq a \sqcap c \Leftrightarrow \alpha \leq a \wedge \alpha \leq c \Rightarrow \alpha \leq b \wedge \alpha \leq c \Leftrightarrow \alpha \leq b \sqcap c.$$

We now show that $c - b \preceq c - a$.

$$\alpha \leq c - a \Leftrightarrow \alpha \leq c \wedge \alpha \sqcap a \leq 0 \Rightarrow \alpha \leq c \wedge \alpha \sqcap b \leq 0 \Leftrightarrow \alpha \leq c - b.$$

The first and third step uses (24), the second step uses the assumption and the fact that $\alpha \leq a \Rightarrow \alpha \leq b$ is equivalent to $\alpha \sqcap b \leq 0 \Rightarrow \alpha \sqcap a \leq 0$ by (33). We now show that $a - c \sim b - c$.

$$\alpha \leq a - c \Leftrightarrow \alpha \leq a \wedge \alpha \sqcap c \leq 0 \Rightarrow \alpha \leq b \wedge \alpha \sqcap c \leq 0 \Leftrightarrow \alpha \leq a - b.$$

(ad ii) Immediate from (i). □

By the arguments of the previous section, we can express the relations $\preceq$ and $\sim$ in terms of the function η.

Lemma 26. *Let $L \in \mathsf{L}_0$. Let $a, b \in L$.*

(i) $a \preceq b \Leftrightarrow \eta(a) \subseteq \eta(b)$.
(ii) $a \sim b \Leftrightarrow \eta(a) = \eta(b)$.

Proof. Immediate from the definition of η. □

Lemma 27. *Let $L \in \mathsf{L}_0$. For all $\alpha, \beta \in L$,*

$$\alpha \sim \beta \Rightarrow \alpha = \beta. \tag{44}$$

Proof. Immediate from the definition of atoms. □

Thus Lemma 27 states that the congruence $\sim$ separates atoms.

The following lemma relates the algebraic notion of extensionality with atomicity.

Lemma 28.

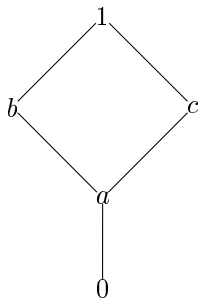
(i) Let $L \in \mathsf{L}_0$. For all $a, b \in L$ and $\alpha \in A(L)$, L is atomic iff

$$a \sim b \Rightarrow a = b. \tag{45}$$

(ii) There is a preatomic distributive lattice, for which (38) (whence (45)) does not hold.

Proof. (ad i) Immediate from Proposition 1 (v) and Lemma 25.

(ad ii) Consider the distributive lattice



It is preatomic with atom a, but not atomic. (38) and therefore (45) does not hold for b and c. □

By Lemma 26 (i), (45) is an algebraic variant of the fact that η is injective, as expressed, for instance, in Proposition 1 (iii). Remember that η is a homomorphism on DL_0.

A rule of the form of (38) is often called *principle of indirect inequality* in order-theory. Four our purposes, extensionality is operationally very important, since it allows the transition between atom-free and atom-wise reasoning. This is similar to the dichotomy between point-free and point-wise reasoning about programs or external and internal reasoning in mathematics using categories.

(45) algebraically expresses an *extensionality principle*: two elements of an atomic lattice are equal, iff they are built from the same atoms. In this sense, the lattice from the proof of Lemma 28 (ii) might be called *intensional*. Similarly, (atomic) expresses a *separability principle*: two elements of an atomic lattice are different, iff they can be distinguished by an atom; that is, there is a witness in terms of an atom which shows that the two elements are different. By Lemma 28 (ii), preatomicity does not suffice to guarantee separability and extensionality, not even for a distributive lattice. Remember that by Lemma 22, every preatomic boolean lattice is atomic.

It is interesting that algebraically, extensionality arises as a special case of a more general congruence. This congruence allows us to identify elements of a lattice as far as their behavior can be observed by measurements on atoms. Two elements who are equivalent with respect to this notion may be called *observational equivalent*. Still, such element may behave differently as a result of their internal or hidden behavior. In this sense, lattices who do not satisfy the extensionality principle might be called *intensional*.

Given our three characterizations of extensionality, the logical one in terms of atoms, our algebraic one in terms of a congruence and our set-theoretic one in terms of the function η, it seems very interesting to compare it with the standard definition in the λ-calculus, that is in terms of η-equality (for a different notion of η), which is in a sense a notion of functional abstraction.

Extensionality is of course a key property in set theory. Semantically, it introduces—no entity without identity—a notion of equality for sets. Operationally, it allows the transition between element-free and element-wise reasoning. This connection is further discussed in the following example.

Example 5. In every field of sets, by Example 3, the singleton sets are precisely the atoms. Hence instead of the set-theoretic expression $a \in s$ we can write $\{a\} \subseteq s$ according to set theory and more abstractly $\alpha_a \leq s$ in AL. Existence of this atom is guaranteed by atomicity. Conversely, in a field of sets, we can write $a \in s \Rightarrow a \in t$ instead of $\alpha_a \leq s \Rightarrow \alpha_a \leq t$. Then (45) becomes the standard axiom of extensionality of set theory,

$$\forall x.(x \in a \Leftrightarrow x \in b) \Rightarrow a = b.$$

We could also introduce the $\in$-relation as syntactic sugar for $L \in \mathsf{AL}$, defining

$$\alpha \in s \Leftrightarrow \alpha \leq s. \tag{46}$$

for all $\alpha \in A(L)$ and $a \in L$. However, the restriction to $\leq$ and atoms yields greater economy of expression.

We have now fulfilled Postulates 1 to 4 of Section 3. These are the main requirements for a core calculus for intuitive set theory and in particular for set-based program development. The remaining sixth postulate requires compatibility of our concepts and properties with extensions. We leave its demonstration to future considerations.

10 Representation and Closure Under Direct Products

We now discuss the relation of our constructions of the previous section with the well-known representation theorems. This is interesting for the following reason. In the examples of previous sections, we have seen that we can do with sets under union and intersection, but without a universal set at most what we can do with lattices. The representation theorems show that we can also do with them at least what we can do with sets.

Lemma 29. *Let $L \in \mathsf{L}$ be finite.*

(i) $L \in \mathsf{pAL}$.
(ii) $L \in \mathsf{AL}$ *if* $L \in \mathsf{L}^{sc}$.
(iii) $L \in \mathsf{AL}$, *if* $L \in \mathsf{BL}$.

Proof. (ad i) By reductio ad absurdum, let L not be preatomic. Then there exists an element $a_0 \in L$ such that for all $b \leq a_0$, $b \in L$ b is not an atom. Consequently, a_0 cannot be an atom and there must exist some $a_1 \leq a_0$. Since a_1 is not an atom, there must be some $a_2 \leq a_1$ that also is not an atom. Iteration of this argument yields an infinite chain $a_0 \geq a_1 \geq a_2 \ldots$, a contradiction to finiteness.

(ad ii) Immediate from (i) and lemma 22 (iii).

(ad iii) Immediate from (i) and Lemma 22 (iv). □

Lemma 30. *Let $L \in \mathsf{L}$ be finite. Then for all $a \in L$,*

$$\eta(a) = \emptyset \Leftrightarrow a = 0.$$

Proof. Let $a = 0$. Then $\eta(a) = \emptyset$ by definition.

Let $a \neq 0$. By Lemma 29 (i), L is preatomic. Thus $\alpha \leq a$ for some $\alpha \in A(L)$ and therefore $\eta(a) \neq \emptyset$. □

In particular, therefore every finite sectionally complemented lattice is atomic and distributive and therefore boolean.

Remember that by lemma 22 (ii), there exists a finite preatomic but not atomic distributive lattice. Lemma 29 and the constructions of Section 8 yield the following representation theorems.

Theorem 6. *Let $L \in \mathsf{pAL}^{sc}$. Then η is an meet-preserving isomorphism between L and a complete sublattice of the ring of sets 2^L.*

Theorem 7.

(i) Every atomic boolean lattice is isomorphic to some field of sets. More precisely, every such lattice L can be embedded into the field of sets $2^{A(L)}$.
(ii) Every atomic distributive lattice is isomorphic to some field of sets. More precisely, every such lattice L can be embedded into the field of sets $2^{A(L)}$.
(iii) Every complete atomic boolean lattice L is isomorphic with the field of sets $2^{A(L)}$.
(iv) Every complete atomic distributive lattice L is isomorphic with the field of sets $2^{A(L)}$.

Hence the complete atomic distributive lattices and the complete atomic boolean lattices coincide. Note that in general the supremum of $A(L)$ is undefined. Remember that every finite boolean lattice is atomic and complete.

Corollary 1.

(i) Every finite boolean lattice is isomorphic with the field of sets $2^{A(L)}$.
(ii) Every atomic finite distributive lattice is isomorphic with the field of sets $2^{A(L)}$.

The representation theorems link atomic lattices with sets. On the one hand this means that every identity between atomic lattice terms holds in the set-theoretic model. On the other hand, every first-order boolean property of a field of sets holds in the class of atomic lattices. Thus the elementary theories of atomic lattices and fields of sets are precisely the same. We will use this fact for our construction of focused calculi for sets.

Note that in particular, in atomic lattices, the computations of Section 6 can be done entirely at the set-side.

Based on the representation theorems we immediately obtain the well-known size bounds for finite lattices. The free boolean lattice, for instance, has 2^n atoms and therefore 2^{2^n} elements.

The following theorem of McKinsey is very interesting for restricting our calculi in certain special cases.

Theorem 8 ([17]). *Let K be a class of algebras closed under direct products and let the clause $\phi_1, \ldots, \phi_m \longrightarrow \psi_1, \ldots, \psi_n$ hold in K. Then $\phi_1, \ldots, \phi_m \longrightarrow \psi_i$ holds in K for some $1 \leq i \leq n$.*

In particular, the converse does also hold. For falsificational reasoning, the following variant is important.

Corollary 2. *Let K be a class of algebras closed under direct products. The clause $\phi_1, \ldots, \phi_m \longrightarrow \psi_1, \ldots, \psi_n$ does not hold in K iff $\phi_1, \ldots, \phi_m \longrightarrow \psi_i$ does not hold in K for all $1 \leq i \leq n$.*

Proof. It remains to show that $\phi_1, \ldots, \phi_m \longrightarrow \psi_1, \ldots, \psi_n$ does not hold in K implies $\phi_1, \ldots, \phi_m \longrightarrow \psi_i$ does not hold in K. So let $\phi_1, \ldots, \phi_m \longrightarrow \psi_1, \ldots, \psi_n$ does not hold in K. Then there is an algebra $A \in \mathsf{K}$ such that $\phi_1 \wedge \cdots \wedge \phi_m$ holds

in A and $\psi_1 \vee \cdots \vee \psi_n$ does not hold in A. The latter condition is satisfied iff ψ_i does not hold in A for all $1 \leq i \leq n$. But then, also $\phi_1, \ldots, \phi_m \longrightarrow \psi_i$ does not hold in K. □

Proposition 2. *The following classes are closed under direct products.*

(i) L, DL, GBL_0, BL.
(ii) pAL, pADL.
(iii) AL, ADL, ABL.

Proof. (ad i) This holds since L, DL, GBL_0 and BL are varieties and therefore closed under direct products.

(ad ii) Let L_1 and L_2 be preatomic lattices. By (i) it remains to show that $L = L_1 \times L_2$ is preatomic. Let

$$A(L) = \{(a,b) \in L_1 \times L_2 : (a \in A(L_1) \wedge y = 0_2) \vee (x = 0_1 \wedge b \in A(L_2)\}.$$

Obviously, all elements of $A(L)$ are covers of $(0_1, 0_2)$. Let $(a,b) \in L$. By preatomicity of L_1 and L_2, there exist $\alpha_1 \in A(L_1)$ and $\alpha_2 \in A(L_2)$ such that $\alpha_1 \leq a$ and $\alpha_2 \leq b$. Thus $(\alpha_1, 0_2) \leq (a,b)$ and $(0_1, \alpha_2) \leq (a,b)$.

(ad iii) Let L_1 and L_2 be atomic lattices. By lemma 1, atomicity is equivalent to η-stability. By (i) it remains to show that $L = L_1 \times L_2$ is η-stable.

$$\begin{aligned}
\bigsqcup \eta((a,b)) &= \bigsqcup\{(x,y) \in A(L) : (x,y) \leq (a,b)\} \\
&= \bigsqcup\{(x,y) \in L : ((x \in A(L_1) \wedge y = 0) \vee (x = 0 \wedge y \in A(L_2))) \\
&\qquad\qquad \wedge x \leq a \wedge y \leq b\} \\
&= \bigsqcup\{(x,0) \in L : ((x \in A(L_1) \wedge x \leq a\} \sqcup \\
&\quad \bigsqcup\{(0,y) \in L : ((y \in A(L_2) \wedge y \leq b\} \\
&= (\bigsqcup \eta_1(a), 0) \sqcup (0, \bigsqcup \eta_2(b)) \\
&= (\bigsqcup \eta_1(a), \bigsqcup \eta_2(b)) \\
&= (a,b).
\end{aligned}$$

□

Note that the product of sectionally complemented lattices is not necessarily sectionally complemented, since, when sectional complements are not uniquely defined, they are defined by an existential statement.

We can therefore use McKinsey's theorem for splitting all universal clauses in the pure language of atomic lattices into universal Horn clauses in refutations.

Closure under products is also interesting for the following reason. Axiomatic set theory is concerned with the foundations of mathematics and therefore with ontological economy. The whole theory is therefore axiomatized using solely axiom schemata of first-order logic (that is axioms of second-order logic) and, besides the inventory of first-order logic, solely the $\in$-relation.

In the context of software engineering or in intuitive set theory, ontological economy is only one goal among others. Ordered pairs are usually introduced in set theory as expressions $(a, b) = \{a, \{a, b\}\}$. To justify appropriateness of this definition, textbooks on set theory then usually verify the intuitive property

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

Here, we can use Proposition 2 to define ordered pairs in ADL algebraically in terms of direct products. According to Proposition 2, we do not leave ADL when building ordered pairs. The construction easily extends to (finite) tuples.

11 Atomic Distributive Lattices and Boolean Rings

In this section, we recapitulate some well-known facts from lattice theory, see for instance [10]. We recall some basic facts about congruences and ideals in distributive lattices. We then put the similarity of behavior of congruences and ideals in sectionally complemented distributive lattices and rings on a formal basis.

As usual, an *ideal* I of a lattice L is a subset of L that is downwards closed and closed under finite joins. Let I and J be ideals of a lattice L. We can then define the meet of I and J by $I \sqcap J = \{a \sqcap b : a \in I, b \in J\}$. Moreover, $I \sqcup J = \{a \sqcup b : a \in I, b \in J\}$ iff L is distributive.

A *congruence* on L is a relation on L such that $a_1 = b_1 \bmod \theta$ and $a_2 = b_2 \bmod \theta$ imply $a_1 \sqcup a_2 = b_1 \sqcup b_2 \bmod \theta$ and $a_1 \sqcap a_2 = b_1 \sqcap b_2 \bmod \theta$. A particularly interesting congruence on distributive lattices is the relation $\theta(I)$ for some ideal $I \subseteq L$ defined by $a = b \bmod \theta(I)$ iff $a \sqcup c = b \sqcup d$ for some $c, d \in I$. It follows that $\theta(I)$ is the smallest congruence on L for which I is contained in one congruence class. The quotient lattice of a lattice L modulo a congruence θ on L is denoted by L/θ. The mapping from L to L/θ that sends every $a \in L$ to its congruence class is a homomorphism. Conversely, for every homomorphism $f : L \to L'$, the (congruence) kernel $\ker(f) = \{(a, b) \in L \times L : f(a) = f(b)\}$ is a congruence on L and L' is isomorphic to $L/\ker(f)$.

Let now $L \in \mathsf{L}_0$. The (ideal) kernel of a homomorphism f is $\mathrm{Ker}(f) = \{a \in L : f(a) = 0\}$. Then, every ideal kernel is an ideal on L. Conversely, every ideal of a distributive lattice is the ideal kernel of some homomorphism. In a boolean lattice, it is even the case that there is a one-to-one correspondence between congruences and ideals, which is given by mapping sending the congruence to the zero of the quotient lattice. This need not be the case in distributive lattices. However, as a slight generalization, this correspondence holds in GBL_0.

Proposition 3. *Let $L \in \mathsf{GBL}_0$ and θ a congruence on L. Then $f : \theta \mapsto [0]_\theta$ is a one-to-one correspondence between congruences and ideals of L.*

Proof. The proof is essentially due to [2]. First, let I be an ideal on L. Then I is the zero of $L/\theta(I)$, whence a congruence class of $\theta(I)$. Second, let θ be a congruence on L and let $(a, b) \in \theta$. Then

$$a - b = a \sqcap (a - b) = b \sqcap (a - b) \bmod \theta = 0 \bmod \theta.$$

The first step uses (10). The third step uses (9). But the congruence class of 0 is an ideal. □

The following stronger result is proven in [11].

Proposition 4. *Let L be a lattice. There is a one-to-one correspondence between ideals and congruence relations of L under which the ideal corresponding to a congruence θ is a whole congruence class under θ iff $L \in \mathsf{GBL}_0$.*

This situation is analogous to ring theory and in fact, as noticed in [10], there is a straightforward correspondence between sectionally complemented lattices and boolean rings, which are multiplicatively idempotent rings with zero that are consequently commutative and satisfy $a + a = 0$.

There is the following correspondence between GBL_0 and boolean rings. Let $L \in \mathsf{GBL}_0$ and define the operations $a \cdot b = a \sqcap b$ and $a + b = (a \sqcup b) - (a \sqcap b)$. Then $(L, \cdot, +, 0)$ is a boolean ring.

Conversely, let B be a boolean ring and define the operations $a \sqcap b = a \cdot b$ and $a \sqcup b = a + b + a \cdot b$. Then $(B, \sqcup, \sqcap, 0) \in \mathsf{GBL}_0$.

Let ρ and λ be the mappings that send a member of GBL_0 to a boolean ring and vice versa. Then $\lambda \circ \rho = 1 = \rho \circ \lambda$. Moreover, I is a (lattice-theoretic) ideal of L iff it is an (arithmetic) ideal of $\rho(L)$; a mapping $f : L_1 \to L_2$ is a homomorphism iff $f : \rho(L_1) \to \rho(L_2)$ is a homomorphism and L_1 is a sublattice of L_2 iff $\rho(L_1)$ is a subring of $\rho(L_2)$.

12 Conclusion

We have developed the mathematical foundations of a core calculus for intuitive set theory as used in operational contexts like mathematical practice and in formal methods like Z or B. The core calculus is based on the theory of atomic distributive lattices. Its axioms consist of a set for distributive lattices, axiom (3) for the zero, axioms (31) and (32) for atoms and axiom (atomic) for atomicity. In opposition to mere boolean reasoning with sets, our calculus supports element-wise reasoning and avoids the ontological commitment to a universal set. The precise connection between our algebra and set-structures is given by representation theorems. The axiom (atomic) motivates an algebraic treatment of intensionality and extensionality in terms of a congruence. Operationally, the axioms support the effective reduction and simplification of terms, inequalities and clauses. The axioms (32) and (atomic), for instance, allow us to completely eliminate negative inequalities and to split certain inequalities containing atoms. This makes our axiomatization particularly suited for an integration into an efficient automated proof-search procedure, as shown in [22]. Moreover, it can also easily be implemented in a standard interactive proof-checker, using equational logic or more precisely the logic of inequalities [3,23].

Further interesting directions of work are the following. The development of a focused automated proof-search procedure for atomic distributive lattices. This has been done in [22]. A precise comparison with variants of naive and axiomatic

set theory and with formal methods like Z and B. An extension of the calculi with entities and principles like types for sets, pairs, comprehension, infinite sets, induction, a choice function, elemenary data-types such as numbers, lists and trees. An intgration of a second layer for relational reasoning based on modal Kleene algebra. Implementations of our calculus in automated and interactive deductive systems. On the long run, we plan to integrate our calculus into an industrial strength formal method. The theoretical results from this paper then open the way for efficient operational reasoning with sets.

Acknowledgements. I would like to thank Wolfram Kahl, Bernhard Möller and Dexter Kozen for helpful remarks.

References

1. J.-R. Abrial. *The B-Book*. Cambridge University Press, 1996.
2. G. Birkhoff. *Lattice Theory*, volume 25 of *Colloquium Publications*. American Mathematical Society, 1984. Reprint.
3. S. L. Bloom. Varieties of ordered algebras. *J. Computer and System Science*, 13:200–212, 1976.
4. B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, 1990.
5. J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. Technical Report 2003-7, Institut für Informatik, Universität Augsburg, 2003.
6. R. P. Dilworth. Lattices with unique complements. *Trans. Amer. Math. Soc.*, 57:123–154, 1945.
7. H. Doornbos, R. C. Backhouse, and J. van der Woude. A calculational approach to mathematical induction. *Theoretical Computer Science*, 179:103–135, 1997.
8. M. Erné, J. Koslowski, A. Melton, and G. E. Strecker. A primer on Galois connections. *Annals of the New York Academy of Sciences*, 704:103–125, 1993. in *Papers on General Topology and Applications*, 7th Summer Conference, in Honor of Mary Ellen Rudin and Her Work.
9. M. Gordon. Set theory, higher-order logic or both? In J. Grundy and J. Harrison, editors, *Theorem Proving in Higher-Order Logic: 9th International Conference*, volume 1125 of *LNCS*, pages 191–202. Springer-Verlag, 1996.
10. G. Grätzer. *General Lattice Theory*. Birkhäuser Verlag, 1978.
11. J. Hashimoto. Ideal theory for lattices. *Math. Japonica*, 2:149–186, 1952.
12. H. Hermes. *Einführung in die Verbandstheorie*. Springer-Verlag, 1967.
13. L. Hines. Str$\dot{+}$ve$\subseteq$: The Str$\dot{+}$ve-based Subset Prover. In M. E. Stickel, editor, *10th International Conference on Automated Deduction*, volume 449 of *LNAI*, pages 193–206. Springer-Verlag, 1990.
14. C. A. R. Hoare and B. von Karger. Sequential calculus. *Information Processing Letters*, 53(3):123–130, 1995.
15. D. Kozen. Kleene algebra with tests. *Transation on Programming Languages and Systems*, 19(3):427–443, 1997.
16. R. N. McKenzie, G. F. McNulty, and W. F. Taylor. *Algebras, Varieties and Lattices*, volume I. Wadsworth & Brooks/Cole, 1987.
17. J. McKinsey. The decision problem for some classes of sentences without quantifiers. *Journal of Symbolic Logic*, 8:61–76, 1943.

18. L. C. Paulson. Set theory for verification: I. From foundations to functions. *J. Automated Reasoning*, 11:353–389, 1993.
19. A. Quaife. Automated deduction in von-Neumann-Bernays-Gödel set theory. *J. Automated Deduction*, 8:91–147, 1993.
20. P. Rudnicki. An overwiev of the MIZAR project. Technical report, Department of Computing Science, University of Alberta, 1992.
21. J. M. Spivey. *Understanding Z.* Cambrigde University Press, 1988.
22. G. Struth. A calculus for set-based program development II: Proof search. Technical Report 2003-16, Institut für Informatik; Universität Augsburg, 2003.
23. W. Wechler. *Uiversal Algebra for Computer Scientists.* Springer-Verlag, 1992.