The completion of a poset in a lattice of antichains

Jason Crampton and George Loizou

Department of Computer Science, Birkbeck College, University of London,
Malet Street, London, WC1E 7HX, England

e-mail: `ccram01@dcs.bbk.ac.uk`

October 17, 2000

Abstract

It is well known that given a poset, X, the lattice of order ideals of X, $\langle \mathcal{I}(X), \subseteq \rangle$, is a completion of X via the order-embedding $\phi : X \hookrightarrow \mathcal{I}(X)$ where $\phi(x) = \downarrow x$. Herein we define a lattice of antichains in X, $\langle \mathcal{A}(X), \preccurlyeq \rangle$, and prove it is isomorphic to $\langle \mathcal{I}(X), \subseteq \rangle$. We establish the "join" and "meet" operations of the lattice, and present results for $\langle \mathcal{A}(X), \preccurlyeq \rangle$ analogous to standard results for $\langle \mathcal{I}(X), \subseteq \rangle$, including Birkhoff's Representation Theorem for finite distributive lattices and a Dedekind-MacNeille-style completion using antichains. We also discuss the relevance and application of completions using antichains to access control in computer science, in particular with reference to role-based access control and to modelling conflict of interest policies.

1 Introduction

Motivation Role-based access control is a new paradigm for security in computer systems [9, 11, 12]. Role-based access control models include a role hierarchy which has a natural interpretation as a set of roles, R, and a partial order defined on R, $\leqslant$. In such models, users (of the computer system) are assigned to roles. The set of roles assigned to a user is an antichain with respect to the ordering on R.

In the course of developing a more sophisticated model for role-based access control than those in the literature we became interested in the possibility of constructing a lattice, L_R, from R such that every subset of R had a least upper bound in L_R, and the ordering of R was preserved in L_R. In short, we wanted a completion of R. Furthermore, for efficiency and to eliminate redundancy, the usual way of representing the role hierarchy has been to store the covering relation on R. This led us to search for a completion which had a more economical representation than a completion using order ideals. Specifically we considered the set of antichains in R. These ideas are covered in detail in [5].

Contribution From this starting point we developed a completion of R by the set of antichains. This paper presents a lattice of antichains, $\langle \mathcal{A}(X), \preccurlyeq \rangle$, and defines the ordering $\preccurlyeq$, and the"join" and "meet" operations. We prove $\langle \mathcal{A}(X), \preccurlyeq \rangle$ is isomorphic to the lattice of order ideals, $\langle \mathcal{I}(X), \subseteq \rangle$. Given that, in most circumstances, the elements of our lattice are smaller and more easy to compute than those of the lattice of order ideals, we feel our construction may provide a useful and alternative insight into the representation theory of finite lattices. In particular we prove an analogous form of Birkhoff's Representation Theorem for finite distributive lattices [2].

Structure The paper is arranged as follows. Section 2 introduces the pre-requisite definitions and results from the theory of posets and lattices, and can be omitted by readers familiar with the subject. In Section 3 we prove that $\mathcal{A}(X)$ is isomorphic to $\mathcal{I}(X)$. In Section 4 we describe the "join" and "meet" operations on $\mathcal{A}(X)$, and present two simple examples. In Section 5 we present some results analogous to well known results for $\mathcal{I}(X)$. In Section 6 we discuss an alternative ordering on the set of antichains of a powerset which also has applications in access control. In the conclusion, we discuss the direction of future work. Appendix A shows Hasse diagrams for completions of a poset X. Appendix B shows a Hasse diagram for an alternative ordering on $\mathcal{A}(X)$.

2 Preliminaries

We now present some pre-requisite concepts. The definitions and proofs of results in this section can be found in any book on order and lattice theory. The following are recommended to the interested reader [3, 4, 8, 10].

Definition 2.1 *A pair $\langle X, \leqslant \rangle$ is a* partially ordered set *or* poset *if for all $x, y, z \in X$*

- *$x \leqslant x$,*
- *$x \leqslant y$ and $y \leqslant x$ implies $x = y$,*
- *$x \leqslant y$ and $y \leqslant z$ implies $x \leqslant z$.*

In other words $\leqslant$ is a binary relation on X which is reflexive, anti-symmetric and transitive, respectively.

We will write "X is a poset" (with an implied ordering $\leqslant$) except when we wish to draw attention to two different orderings (see Definition 2.5, for example). We will also write $x < y$ if $x \leqslant y$ and $x \neq y$.

Definition 2.2 *If X is a poset, $Y \subseteq X$ is a* chain *if for all $y_1, y_2 \in Y$ either $y_1 \leqslant y_2$ or $y_2 \leqslant y_1$. Y is an* antichain *if $y_1 \leqslant y_2$ only if $y_1 = y_2$.*

Definition 2.3 *Let X be a poset, and let $Y \subseteq X$.*

- *An element* $x \in X$ *is an* upper bound *for* Y *if, for all* $y \in Y$, $y \leqslant x$.

- *An element* $x \in X$ *is a* least upper bound *or* supremum *for* Y, *denoted* $\sup Y$, *if* x *is an upper bound of* Y *and, for all* $y \in Y$, $z \in X$, $y \leqslant z$ *implies* $x \leqslant z$. *In other words,* x *is the smallest of the upper bounds of* Y.

- *An element* $x \in X$ *is a* lower bound *for* Y *if, for all* $y \in Y$, $x \leqslant y$.

- *An element* $x \in X$ *is a* greatest lower bound *or* infimum *for* Y, *denoted* $\inf Y$, *if* x *is a lower bound of* Y *and, for all* $y \in Y$, $z \in X$, $z \leqslant y$ *implies* $z \leqslant x$. *In other words,* x *is the greatest of the lower bounds of* Y.

Definition 2.4 *A poset,* X, *is a* lattice *if, and only if, for all* $x, y \in X$ *both* $\inf\{x, y\}$ *and* $\sup\{x, y\}$ *exist in* X. *If for all* $Y \subseteq X$, $\sup Y$ *and* $\inf Y$ *exist (in* X*), then* X *is called a* complete *lattice.*

If L is a lattice it is usual to write $x \wedge y$, the "meet" of x and y, and $x \vee y$, the "join" of x and y, for $\inf\{x, y\}$ and $\sup\{x, y\}$, respectively. We will also write $\langle L, \vee, \wedge \rangle$ to mean that the set L is a lattice with the operations $\vee$ and $\wedge$. Indeed a lattice can be defined as a purely algebraic structure in terms of these operations [4].

Definition 2.5 *Let* $\langle X_1, \leqslant_1 \rangle$ *and* $\langle X_2, \leqslant_2 \rangle$ *be two posets. Then* $f : X_1 \to X_2$ *is*

- *an* order-preserving function *if* $x \leqslant_1 y$ *implies* $f(x) \leqslant_2 f(y)$,

- *an* order-embedding *if* $x \leqslant_1 y$ *if, and only if,* $f(x) \leqslant_2 f(y)$.

If f *is an order-embedding we will write* $f : X_1 \hookrightarrow X_2$.

Definition 2.6 *Let* X *be a poset. If* $f : X \hookrightarrow L$ *where* L *is a complete lattice, then we say that* L *is a* completion *of* X.

Definition 2.7 *Two lattices,* $\langle L_1, \vee_1, \wedge_1 \rangle$, $\langle L_2, \vee_2, \wedge_2 \rangle$, *are* isomorphic *if there is a bijection* $f : L_1 \to L_2$ *such that* $f(a \vee_1 b) = f(a) \vee_2 f(b)$ *and* $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$ *for all* $a, b \in L_1$.

The following result connects isomorphic lattices using the respective partial orderings on the lattices.

Theorem 2.1 *Two lattices* L_1 *and* L_2 *are isomorphic if, and only if, there is a bijection* f *from* L_1 *to* L_2 *such that both* f *and* f^{-1} *are order-preserving.*

Definition 2.8 *If* X *is a poset then* $Y \subseteq X$ *is an* order ideal *if for all* $y \in Y$, $x \in X$,

$$x \leqslant y \text{ implies } x \in Y.$$

If X *is a poset then* $Y \subseteq X$ *is an* order filter *if for all* $y \in Y$, $x \in X$,

$$x \geqslant y \text{ implies } x \in Y.$$

The set of order ideals of X *is denoted* $\mathcal{I}(X)$. *The set of order filters of* X *is denoted* $\mathcal{F}(X)$.

Definition 2.9 *If X is a poset and $Y \subseteq X$, we define $\downarrow Y$ read "down Y" as follows:*

$$\downarrow Y = \{x \in X : \text{ there exists } y \in Y \text{ such that } x \leqslant y\ \}.$$

Similarly we define $\uparrow Y$ read "up Y" as follows:

$$\uparrow Y = \{x \in X : \text{ there exists } y \in Y \text{ such that } x \geqslant y\ \}.$$

We will denote $\downarrow\{x\}$ by $\downarrow x$ (and $\uparrow\{x\}$ by $\uparrow x$).

Remark 2.1 *Clearly $Y \subseteq \downarrow Y$ (since for all $y \in Y$, $y \leqslant y$), and $\downarrow Y \in \mathcal{I}(X)$.*

Lemma 2.1 *Given a poset X, for all $x, y \in X$*

$$x \leqslant y \text{ if, and only if, } \downarrow x \subseteq \downarrow y.$$

Lemma 2.2 *For any poset X, $\langle \mathcal{I}(X), \subseteq \rangle$ and $\langle \mathcal{F}(X), \supseteq \rangle$ are complete lattices. Furthermore, $\langle \mathcal{I}(X), \subseteq \rangle$ and $\langle \mathcal{F}(X), \supseteq \rangle$ are completions of X via the mappings $x \mapsto \downarrow x$ and $x \mapsto \uparrow x$, respectively.*

Definition 2.10 *Let X be a poset, and $x, y, \in X$. We say y* covers *x, (or x is* covered by *y), denoted $x \lessdot y$, if $x < y$ and for all $z \in X$, $x \leqslant z < y$ implies $x = z$.*

Posets have a natural representation in the form of *Hasse diagrams.* The Hasse diagram of a poset $\langle X, \leqslant \rangle$ is a graph $G = \langle X, \lessdot \rangle$. That is, the nodes of the graph are members of X, and an edge exists between x and y if x is covered by y. (By convention, if $x \lessdot y$, the node labelled x will be lower than the node labelled y in the Hasse diagram.) We conclude this section with some examples of posets.

Example 2.1 *Three posets, represented by their Hasse diagrams, are shown in Figure 1. It can be easily checked that Figure 1a represents a lattice. However, Figures 1b and 1c do not.*

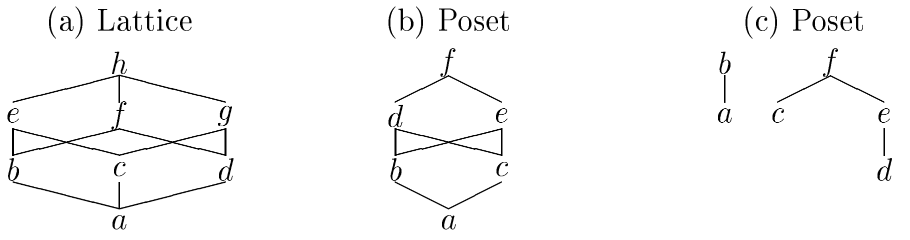

Figure 1: Hasse Diagrams

3 The Lattice $\langle \mathcal{A}(X), \preccurlyeq \rangle$

Definition 3.1 *Let $\langle X, \leqslant \rangle$ be a poset. We will denote the set of antichains of X by $\mathcal{A}(X)$, and define the following order on $\mathcal{A}(X)$. For all $\alpha, \beta \in \mathcal{A}(X)$,*

$$\alpha \preccurlyeq \beta \text{ if, and only if, for all } a \in \alpha, \text{ there exists } b \in \beta \text{ such that } a \leqslant b.$$

An example of $\langle \mathcal{A}(X), \preccurlyeq \rangle$ is shown in Figure 3. In order to prove the main result of this section, namely Theorem 3.1, we first state and prove some preparatory lemmas.

Lemma 3.1 *Let $\langle X, \leqslant \rangle$ be a poset. Then $\langle \mathcal{A}(X), \preccurlyeq \rangle$ is a poset.*

Proof: Clearly $\preccurlyeq$ is reflexive and transitive. We now prove $\preccurlyeq$ is anti-symmetric. We proceed by contradiction. Suppose that $\alpha \preccurlyeq \beta$ and $\beta \preccurlyeq \alpha$, but $\alpha \neq \beta$. Without loss of generality we can choose $a \in \alpha$ such that $a \notin \beta$. Since $\alpha \preccurlyeq \beta$, there exists $b \in \beta$ such that $a < b$. Furthermore, $b \notin \alpha$ since $\alpha \in \mathcal{A}(X)$ and hence contains no chain. Therefore, there exists $a' \in \alpha$ such that $b < a'$ since $\beta \preccurlyeq \alpha$. Therefore, we have $a < b < a'$ with $a, a' \in \alpha$, but, since α is an antichain, $a \notin \alpha$. ■

Remark 3.1 *$\preccurlyeq$ is a pre-order, not a partial order, on $\mathcal{P}(X)$ as $\preccurlyeq$ is not anti-symmetric. For example, using the poset of Figure 1c, $\{d, e\} \preccurlyeq \{e\}$ and $\{e\} \preccurlyeq \{d, e\}$, but $\{d, e\} \neq \{e\}$.*

Definition 3.2 *Let $\alpha \subseteq X$. Then $a \in \alpha$ is a* maximal element *in α if for all $b \in \alpha$, $a \leqslant b$ implies $a = b$. We denote the set of maximal elements of α by $\overline{\alpha}$.*

Remark 3.2 *For all $\alpha \subseteq X$, $a \in \alpha$,*

$$\overline{\alpha} \subseteq \alpha, \tag{1}$$
$$\text{there exists } a' \in \overline{\alpha} \text{ such that } a \leqslant a', \tag{2}$$
$$\overline{\alpha} \in \mathcal{A}(X). \tag{3}$$

The (trivial) proof of the preceding remark follows immediately from Definition 3.2, and is left as an exercise for the interested reader.

Lemma 3.2 *Let $f : \mathcal{P}(X) \to \mathcal{A}(X)$ and $g : \mathcal{P}(X) \to \mathcal{I}(X)$ be defined as follows.*

$$f(\alpha) = \overline{\alpha} \quad \text{and} \quad g(\alpha) = \downarrow\alpha$$

Then f and g are well-defined functions.

Proof: The proof for f is similar to that for Lemma 3.1 and proceeds by contradiction. Suppose $f(\alpha) = \beta_1$, $f(\alpha) = \beta_2$, and $\beta_1 \neq \beta_2$. Then without loss of generality there exists $b_1 \in \beta_1$ such that $b_1 \notin \beta_2$. Since $\beta_1 \subseteq \alpha$, $b_1 \in \alpha$, and, by (2), there exists $b_2 \in \beta_2$ such that $b_1 < b_2$. Now, by (3), $\beta_1 \in \mathcal{A}(X)$ and hence $b_2 \notin \beta_1$ (otherwise there is a chain

$\{b_1, b_2\} \subseteq \beta_1$). Therefore, by (2), there exists $b_3 \in \beta_1$ such that $b_2 < b_3$ (since $b_2 \in \alpha$). Therefore we have $b_1 < b_2 < b_3$ with $b_1, b_3 \in \beta_1$, but β_1 is chain free by assumption.

The proof for g is also by contradiction. (Note that it is equivalent to proving that for any $Y \subseteq X$, $\downarrow Y$ is unique.) Suppose $g(\alpha) = \beta_1$, $g(\alpha) = \beta_2$, and $\beta_1 \neq \beta_2$. Then without loss of generality there exists $b_1 \in \beta_1$ such that $b_1 \notin \beta_2$. $\alpha \subseteq \beta_1$, $\alpha \subseteq \beta_2$, and hence $b_1 \notin \alpha$. Therefore, by the definition of $g(\alpha)$, there exists $a \in \alpha$ such that $b_1 < a$. Now we have $a \in \beta_2$ and $b_1 \notin \beta_2$. In other words, β_2 is not an order ideal. ■

Lemma 3.3 *For all $\alpha \in \mathcal{A}(X)$, $\beta \in \mathcal{I}(X)$,*

$$\overline{\downarrow\alpha} = \alpha \quad \text{and} \quad \downarrow\overline{\beta} = \beta.$$

Proof: It follows immediately from the definitions of $\overline{\alpha}$ and $\downarrow\alpha$. ■

Theorem 3.1 *$\langle \mathcal{A}(X), \preccurlyeq \rangle$ is isomorphic to the lattice $\langle \mathcal{I}(X), \subseteq \rangle$. Furthermore, $\mathcal{A}(X)$ is a completion of X.*

Proof: By Lemma 3.2, the functions $\phi : \mathcal{I}(X) \to \mathcal{A}(X)$ and $\psi : \mathcal{A}(X) \to \mathcal{I}(X)$ where $\phi(\alpha) = \overline{\alpha}$ and $\psi(\alpha) = \downarrow\alpha$ are well defined, and by Lemma 3.3, ϕ and ψ are mutually inverse functions, and hence bijections.

- ϕ is order-preserving - that is, for all $\alpha, \beta \in \mathcal{I}(X)$,

$$\alpha \subseteq \beta \text{ implies } \overline{\alpha} \preccurlyeq \overline{\beta} \tag{4}$$

  Suppose $\alpha \subseteq \beta$. Then $\overline{\alpha} \subseteq \alpha \subseteq \beta$. Hence, if $a \in \overline{\alpha}$ then $a \in \beta$. Therefore, by (2), there exists $b \in \overline{\beta}$ such that $a \leqslant b$. That is $\overline{\alpha} \preccurlyeq \overline{\beta}$.

- $\psi = \phi^{-1}$ is order-preserving - that is, for all $\alpha, \beta \in \mathcal{A}(X)$,

$$\alpha \preccurlyeq \beta \text{ implies } \downarrow\alpha \subseteq \downarrow\beta \tag{5}$$

  Suppose $\alpha \preccurlyeq \beta$ and $a \in \downarrow\alpha$. Then there exists $a' \in \alpha$ such that $a \leqslant a'$. Since $\alpha \preccurlyeq \beta$ there exists $b \in \beta$ such that $a \leqslant a' \leqslant b$. Hence $a \in \downarrow\beta$. That is $\downarrow\alpha \subseteq \downarrow\beta$.

The first part of the result now follows by Theorem 2.1, while the second part follows immediately from Definition 3.1 on defining $h : X \to \mathcal{A}(X)$ where $h(x) = \{x\}$ is the order-embedding. ■

We now consider the binary operations on the lattice $\langle \mathcal{A}(X), \preccurlyeq \rangle$.

4 The Binary Operations on the Lattice $\langle \mathcal{A}(X), \preccurlyeq \rangle$

The binary operations are explicitly described by the following lemma.

Lemma 4.1 *For all $\alpha, \beta \in \mathcal{A}(X)$*

$$\begin{aligned} \alpha \wedge \beta &= \inf\{\alpha, \beta\} = \overline{\downarrow\alpha \cap \downarrow\beta}, \\ \alpha \vee \beta &= \sup\{\alpha, \beta\} = \overline{\alpha \cup \beta}. \end{aligned}$$

Proof: We first make the observation that, by construction, $\overline{\downarrow\alpha \cap \downarrow\beta}, \overline{\alpha \cup \beta} \in \mathcal{A}(X)$.

- $\overline{\downarrow\alpha \cap \downarrow\beta}$ is a lower bound of α and β. Suppose $x \in \overline{\downarrow\alpha \cap \downarrow\beta}$. Then by (1) $x \in \downarrow\alpha \cap \downarrow\beta$, and therefore $x \in \downarrow\alpha$ and $x \in \downarrow\beta$. Hence there exists $a \in \alpha$ such that $x \leqslant a$ and there exists $b \in \beta$ such that $x \leqslant b$. Therefore $\overline{\downarrow\alpha \cap \downarrow\beta} \preccurlyeq \alpha$ and $\overline{\downarrow\alpha \cap \downarrow\beta} \preccurlyeq \beta$.

- $\overline{\alpha \cup \beta}$ is an upper bound of α and β. Suppose $a \in \alpha$. Then $a \in \alpha \cup \beta$ and hence there exists $a' \in \overline{\alpha \cup \beta}$ such that $a \leqslant a'$. Therefore, $\alpha \preccurlyeq \overline{\alpha \cup \beta}$. Similarly $\beta \preccurlyeq \overline{\alpha \cup \beta}$.

- $\overline{\downarrow\alpha \cap \downarrow\beta}$ is the greatest lower bound of α and β. Suppose $\gamma \in \mathcal{A}(X)$, and $\gamma \preccurlyeq \alpha$, $\gamma \preccurlyeq \beta$. Then, by Remark 2.1 and (5) $\gamma \subseteq \downarrow\gamma \subseteq \downarrow\alpha$, $\gamma \subseteq \downarrow\gamma \subseteq \downarrow\beta$, and therefore $\gamma \subseteq \downarrow\alpha \cap \downarrow\beta$. Hence, by (4), and since $\gamma \in \mathcal{A}(X)$, $\gamma = \overline{\gamma} \preccurlyeq \overline{\downarrow\alpha \cap \downarrow\beta}$, on using Lemma 3.3.

- $\overline{\alpha \cup \beta}$ is the least upper bound of α and β. Suppose $\gamma \in \mathcal{A}(X)$, and $\alpha \preccurlyeq \gamma$, $\beta \preccurlyeq \gamma$. Then $\alpha \subseteq \downarrow\alpha \subseteq \downarrow\gamma$ and $\beta \subseteq \downarrow\beta \subseteq \downarrow\gamma$. Therefore $\alpha \cup \beta \subseteq \downarrow\gamma$, and, by (4), $\overline{\alpha \cup \beta} \preccurlyeq \overline{\downarrow\gamma} = \gamma$, on using Lemma 3.3.

■

We conclude this section with a simple example.

Example 4.1 *Let $X = \{a, b, c, d, e, f\}$ with the partial order given by the Hasse diagram in Figure 1c, and let $\alpha = \{b, e\}$, $\beta = \{a, f\}$. Then*

$$\begin{aligned} \alpha \vee \beta &= \overline{\alpha \cup \beta} \\ &= \overline{\{a, b, e, f\}} \\ &= \{b, f\} \end{aligned}$$

$$\begin{aligned} \alpha \wedge \beta &= \overline{\downarrow\alpha \cap \downarrow\beta} \\ &= \overline{\{a, b, d, e\} \cap \{a, c, d, e, f\}} \\ &= \overline{\{a, d, e\}} \\ &= \{a, e\} \end{aligned}$$

5 Further Results

This section presents further results for $\mathcal{A}(X)$ which are analogous to standard results for $\mathcal{I}(X)$. For brevity, we have not explicitly defined some of the terms in this section. Therefore, this section may only be of interest to readers who are already familiar with poset theory. However, we note that the appropriate definitions can be found in [8] as can the analogues of Propositions 5.1, 5.2 and 5.3, labelled therein as Theorems 8.17, 2.31 and 8.22, respectively.

Proposition 5.1 *Let L be a finite distributive lattice. Then L is isomorphic to $\mathcal{A}(\mathcal{J}(L))$, where $\mathcal{J}(L)$ is the set of join irreducible elements in L.*

Proof: Consider the function $\phi : L \to \mathcal{A}(\mathcal{J}(L))$ where

$$\phi(a) = \overline{\mathcal{J}(L) \cap \downarrow a}.$$

We first prove that ϕ is an order-embedding.

$$\begin{aligned}
a \leqslant b &\Rightarrow {\downarrow}a \subseteq {\downarrow}b \\
&\Rightarrow \mathcal{J}(L) \cap \downarrow a \subseteq \mathcal{J}(L) \cap \downarrow b \\
&\Rightarrow \overline{\mathcal{J}(L) \cap \downarrow a} \preccurlyeq \overline{\mathcal{J}(L) \cap \downarrow b} \quad \text{by (4)} \\
&\Rightarrow \phi(a) \preccurlyeq \phi(b) \\
\phi(a) \preccurlyeq \phi(b) &\Rightarrow \overline{\mathcal{J}(L) \cap \downarrow a} \preccurlyeq \overline{\mathcal{J}(L) \cap \downarrow b} \\
&\Rightarrow {\downarrow}\overline{\mathcal{J}(L) \cap \downarrow a} \subseteq {\downarrow}\overline{\mathcal{J}(L) \cap \downarrow b} \quad \text{by (5)} \\
&\Rightarrow \mathcal{J}(L) \cap \downarrow a \subseteq \mathcal{J}(L) \cap \downarrow b \quad \text{by Lemma 3.3} \\
&\Rightarrow {\downarrow}a \subseteq {\downarrow}b \\
&\Rightarrow a \leqslant b
\end{aligned}$$

It remains to prove that ϕ is a bijection. Suppose that $\phi(a) = \phi(b)$. Then we have

$$\begin{aligned}
\mathcal{J}(L) \cap \downarrow a = \mathcal{J}(L) \cap \downarrow b &\Rightarrow {\downarrow}a = {\downarrow}b \\
&\Rightarrow {\downarrow}a \subseteq {\downarrow}b \quad \text{and} \quad {\downarrow}b \subseteq {\downarrow}a \\
&\Rightarrow a \leqslant b \quad \text{and} \quad b \leqslant a \\
&\Rightarrow a = b.
\end{aligned}$$

Hence ϕ is one-to-one, and since L is finite, ϕ is a bijection. ■

Figure 2 illustrates Proposition 5.1, and compares $\mathcal{A}(\mathcal{J}(L))$ and $\mathcal{I}(\mathcal{J}(L))$. The join irreducible elements are shown in bold type. It can be seen that a join irreducible element, x, is mapped to the set $\{x\}$ by ϕ, which means the construction of $\mathcal{A}(\mathcal{J}(L))$ is more straightforward than that of $\mathcal{I}(\mathcal{J}(L))$. In the interests of clarity, the set delimiters have

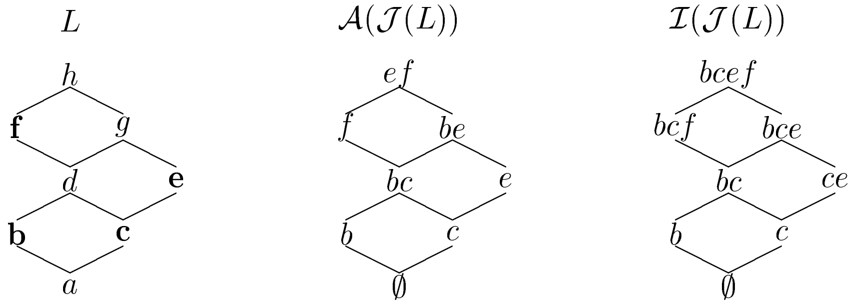

Figure 2: L, $\mathcal{A}(\mathcal{J}(L))$ and $\mathcal{I}(\mathcal{J}(L))$

been omitted in $\mathcal{A}(\mathcal{J}(L))$ and $\mathcal{I}(\mathcal{J}(L))$. That is, $bcef$, for example, should be read as $\{b, c, e, f\}$.

Of course, Proposition 5.1 is merely a re-statement of Birkhoff's Representation Theorem for finite distributive lattices [2], and as such can be proved as a corollary of that result and Theorem 3.1. We now state without proof two further propositions. Proposition 5.2 states the existence of a Dedekind-MacNeille-style completion using antichains; and Proposition 5.3 states several results regarding standard constructions on posets.

It is necessary to introduce some notation in order to state Proposition 5.2.

Definition 5.1 *Given a poset, X, and a subset Y of X, define*

$$Y^u = \{x \in X : \text{ for all } y \in Y, y \leqslant x\} \quad \text{and} \quad Y^l = \{x \in X : \text{ for all } y \in Y, y \geqslant x\}.$$

Theorem 5.1 *The lattice $\langle DM(X), \subseteq\rangle$, where $DM(X) = \{Y \subseteq X : Y^{ul} = Y\}$, is a completion of X via the order-embedding $\phi : X \hookrightarrow DM(X)$ such that $\phi(x) = {\downarrow}x$. It is known as the* Dedekind-MacNeille completion *(of X).*

Proposition 5.2 *The lattice $\langle DM_{\mathcal{A}}(X), \subseteq\rangle$, where $DM_{\mathcal{A}}(X) = \{\overline{Y} : Y \subseteq X,\ Y^{ul} = Y\}$, is a completion of X via the order-embedding $\phi : X \hookrightarrow DM_{\mathcal{A}}(X)$ such that $\phi(x) = \{x\}$. Furthermore, $DM(X)$ is isomorphic to $DM_{\mathcal{A}}(X)$.*

Figure 3 in Appendix A shows $DM(X)$, $DM_{\mathcal{A}}(X)$, $\mathcal{A}(X)$ and $\mathcal{I}(X)$ for the poset, X, of Figure 1c.

Proposition 5.3 *Let X be a finite poset. Then*

- $\mathcal{A}(X)^{\vartheta} \cong \mathcal{A}(X^{\vartheta})$,
- $\mathcal{A}(\bot \oplus X) \cong \emptyset \oplus (\{\bot\} \oplus \mathcal{A}(X))$,
- $\mathcal{A}(X \oplus \top) \cong \mathcal{A}(X) \oplus \{\top\}$,
- $\mathcal{A}(X_1 \dot{\cup} X_2) \cong \mathcal{A}(X_1) \times \mathcal{A}(X_2)$,

where X^{ϑ} denotes the dual of X, $\cong$ is to be read "is isomorphic to", $\oplus$ is the direct sum, $\bot$ is a bottom element, $\top$ is a top element, $\dot{\cup}$ denotes disjoint union, and $\times$ denotes Cartesian product.

6 Conflict of Interest Policies

We now briefly discuss an alternative application of antichains in access control modelling. Suppose we have some (unordered) set, X, and an *environment*, $E \subseteq X$.

Definition 6.1 *A* conflict of interest policy*, $\alpha \in \mathcal{P}(\mathcal{P}(X))$, is* satisfied by *$E$ if, and only if, for all $a \in \alpha$, $a \cap E \subset a$. We denote the set of environments which satisfy α by $\mathcal{E}(\alpha)$.*

In other words, a conflict of interest policy states which subsets of X cannot be present simultaneously in the environment, and is satisfied provided the environment does not include any member of the policy. We make the following observations about this definition.

- A singleton set $\{a\} \in \alpha,\ a \in X$ implies that a is prohibited from ever entering the environment E.
- If $\alpha = \{\emptyset\}$ then no environment satisfies α.
- If $\alpha = \emptyset$ then every environment satisfies α.

Definition 6.2 *Given two conflict of interest policies, α, β, we say α is* weaker than *(or* less restrictive than *or* is enforced by*) β if $\mathcal{E}(\alpha) \supset \mathcal{E}(\beta)$. We will also say β is* stronger *(or* more restrictive than *or* enforces*) α; α and β are* equivalent *if $\mathcal{E}(\alpha) = \mathcal{E}(\beta)$.*

It is not hard to convince oneself that conflict of interest policies can be regarded as members of $\mathcal{A}(\mathcal{P}(X))$ rather than $\mathcal{P}(\mathcal{P}(X))$ (see [6] for further details). Formally, it is easy to prove the following result [6].

Proposition 6.1 *Suppose $\alpha \in \mathcal{P}(\mathcal{P}(X))$ and $a \subset b$ for some $a, b \in \alpha$. Define $\alpha' = \alpha \setminus \{b\}$. Then an environment, E, satisfies α if, and only if, E satisfies α'.*

In other words, any conflict of interest policy, $\alpha \in \mathcal{P}(\mathcal{P}(X))$, can be reduced to the (*canonical*) conflict of interest policy, $\alpha' \in \mathcal{A}(\mathcal{P}(X))$, which is equivalent to α. For example, let $X = \{1, 2, 3\}$ and consider the policy $\alpha = \big\{\{1\}, \{2, 3\}, \{1, 3\}\big\}$. This can be reduced to $\alpha' = \big\{\{1\}, \{2, 3\}\big\}$ since $\{1\}$ renders $\{1, 3\}$ redundant.

Suppose now that we have two conflict of interest policies

$$\alpha = \big\{\{1\}, \{2, 3\}\big\} \quad \text{and} \quad \beta = \big\{\{2\}, \{1, 3\}\big\}.$$

Then the only environments which satisfy both α and β are $E = \emptyset$ and $E = \{3\}$. That is $\mathcal{E}(\alpha) \cap \mathcal{E}(\beta) = \big\{\emptyset, \{3\}\big\}$. Now, recalling the binary operations of Section 4, $\alpha \wedge \beta = \big\{\{1\}, \{2\}, \{3\}\big\}$, and $\mathcal{E}(\alpha \wedge \beta) = \emptyset$. That is, $\wedge$ is not the appropriate binary operation for combining conflict of interest policies if the required semantics of $\alpha \wedge \beta$ is to form the weakest policy which enforces both α and β.

Definition 6.3 *For all $\alpha, \beta \in \mathcal{A}(X)$,*

$$\alpha \preccurlyeq' \beta \textit{ if, and only if, for all } b \in \beta, \textit{there exists } a \in \alpha \textit{ such that } a \leqslant b.$$

Definition 6.4 *For all $\alpha, \beta \in \mathcal{A}(X)$, define*

$$\alpha \times \beta = \underline{\alpha \cup \beta},$$

where $\underline{\alpha}$ is the set of minimal elements in α (defined analogously to $\overline{\alpha}$ in Definition 3.2).

It should be clear from the discussion preceding Definition 6.3 that the binary operation $\times$ combines α and β in such a way as to incorporate necessary and sufficient information to enforce them simultaneously. For example, $\alpha \times \beta = \big\{\{1\}, \{2\}\big\}$. We conclude with results analogous to those proved in Sections 3 and 4.

Proposition 6.2 *For any poset X, $\alpha, \beta \in \mathcal{A}(X)$,*

- $\langle \mathcal{A}(X), \preccurlyeq' \rangle$ *is a lattice;*
- $\inf\{\alpha, \beta\} = \underline{\alpha \cup \beta}$ *and* $\sup\{\alpha, \beta\} = \underline{\uparrow\alpha \cap \uparrow\beta}$*;*
- *The lattices $\langle \mathcal{A}(X), \preccurlyeq' \rangle$ and $\langle \mathcal{A}(X), \preccurlyeq \rangle$ are isomorphic via the mapping $\alpha \mapsto \overline{X \setminus \uparrow\alpha}$;*
- *$x \mapsto \{x\}$ is an order-embedding.*

The proofs of the results in Proposition 6.2 are available as a research note [7], and use the same methods of proof as those in Sections 3 and 4. We summarise the relationships between the lattices $\langle \mathcal{A}(X), \preccurlyeq \rangle$, $\langle \mathcal{A}(X), \preccurlyeq' \rangle$, $\langle \mathcal{I}(X), \subseteq \rangle$, and $\langle \mathcal{F}(X), \supseteq \rangle$ in the diagram below. Figure 4 in Appendix B shows the lattice of policies, $\langle \mathcal{A}(X), \preccurlyeq' \rangle$, when $X = \{1, 2, 3\}$.

$$\begin{tikzcd}
\langle \mathcal{I}(X), \subseteq \rangle \arrow[r, "\alpha \mapsto X \setminus \alpha"] \arrow[d, "\alpha \mapsto \overline{\alpha}"'] & \langle \mathcal{F}(X), \supseteq \rangle \arrow[d, "\alpha \mapsto \underline{\alpha}"] \\
\langle \mathcal{A}(X), \preccurlyeq \rangle & \langle \mathcal{A}(X), \preccurlyeq' \rangle \arrow[l, "\alpha \mapsto \overline{X \setminus \uparrow\alpha}"]
\end{tikzcd}$$

7 Conclusion

We have shown that the lattice of antichains, $\langle \mathcal{A}(X), \preccurlyeq \rangle$ is isomorphic to $\langle \mathcal{I}(X), \subseteq \rangle$, and hence that many results for $\mathcal{I}(X)$ can be applied to $\mathcal{A}(X)$. In particular, there exists a Dedekind-MacNeille-style completion $\langle DM_{\mathcal{A}}(X), \preccurlyeq \rangle$ with $DM_{\mathcal{A}}(X) \subseteq \mathcal{A}(X)$, and an analogue of Birkhoff's Representation Theorem for finite distributive lattices.

We believe that, in general, it is easier to determine the elements of $\mathcal{A}(X)$ than those of $\mathcal{I}(X)$, and hence to determine the structure of $\mathcal{I}(X)$ via the isomorphism. In particular, every singleton subset of X is an antichain, and no element of $\mathcal{A}(X)$ has more elements than the *width* of X [8]. We hope to investigate whether an algorithm to compute $\mathcal{A}(X)$ exists which necessarily has lower time and space complexity [1] than one to compute $\mathcal{I}(X)$.

(It is easy to see that a description of $\mathcal{A}(X)$ requires less space than $\mathcal{I}(X)$.) We also hope to provide a simpler characterisation of the elements of $DM_{\mathcal{A}}(X)$ and hence develop an algorithm for computing the Dedekind-MacNeille completion.

In addition we intend to investigate whether the operation $\alpha + \beta = \sup\{\alpha, \beta\}$ for the lattice $\langle \mathcal{A}(X), \preccurlyeq' \rangle$ has a meaningful interpretation in the context of conflict of interest policies.

Acknowledgements The work of Jason Crampton is supported by EPSRC award 98317878. The authors would like to thank Szabolcs Mikulás for his careful reading of the manuscript and helpful suggestions.

References

[1] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, MA, 1975.

[2] G. Birkhoff. On the combination of subalgebras. *Proceedings of the Cambridge Philosophical Society*, 29:441–464, 1933.

[3] G. Birkhoff. *Lattice Theory*. American Mathematical Society, 1948.

[4] S. Burris and H.P. Sankappanavar. *A Course in Universal Algebra*. Springer-Verlag, New York, 1981.

[5] J. Crampton and G. Loizou. Role-based access control: A constructive appraisal. In preparation.

[6] J. Crampton and G. Loizou. On the structural complexity of conflict of interest policies. Research note, September 2000.

[7] J. Crampton and G. Loizou. Two partial orders on the set of antichains. Research note, September 2000.

[8] B.A. Davey and H.A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, 1990.

[9] D.F. Ferriaolo, J.A. Cugini, and D.R. Kuhn. Role-based access control (RBAC): Features and motivations. In *Proceedings of 11th Annual Computer Security Applications Conference*, pages 241–248, New Orleans, Louisiana, December 1995.

[10] G. Grätzer. *General Lattice Theory*. Academic Press, London, 1978.

[11] M. Nyanchama and S. Osborn. The role graph model. In *Proceedings of First ACM Workshop on Role-Based Access Control*, pages II25–II31, Gaithersburg, Maryland, October 1995.

[12] R.S. Sandhu, E.J. Coyne, H. Feinstein, and C.E. Youman. Role-based access control. *IEEE Computer*, 29(2):38–47, 1996.

Appendix A: Completions of a Poset

We take as our example the poset of Figure 1c.

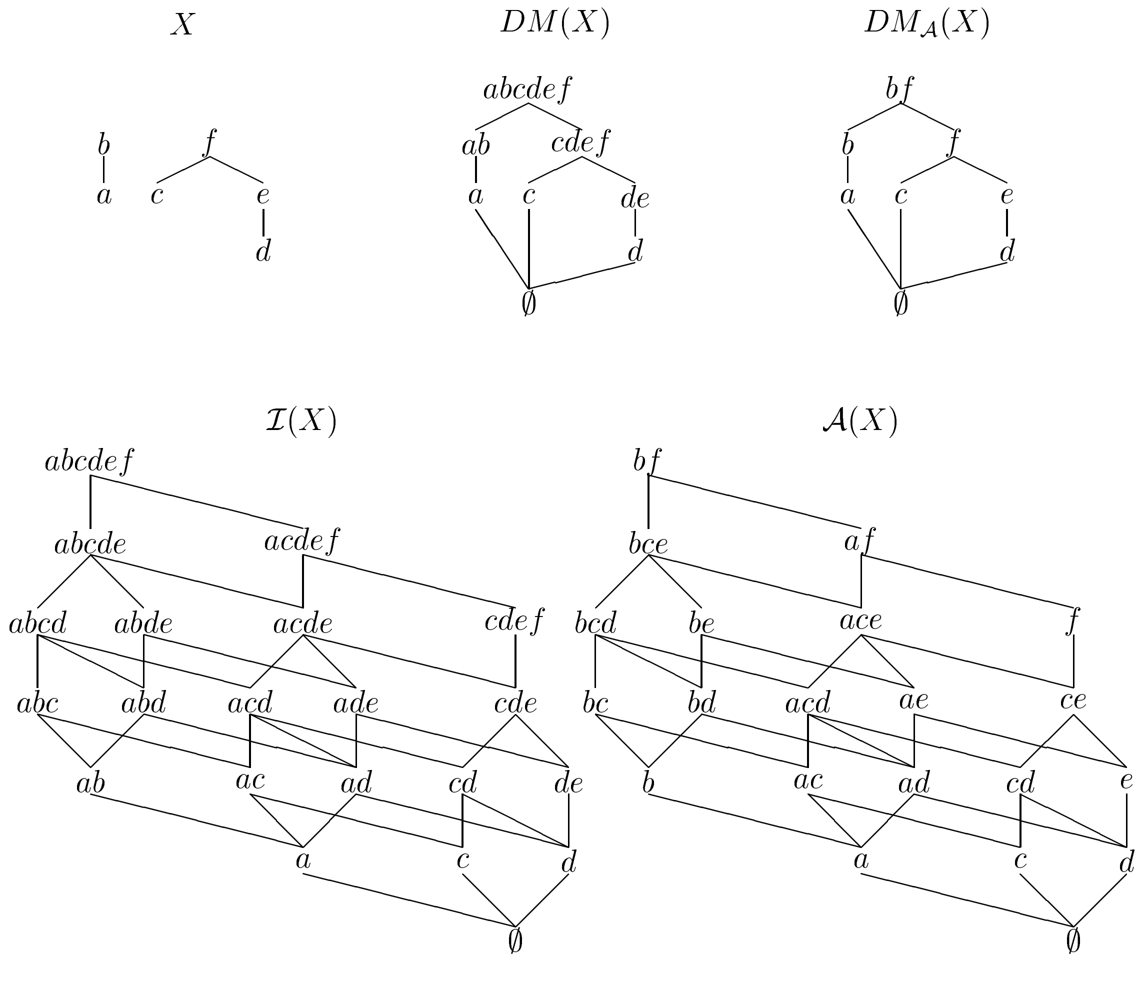

Figure 3: Completions of the poset of Figure 1c

Appendix B: Conflict of Interest Policies

Figure 4 shows Hasse diagrams for $\mathcal{P}(X)$, $\langle \mathcal{A}(\mathcal{P}(X)), \preccurlyeq' \rangle$ and $\langle \mathcal{A}(\mathcal{P}(X)), \preccurlyeq \rangle$, where $X = \{1, 2, 3\}$. We see, for example, that $\{\{1, 2\}, \{1, 3\}\} \mapsto \{\{1\}, \{2, 3\}\}$.

Note that the conflict of interest policies become more restrictive the lower down the lattice they appear.

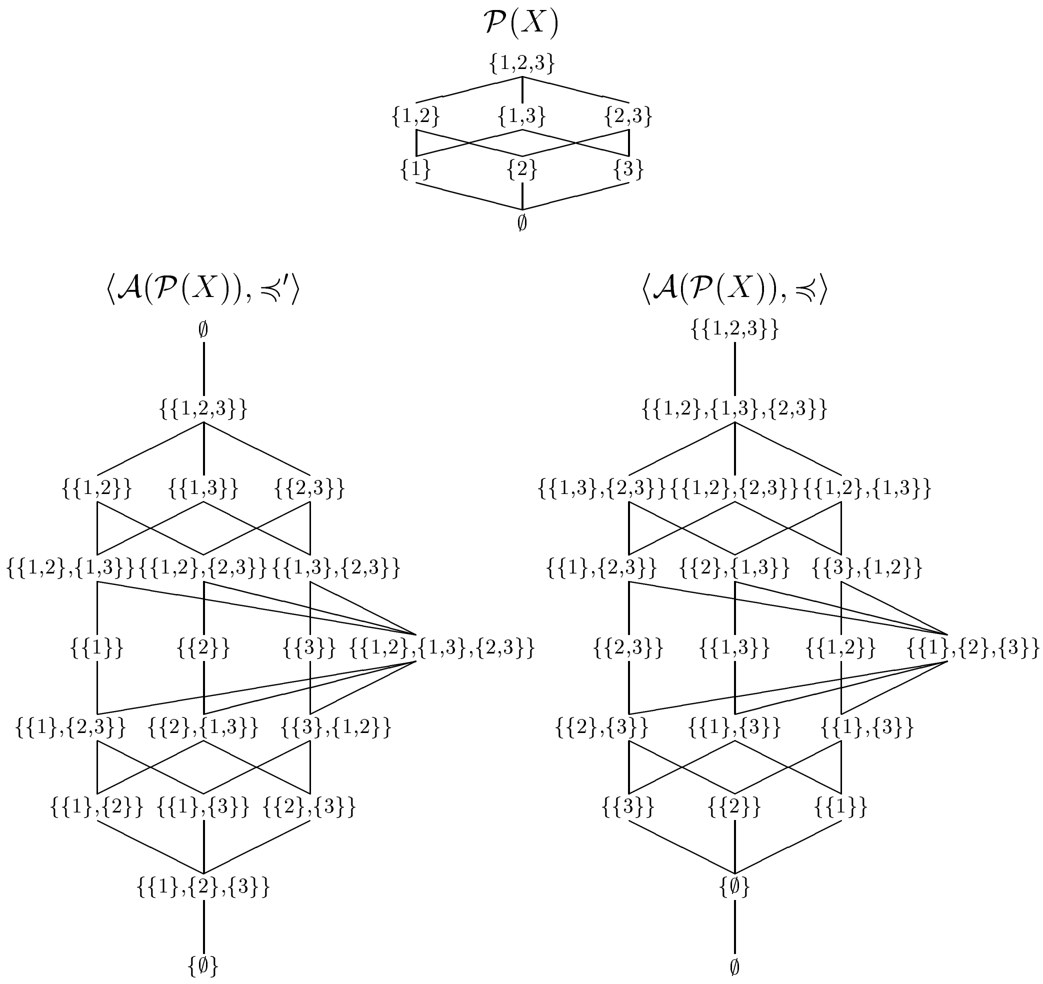

Figure 4: $\mathcal{P}(X)$, $\langle \mathcal{A}(\mathcal{P}(X)), \preccurlyeq' \rangle$ and $\langle \mathcal{A}(\mathcal{P}(X)), \preccurlyeq \rangle$