On the structural complexity of conflict of interest policies

Jason Crampton* and George Loizou

Department of Computer Science, Birkbeck College, University of London

{ccram01,george}@dcs.bbk.ac.uk

6th November 2000

Abstract

We define a conflict of interest policy and show that the definition is sufficiently general to include several well-known generic policies as special cases and to articulate policies in different models of access control. We show that conflict of interest policies can be regarded as members of $\mathcal{P}(\mathcal{P}(X))$, for some set X, where $\mathcal{P}(X)$ denotes the powerset of X, and that such policies can be reduced to a canonical form. The set of canonical conflict of interest policies can be modelled by a subset of $\mathcal{P}(\mathcal{P}(X))$, $\mathcal{A}(\mathcal{P}(X))$. We derive upper and lower bounds for $|\mathcal{A}(\mathcal{P}(X))|$ and for the maximum length of a string that would be required to describe a conflict of interest policy. We also discuss the composition of two conflict of interest policies, an ordering for conflict of interest policies, and possible simplifications in the expression of such policies.

*The work of Jason Crampton is supported by EPSRC Award 98317878.

1 Introduction

Our recent work [8, 9, 21] is concerned with modelling the behaviour of a discretionary access control mechanism of a computer system using a deductive database. The purpose of this work is to reason about the correctness of the implementation (that is, the configuration of access control lists, say) of an abstract access control policy. We model the state of the access control mechanism as a set of (access right) triples $M \subseteq O \times S \times R$, where O is the set of objects, S is the set of subjects, and R is the set of access rights supported by the system. Our model is essentially the same as that of Harrison, Ruzzo and Ullman [17] with $(o, s, r) \in M$ if, and only if, $r \in [s, o]$ where $[s, o]$ denotes the entry in the protection matrix for subject s and object o.

We then considered access control policies, which are considered to be an abstract specification of what an access control mechanism should implement. In their simplest form, access control policies can be confidentiality policies (controlling read access) or integrity policies (controlling write access). In [21] a classification of access control policies was presented, and in [8] we discussed a way in which access control policies could be modelled as elements or subsets of $\mathcal{P}(O \times S \times R)$.

We observed that a policy, $P^+ \subseteq O \times S \times R$, which specifies the triples that are authorised, should be implemented as follows: the access control mechanism grants subject s access to object o in mode r only if $(o, s, r) \in P^+$. Similarly a policy, $P^- \subseteq O \times S \times R$, which specifies which triples are prohibited, should be implemented as follows: the access control mechanism grants subject s access to object o in mode r only if $(o, s, r) \notin P^-$. (The Bell-LaPadula model [3] implements a confidentiality policy through a somewhat different mechanism, although the policy itself could be expressed in the way we have suggested.) It should be obvious that a policy of type P^+ or P^- can be used to specify a given integrity or confidentiality policy - they are merely complementary views of the same issue. P^+ and P^- are similar to the positive authorisation and negative authorisation policies in Ponder [10], from which we borrow the superscript notation.

However, when one considers separation of duty policies [5], it becomes clear that each element of the policy must be a set of triples. Specifically such a policy must specify those sets of triples which form a conflict of interest. Hence a conflict of interest policy, $P^{\ominus}$, can be represented as

$$P^{\ominus} = \{A_i \subseteq O \times S \times R : i \in I\} \text{ where } I \text{ is some index set.}$$

Clearly if $|A_i| = 1$, for all $i \in I$, then $P^{\oplus}$ corresponds to a P^{-} policy. Thus we can and will use a conflict of interest policy of type $P^{\oplus}$ to model both P^{-}-type policies and separation of duty policies. Hence we assume a conflict of interest policy defines any scenario which conflicts with the integrity and confidentiality of the system (and not just separation of duty constraints).

We note that, as with confidentiality and integrity policies, we could define a complementary policy, $P^{\oplus}$, which specifies all permissible combinations of roles. However, we will adopt the prevailing (and intuitively more reasonable) practice and regard a separation of duty policy as an explicit specification of conflict of interest requirements.

There are two ways of implementing a conflict of interest policy - static and dynamic. In the former, the access control mechanism has the requirements of the conflict of interest policy "embedded" into it, while in the latter the access control mechanism prevents the current configuration of the system from violating the conflict of interest policy. For a more detailed account of such considerations and the development of modelling conflict of interest policies, with particular reference to role-based access control (RBAC), see [1].

The first contribution of this paper is to provide a general framework and notation for considering conflict of interest policies. We will see that this framework permits the specification of policies of type P^{-} and $P^{\ominus}$. We regard a conflict of interest policy as a set of conflict of interest constraints which are subsets of some suitable choice of set, X. Hence a conflict of interest policy is a member of $\mathcal{P}(\mathcal{P}(X))$. We also define rigorously how to compare and combine two conflict of interest policies.

Since $|\mathcal{P}(\mathcal{P}(X))| = 2^{2^n}$, where $n = |X|$, the number of conflict of interest policies appears to increase doubly exponentially in the size of X, and the length (or description) of such a policy is potentially very large.

The second contribution is to demonstrate that a simple observation about the characteristics of conflict of interest policies leads to a natural reduction of elements of $\mathcal{P}(\mathcal{P}(X))$ to a *canonical* representation of conflict of interest policies.

The third contribution of this paper is to state and prove an explicit value for (the length of) the longest canonical representation and upper and lower bounds for the size of the set of all canonical representations, $\mathcal{A}(\mathcal{P}(X))$. The lower bound for $|\mathcal{A}(\mathcal{P}(X))|$ is a corollary of Sperner's Theorem [27]. The upper bound is equivalent to a result of Hansel [16] which is proved using a *symmetric chain partition* of $\mathcal{P}(X)$ [4], and some elementary theory of partially ordered sets [11].

The final contribution of this paper is to significantly improve on Hansel's upper bound for $|\mathcal{A}(\mathcal{P}(X))|$ by introducing the concept of a *bi-symmetric chain partition*.

The remainder of this paper is organised as follows. In Section 2 we introduce some fundamental definitions and results from the theory of partially ordered sets and combinatorics. In Section 3 we introduce conflict of interest policies, their canonical representation and an ordering and binary operations on the set of canonical conflict of interest policies. In Section 4 we give some examples of conflict of interest policies in order to illustrate the generality and utility of our approach. Section 5 contains our theoretic results. Therein we state and prove results leading to bounds for $\mathcal{A}(\mathcal{P}(X))$ and for the length of the largest conflict of interest policy. We include a table of results for $1 \leqslant |X| \leqslant 8$. In conclusion we discuss certain simplifications to the model of a conflict of interest policy which lead immediately to an explicit value for the number of conflict of interest policies and discuss future directions for our work. The paper is intended to be self-contained, and hence we include the proof of Hansel's result in Appendix A.

2 Preliminaries

2.1 Partially Ordered Sets

Definition 2.1 *A pair* $\langle P, \leqslant \rangle$ *is a* partially ordered set *or* poset *if for all* $p, q, r \in P$*,*

- $p \leqslant p$*,*
- $p \leqslant q$ *and* $q \leqslant p$ *implies* $p = q$*,*
- $p \leqslant q$ *and* $q \leqslant r$ *implies* $p \leqslant r$*.*

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

- $p < q$ if, and only if, $p \leqslant q$ and $p \neq q$; and
- $p \parallel q$ if, and only if, $p \nleqslant q$ and $p \ngeqslant q$.

In the remainder of this section, we will write P to mean the pair $\langle P, \leqslant \rangle$.

Definition 2.2 *Given a poset* P*,* $Q \subseteq P$ *is a* chain *if for all* $q_1, q_2 \in Q$ *either* $q_1 \leqslant q_2$ *or* $q_2 \leqslant q_1$*.* Q *is an* antichain *if for all* $q_1, q_2 \in Q, q_1 \parallel q_2$*. We denote the set of antichains by* $\mathcal{A}(P)$*.*

Definition 2.3 *Given a poset* P *and* $Q \subseteq P$*, we say* $q \in Q$ *is a* minimal *element if for all* $q' \in Q$*,* $q' \leqslant q$ *implies* $q = q'$*. Similarly,* $q \in Q$ *is a* maximal *element if for all* $q' \in Q$*,* $q \leqslant q'$ *implies* $q = q'$*. We denote the set of minimal elements in* Q *by* $\underline{Q}$*; and the set of maximal elements in* Q *by* $\overline{Q}$*.*

Lemma 2.1 *For all* $Q \subseteq P$*,* $q \in Q$*,*

$$\underline{Q} \subseteq Q, \tag{1}$$

$$\text{there exists } q' \in \underline{Q} \text{ such that } q' \leqslant q, \tag{2}$$

$$\underline{Q} \in \mathcal{A}(P), \tag{3}$$

$$\underline{Q} \text{ is unique.} \tag{4}$$

Proof The proof is trivial, following immediately from Definition 2.3, and is left as an exercise for the interested reader. ■

Definition 2.4 *Given a poset P and $p, q, \in P$, we say q* covers *p, denoted $p \lessdot q$, if $p < q$ and $p \leqslant r < q$ implies $p = r$.*

Definition 2.5 *Given a poset P, a non-empty subset Q of P is an* order ideal *if for all $p \in P, q \in Q$, $p \leqslant q$ implies $p \in P$. We denote the set of order ideals of P by $\mathcal{I}(P)$. A non-empty subset Q of P is called an* order filter *if for all $p \in P, q \in Q$, $p \geqslant q$ implies $p \in P$. We denote the set of order filters of P by $\mathcal{F}(P)$*

Definition 2.6 *Given a poset P, and $Q \subseteq P$, we define $\downarrow Q$ read "down Q" as follows:*

$$\downarrow Q = \{p \in P : \textit{there exists } q \in Q \textit{ such that } p \leqslant q \ \}.$$

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

$$\uparrow Q = \{p \in P : \textit{there exists } q \in Q \textit{ such that } p \geqslant q \ \}.$$

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

It can be easily verified that $\downarrow Q$ is the smallest order ideal that contains Q. Dual results apply to $\uparrow Q$ [11].

2.2 Symmetric Chain Partitions

We note that $\langle \mathcal{P}(X), \subseteq \rangle$ is a poset. We will freely interchange the symbols $\subseteq$ and $\leqslant$. In particular, for $Y, Z \in \mathcal{P}(X)$ we will write $Y \lessdot Z$ to represent the two conditions $Y \subset Z$ and $|Y| = |Z| - 1$ more conveniently. For example, $\{1, 2\} \lessdot \{1, 2, 3\}$.

Definition 2.7 *A* partition *of a set X is a set of subsets of X, $\{X_1, \ldots, X_k\}$, such that*

$$X = \bigcup_{i=1}^{k} X_i \quad \textit{and} \quad X_i \cap X_j = \emptyset \textit{ for all } 1 \leqslant i < j \leqslant k.$$

Definition 2.8 *A* symmetric chain partition *of $\mathcal{P}(X)$ is a partition $\mathcal{C}$ such that for each $C = \{c_0, \dots, c_k\} \in \mathcal{C}$:*

$$c_0 \lessdot c_1 \lessdot \dots \lessdot c_k \quad \textit{and} \quad |c_0| + |c_k| = |X|.$$

We will denote a symmetric chain partition of $\mathcal{P}(X)$ by SCP_n where $n = |X|$.

Example 2.1 *A symmetric chain partition for $X = \{1, 2, 3\}$ is shown below.*

$$\begin{aligned} \emptyset \subset &\{1\} \subset \{1,2\} \subset \{1,2,3\} \\ &\{2\} \subset \{2,3\} \\ &\{3\} \subset \{1,3\} \end{aligned}$$

It can be proved (by induction on $|X|$, see Theorem A.1) that there exists a symmetric chain partition of $\mathcal{P}(X)$.

Lemma 2.2 *SCP_n has $\binom{n}{\lfloor n/2 \rfloor}$ chains.*

Proof For a proof of this elementary result see [4], for example. ■

The following classical result provides an insight to, and constructive method of proof for, two of the results of Section 5.

Theorem 2.1 (Sperner's Theorem [27]) *For all $\alpha \in \mathcal{A}_n$,*

$$|\alpha| \leqslant \binom{n}{\lfloor n/2 \rfloor},$$

with equality if, and only if,

$$\alpha = \begin{cases} \{A \subseteq X : |A| = \frac{n}{2}\} & n \textit{ even}, \\ \{A \subseteq X : |A| = \frac{n-1}{2}\} \quad \textit{or} \quad \{A \subseteq X : |A| = \frac{n+1}{2}\} & n \textit{ odd}. \end{cases}$$

Proof (Sketch) Sperner's Theorem can be proved as a corollary of Lemma 2.2 by noting that if $\alpha \in \mathcal{A}_n$ then for all $C \in SCP_n$, $|\alpha \cap C| \leqslant 1$, and hence $|\alpha| \leqslant |SCP_n| = \binom{n}{\lfloor n/2 \rfloor}$. ■

3 Conflict of Interest Policies

Let X be some set of access control artefacts. We will refer to X as an *access control context* (or simply *context*). For example, X may be the set of all possible triples in the Harrison-Ruzzo-Ullman model.

An *access control environment* (or simply *environment*), E, is a subset of X. The environment models the relevant access control system data structure. For example, in the Harrison-Ruzzo-Ullman model E is the set of triples encoded by the access control matrix. A conflict of interest policy specifies how an access control mechanism should control the addition of elements to the environment.

Definition 3.1 *A* conflict of interest constraint *or* separation of duty constraint *is a subset of X. A* conflict of interest policy *or* separation of duty policy *is a set of conflict of interest constraints.*

An environment, E, satisfies *a conflict of interest policy, α, if, and only if, for all $A \in \alpha$, $A \cap E \subset A$. We denote the set of environments which satisfy α by $\mathcal{E}(\alpha)$. (We also say that α is* violated *by E if there exists $A \in \alpha$ such that $A \subseteq E$.)*

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 conflict of interest constraint in the policy. We make the following observations about this definition.

- A singleton set $\{a\} \in \alpha$, implies that $a \in X$ is prohibited from ever entering the environment E. Specifically, the policy

  $$P^- = \{x_1, \ldots, x_n\}$$

  can be expressed as the conflict of interest policy

  $$\alpha = \{\{x_1\}, \ldots, \{x_n\}\}.$$

It is because our framework can accommodate policies which articulate confidentiality and integrity constraints, as well as separation of duty constraints that we prefer the terminology "conflict of interest" rather than "separation of duty" policies. In this sense, conflict of interest policy means a policy which conflicts with the interest of the system.

- If $\alpha = \{\emptyset\}$ then no environment satisfies α (since $\emptyset \subseteq E$ for all $E \subseteq X$).
- If $\alpha = \emptyset$ then every environment satisfies α (since α contains no constraints).

Table 1 shows three conflict of interest policies

$$\alpha_1 = \{\{1,2\},\{2,3\}\}, \quad \alpha_2 = \{\{1\},\{2,3\}\}, \quad \alpha_3 = \{\{1\},\{1,2\},\{2,3\}\},$$

and the environments which satisfy (ticked) and violate (crossed) each policy. These policies could be regarded as being defined on the subscripts of some set of roles $\{r_1,\ldots,r_n\}$. (For example in α_1, the roles r_2 and r_3 form a conflict of interest constraint.)

Environment	$\alpha_1 = \{\{1,2\},\{2,3\}\}$	$\alpha_2 = \{\{1\},\{2,3\}\}$	$\alpha_3 = \{\{1\},\{1,2\},\{2,3\}\}$
$\emptyset$	✓	✓	✓
$\{1\}$	✓	✗	✗
$\{2\}$	✓	✓	✓
$\{3\}$	✓	✓	✓
$\{1,2\}$	✗	✗	✗
$\{1,3\}$	✓	✗	✗
$\{2,3\}$	✗	✗	✗
$\{1,2,3\}$	✗	✗	✗

Table 1: A comparison of conflict of interest policies and environments

Definition 3.2 *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 $\mathcal{E}(\alpha) = \mathcal{E}(\beta)$.*

In Table 1, α_1 is weaker than α_2, for example. From Table 1 we also see that α_2 and α_3 are equivalent. In fact we have the following result.

Proposition 3.1 *Suppose $\alpha \in \mathcal{P}(\mathcal{P}(X))$ and $A \subset B$ for some $A, B \in \alpha$. Define $\alpha' = \alpha \setminus \{B\}$. Then $\mathcal{E}(\alpha) = \mathcal{E}(\alpha')$. In other words, α and α' are equivalent.*

Proof We prove the equivalent statement that an environment E satisfies α if, and only if E satisfies α'.

- $\Rightarrow$ It follows immediately from the fact that $\alpha' \subset \alpha$.
- $\Leftarrow$ The proof proceeds by contradiction. Suppose, then, that E satisfies α' but does not satisfy α. Clearly $B \subseteq E$ is the only possible way in which E does not satisfy α. However, by construction, $A \subset B \subset E$, and hence E does not satisfy α'.

$\blacksquare$

We note that $\langle \mathcal{P}(\mathcal{P}(X)), \subseteq \rangle$ is a poset, and propose the following definition of a canonical representation of a conflict of interest policy.

Definition 3.3 *Given a conflict of interest policy $\alpha \in \mathcal{P}(\mathcal{P}(X))$, we define the* canonical representation *of α to be $\underline{\alpha} \in \mathcal{A}(\mathcal{P}(X))$.*

In other words, given a conflict of interest policy, its canonical representation is obtained by removing all conflict of interest constraints which are a superset of another constraint in the policy. By Proposition 3.1, the canonical representation of a policy is equivalent to the original policy, and by (4), it is unique. For example α_2 is the canonical representation of α_3 in the example given in Table 1. Henceforth, therefore, we assume that all policies are in their canonical form. We denote the set of canonical conflict of interest policies by $\mathcal{A}_n$ where $n = |X|$. We now define an ordering on $\mathcal{A}_n$ and prove it is a partial order.

Lemma 3.1 *For all $\alpha, \beta \in \mathcal{A}_n$, define*

$$\alpha \preccurlyeq \beta \text{ if, and only if, for all } A \in \alpha \text{ there exists } B \in \beta \text{ such that } A \subseteq B.$$

Then $\langle \mathcal{A}_n, \preccurlyeq \rangle$ is a poset.

Proof We need to prove that $\preccurlyeq$ is reflexive, anti-symmetric and transitive. It is clear that the first and third of these properties hold. We prove $\preccurlyeq$ is anti-symmetric 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 $\alpha \in \mathcal{A}_n$ and hence contains no chain. Therefore, there exists $C \in \alpha$ such that $B < C$ since $\beta \leqslant \alpha$. Therefore, we have $A < B < C$ with $A, C \in \alpha$, but α is an antichain.

■

As usual we will write $\alpha \prec \beta$ if $\alpha \preccurlyeq \beta$ and $\alpha \neq \beta$. Note that $\langle \mathcal{P}(\mathcal{P}(X)), \preccurlyeq \rangle$ is not a poset, since, for example, $\{\{1\}, \{1,2\}\} \preccurlyeq \{\{1,2\}\}$ and $\{\{1,2\}\} \preccurlyeq \{\{1\}, \{1,2\}\}$ but $\{\{1,2\}\} \neq \{\{1\}, \{1,2\}\}$.

The following proposition demonstrates that the formal definition of an ordering on the set of conflict of interest policies, $\preccurlyeq$, corresponds exactly to the intuitive definition of strength given in Definition 3.2.

Proposition 3.2 *For all $\alpha, \beta \in \mathcal{A}(X)$, $\alpha \preccurlyeq \beta$ if, and only if, α is stronger than β.*

Proof The proof in both directions proceeds by contradiction.

- $\Rightarrow$ Given $\alpha \preccurlyeq \beta$, suppose $\mathcal{E}(\alpha) \not\subseteq \mathcal{E}(\beta)$. Then there exists $E \in \mathcal{E}(\alpha)$ such that $E \notin \mathcal{E}(\beta)$. Hence there exists $B \in \beta$ such that $B \subseteq E$. Since, by assumption, $\alpha \preccurlyeq \beta$, for all $B \in \beta$ there exists $A \in \alpha$ such that $A \subseteq B$, and hence we have $A \subseteq B \subseteq E$. That is, $E \notin \mathcal{E}(\alpha)$ which is a contradiction.

- $\Leftarrow$ Given α is stronger than β, suppose $\alpha \not\preccurlyeq \beta$. Then, by definition, for some $B \in \beta$ and for all $A \in \alpha$, $A \not\subseteq B$. In other words, for all $A \in \alpha$, $A \cap B \subset A$. Therefore, by definition, $B \in \mathcal{E}(\alpha)$, and since α is stronger than β, $\mathcal{E}(\alpha) \subseteq \mathcal{E}(\beta)$. That is B satisfies the policy β. This is a contradiction since $B \in \beta$.

■

Definition 3.4 *For all $\alpha, \beta \in \mathcal{A}_n$, define*

$$\alpha \times \beta = \underline{\alpha \cup \beta}, \text{ and } \alpha + \beta = \underline{\uparrow\alpha \cap \uparrow\beta}.$$

The operation $\times$ merges two policies by including the stronger aspects of the two policies. That is, the policy $\alpha \times \beta$ is the weakest policy which enforces both α and β. In fact, we have the following result.

Theorem 3.1 *$\langle \mathcal{A}_n, \preccurlyeq \rangle$ is a complete lattice. Moreover, the join and meet operations of the lattice are $+$ and $\times$ respectively.*

Proof This is a special case of two results we proved in [6]. ■

Figure 1 shows the lattices $\langle \mathcal{P}(X), \subseteq \rangle$ and $\langle \mathcal{A}(\mathcal{P}(X)), \preccurlyeq \rangle$ for $X = \{1, 2, 3\}$. By Theorem 3.1, $+$ and $\times$ are associative, commutative, and closed. Furthermore, the policies $\{\emptyset\}$ and $\emptyset$ are identity elements for $+$ and $\times$, respectively.

Example 3.1 *Let $X = \{1, 2, 3\}$. We have, for example,*

$$\{\{1\}, \{2, 3\}\} \prec \{\{1, 2\}, \{2, 3\}\} \prec \{\{1, 2, 3\}\},$$

$$\begin{aligned}
&\{\{1\}, \{2, 3\}\} \times \{\{2\}, \{1, 3\}\} = \{\{1\}, \{2\}\}, \\
&\{\{1\}, \{2, 3\}\} + \{\{2\}, \{1, 3\}\} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}.
\end{aligned}$$

Definition 3.5 *Let $Y \subseteq X$. We define the $Y-$*constrained subset *of $\mathcal{A}_n$, denoted $\mathcal{A}_n/Y$, as follows:*

$$\mathcal{A}_n/Y = \{\alpha \in \mathcal{A}_n : A \subseteq Y \text{ for all } A \in \alpha\}.$$

Informally, a Y-constrained subset of $\mathcal{A}_n$ is the set of policies in which each of the constraints is a subset of a fixed set of elements, namely Y. Clearly there is a bijection $\theta : \mathcal{A}_n/Y \to \mathcal{A}_m$ where $m = |Y|$.

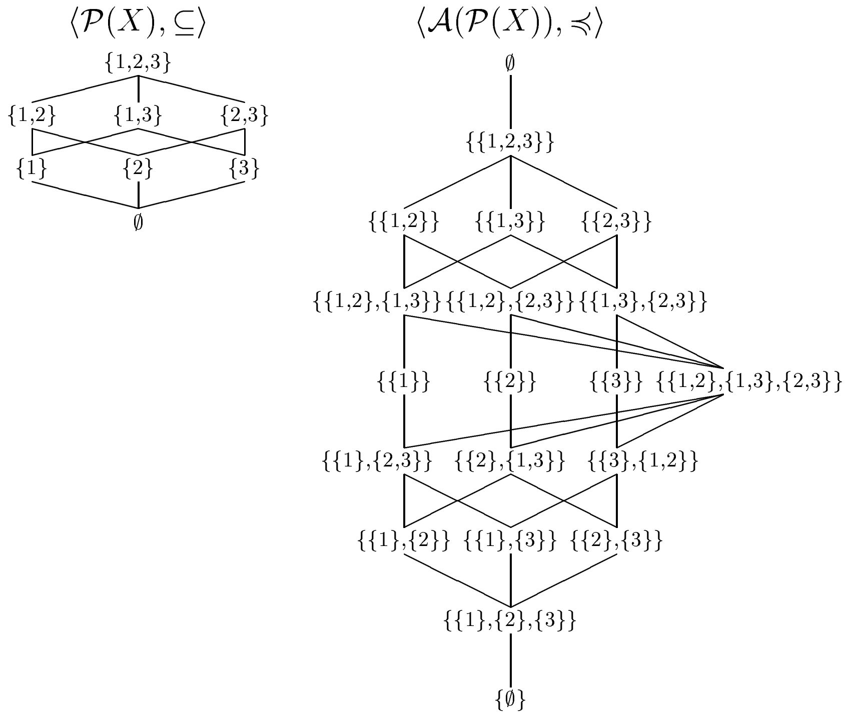

Figure 1: The Lattices $\langle \mathcal{P}(X), \subseteq \rangle$ and $\langle \mathcal{A}(\mathcal{P}(X)), \preccurlyeq \rangle$ for $X = \{1, 2, 3\}$

Definition 3.6 *For* $0 \leqslant r \leqslant n$*,*

$$\phi(n) = |\mathcal{A}_n|, \qquad \phi(n,r) = \sum_{|Y|=r} |\mathcal{A}_n/Y|, \qquad \binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Proposition 3.3 *For all* $1 \leqslant r \leqslant n$*,*

$$\phi(n,r) = \binom{n}{r}\phi(r), \qquad \phi(n) = \sum_{r=0}^{n} \phi(n,r) = \sum_{r=0}^{n} \binom{n}{r}\phi(r)$$

Proof The results follow immediately from Definitions 3.5 and 3.6. ■

4 Examples of Conflict of Interest Policies

In this section we will illustrate the application of our approach using two different access control models. This section has no impact on the development of the theoretical results of Section 5 and can be omitted if the reader has little experience of access control models. In the first set of examples we assume the protection matrix model, and in the second a role-based access control model (RBAC). In both examples we indicate the sets which correspond to X and E. We conclude the section with a brief discussion of RCL 2000 [1], a role authorisation constraint language for expressing separation of duty constraints within the RBAC96 [23] models.

4.1 The Protection Matrix Model

Let M denote the protection matrix, O the set of objects, S the set of subjects and R the set of access modes. We will write $[s, o] \subseteq R$ to denote the access modes available to subject s for object o. (Most systems which employ this model use access control lists, corresponding to a row in M, or capability lists, corresponding to a column in M, to represent the matrix [21].) In this case $X = O \times S \times R$ and (for static conflict of interest policies) E is the set of triples encoded by M. (The environment in the dynamic case is the set of active triples which have been invoked by subjects and granted by the access control mechanism.)

Suppose now that $o_1, o_2 \in O$, $S = \{s_1, \ldots, s_n\}$ and $x \in R$ where x denotes "execute" access. We now give some simple examples of conflict of interest policies.

- Subject s_1 is prohibited from executing o_1.

$$\alpha_1 = \{\{(o_1, s_1, x)\}\}$$

  α_1 is satisfied provided $x \notin [s_1, o_1]$. This is a trivial example of a negative authorisation policy.

- No subject can execute both o_1 and o_2.

$$\alpha_2 = \{\{(o_1, s, x), (o_2, s, x)\} : s \in S\}$$

α_2 is satisfied provided $x \notin ([s, o_1] \cap [s, o_2])$ for all $s \in S$. This is a trivial example of a separation of duty policy.

- There is no "super-user".

$$\alpha_3 = \bigcup_{i=1}^{n} \{O \times \{s_i\} \times R\}$$

- No subject is permitted to execute any file.

$$\alpha_4 = \{\{(o, s, x)\} : o \in O, s \in S\}$$

  α_4 is satisfied if for all $o \in O$ and for all $s \in S$, $x \notin [s, o]$.

- If we combine the features of α_1 and α_2 we see that the composite policy

$$\alpha' = \alpha_1 \cup \alpha_2 \setminus \{(o_1, s_1, x), (o_2, s_1, x)\}$$

  since $\{(o_1, s_1, x)\} \subseteq \{(o_1, s_1, x), (o_2, s_1, x)\}$ (see Proposition 3.1).

4.2 The Role-Based Access Control Model

We assume the existence of a set of roles, $R = \{r_1, \ldots, r_n\}$, a set of users, $U = \{u_1, \ldots, u_m\}$, and a user-role assignment relation, $UA \subseteq U \times R$, [23]. We will denote the set of roles assigned to a user, u, by ρ_u.

In the simplest case, we consider $X = R$ and in the static case we have a family of environments $E(u_i) = \{r : (u_i, r) \in UA\} = \rho_{u_i}$, $1 \leqslant i \leqslant m$. (The environment in the dynamic case is the "active" user-role assignments determined by the sessions which a user is running [23].)

We now give some typical examples of simple policies.

- No user can be assigned to the role r. Such a policy may be useful when there is a `MaxRole` which is too powerful for any user to be assigned to (see [19], for example);

or when a role has been "de-commissioned" and should no longer be used (see [26], for example).

$$\beta_1 = \{\{r\}\}$$

- No user can be assigned to both the roles r_1 and r_2. This is an example of the classical separation of duty constraint in role-based access control.

$$\beta_2 = \{\{r_1, r_2\}\}$$

We now briefly consider the case when $X = U \times R$. In this case $E = UA$. This expands the range of policies enormously. We have the following simple examples.

- User u_1 cannot be assigned to role r_1. (Strangely this type of constraint or policy is rarely mentioned in RBAC literature. The administrative model URA97 provides constraints which can prevent users being assigned to roles, but these constraints are usually articulated in terms of existing user-role assignments [22]. It is not immediately obvious how such constraints could be used to implement a policy which prohibits particular user-role assignments.)

$$\beta_3 = \{\{(u_1, r_1)\}\}$$

We note the following useful application of such a policy. We recall that the role-based access control model is policy neutral [23], and that it is of considerable value to demonstrate that such a model can be used to simulate mandatory and discretionary access control models [18, 25, 20]. It has been convincingly shown that role-based access control can indeed simulate mandatory access control [20] by considering the security lattice, L, as two distinct read and write role hierarchies L_R and L_W, respectively. L_R is *isomorphic* to L and L_W is the *dual* of L_R [11].

However, we believe the constraints introduced in [20] to enforce the information flow policy that is an integral part of the mandatory access control model are rather complicated. We suggest that to achieve this we can simply define a role exclusion policy of a similar form to β_3 for each user u, where $\{r_1, \ldots, r_n\}$ is an antichain in L. Figure 2 shows a security lattice for the security labels

$$\texttt{unclassified} < \texttt{classified} < \texttt{secret} < \texttt{top secret}$$

which we will abbreviate to `u`, `c`, `s`, and `t`, respectively; and two security categories, `a` and `b`. If a user, u, has security clearance `ca`, the conflict of interest policy

$$\{\{(u, \texttt{sa})\}, \{(u, \texttt{cb})\}\}$$

preserves the information flow policy defined by the lattice by preventing u being assigned to, and hence activating, any roles other than `u` and `ca`. (Of course, in a role-based access control implementation there would actually be a read and a write lattice, but the example policy can be extended in the obvious way to accommodate this.)

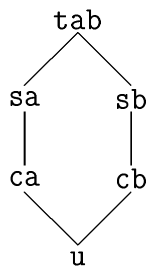

Figure 2: A security lattice

- Users u_1 and u_2 cannot occupy both or one of each of the two roles r_1 and r_2. This kind of policy was identified in [2] and aims to prevent collusion between two (or more) individuals to compromise system security.

$$\beta_4 = \{\{(u_1, r_1), (u_1, r_2)\}, \{(u_2, r_1), (u_2, r_2\rangle\},$$
$$\{(u_1, r_1), (u_2, r_2)\}, \{(u_1, r_2), (u_2, r_1\rangle\}\}$$

The first two constraints are simple separation of duty constraints for each of the users, while the other two constraints prevent collusion by the two users.

We now consider the two most significant existing approaches to separation of duty in role-based access control and compare them to our approach. It should be mentioned that most RBAC models include a role hierarchy [23, 18, 14, 24], which can be regarded as a partially ordered set, $\langle R, \leqslant \rangle$. Unlike the standard literature, we will use the notation of partial order theory to develop our material.

The NIST Model The most detailed discussion of separation of duty constraints and their realisation within a functioning access control system is found in [15] (which is a realisation and refinement of the NIST model outlined in [14]). The RBAC database includes two binary, irreflexive, symmetric relations *ssd* and *dsd* standing for static and dynamic separation of duty, respectively. A pair $(r_1, r_2) \in ssd$ is, in our terminology, a conflict of interest constraint. A conflict of interest policy corresponds to the set *ssd* and is violated if $\{r_1, r_2\} \subseteq \rho_u$ for some $u \in U$.

We now discuss the additional constraints identified in [15] which *ssd* (and *dsd*) must satisfy in a role-based context. The *ssd* relation must be irreflexive and symmetric. The irreflexivity condition is introduced to prevent a mutually exclusive pair (r, r) from being entered into the *ssd* relation. The assumption being that such a pair would only have the meaning that no user could be assigned to the role r. We would argue that, as in policy β_1, there is a useful place for such constraints when one includes a user component. (The symmetric condition is introduced in order to establish certain logical equivalences between constraints in the NIST model in the presence of a role hierarchy, and to thereby reduce the number of logical tests in the implementation of the database update operations.)

Furthermore, if $(r_1, r_2) \in ssd$ then we have the following additional constraints.

- $\{r_1, r_2\} \in \mathcal{A}(R)$

  As noted above this constraint is not articulated in this way in [15]. It is obvious that this is necessary when one considers that if, without loss of generality, $r_1 \leqslant r_2$ and $(r_1, r_2) \in ssd$ then no user can be assigned to r_2 or any role senior to it.

  Note that in Definition 3.1 we assumed nothing about the set X. If, in fact, the context supports some sort of inheritance, that is $\langle X, \leqslant \rangle$ is a partially ordered set, then we observe that in general a conflict of interest constraint should be defined to be an antichain in X rather than a subset of X.

  For example, consider the role hierarchy in Figure 3 and the policy $\alpha = \{\{r_1, r_3\}, \{r_2, r_3\}\}$. It is clear that if r_1 enters the environment, then so do r_2 and r_3, violating both constraints. Hence the policy α can be reduced to the policy $\alpha' = \{\{r_1\}\}$.

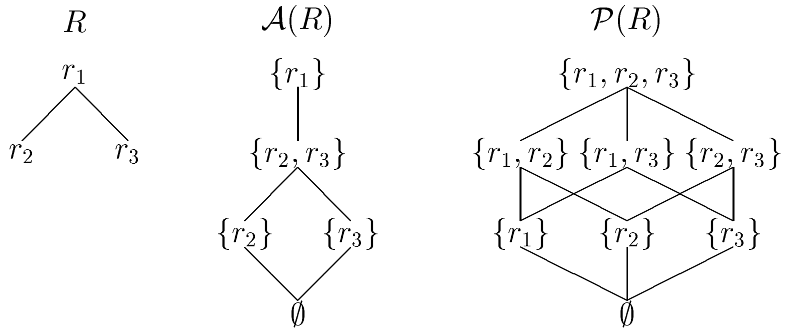

Figure 3: A simple role hierarchy, R, $\mathcal{A}(R)$ and $\mathcal{P}(R)$

  In general, therefore, a conflict of interest policy in a role-based access control model is a member of $\mathcal{A}(\mathcal{A}(R))$. In other words, the constraints of a conflict of interest policy are elements of $\mathcal{A}(R)$ rather than $\mathcal{A}(\mathcal{P}(X))$; see Figure 3, for example. (In the case of an unordered set X - that is, the order relation is the empty set - the set of antichains is simply $\mathcal{P}(X)$.)

- $\uparrow r_1 \cap \uparrow r_2 = \emptyset$

The justification for this condition is because if $r \in \uparrow r_1 \cap \uparrow r_2$ no user can be assigned to the role r. We would not wish to impose such a condition on conflict of interest policies in general, particularly if finer granularity is required where users are included in the policies, as in our examples above.

In short, we believe the NIST approach (and the broadly similar approach adopted in the Role Graph Model [18]) to separation of duty policies omits the vitally important user perspective.

The RCL 2000 Language A more flexible and wide-ranging discussion of separation of duty policies was presented in [1], and included policies in which users were a factor in policy specification. The paper introduces a role authorisation constraints specification language, RCL 2000, in which separation of duty policies are expressed. The language includes a conflicting role set, $\mathtt{CR} = \{R_1, \ldots, R_n\}$, where $R_i \subseteq R$, $1 \leqslant i \leqslant n$. In our terminology, `CR` is a set of constraints, and hence, a conflict of interest policy.

The RCL 2000 expression

$$|\mathtt{roles}^*(\mathtt{OE(U)} \cap \mathtt{OE(CR)})| \leqslant 1 \tag{5}$$

is interpreted in the following way: for the collection of sets of roles (or conflict of interest policy), `CR`, no user can be assigned more than one role in any of the sets contained in `CR`. In other words, in our terminology, (5) states the conditions for satisfaction of the conflict of interest policy `CR`. Therefore, we would argue that we could simply express the policy `CR` and (5) as a set of mutually exclusive pairs. Specifically, if we replace `CR` by $\alpha = \{P_1, \ldots, P_m\}$ where for each pair of roles, (r_1, r_2), in a constraint in `CR` there exists an i such that $1 \leqslant i \leqslant m$ and $P_i = (r_1, r_2)$, then the policy α is equivalent to the collection `CR` and the RCL 2000 statement (5) above. We pursue this line of thought in Section 6.

5 Structural Complexity Results

Definition 5.1 *The* length *of a conflict of interest policy is defined by the function* $l : \mathcal{A}_n \to \mathbb{N}$ *where*

$$l(\alpha) = \begin{cases} 0 & \alpha = \emptyset, \\ \displaystyle\sum_{A \in \alpha} |A| & \textit{otherwise.} \end{cases}$$

The length of a conflict of interest policy is a measure of the complexity of describing it (by a string, for example).

We now state and prove two results similar in spirit to Sperner's Theorem. Lemma 5.1 states the maximum length of a conflict of interest policy, while Lemma 5.2 states the largest element of $\mathcal{A}_n^r$ (see Definition 5.2).

Lemma 5.1 *For all* $\alpha \in \mathcal{A}_n$*,*

$$l(\alpha) \leqslant \lceil n/2 \rceil \binom{n}{\lceil n/2 \rceil},$$

with equality if, and only if,

$$\alpha = \begin{cases} \{A \subseteq X : |A| = \frac{n}{2}\} \quad \textit{or} \quad \{A \subseteq X : |A| = \frac{n+2}{2}\} & n \textit{ even}, \\ \{A \subseteq X : |A| = \frac{n+1}{2}\} & n \textit{ odd}. \end{cases} \tag{6}$$

Proof We first note that α as defined in (6)

- belongs to $\mathcal{A}_n$ by construction; and
- $l(\alpha) = \lceil n/2 \rceil \binom{n}{\lceil n/2 \rceil}$.

  This is obvious when n is odd. Note that for $0 \leqslant r < n$,

$$(n-r)\binom{n}{r} = (r+1)\binom{n}{r+1}, \tag{7}$$

and that when n is even $\lceil n/2 \rceil =$ n/2. Hence, if n is even, substituting $r = n/2$ into (7) we obtain

$$\frac{n}{2}\binom{n}{n/2} = (n/2+1)\binom{n}{(n/2)+1} = \left(\frac{n+2}{2}\right)\binom{n}{(n+2)/2}.$$

We follow the approach of the original proof of Sperner's Theorem [27]. Let $\beta \in \mathcal{A}_n$ be any policy with maximal length. We will prove that $\beta = \alpha$. Define

$$\lfloor \beta \rfloor = \{B \in \beta : |B| = l\} \quad \text{where} \quad l = \min_{B \in \beta} |B|,$$

$$\gamma = \{C \subseteq X : \text{there exists } B \in \lfloor \beta \rfloor \text{ such that } B \lessdot C\};$$

and

$$\lceil \beta \rceil = \{B \in \beta : |B| = u\} \quad \text{where} \quad u = \max_{B \in \beta} |B|,$$

$$\delta = \{D \subseteq X : \text{there exists } B \in \lceil \beta \rceil \text{ such that } D \lessdot B\}.$$

Define

$$\beta' = (\beta \setminus \lceil \beta \rceil) \cup \delta.$$

Then, for all $\beta \in \mathcal{A}_n$,

$$\beta' \in \mathcal{A}_n, \tag{8}$$

and, for all $u \geqslant \frac{n+2}{2}$,

$$l(\beta') \geqslant l(\beta) \quad \text{with equality if } u = \frac{n+2}{2}. \tag{9}$$

Analogous results can be proved for $\beta'' = (\beta \setminus \lfloor \beta \rfloor) \cup \gamma$ (These are left as an exercise for the interested reader.)

Proof of (8) (By contradiction) Therefore, suppose $\beta' \notin \mathcal{A}_n$. Then there exists $D \in \delta$ such that $B \subseteq D$ for some $B \in \beta \setminus \lceil\beta\rceil$. However, this implies that there exists $B' \in \lceil\beta\rceil$ such that $D \subseteq B'$ by construction of δ, and hence that $B \subset B'$ and $\beta \notin \mathcal{A}_n$.

Proof of (9) We count N, the number of pairs (B, D) such that $B \in \lceil\beta\rceil$, $D \in \delta$ and $D \lessdot B$, in two different ways. For a particular $B \in \lceil\beta\rceil$ there are exactly u such subsets D (obtained by omitting one of the u elements of B). For a particular $D \in \delta$ there are $(n-(u-1)) = (n-u+1)$ possible subsets B which cover D, since $|D| = u-1$. However, not all of these are necessarily in $\lceil\beta\rceil$. Therefore, we have

$$u|\lceil\beta\rceil| = N \leqslant (n-u+1)|\delta|. \tag{10}$$

Hence

$$\frac{|\delta|}{|\lceil\beta\rceil|} \geqslant \frac{u}{n-u+1} \geqslant \frac{u}{u-1} \quad \text{since } u \geqslant \frac{n+2}{2} \text{ implies } n-u+1 \leqslant u-1,$$

and therefore

$$(u-1)|\delta| \geqslant u|\lceil\beta\rceil| \tag{11}$$

Now, by definition,

$$l(\beta') = l(\beta) - u|\lceil\beta\rceil| + (u-1)|\delta|,$$

and hence we have, by (11),

$$l(\beta') \geqslant l(\beta) \quad \text{with equality when } u = \frac{n+2}{2}.$$

Since, by assumption, β has maximal length, (8) and (9) imply

$$u \leqslant \frac{n+2}{2} \text{ and, analogously, } l \geqslant \frac{n}{2}.$$

We now have three cases:

- n odd

  Then $u = l = \lceil n/2 \rceil$ and $\beta = \alpha$;

- n even, $l = u$

  Then either $u = l = \frac{n}{2}$ or $u = l = \frac{n+2}{2}$ and $\beta = \alpha$;

- n even, $l < u$

  Then we derive a contradiction as follows. Since $l(\beta)$ is assumed to be maximal and

  $$l(\beta) \leqslant l(\beta') \leqslant \lceil n/2 \rceil \binom{n}{\lceil n/2 \rceil} \tag{12}$$

  we must have equality in (12), and hence equality in (10). In other words, for each $C \in \gamma$ every superset B of C must be in $\lceil \beta \rceil$. Now choose some $B \in \beta \setminus \lceil \beta \rceil$ and $C \in \gamma$ such that $|B \cap C|$ is a maximum. Since $|B| = |C| = u - 1$ ($|B| = u - 1$ because $l = u - 1$) and $B \neq C$, there exists some $b \in B \setminus C$ and some $c \in C \setminus B$. Hence, because of the required equality in (10), $C \cup \{b\} \in \lceil \beta \rceil$, $C' = C \cup \{b\} \setminus \{c\} \in \gamma$ and $|B \cap C'| = |B \cap C| + 1$ contradicting the maximality of $B \cap C$.

■

Definition 5.2 *For $0 \leqslant r \leqslant n$, we define $\mathcal{A}_n^r \subset \mathcal{A}_n$ as follows:*

$$\mathcal{A}_n^r = \{\alpha \in \mathcal{A}_n : \max_{A \in \alpha}(|A|) = r\}$$

In other words, $\mathcal{A}_n^r$ is the set of all conflict of interest policies in which the largest constraint has cardinality r.

Example 5.1 *Let* $X = \{1,2,3\}$. *Then*

$$\begin{aligned}\mathcal{A}_3^2 = \big\{&\{\{1,2\}\},\{\{1,3\}\},\{\{2,3\}\},\\ &\{\{1\},\{2,3\}\},\{\{2\},\{1,3\}\},\{\{3\},\{1,2\}\},\\ &\{\{1,2\},\{1,3\}\},\{\{1,2\},\{2,3\}\},\{\{1,3\},\{2,3\}\},\\ &\{\{1,2\},\{1,3\},\{2,3\}\}\big\}.\end{aligned}$$

Lemma 5.2 *For all* $\alpha \in \mathcal{A}_n^r$,

$$|\alpha| \leqslant \begin{cases} \binom{n}{r} & \text{if } r \leqslant \lceil n/2 \rceil, \\ \binom{n}{\lceil n/2 \rceil} - \binom{r}{\lceil n/2 \rceil} + 1 & \text{if } \lceil n/2 \rceil \leqslant r \leqslant n, \end{cases}$$

with equality if, and only if,

$$\alpha = \begin{cases} \{A \subseteq X : |A| = r\} & \text{if } r \leqslant \lceil n/2 \rceil, \\ A' \cup \{A \subseteq X : |A| = \lceil n/2 \rceil, A \nsubseteq A'\} & \text{if } \lceil n/2 \rceil \leqslant r \leqslant n, \end{cases}$$

and $|A'| = r$.

Proof It is immediate by inspection that if $r \leqslant \lceil n/2 \rceil$ then the choice of α such that $|\alpha|$ is a maximum is simply the set of all subsets of size r. This can be most clearly seen by considering SCP_n and noting that a choice of α must take at most one element from any chain in SCP_n (because of the restriction on α with respect to set inclusion) and that precisely $\binom{n}{r}$ chains have an element of size r.

Consider the case when $r \geqslant \lceil n/2 \rceil$. We prove the result in the same way as for Lemma 5.1 (but omitting some of the details). Let $\beta \in \mathcal{A}_n^r$ such that $|\beta|$ is maximal, select $B' \in \beta$ such that $|B'| = r$ and define

$$\lfloor\beta\rfloor = \{B \in \beta \setminus \{B'\} : |B| = l\} \quad \text{where} \quad l = \min_{B \in \beta \setminus \{B'\}} |B|,$$
$$\gamma = \{C \subseteq X : \text{there exists } B \in \lfloor\beta\rfloor \text{ such that } B \lessdot C\};$$

and

$$\lceil\beta\rceil = \{B \in \beta \setminus \{B'\} : |B| = u\} \quad \text{where} \quad u = \max_{B \in \beta \setminus \{B'\}} |B|,$$
$$\delta = \{D \subseteq X : \text{there exists } B \in \lceil\beta\rceil \text{ such that } D \lessdot B\}.$$

Define

$$\beta' = (\beta \setminus \lceil\beta\rceil) \cup \delta.$$

As before, $\beta \in \mathcal{A}_n^r$. Furthermore, $|\beta'| = |\beta| - |\lceil\beta\rceil| + |\delta| \geqslant |\beta|$ for all $u \geqslant \frac{n+1}{2}$ with equality when $u = \frac{n+1}{2}$, since

$$\frac{|\delta|}{|\lceil\beta\rceil|} \geqslant \frac{u}{n-u+1} \geqslant \frac{\frac{n+1}{2}}{n - \frac{n+1}{2} + 1} = 1 \quad \text{for } \frac{n+1}{2} \leqslant u \leqslant n.$$

Hence we have $l \geqslant \frac{n-1}{2}$ and $u \leqslant \frac{n+1}{2}$. We arrive at the same three cases, the only difference being that $l = u = \frac{n-1}{2}$ is no longer an optimal choice because there are more subsets of B' of size $\binom{r}{\lfloor n/2\rfloor}$ than of size $\binom{r}{\lceil n/2\rceil}$. Therefore, the number of subsets (which are not subsets of B') of size $\binom{n}{\lceil n/2\rceil} - \binom{r}{\lceil n/2\rceil}$ exceeds the number of subsets of size $\binom{n}{\lceil n/2\rceil} - \binom{r}{\lfloor n/2\rfloor}$. ■

Example 5.2 *Consider the symmetric chain partition in Table 2. Suppose we are considering $\mathcal{A}_5^4$ and that $\{1, 2, 3, 4\}$ has already been chosen as an element of length 4 in α. The elements that cannot be included in a valid set of elements for $\alpha \in \mathcal{A}_5^4$ are shown in bold typeface. Note that there are more such subsets in the 2-element column than the 3-element column.*

$$
\begin{array}{|llllll|}
\hline
\emptyset & \subset\{1\} & \subset\{\mathbf{1,2}\} & \subset\{\mathbf{1,2,3}\} & \subset\{1,2,3,4\} & \subset\{1,2,3,4,5\} \\
 & \{2\} & \subset\{\mathbf{2,3}\} & \subset\{\mathbf{2,3,4}\} & \subset\{2,3,4,5\} & \\
 & \{3\} & \subset\{\mathbf{1,3}\} & \subset\{\mathbf{1,3,4}\} & \subset\{1,3,4,5\} & \\
 & \{4\} & \subset\{\mathbf{1,4}\} & \subset\{\mathbf{1,2,4}\} & \subset\{1,2,4,5\} & \\
 & \{5\} & \subset\{1,5\} & \subset\{1,2,5\} & \subset\{1,2,3,5\} & \\
 & & \{\mathbf{2,4}\} & \subset\{2,4,5\} & & \\
 & & \{2,5\} & \subset\{2,3,5\} & & \\
 & & \{\mathbf{3,4}\} & \subset\{3,4,5\} & & \\
 & & \{3,5\} & \subset\{1,3,5\} & & \\
 & & \{4,5\} & \subset\{1,4,5\} & & \\
\hline
\end{array}
$$

Table 2: SCP_5 and subsets of $\{1,2,3,4\}$

An example of $\alpha \in \mathcal{A}_5^4$ such that $|\alpha|$ is maximal is

$$\big\{\{1,2,3,4\},\{1,2,5\},\{2,4,5\},\{2,3,5\},\{3,4,5\},\{1,3,5\},\{1,4,5\}\big\}.$$

Corollary 5.1 *For all $n \geqslant 1$,*

$$\phi(n) \geqslant \sum_{r=0}^{n} 2^{\binom{n}{r}} - (n+1) \geqslant 2^{\nu},$$

where $\phi(n) = |\mathcal{A}_n|$ and $\nu = \binom{n}{\lfloor n/2 \rfloor}$.

Proof First note that

$$\phi(n) = \sum_{r=0}^{n} |\mathcal{A}_n^r| \geqslant |\mathcal{A}_n^{\lfloor n/2 \rfloor}|.$$

Furthermore, by Lemma 5.2, there exists $\alpha \in \mathcal{A}_n^r$ such that $|\alpha| \geqslant \binom{n}{r}$ for all $0 \leqslant r \leqslant n$. Every subset of such an α belongs to $\mathcal{A}_n^r$. The number of ways of choosing such elements (excluding the empty set) is $2^{\binom{n}{r}} - 1$. Hence

$$\phi(n) \geqslant \sum_{r=0}^{n} (2^{\binom{n}{r}} - 1) = \sum_{r=0}^{n} 2^{\binom{n}{r}} - (n+1).$$

$\blacksquare$

The following theorem is a re-statement of a result due to Hansel [16]. The proof of this result can be found in Appendix A. The reader is strongly urged to read this appendix before attempting the proof of Theorem 5.2.

Theorem 5.1 (Hansel [16]) *For all $n \geqslant 1$,*

$$2^{\nu} \leqslant \phi(n) \leqslant 3^{\nu}, \text{ where } \nu = \binom{n}{\lfloor n/2 \rfloor}.$$

It was also observed in [16] that for n even we have

$$\phi(n) \leqslant 2^{(\nu-\mu)}3^{\mu}, \text{ where } \mu = \binom{n}{\lfloor n/2 \rfloor - 1}.$$

Prior to stating and proving a theorem which significantly improves the upper bound for $\phi(n)$ we define a *bi-symmetric chain partition.*

Definition 5.3 *Let SCP_n be a symmetric chain partition of $\{1, \ldots, n\}$. For all $C \in SCP_n$ where $C = \{c_0, \ldots, c_k\}$ and $c_0 \lessdot c_1 \lessdot \cdots \lessdot c_k$ let $C \cup \{n+1\} = \{c_0 \cup \{n+1\}, \ldots, c_k \cup \{n+1\}\}$. Then a* bi-symmetric chain partition *of $\{1, \ldots, n+1\}$, BCP_{n+1}, is defined as follows.*

$$BCP_{n+1} = \{C \in SCP_n\} \cup \{C \cup \{n+1\} : C \in SCP_n\}.$$

A bi-symmetric chain partition of $\{1, 2, 3, 4, 5\}$ is shown in Table 3.

Theorem 5.2 *For all $n \geqslant 3$,*

$$\phi(n+1) < 6^{\binom{n}{\lfloor n/2 \rfloor}} < 3^{\binom{n+1}{\lfloor (n+1)/2 \rfloor}}.$$

Moreover,

$$\lim_{n \to \infty} \frac{6^{\binom{n}{\lfloor n/2 \rfloor}}}{3^{\binom{n+1}{\lfloor (n+1)/2 \rfloor}}} = 0.$$

$\emptyset \subset \{1\} \subset \{1,2\} \subset \{1,2,3\} \subset \{1,2,3,4\}$	$\{5\} \subset \{1,5\} \subset \{1,2,5\} \subset \{1,2,3,5\} \subset \{1,2,3,4,5\}$
$\{2\} \subset \{2,3\} \subset \{2,3,4\}$	$\{2,5\} \subset \{2,3,5\} \subset \{2,3,4,5\}$
$\{3\} \subset \{1,3\} \subset \{1,3,4\}$	$\{3,5\} \subset \{1,3,5\} \subset \{1,3,4,5\}$
$\{4\} \subset \{1,4\} \subset \{1,2,4\}$	$\{4,5\} \subset \{1,4,5\} \subset \{1,2,4,5\}$
$\{2,4\}$	$\{2,4,5\}$
$\{3,4\}$	$\{3,4,5\}$

Table 3: BCP_5

Proof We prove the right-hand inequality first. By considering Pascal's Triangle, we have for all $n > 1$,

$$\binom{n+1}{\lfloor (n+1)/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} + \binom{n}{\lceil n/2 \rceil - 1}; \tag{13}$$

and if n is odd then,

$$\binom{n}{\lceil n/2 \rceil} = \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil - 1}. \tag{14}$$

For all $n \geqslant 1$,

$$\binom{2n}{n-1} = \frac{(2n)!}{(n-1)!(n+1)!} = \frac{(2n!)n}{(n!)(n!)(n+1)} = \frac{n}{n+1}\binom{2n}{n}. \tag{15}$$

Hence, if n is odd we have

$$\begin{aligned}
3^{\binom{n+1}{\lfloor (n+1)/2 \rfloor}} &= 3^{\left(\binom{n}{\lceil n/2 \rceil}+\binom{n}{\lceil n/2 \rceil -1}\right)} \quad \text{by (13)} \\
&= 3^{\left(\binom{n}{\lfloor n/2 \rfloor}+\binom{n}{\lfloor n/2 \rfloor}\right)} \quad \text{by (14)} \\
&= 3^{\binom{n}{\lfloor n/2 \rfloor}} 3^{\binom{n}{\lfloor n/2 \rfloor}} \\
&> 3^{\binom{n}{\lfloor n/2 \rfloor}} 2^{\binom{n}{\lfloor n/2 \rfloor}} \\
&= 6^{\binom{n}{\lfloor n/2 \rfloor}}.
\end{aligned}$$

Now suppose n is even and let $n = 2m$, $m > 1$. Consider

$$\begin{aligned}
\frac{3^{\binom{n+1}{\lfloor (n+1)/2 \rfloor}}}{6^{\binom{n}{\lfloor n/2 \rfloor}}} &= \frac{3^{\binom{n}{\lceil n/2 \rceil}} 3^{\binom{n}{\lceil n/2 \rceil -1}}}{6^{\binom{n}{\lfloor n/2 \rfloor}}} \quad \text{by (13)} \\
&= \frac{3^{\binom{2m}{m}} 3^{\binom{2m}{m-1}}}{3^{\binom{2m}{m}} 2^{\binom{2m}{m}}} \\
&= \frac{3^{\binom{2m}{m-1}}}{2^{\binom{2m}{m}}} \\
&= \frac{\left(3^{\left(\frac{m}{m+1}\right)}\right)^{\binom{2m}{m}}}{2^{\binom{2m}{m}}} \quad \text{by (15)} \\
&= \left(\frac{3^{\left(\frac{m}{m+1}\right)}}{2}\right)^{\binom{2m}{m}} \\
&> 1 \quad \text{since } \binom{2m}{m} > 1 \text{ and } \frac{3^{\left(\frac{m}{m+1}\right)}}{2} > 1 \text{ for all } m > 1.
\end{aligned}$$

The result follows.

We now prove the left-hand inequality. Consider BCP_n as constructed from SCP_{n-1}. We will identify all chains in BCP_n which are a copy of a chain in SCP_{n-1} by C, and all chains in BCP_n which are of the form $c_0 \cup \{n\}, \ldots, c_k \cup \{n\}$ (where $c_0 \lessdot \cdots \lessdot c_k$ is a chain C) by D. If $c \in C$ we denote the corresponding element in D, $c \cup \{n\}$, by d. We will construct a filter by choosing elements from each pair of chains C and D.

The proof now proceeds in a similar way to that for Theorem 5.1. Consider first a pair of chains of length at most two.

$$c_0 \lessdot c_1 \qquad d_0 \lessdot d_1$$

By making our choices from C first, we can see there are at most $3! = 6$ choices of elements from these two chains. In the table below a tick indicates the choice to include the element in the filter, a cross indicates the choice to exclude the element from the filter, a hyphen indicates there is no choice involved because of the inclusion dependencies within the pairs of chains.

c_0	c_1	d_0	d_1
✓	-	-	-
✗	✓	✓	-
✗	✓	✗	-
✗	✗	✓	-
✗	✗	✗	✓
✗	✗	✗	✗

Now suppose we have chains C and D of length k and that we have dealt with all smaller chains.

$$c_0 \lessdot \cdots \lessdot c_k \qquad d_0 \lessdot \cdots \lessdot d_k$$

By Theorem A.2 we can find $\overline{c}_1, \ldots, \overline{c}_{k-1}$ and $\overline{d}_1, \ldots, \overline{d}_{k-1}$ belonging to shorter chains (than C and D) such that

$$c_{i-1} \lessdot \overline{c}_i \lessdot c_{i+1} \quad \text{and} \quad d_{i-1} \lessdot \overline{d}_i \lessdot d_{i+1} \quad \text{for } 0 < i < k.$$

Define l_c, u_c, l_d, u_d in an analogous way to l and u. We first note that, as in Theorem 5.1, when $l_c > u_c$ or $l_d > u_d$, we will not be able to make any choices from C or D, respectively.

We now have to prove that when we extend F by choosing elements from l_c, u_c, l_d, u_d we do not contradict any decisions that have already been made with respect to F. There are two cases.

- Include d_{l_d} from D in F. We need to prove that $d_{l_d} \not< \overline{c}_i$, $1 \leqslant i \leqslant l_c$. (In other words, none of the elements $\overline{c}_1, \ldots, \overline{c}_{l_c}$ already excluded from F can be included in F if d_{l_d} is chosen to be included in F. Clearly, if this holds then the inclusion of d_{u_d} in F is legitimate since we can only include d_{u_d} when $l_d < u_d$ and hence $d_{l_d} < d_{u_d} \not< \overline{c}_i$. Analogous remarks apply to the second case below.) As $n \in d$ for all $d \in D$ and $n \notin c$ for all $c \in C$, it is clearly the case that $d_{l_d} \not< \overline{c}_i$.

- Include c_{l_c} from C in F. We need to prove that $c_{l_c} \not< \overline{d}_i$, $1 \leqslant i \leqslant l_d$. The proof proceeds as follows. We prove that

$$l_d \leqslant l_c \quad \text{and} \tag{16}$$

$$c_{l_c} \not< d_{l_c}. \tag{17}$$

  By (16), $\overline{d}_{l_d} \leqslant \overline{d}_{l_c}$, and hence, by (17), $c_{l_c} \not< d_{l_d}$.

We conclude by proving (16) and (17).

Proof of (16) (By contradiction) Suppose that $l_c \leqslant l_d$. Then $c_{l_c} < c_{l_d}$ and $c_{l_d} \in F$ by definition of l_c. Therefore $d_{l_d} \in F$ since $c_{l_d} \lessdot d_{l_d}$, but, by definition, $d_{l_d} \notin F$.

Proof of (17) (By contradiction) Suppose that $c_{l_c} < \overline{d}_{l_c}$. By construction, $|c_{l_c}| = |\overline{d}_{l_c}| - 1$, and $n \notin c_{l_c}$. Therefore, $c_{l_c} < (\overline{d}_{l_c} \setminus \{n\})$ and $|c_{l_c}| = |(\overline{d}_{l_c} \setminus \{n\})|$. Hence $c_{l_c} = (\overline{d}_{l_c} \setminus \{n\}) = \overline{c}_{l_c}$, which is a contradiction. ■

As with Hansel's result, we can improve the upper bound for half the cases. Specifically, if we define

$$\nu(n) = \binom{n}{\lfloor n/2 \rfloor} \quad \text{and} \quad \mu(n) = \binom{n}{\lfloor n/2 \rfloor - 1}$$

we can restate Theorem 5.2 as

$$\phi(n) < 6^{\nu(n-1)} < 3^{\nu(n)},$$

and for n odd, we can improve the upper bound to

$$\phi(n) < 3^{\nu(n-1)-\mu(n-1)}6^{\mu(n-1)} = 2^{\mu(n-1)}3^{\nu(n-1)}.$$

To see this, consider BCP_5 in Table 3 and notice that for the pairs of chains of length 1 we can choose either none, D or C (which necessarily includes D) in the filter.

Postscript The problem of determining $\phi(n)$ was first posed by Dedekind [12] and is known to be very difficult. The value of $\phi(n)$ for $n \geqslant 9$ is not known. Table 4 shows values of $\phi(n)$ and the upper and lower bounds derived in this paper for $1 \leqslant n \leqslant 10$. The values of $\phi(n)$ are reproduced from [11].

n	$2^{\nu(n)}$	$\phi(n)$	$6^{\nu(n-1)}$	$3^{\nu(n)}$	2^{2^n}
1	2	2	1	3	4
2	4	5	6	9	16
3	8	19	36	27	256
4	64	167	216	729	65536
5	1024	7580	46656	59049	4294967296
6	1.048576×10^{6}	7.828354×10^{6}	6.046618×10^{7}	3.486784×10^{12}	1.844674×10^{18}
7	3.435974×10^{10}	2.414682×10^{12}	3.656158×10^{15}	5.003155×10^{16}	3.402824×10^{38}
8	1.180592×10^{21}	5.613044×10^{22}	1.719071×10^{27}	2.503156×10^{33}	1.157921×10^{77}
9	8.507059×10^{37}	?	2.955204×10^{54}	1.310021×10^{60}	1.340781×10^{154}
10	7.237001×10^{75}	?	1.114442×10^{98}	1.716154×10^{120}	1.797693×10^{308}

Table 4: A comparison of the upper and lower bounds of $\phi(n)$

6 Conclusion

We have presented a general framework for the articulation of conflict of interest policies which includes negative authorisation policies and separation of duty policies as special cases. We believe our approach offers a more complete characterisation of such policies, and significantly extends the class of policies for role-based access control.

We have not restricted our attention to policies comprised of mutually exclusive pairs, but noted in Section 4 that separation of duty policies are usually modelled in this way. The only exception we have found is [2], but the fragments of the language the authors offer as examples suggest that although the constraints may have cardinality greater than two, the policy is violated if any pair of elements from a constraint enters the environment.

With this in mind, we can rewrite an arbitrary conflict of interest policy $\alpha \in \mathcal{A}_n$ as a policy $\alpha' \in \mathcal{A}_n^2$. Specifically, let

$$\alpha = \{A_i : 1 \leqslant i \leqslant n\},$$

then

$$\alpha' = \{\{a_{i_j}, a_{i_k}\} : 1 \leqslant j < k \leqslant |A_i|, |A_i| > 1, 1 \leqslant i \leqslant n\} \cup \{A_i : |A_i| = 1, 1 \leqslant i \leqslant n\}.$$

In other words, for all $A_i \in \alpha$, if $|A_i| = 1$ then include A_i in α'; otherwise replace A_i by all pairs of elements in A_i. Clearly $\alpha' \preccurlyeq \alpha$ with equality when $|A_i| \leqslant 2$, for all $i \in I$, so α' is, in general, more restrictive than α. Therefore, an arbitrary conflict of interest policy, $\alpha \in \mathcal{A}_n$, can be expressed as a conflict of interest policy, $\alpha' \in \mathcal{A}_n^2$, which is at least as strong as α. It can easily be seen that

$$|\mathcal{A}_n^2| > 2^{\binom{n}{2}} = 2^{\frac{n(n-1)}{2}}$$

since there are $\binom{n}{2}$ distinct pairs, and any subset of the set of pairs is a valid policy; and that the longest policy in $\mathcal{A}_n^2$ is

$$2\binom{n}{2} = n(n-1).$$

Therefore, assuming that it takes constant time to determine whether $x \in E$ for any element $x \in X$, the complexity of checking whether adding x to E will violate a policy in $\mathcal{A}_n^2$ is $\mathcal{O}(n^2)$.

Hence, if the usual assumptions are made about the definition of conflict of interest policies, the complexity of such policies can be readily described. However, we feel that the effort involved in investigating the general case has been worthwhile. It has led to us developing a general theorem about finite partially ordered sets and their embedding into a complete lattice of subsets of that set [6, 7], which in turn we hope to use to develop a more sophisticated model of role-based access control.

Lemma 5.1 shows that at worst we will require

$$\lceil n/2 \rceil \binom{n}{\lceil n/2 \rceil}$$

tests to determine whether adding $x \in X$ to E will violate a policy $\alpha \in \mathcal{A}_n$. It is clear therefore, that implementing conflict of interest policies using elements of $\mathcal{A}_n^2$ will in general be far more efficient than using unrestricted elements of $\mathcal{A}_n$.

In future work we will consider the advantages of adopting our approach (to conflict of interest policies) in role-based access control in more detail. In particular we hope to show that our approach leads to the possibility of a simpler implementation of conflict of interest policies and to greater expressiveness and granularity in the specification of such policies.

We hope to find upper and lower bounds for $|\mathcal{A}_n^r|$. It seems clear that for $r \leqslant \lceil n/2 \rceil$,

$$2^{\binom{n}{r}} < |\mathcal{A}_n^r| < 3^{\binom{n}{r}},$$

but less clear for the remaining values of r. Nor is it immediately obvious whether the proofs of Theorem 5.1 and 5.2 can be amended in some significant way to dramatically improve on these bounds. Our intuition is that these bounds can be considerably improved for $r \leqslant \lfloor n/2 \rfloor$.

Finally, we intend to generalise the definition of symmetric chain partition to an arbitrary poset, P, and thereby produce an upper bound for $|\mathcal{A}(P)|$. This may well be of particular interest when considering conflict of interest policies in a role-based access control context, since conflict of interest policies are members of $\mathcal{A}(\mathcal{A}(R))$.

References

[1] G-J Ahn and R. Sandhu. Role-based authorization constraints specification. *ACM Transactions on Information and System Security*, 3(4), November 2000.

[2] G-J. Ahn and R.S. Sandhu. The RSL99 language for role-based separation of duty constraints. In *Proceedings of Fourth ACM Workshop on Role-Based Access Control*, pages 43–54, Fairfax, Virginia, October 1999.

[3] D.E. Bell and L. LaPadula. Secure computer systems: Unified exposition and MULTICS interpretation. Technical Report MTR-2997, Mitre Corporation, March 1976.

[4] R.A. Brualdi. *Introductory Combinatorics.* Prentice Hall, New Jersey, 1999.

[5] D.D. Clark and D.R. Wilson. A comparison of commercial and military computer security policies. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 184–194, April 1987.

[6] J. Crampton and G. Loizou. The completion of a poset in a lattice of antichains. Technical Report BBKCS-0001, Birkbeck College, University of London, September 2000.

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

[8] J. Crampton, G. Loizou, and G. O'Shea. Evaluating access control. Technical Report BBKCS-9905, Birkbeck College, University of London, 1999. Submitted to Computers & Security.

[9] J. Crampton, G. Loizou, and G. O'Shea. A logic of access control. *The Computer Journal*, 2000. To appear.

[10] N. Damianou, E.C. Lupu, N. Dulay, and M. Sloman. Ponder: A language for specifying security and management policies for distributed systems. Technical Report DOC 2000/1, Imperial College, University of London, January 2000.

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

[12] R. Dedekind. Über Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler. In *Festschrift der Techn. Hochsh. Braunschweig bei Gelegenheit der 69. Versammlung deutscher Naturforscher und Ärzte*, pages 1–40, 1897.

[13] K. Engel. *Sperner Theory*. Cambridge University Press, Cambridge, England, 1997.

[14] 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.

[15] S.I. Gavrila and J.F. Barkley. Formal specification for role based access control user/role and role/role relationship management. In *Proceedings of Third ACM Workshop on Role-Based Access Control*, pages 81–90, Fairfax, Virginia, October 1998.

[16] G. Hansel. Sur le nombre des fonctions Booléennes monotones de n variables. *Comptes Rendus Hebdomadaires des Séances Academie des Sciences (Paris Série A et B)*, 262:1088–1090, 1966.

[17] M.A. Harrison, W.L. Ruzzo, and J.D. Ullman. Protection in operating systems. *Communications of the ACM*, 19(8):461–471, August 1976.

[18] 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.

[19] M. Nyanchama and S. Osborn. The role graph model and conflict of interest. *ACM Transactions on Information and System Security*, 2(1):3–33, 1999.

[20] S. Osborn, R. Sandhu, and Q. Munawer. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security*, 3(2), May 2000.

[21] G. O'Shea. *Access Control in Operating Systems.* PhD thesis, Birkbeck College, University of London, July 1997.

[22] R.S. Sandhu, V. Bhamidipati, and Q. Munawer. The ARBAC97 model for role-based administration of roles. *ACM Transactions on Information and System Security*, 1(2):105–135, February 1999.

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

[24] R.S. Sandhu, D.F. Ferraiolo, and D.R. Kuhn. The NIST model for role-based access control: Towards a unified standard. In *Proceedings of the 5th ACM Workshop on Role-Based Access Control*, Phoenix, Arizona, USA, 2000. http://www.acm.org/sigsac/nist.pdf.

[25] R.S. Sandhu and Q. Munawer. How to do discretionary access control using roles. In *Proceedings of Third ACM Workshop on Role-Based Access Control*, pages 47–54, Fairfax, Virginia, October 1998.

[26] R.S. Sandhu and Q. Munawer. The RRA97 model for role-based administration of role hierarchies. In *Proceedings of 14th Annual Computer Security Applications Conference*, Phoenix, Arizona, USA, 1998.

[27] E. Sperner. Ein Satz über Untermengen einer endlichen Menger. *Mathemathische Zeitschrift*, 27:544–548, 1928.

Appendix A: [Hansel's Result]

We first prove three preparatory results. Theorem A.1 asserts that the power set of every set has a symmetric chain partition. The proof of this result is constructive and we make use of the notation introduced in this proof in the remainder of the appendix.

We note that Lemma A.1 and Theorems A.2 and 5.1 form the original result due to Hansel and proved in [16]. We have adopted the style of proof in [13] and split the result into three parts for ease of presentation. In conclusion we present two examples to illustrate the construction given in the proof of Theorem 5.1.

Theorem A.1 *There exists a symmetric chain partition of* $\mathcal{P}(X)$.

Proof (By induction on $|X|$) We present this constructive proof [4, 13] in detail, as it gives rise to some notation which will be used later in the paper. Clearly from Example 2.1 there is a symmetric chain partition of $\{1,2,3\}$. Suppose now that $|X| = N$ and that there is a symmetric chain partition SCP_{N-1}. For each chain $C = c_0 \lessdot \ldots \lessdot c_k$ of SCP_{N-1} we construct the chains

$$C' = c_0 \lessdot \ldots \lessdot c_k \lessdot (c_k \cup \{N+1\}) \quad \text{and} \tag{18}$$

$$C'' = (c_1 \cup \{N+1\}) \lessdot \ldots \lessdot (c_{k-1} \cup \{N+1\}). \tag{19}$$

(If $|C| = 1$ we only construct C'.) Clearly, by construction, the resulting chains form a symmetric chain partition of SCP_{N+1}. ■

Example A.1 *The construction of a symmetric chain partition of* $\{1,2,3,4\}$ *from that of*

$\{1,2,3\}$ *given in Example 2.1 is shown below.*

$$\emptyset \subset \{1\} \subset \{1,2\} \subset \{1,2,3\} \to \begin{cases} \emptyset \subset \{1\} \subset \{1,2\} \subset \{1,2,3\} \subset \{1,2,3,4\} \\ \{4\} \subset \{1,4\} \subset \{1,2,4\} \end{cases}$$

$$\{2\} \subset \{2,3\} \to \begin{cases} \{2\} \subset \{2,3\} \subset \{2,3,4\} \\ \{2,4\} \end{cases}$$

$$\{3\} \subset \{1,3\} \to \begin{cases} \{3\} \subset \{1,3\} \subset \{1,3,4\} \\ \{3,4\} \end{cases}$$

Lemma A.1 *Let $c_0 \lessdot c_1 \lessdot \cdots \lessdot c_r$ be a chain in SCP_n. If $|c_0| = i$ then $r = n - 2i + 1$.*

Proof If $|c_0| = i$ then $|c_r| = n - i$ since $|c_0| + |c_r| = n$. Since $c_0 \lessdot \cdots \lessdot c_r$, $|c_0|, \ldots, |c_r|$ are consecutive integers. There are $|c_r| - |c_0| + 1 = (n-i) - i + 1 = n - 2i + 1$ such integers.

■

Theorem A.2 *For every chain, C, in SCP_n, and for every set of three consecutive members $c_{a-1} \lessdot c_a \lessdot c_{a+1}$ of C, there is some $\overline{c}_a$ such that $c_{a-1} \lessdot \overline{c}_a \lessdot c_{a+1}$ and $\overline{c}_a$ is contained in a chain D with $|D| = |C| - 2$.*

Proof (Induction on n) Clearly the theorem is true for the case $n = 2$ by inspection of the symmetric chain partition of $\{1,2\}$ below.

$$\emptyset \subset \{1\} \subset \{1,2\}$$
$$\{2\}$$

Suppose the result is true for all $n \leqslant N$, and let SCP_{N+1} be constructed inductively from SCP_N (see the proof of Theorem A.1).

We first consider the case where c_{a-1}, c_a, c_{a+1} belong to a chain of the form C' - see (18). If $N+1 \notin c_{a+1}$, then $c_{a-1}, c_a, c_{a+1} \in C$ where $C \in SCP_N$, and by the inductive hypothesis there exists a chain $D \in SCP_N$ such that $\overline{c}_a \in D$, $|D| = |C| - 2$ and $c_{a-1} \lessdot c_a \lessdot c_{a+1}$. Furthermore, $\overline{c}_a \in D'$, $D' \in SCP_{N+1}$ and $|D'| = |C'| - 2$ since $|D| = |C| - 2$. If $N+1 \in c_{a+1}$ then $c_a = c_k$ (where c_k is the maximal element in C, the chain from C' is constructed) and we can take $\overline{c}_a$ to be $c_{a-1} \cup \{N+1\}$ which belongs to the chain C'' - see (19), and $|C''| = |C'| - 2$ by construction.

We now consider the case where c_{a-1}, c_a, c_{a+1} belong to a chain of the form C''. Then there exists $C \in SCP_N$ such that $C = d_0 \lessdot \cdots \lessdot d_k$ and $c_i = d_i \cup \{N+1\}$ for $0 \leqslant i \leqslant k-1$. By the inductive hypothesis, there exists a chain $D \in SCP_N$ containing an element $\overline{d}_a$ with $d_{a-1} \lessdot \overline{d}_a \lessdot d_{a+1}$ and $|D| = |C| - 2$. Note that d_{a+1} cannot be the maximal element in C since $C'' = d_0 \cup \{N+1\} \lessdot \cdots \lessdot d_{k-1} \cup \{N+1\}$. Therefore $\overline{d}_a$ is not the maximal element of D. (If $\overline{d}_a$ is maximal then $|D| \leqslant |C| - 4$ since $\overline{d}_a \lessdot d_{a+1} \lessdot \cdots \lessdot d_k$ and, by Lemma A.1, the length of a chain reduces by two when the size of a maximal element is reduced by one.) Thus $\overline{d}_a \cup \{N+1\}$ belongs to D'' and is the required element since $|D''| = |D| - 1 = |C| - 3 = |C''| - 2$. ■

Proof of Theorem 5.1 We first recall we wish to prove that for all $n \geqslant 2$

$$2^\nu \leqslant \phi(n) \leqslant 3^\nu \text{ where } \nu = \binom{n}{\lfloor n/2 \rfloor}.$$

The left-hand side of the inequality is proved in Corollary 5.1. To prove the right-hand side of the inequality we assume we have a symmetric chain partition of $\mathcal{P}(X)$, SCP_n, which has been constructed inductively, and in which we have arranged the chains in order of increasing length. We proceed to construct all the filters of $\mathcal{P}(X)$ (noting that the set of filters has the same magnitude as the set of antichains), by deciding whether the elements of each chain in SCP_n belong to a filter, F. For chains of length at most two, we have at most three choices of elements to include in F, namely neither element, the maximal element or the minimal element (and hence the maximal element as well).

Suppose now that we now have to make a choice of elements from the chain $c_0 \lessdot c_1 \lessdot \cdots \lessdot c_k$ and that we have already chosen the elements from the preceding chains (ordered by length), thus fixing some part of a filter F. By Theorem A.2 there exist $\overline{c}_1, \ldots, \overline{c}_{k-1}$

such that $c_{i-1} \lessdot \overline{c}_i \lessdot c_{i+1}$ for $1 \leqslant i \leqslant k-1$ and each $\overline{c}_i$ belongs to a shorter chain. In other words we already know whether $\overline{c}_i \in F$ for $1 \leqslant i \leqslant k-1$. Define l to be the largest index such that $\overline{c}_l \notin F$ and u to be the smallest index such that $\overline{c}_u \in F$. If $\overline{c}_i \in F$ for $1 \leqslant i \leqslant k-1$ define $l = 0$ and if $\overline{c}_i \notin F$ for $1 \leqslant i \leqslant k-1$ define $u = k$. Note that either $u - l = 1$ or $u - l \leqslant -1$.

When $u - l = 1$ we have

$$\underbrace{\overline{c}_0 \lessdot \cdots \lessdot \overline{c}_l}_{\notin F} \lessdot \underbrace{\overline{c}_u \lessdot \cdots \lessdot \overline{c}_k}_{\in F};$$

and when $u - l \leqslant -1$ we have

$$\underbrace{\overline{c}_0 \lessdot \cdots \lessdot \overline{c}_{u-1}}_{\notin F} \lessdot \underset{\in F}{\overline{c}_u} \lessdot \underbrace{\overline{c}_{u+1} \lessdot \cdots \lessdot \overline{c}_{l-1}}_{?} \lessdot \underset{\notin F}{\overline{c}_l} \lessdot \underbrace{\overline{c}_{l+1} \lessdot \cdots \lessdot \overline{c}_k}_{\in F}.$$

Now $c_1, \ldots, c_{l-1} \notin F$ since $c_1 \lessdot \cdots \lessdot c_{l-1} \lessdot \overline{c}_l$; and $c_{u+1}, \ldots, c_k \in F$ since $\overline{c}_u \lessdot c_{u+1} \lessdot \cdots \lessdot c_k$. Hence F can only be extended by the inclusion of c_l and c_u.

If $u - l \leqslant -1$ we cannot extend F without either duplication (since $c_{u+1} \leqslant c_l \in F$) or violation of the conditions outlined in the preceding paragraph (since $c_u \leqslant c_{l-1} \notin F$).

If $u - l = 1$ then we have

$$\underbrace{c_0 \lessdot \cdots \lessdot c_{l-1}}_{\notin F} \lessdot c_l \lessdot c_u \lessdot \underbrace{c_{u+1} \lessdot \cdots \lessdot c_k}_{\in F}$$

and hence we can make at most three choices to extend F. Namely, we can choose neither c_l nor c_u, choose c_u, or choose c_l (which is equivalent to choosing both c_l and c_u).

Example A.2 below gives explicit examples of the construction of filters and how the value of $u - l$ affects the choice of elements from a chain.

Hence for each of the ν chains we have at most three choices. The result follows. $\blacksquare$

Example A.2 *Tables 5 and 6 illustrate the construction used in the proof of Theorem 5.1. Column C contains the chains in SCP_4. Bold entries in this column indicate that an element has been selected from the chain for inclusion in the filter F. Column $\overline{C}$ contains the elements $\overline{c}_1, \ldots, \overline{c}_{k-1}$. Bold entries in this column indicate that an element has already been included in F by the construction to date. The next two columns indicate the elements c_l and c_k, respectively, and the final column denotes the reduction of the filter F to canonical form (in order to conserve space, and to emphasise that counting filters is equivalent to counting CIPs).*

C	$\overline{C}$	c_l	c_u	α
$\{2,4\}$	–	–	–	$\emptyset$
$\{\mathbf{3},\mathbf{4}\}$	–	–	–	$\{3,4\}$
$\{2\}\subset\{2,3\}\subset\{2,3,4\}$	$\{2,4\}$	$\{2,3\}$	$\{2,3,4\}$	$\{3,4\}$
$\{\mathbf{3}\}\subset\{\mathbf{1},\mathbf{3}\}\subset\{1,3,4\}$	$\{\mathbf{3},\mathbf{4}\}$	$\{3\}$	$\{1,3\}$	$\{3\}$
$\{4\}\subset\{1,4\}\subset\{1,2,4\}$	$\{2,4\}$	$\{2,4\}$	$\{1,2,4\}$	$\{3\}$
$\emptyset\subset\{1\}\subset\{1,2\}\subset\{1,2,3\}\subset\{1,2,3,4\}$	$\{2\},\{\mathbf{1},\mathbf{3}\},\{1,2,4\}$	$\{1,2,3\}$	$\{1,2\}$	$\{3\}$

Table 5: A filter construction in which $u-l \leqslant -1$ for a chain in SCP_4

In the final row of Table 5 we have $u-l=-1$. Notice that $\{1,2,3\}\in F$ since $\{3\}\in F$, and that $\{1,2\}$ cannot be added to F since it is known that $\{1,2,4\}\notin F$. In other words, as noted in the proof, if $u-l\leqslant -1$ for some chain then we cannot make any choices from that chain to extend the filter.

1.5

C	$\overline{C}$	c_l	c_u	α
$\{2,4\}$	$-$	$-$	$-$	$\emptyset$
$\{\mathbf{3},\mathbf{4}\}$	$-$	$-$	$-$	$\{3,4\}$
$\{2\} \subset \{2,3\} \subset \{2,3,4\}$	$\{2,4\}$	$\{2,3\}$	$\{2,3,4\}$	$\{3,4\}$
$\{\mathbf{3}\} \subset \{\mathbf{1},\mathbf{3}\} \subset \{1,3,4\}$	$\{\mathbf{3},\mathbf{4}\}$	$\{3\}$	$\{1,3\}$	$\{3\}$
$\{4\} \subset \{1,4\} \subset \{\mathbf{1},\mathbf{2},\mathbf{4}\}$	$\{2,4\}$	$\{1,4\}$	$\{1,2,4\}$	$\{3\}, \{1,2,4\}$
$\emptyset \subset \{1\} \subset \{\mathbf{1},\mathbf{2}\} \subset \{1,2,3\} \subset \{1,2,3,4\}$	$\{2\}, \{\mathbf{1},\mathbf{3}\}, \{\mathbf{1},\mathbf{2},\mathbf{4}\}$	$\{1\}$	$\{1,2\}$	$\{3\}, \{1,2\}$

Table 6: A filter construction in which $u - l = 1$ for all chains in SCP_4