Partially-ordered Sets

Material taken from Appendix A in NNH.

Partial Ordering

- Relation $\sqsubseteq$ on L.
- $\sqsubseteq$ is reflexive, *anti*-symmetric, transitive. (Antisymmetric means: $\forall \ell_1, \ell_2 \in \mathrm{L} : \ell_1 \sqsubseteq \ell_2 \wedge \ell_2 \sqsubseteq \ell_1 \Rightarrow \ell_1 = \ell_2$.)

L is a *partially ordered set (poset)* if L is equipped with a partial ordering $\sqsubseteq$.

Upper and lower bounds

$\ell \in \mathrm{L}$ is an *upper bound* (resp. *lower bound*) for $\mathrm{Y} \subseteq \mathrm{L}$ if:

- For all $\ell' \in \mathrm{Y} : \ell' \sqsubseteq \ell$.
- Resp.: For all $\ell' \in \mathrm{Y} : \ell \sqsubseteq \ell'$.

A *least upper bound (lub)* ℓ of Y is:

- An upper bound of Y.
- Whenever ℓ_0 is another upper bound of Y, we have $\ell \sqsubseteq \ell_0$.

A *greatest lower bound (glb)* ℓ of Y is:

- A lower bound of Y.
- Whenever ℓ_0 is another lower bound of Y, we have $\ell_0 \sqsubseteq \ell$.

Note: $\mathrm{Y} \subseteq \mathrm{L}$ need not have lub's and glb's. When they exist they are unique and written $\bigsqcup \mathrm{Y}$ and $\sqcap \mathrm{Y}$.

Complete lattice

A *complete lattice* L is a poset $(\mathrm{L}, \sqsubseteq)$ such that all subsets of L have least upper bounds and greatest lower bounds.

- $\bot = \bigsqcup \emptyset = \sqcap \mathrm{L}$ is the *least element*
- $\top = \sqcap \emptyset = \bigsqcup \mathrm{L}$ is the *greatest element*.

Note that $\sqcap \mathrm{Y} = \bigsqcup \{\ell \in \mathrm{L} \mid \forall \ell' \in \mathrm{Y} : \ell \sqsubseteq \ell'\}$. Hence $\sqcap \emptyset = \bigsqcup \{\ell \in \mathrm{L}\} = \top$.

Example

For some set S, $L = (\wp(S), \subseteq)$ is a complete lattice.

- $\sqsubseteq$ is $\subseteq$
- $\bigsqcup Y = \bigcup Y$
- $\sqcap Y = \bigcap Y$
- $\bot = \emptyset$
- $\top = S$.

Lemma

For a poset $\mathbb{L} = (L, \sqsubseteq)$, t.a.e.:

(i) $\mathbb{L}$ is a complete lattice.

(ii) every subset of L has a lub.

(iii) every subset of L has a glb.

Proof: (i) implies (ii) and (iii). Then we show (ii) implies (i) and (iii) implies (i).

Moore Family

A *Moore family* is a subset Y of a complete lattice $L = (L, \sqsubseteq)$ that is closed under glb's: $\forall Y' \subseteq Y : \sqcap Y' \in Y$.

- A Moore family, Y, always contains a least element $\sqcap Y$.
- A Moore family, Y, always contains a greatest element $\sqcap\emptyset = \top$, where $\top$ is the greatest element in L.

Example: For the powerset lattice formed from the set $\{1,2,3\}$, consider the subsets $\{\{2\},\{1,2\},\{2,3\},\{1,2,3\}\}$ and $\{\emptyset,\{1,2,3\}\}$. These are both Moore families. Neither of $\{\{1\},\{2\}$ and $\{\emptyset,\{1\},\{2\},\{1,2\}\}$ are.

For example, $\{\emptyset,\{1\},\{2\},\{1,2\}\}$ does not contain the set $\{1,2,3\}$.

Security type system

Idea: Attacker should not be able to view changes in sensitive data. So classifying data as ℓ (for Low) and h (for High), want to disallow "bad flows":

- $\ell :=$ h
- if h then $\ell :=$ 0 else $\ell := 1$

Attacker is considered Low.

Semantically, what policy is guaranteed to hold?

The JDK getSigners bug

```
public class Class {
    private Identity [] signers;
    public  Identity[] getSigners() { return signers;}
}
```

The call to Class.getSigners() can be used to create an alias between the *private* array signers and a malicious client. Then the client can install itself as a valid signer by updating the alias.