Delegation

March 2021

Definition 1: Lattice Congruence For each lattice L, let θ be an equivalence relation on L. θ is a *Congruence* iff for all $a, b, c \in L$:

$$a \equiv b \ (mod\ \theta) \Rightarrow a \vee c \equiv b \vee c \ (mod\ \theta) \ and \ a \wedge c \equiv b \wedge c \ (mod\ \theta)$$

Note 1: For any lattice L, The set of congruences on L form a subset lattice of L^2. We denote it as $\mathsf{Con}L$.

Definition 2: Quotient Lattice Let L be a lattice and θ be a congruence of L. Define $L/\theta = \{[a]_\theta \mid a \in L\}$.

Note 2.1: Join and meet operations are preserved in the quotient lattice.
Note 2.2: Each equivalent class of L/θ is a sublattice of L.

Definition 3: Principal congruence Let L be a lattice, θ be a congruence of L and $a, b \in L$. The *principle congruence* generated by a and b is defined as:

$$\theta(a, b) = \bigwedge\{\theta \in \mathsf{Con}L \mid (a, b) \in \theta\}$$

An extension of the definition above:

$$\theta(\{a_1, b_1\}, \{a_2, b_2\}, \cdots \{a_n, b_n\}) = \bigwedge\{\theta \in \mathsf{Con}L \mid (a_1, b_1) \in \theta, \cdots (a_n, b_n) \in \theta\}$$

Note 3: $\theta(a, b)$ is the smallest congruence in $\mathsf{Con}L$ that contains (a, b).

Lattice representation of delegation Let $\{A_1 \sqsubseteq B_1\}, \{A_2 \sqsubseteq B_2\}, \cdots, \{A_n \sqsubseteq B_n\}$ be delegations in an authority lattice L. It follows from definition that the authority lattice of the program is effectively:

$$L/\theta(\{A_1, A_1 \wedge B_1\}, \cdots \{A_n, A_n \wedge B_n\})$$

Theorem 4: Equivalence class membership criteria Let L be distributive lattice and assume that $c \leq d$ in L. Then:

$$[a]_{\theta(c,d)} = [b]_{\theta(c,d)} \iff a \wedge c = b \wedge c \; and \; a \vee d = b \vee d$$

Note 4: This theorem provides a practical way for us to check whether two labels are in $\theta(A_i, A_i \wedge B_i)$.

Theorem 5: Join of principal congruences

$$\theta(\{a_1, b_1\}, \{a_2, b_2\}, \cdots \{a_n, b_n\}) = \theta(a_1, b_1) \vee \cdots \vee \theta(a_n, b_n)$$

Note 5: Intuitively, this theorem means that the smallest congruence that contains n relation elements is the join (union) of their principle congruences.

Corollary 6: Extended equivalence class membership criteria Let L be distributive lattice and assume that for all i, $c_i \leq d_i$ in L. Let $c = \bigwedge_1^n c_i$ and $d = \bigvee_1^n d_i$ We can prove from the two theorems above that:

$$[a]_{\theta(\{c_1,d_1\},\cdots\{c_n,d_n\})} = [b]_{\theta(\{c_1,d_1\},\cdots\{c_n,d_n\})} \iff a \wedge c = b \wedge c \; and \; a \vee d = b \vee d$$

Algorithm 7: Modifying existing inference algorithm Let $\{A_1 \sqsubseteq B_1\}, \{A_2 \sqsubseteq B_2\}, \cdots, \{A_n \sqsubseteq B_n\}$ be delegations in an authority lattice L. Let $C = \bigwedge(A_i \wedge B_i)$ $D = \bigvee A_i$. We override equality operator between labels to:

$$\mathsf{Equal}(X, Y)\{ \text{ return } X \wedge C = Y \wedge X \; and \; X \vee D = Y \vee D \; \}$$

Note 7: The correctness of the algorithm follows from the correctness of corollary 6.

polymorphisms