# ECS 235B Module 17 Lattices

### Overview

- Lattices used to analyze several models
  - Bell-LaPadula confidentiality model
  - Biba integrity model
- A lattice consists of a set and a relation
- Relation must partially order set
  - Relation orders some, but not all, elements of set

### Sets and Relations

- S set, R: S × S relation
  - If  $a, b \in S$ , and  $(a, b) \in R$ , write aRb
- Example
  - *I* = { 1, 2, 3 }; *R* is ≤
  - $R = \{ (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3) \}$
  - So we write  $1 \le 2$  and  $3 \le 3$  but not  $3 \le 2$

### **Relation Properties**

- Reflexive
  - For all  $a \in S$ , aRa
  - On I,  $\leq$  is reflexive as  $1 \leq 1$ ,  $2 \leq 2$ ,  $3 \leq 3$
- Antisymmetric
  - For all  $a, b \in S$ ,  $aRb \land bRa \Rightarrow a = b$
  - On *I*,  $\leq$  is antisymmetric as  $1 \leq x$  and  $x \leq 1$  means x = 1
- Transitive
  - For all  $a, b, c \in S$ ,  $aRb \land bRc \Rightarrow aRc$
  - On *I*,  $\leq$  is transitive as  $1 \leq 2$  and  $2 \leq 3$  means  $1 \leq 3$

### Example

- ${\mathbb C}$  set of complex numbers
- $a \in \mathbb{C} \Rightarrow a = a_{R} + a_{I}i$ , where  $a_{R}$ ,  $a_{I}$  integers
- $a \leq_{\mathbf{C}} b$  if, and only if,  $a_{\mathbf{R}} \leq b_{\mathbf{R}}$  and  $a_{\mathbf{I}} \leq b_{\mathbf{I}}$
- $a \leq_{\mathbf{C}} b$  is reflexive, antisymmetric, transitive
  - As  $\leq$  is over integers, and  $a_{\mathbf{R}}$ ,  $a_{\mathbf{I}}$  are integers

## Partial Ordering

- Relation R orders some members of set S
  - If all ordered, it's a total ordering
- Example
  - ≤ on integers is total ordering
  - $\leq_{\mathbb{C}}$  is partial ordering on  $\mathbb{C}$ 
    - Neither  $3+5i \leq_{\mathbb{C}} 4+2i$  nor  $4+2i \leq_{\mathbb{C}} 3+5i$  holds

### Upper Bounds

- For  $a, b \in S$ , if u in S with aRu, bRu exists, then u is an upper bound
  - A *least upper bound* if there is no *t* ∈ *S* such that *aRt*, *bRt*, and *tRu*
- Example
  - For 1 + 5i,  $2 + 4i \in \mathbb{C}$ 
    - Some upper bounds are 2 + 5*i*, 3 + 8*i*, and 9 + 100*i*
    - Least upper bound is 2 + 5*i*

### Lower Bounds

- For *a*, *b* ∈ *S*, if *I* in *S* with *IRa*, *IRb* exists, then *I* is a *lower bound* 
  - A greatest lower bound if there is no  $t \in S$  such that tRa, tRb, and lRt
- Example
  - For 1 + 5i,  $2 + 4i \in \mathbb{C}$ 
    - Some lower bounds are 0, -1 + 2i, 1 + 1i, and 1+4i
    - Greatest lower bound is 1 + 4*i*

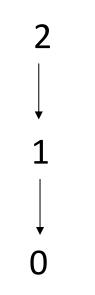
#### Lattices

- Set S, relation R
  - *R* is reflexive, antisymmetric, transitive on elements of *S*
  - For every *s*, *t*  $\in$  *S*, there exists a greatest lower bound under *R*
  - For every *s*, *t* ∈ *S*, there exists a least upper bound under *R*

### Example

- $S = \{0, 1, 2\}; R = \le$  is a lattice
  - *R* is clearly reflexive, antisymmetric, transitive on elements of *S*
  - Least upper bound of any two elements of *S* is the greater of the elements
  - Greatest lower bound of any two elements of *S* is the lesser of the elements

### Picture

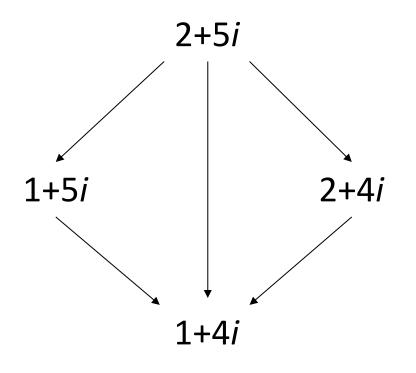


#### Arrows represent ≤; this forms a total ordering

## Example

- $\mathbb{C}$ ,  $\leq_{\mathbb{C}}$  form a lattice
  - $\leq_{\mathbb{C}}$  is reflexive, antisymmetric, and transitive
    - Shown earlier
  - Least upper bound for *a* and *b*:
    - $c_{R} = \max(a_{R}, b_{R}), c_{I} = \max(a_{I}, b_{I}); \text{ then } c = c_{R} + c_{I}i$
  - Greatest lower bound for *a* and *b*:
    - $c_{R} = \min(a_{R}, b_{R}), c_{I} = \min(a_{I}, b_{I}); \text{ then } c = c_{R} + c_{I}i$

### Picture



#### Arrows represent $\leq_{\mathbb{C}}$