Information Flow

Def: Information flows from an object x to an object y if the application of a sequence of commands c cause the information initially in x to affect the information in y.

Information Flow

- 1 VM 2 users, A and B
  - A is secret clearance
  - B is top secret clearance
- Can B talk to A?

Information Flow

- 1 VM 2 users, A and B
  - A is secret clearance
  - B is top secret clearance
- Can A talk to B?
  - Does this violate the *-property?
    - *-property no reads up no rights down

Information Flow

- Noninterference
  - A computer is modeled as a machine with inputs and outputs. Inputs and outputs are classified as either low or high. A computer has the non-interference property iff any sequence of low inputs will produce the same low outputs, regardless of what the high level inputs are.

Information Flow

- Nondeducibility
  - If an observer cleared only for *Low* can take a sequence of *Low* inputs and outputs, and from them deduce information about *High* inputs or outputs then information has leaked.

Measure Information Flow

- How do we measure information flow?

Entropy (Uncertainty)

- Think of the the entropy of something as the amount of uncertainty there is.

Entropy

Which has more entropy?

a) abababababababab

b) qazifutbhfe40pl

Entropy

$$-\sum p_x \times \log_2 p_x$$

Conditional Entropy

$$\mathrm{H}(\mathrm{X} \mid \mathrm{Y}) = -\sum_{j=1}^{m} p(Y = y_j)\left[\sum_{i=1}^{n} p(X = x_i | Y = y_j) \log p(X = x_i | Y = y_j)\right]$$

Entropy

Which has more entropy?

a) abababababababab

b) qazifutbhfe40pl

$$Y := X$$

- What is the uncertainty of Y given X = 4 ?

$$Y := X$$

- What is the uncertainty of Y given X is between 0 and 15?

```
Y := X / Z
```

- What is the uncertainty of Y given X ?

```
if x = 1 then y := 0;
  else y:=1
```

- Is information flowing from x to y?

Lattice Review

- What is a lattice
  - Antisymmetric, transitive, and reflexive
  - Has GLB, LUB

Lattice Review

Antisymmetric, transitive, and reflexive

- Antisymmetric?

Lattice Review

Antisymmetric, transitive, and reflexive

- Antisymmetric?
  - If a <= b and b <= a then a == b

Transitive?

Lattice Review

Antisymmetric, transitive, and reflexive

- Antisymmetric -
  - If a <= b and b <= a then a == b
- Transitive -
  - If a < b and b < c then a < c
- Reflexive?

Lattice Review

Antisymmetric, transitive, and reflexive

- Antisymmetric -
  - If a <= b and b <= a then a == b
- Transitive -
  - If a > b and b > c then a > c
- Reflexive -
  - a <= a for all a in P

Lattice Review

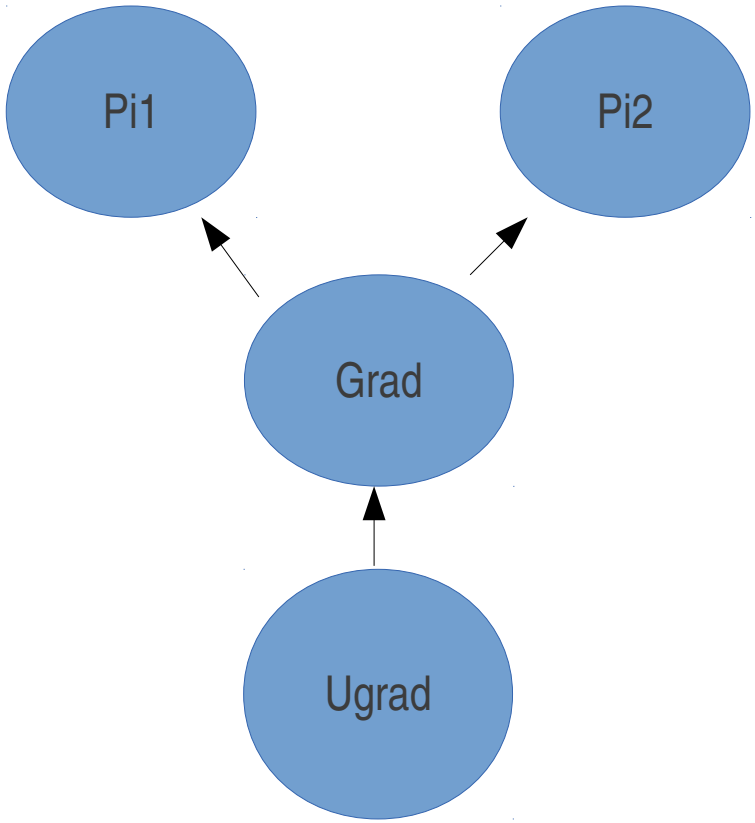
- LUB, GLB
  - Element that is greater than or equal to all elements of S
  - Greatest element that is less than or equal to all elements in S

Nonlattice Model

- What would a nonlattice model look like?

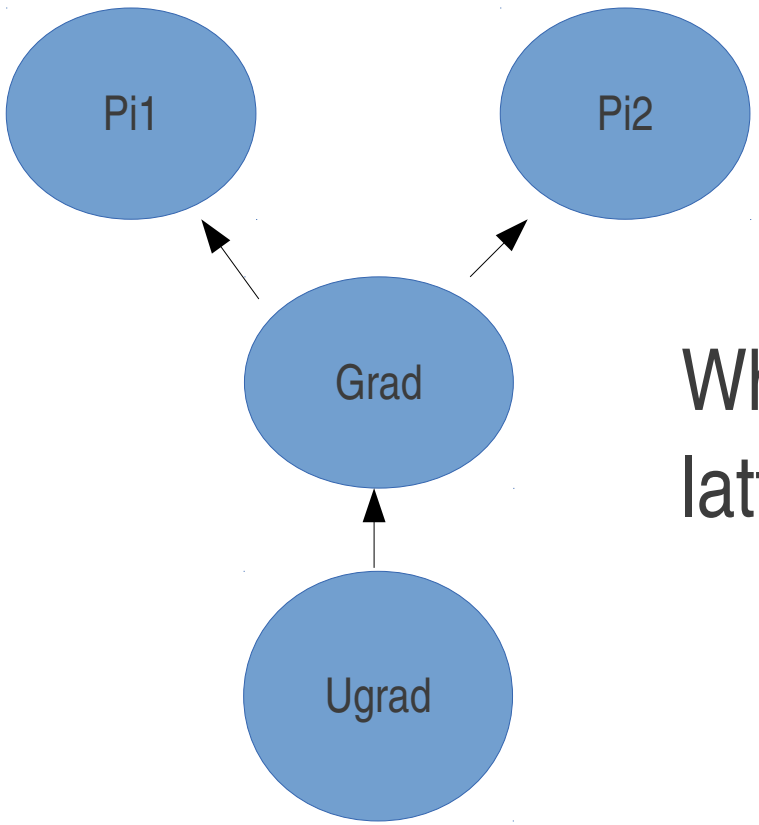
Nonlattice Model

- What would a nonlattice model look like?



Nonlattice Model

- What would a nonlattice model look like?



Why is this not a lattice?

Nonlattice Model

- Can we make it into a lattice?

Nonlattice Model