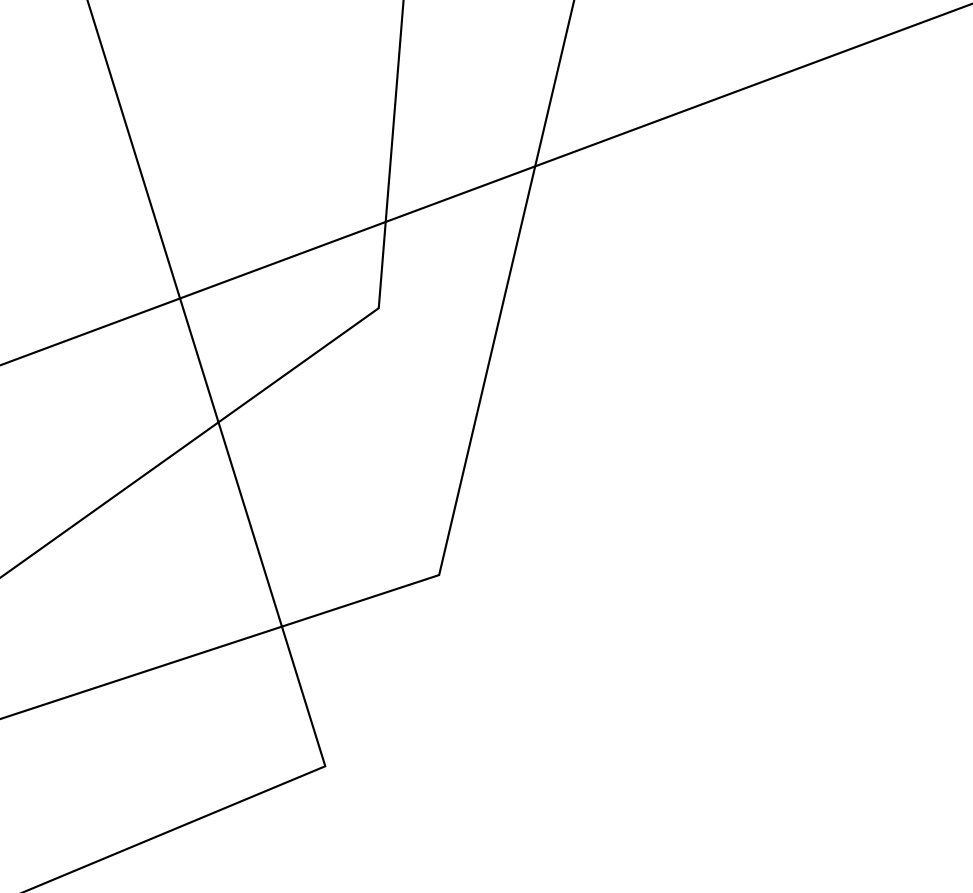


EXERCISE

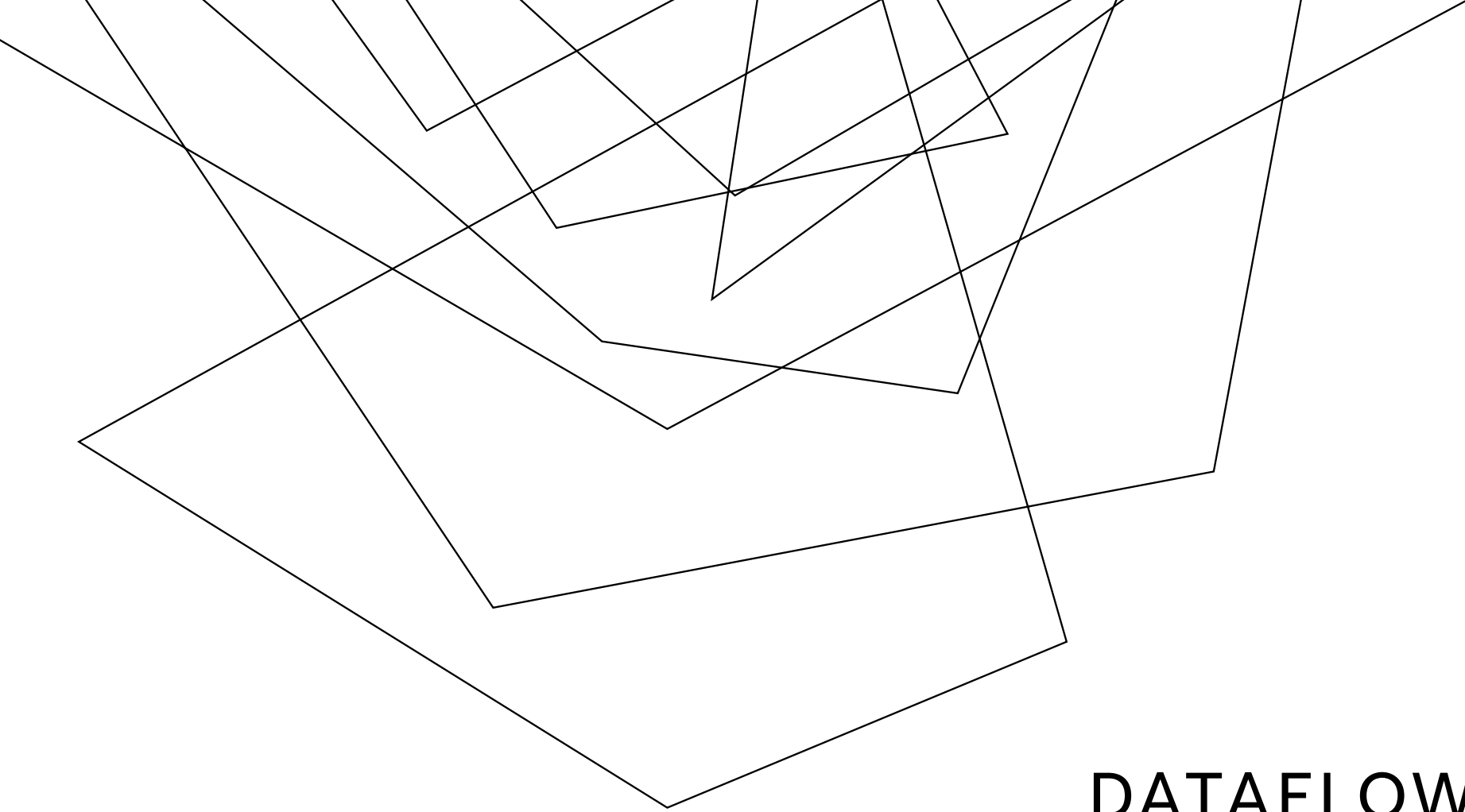
LATTICES REVIEW

Write your name and answer the following on a piece of paper

- Recall that the set of English words, ranked by substring inclusion, forms a poset but NOT a lattice. Explain why and give an example

Abstract geometric lines in the top left corner, consisting of several thin black lines that intersect and form various angles and shapes, creating a modern, architectural feel.

ADMINISTRIVIA AND ANNOUNCEMENTS

Abstract geometric lines in the top-left corner of the slide, consisting of several thin black lines forming overlapping, irregular polygons and triangles.

DATAFLOW FRAMEWORKS

EECS 677: Software Security Evaluation

Drew Davidson

DATAFLOW: THE BIG IDEAS

DATAFLOW FRAMEWORKS

FLOW-SENSITIVE ANALYSIS

Annotate each block with facts about data at entry to the block

Annotate each edge with facts about data flowing on that edge

Propagate facts until saturation

LATTICES

If ...

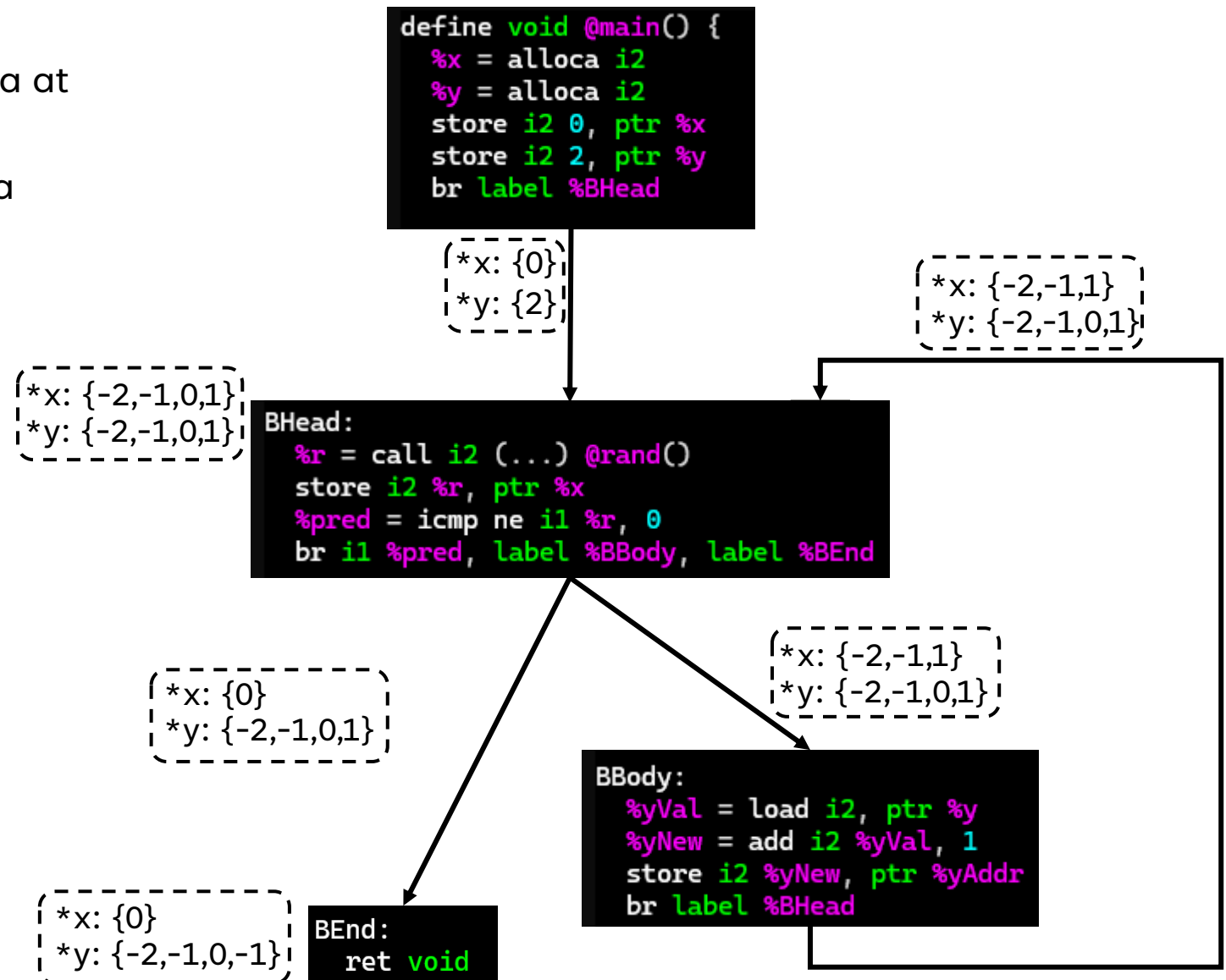
Domain of facts form a complete lattice

Merges use the lattice join operation

Facts over-approximate concrete values

... Then

Guaranteed termination and completeness



DATAFLOW: THE BIG IDEAS

DATAFLOW FRAMEWORKS

LATTICES

If ...

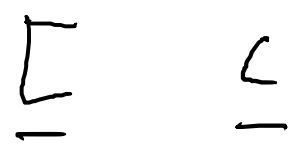
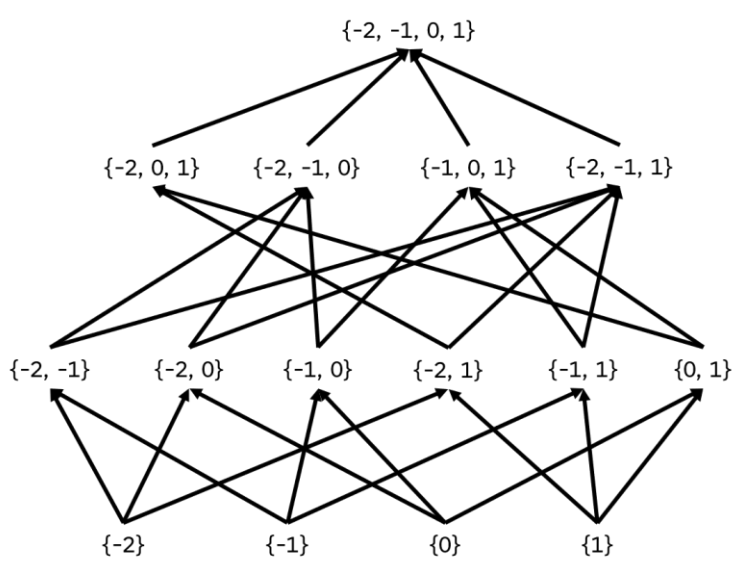
Domain of facts form a complete lattice

Merges use the lattice join operation

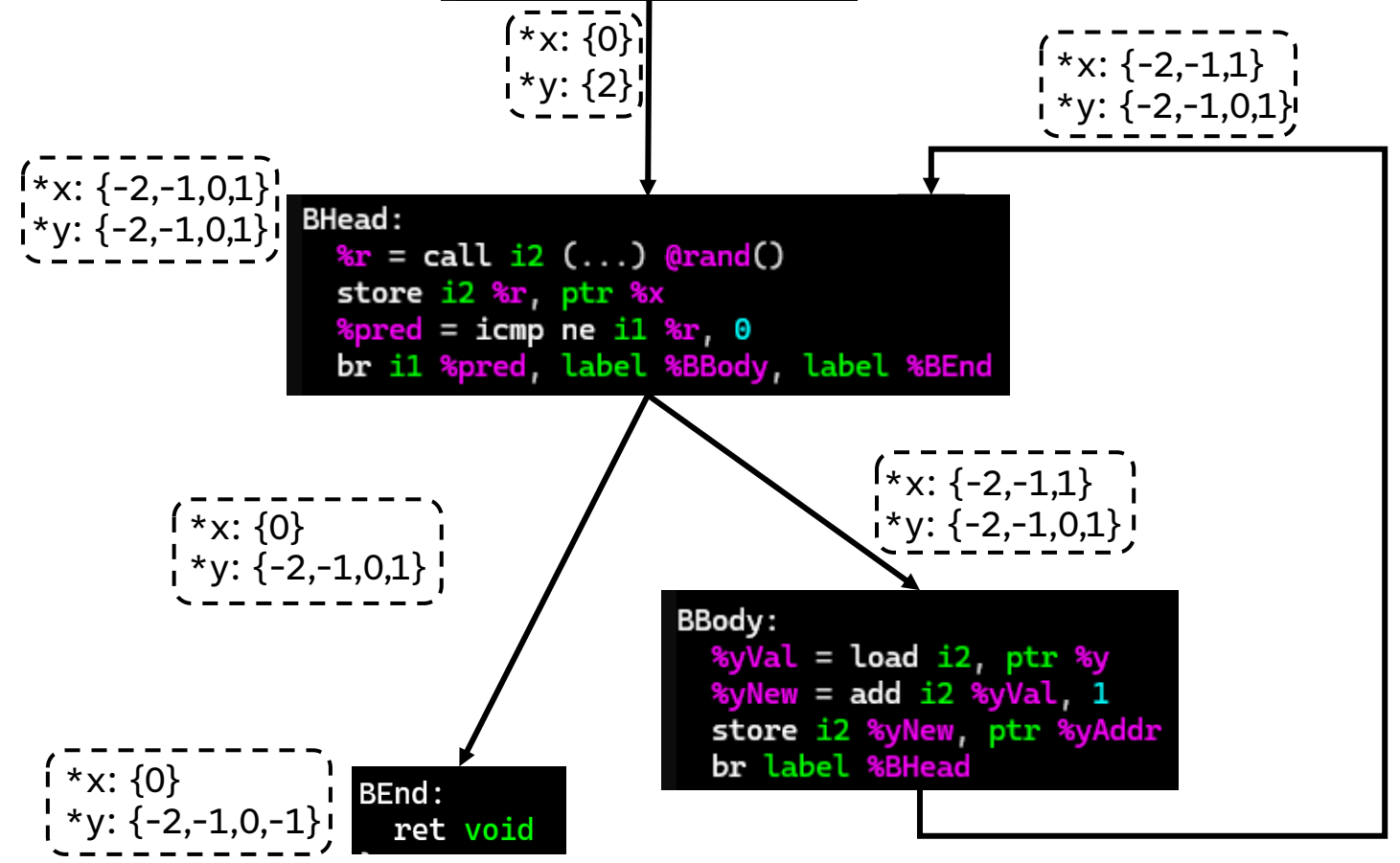
Facts over-approximate concrete values

... Then

Guaranteed termination and completeness



```
define void @main() {  
  %x = alloca i2  
  %y = alloca i2  
  store i2 0, ptr %x  
  store i2 2, ptr %y  
  br label %BHead
```



DATAFLOW: THE BIG IDEAS

DATAFLOW FRAMEWORKS

LATTICES

If ...

Domain of facts form a complete lattice

Merges use the lattice join operation

Facts over-approximate concrete values

... Then

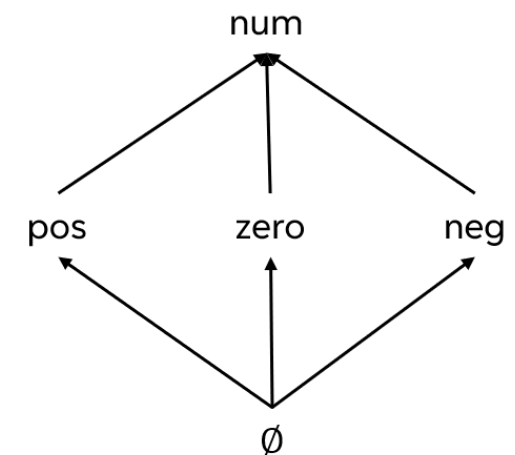
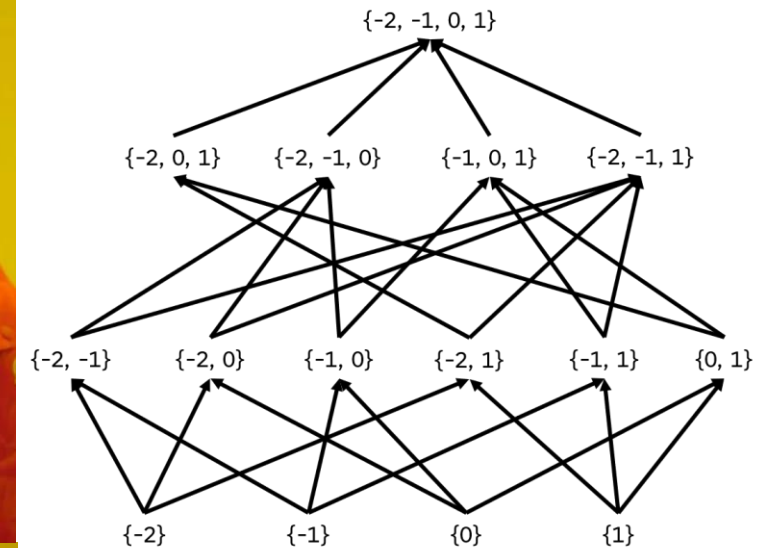
Guaranteed termination and completeness

ABSTRACT INTERPRETATION

Use a coarse-grained domain of facts

Maintain analysis guarantees

Reach saturation faster



DATAFLOW: THE BIG IDEAS

DATAFLOW FRAMEWORKS

LATTICES

If ...

Domain of facts form a complete lattice

Merges use the lattice join operation

Facts over-approximate concrete values

... Then

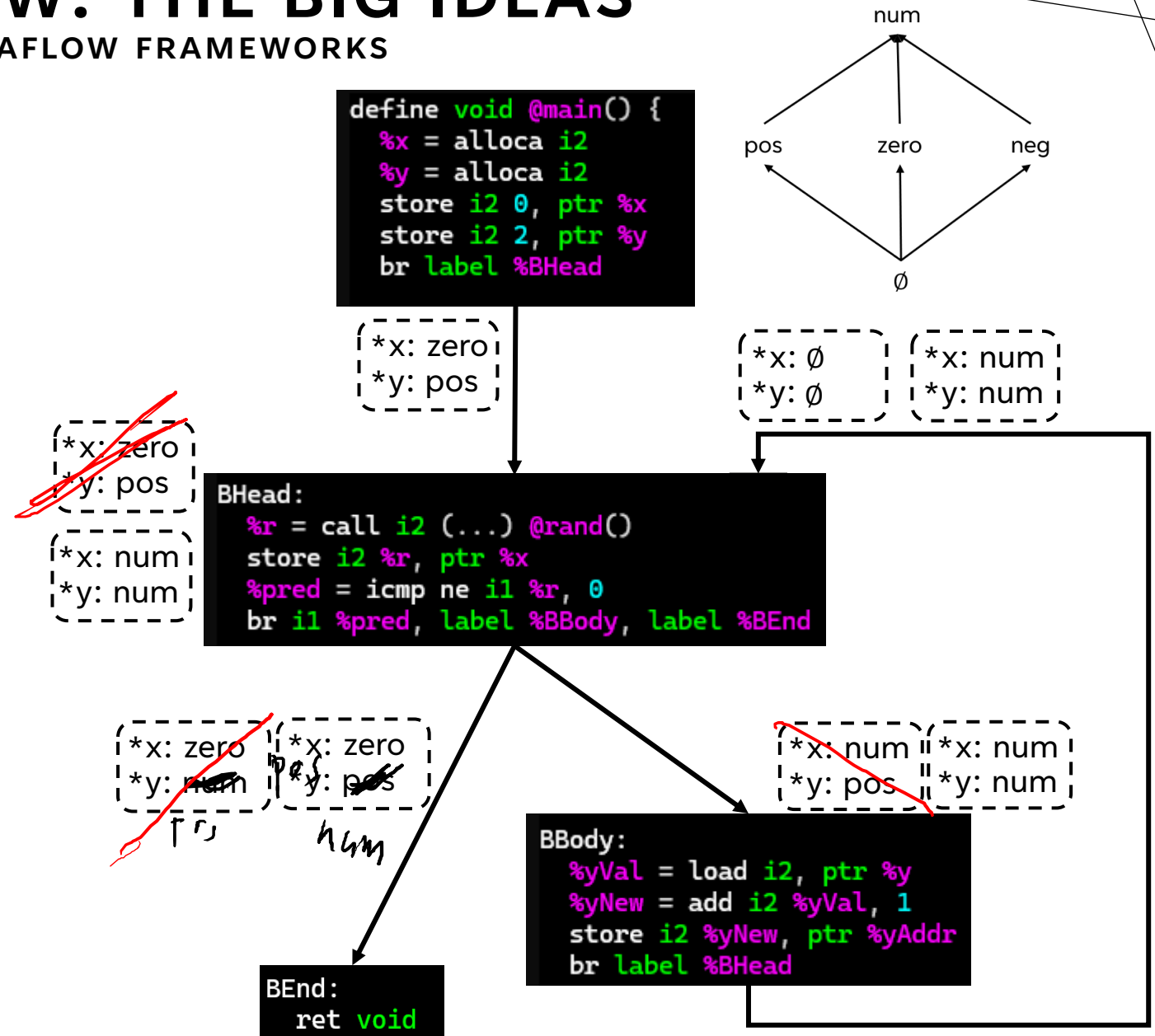
Guaranteed termination and completeness

ABSTRACT INTERPRETATION

Use a coarse-grained domain of facts

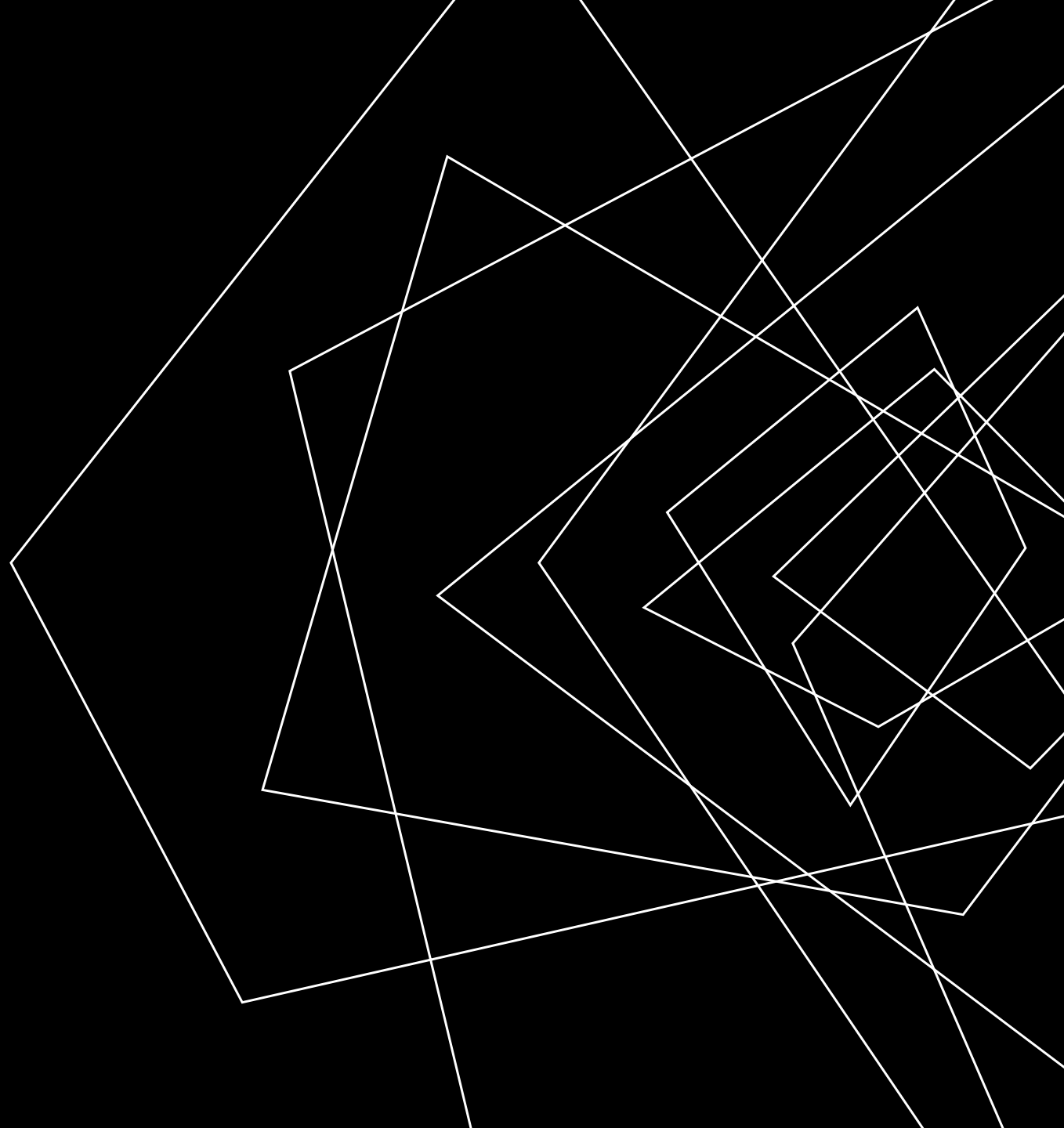
Maintain analysis guarantees

Reach saturation faster



LECTURE OUTLINE

- Formalizing dataflow
- Implementation



ABSTRACT DOMAINS

DATAFLOW FRAMEWORKS

BIG IDEA:

OPERATE OVER ABSTRACT VALUES THAT REPRESENT SETS OF CONCRETE VALUES

FROM THE CONCRETE DOMAIN TO THE ABSTRACT

$\alpha(\{0\}) =$ **zero**

$\alpha(S) =$ if all values in S are greater than 0 then **pos**
 else if all values in S are less than 0 then **neg**
 else **num**

FROM THE ABSTRACT DOMAIN TO THE CONCRETE

$\gamma(\text{zero}) = \{0\}$

$\gamma(\text{pos}) = \{\text{all positive ints}\}$

$\gamma(\text{neg}) = \{\text{all negative ints}\}$

$\gamma(\text{num}) = \text{Int (i.e., all ints)}$

WHY DOES THIS MATTER?

DATAFLOW FRAMEWORKS

*Every finite lattice
is a complete lattice*

PRACTICAL UPSHOT

If L is a complete lattice and f is monotonic, then f has a greatest fixpoint and a least fixpoint

If L has no infinite ascending chains, the least fixpoint can be computed by iterative application of f

So the analysis will terminate



CHAOTIC ITERATION

STATIC ANALYSIS: CONTROL FLOW GRAPHS

A WORKLIST ALGORITHM

- Select the next worklist item in any order
- Necessarily assumes progress towards some goal

DEALING WITH “UNCOMPUTED” SETS

- Assume a reasonable “initial” value



Surprisingly, not a band with merch at Hot Topic

ANALYSIS PRECISION

ABSTRACT INTERPRETATION

PRECISION / EFFICIENCY TRADEOFF

With a complete lattice we can, in theory, eventually terminate

That's not a very strong guarantee!

The shallower the lattice, the faster the fixpoint

Choose to approximate the lattice



ANALYSIS PRECISION

ABSTRACT INTERPRETATION

PRECISION / EFFICIENCY TRADEOFF

With a complete lattice we can, in theory, eventually terminate

That's not a very strong guarantee!

The shallower the lattice, the faster the fixpoint

Choose to approximate the lattice

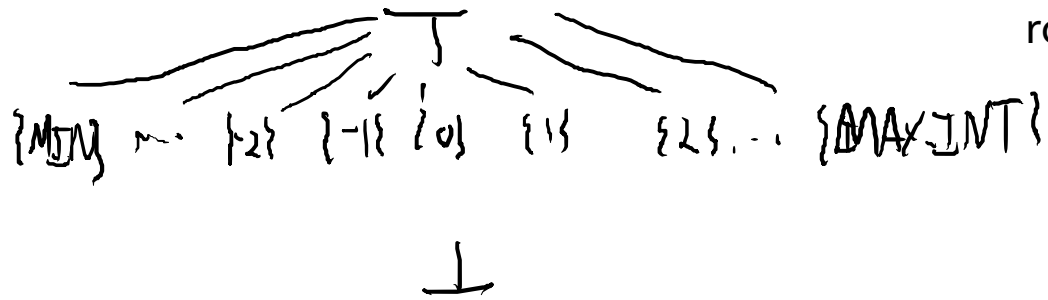


ABSTRACT DOMAINS IN PRACTICE

STATIC ANALYSIS

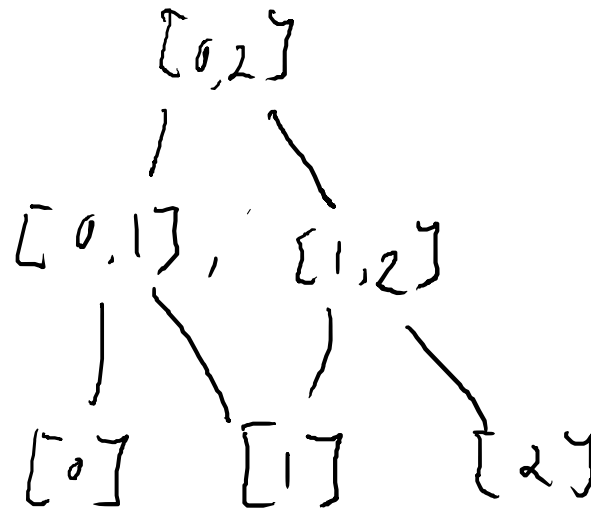
“SINGLETON INTEGER SETS”

- You know the number, or you don't



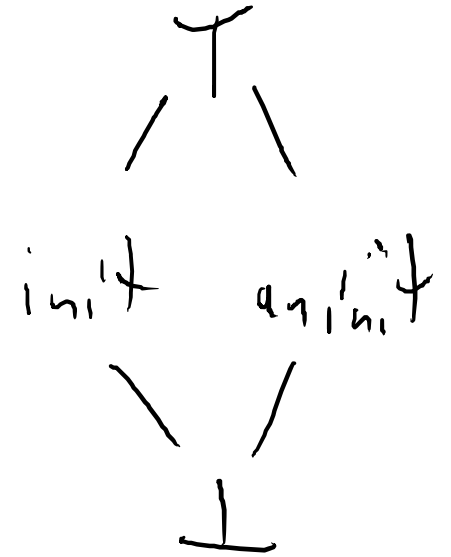
INTERVALS

- You know a concrete range



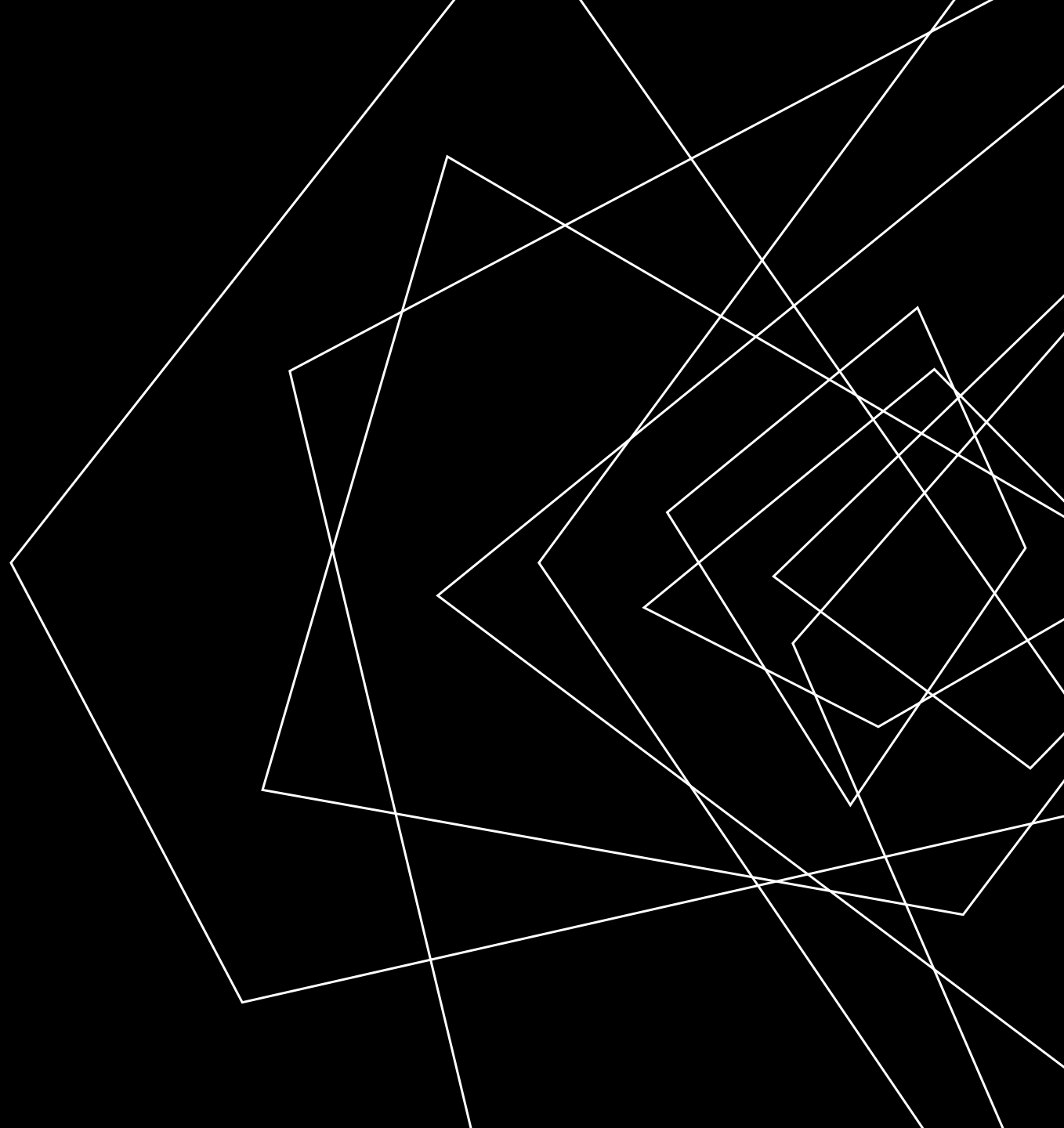
PROPERTY EXISTENCE

- A property does or does not hold



LECTURE OUTLINE

- Formalizing dataflow
- Implementation



COMPUTATION WITHIN A BLOCK

STATIC ANALYSIS

EACH INSTRUCTION IS A FACT TRANSFORMER

- Define as a function with domain and range in the fact space

DEALING WITH CONDITIONALS

STATIC ANALYSIS

CONSIDER THE FOLLOWING SNIPPET