Alcoa (Lecture 11)

Analysis of Software Artifacts

Alcoa

- *alloy:* the object modeling language
- *alcoa:* a tool for analyzing specifications written in alloy
- graphical notation corresponds to text

Revisit the file system example

```
model FileSystem {
domain {Object, DirEntry, Name}
```

File system (continued)

```
state {
  partition File, Dir : Object
  Root: fixed Dir!
  Cur: Dir?
  entries: Dir! -> DirEntry
  name: DirEntry -> Name!
  contents: DirEntry  -> Object!
  parent : Dir -> Dir?
}
```

File system (continued)

```
 def parent {

    all o | o.parent = o.~contents.~entries

}
```

File system (continued)

```
inv {
      all d | all e1, e2: d.entries | e1.name = e2.name

      no Root.parent

      all d: Dir - Root | one d.parent

      no d | d in d.+parent
```

```
    all d | d != Root -> Root in d.+parent

    all f: File | some d | f in d.entries.contents
}
```

File system continued

```
assert NoDirAliases {
   all o: Dir | sole o.~contents
}
```