

# Formalism in the Fortress Programming Language

Eric Allen  
Eric.Allen@sun.com

Sukyoung Ryu  
Sukyoung.Ryu@sun.com

Joe Hallett  
Joseph.Hallett@sun.com

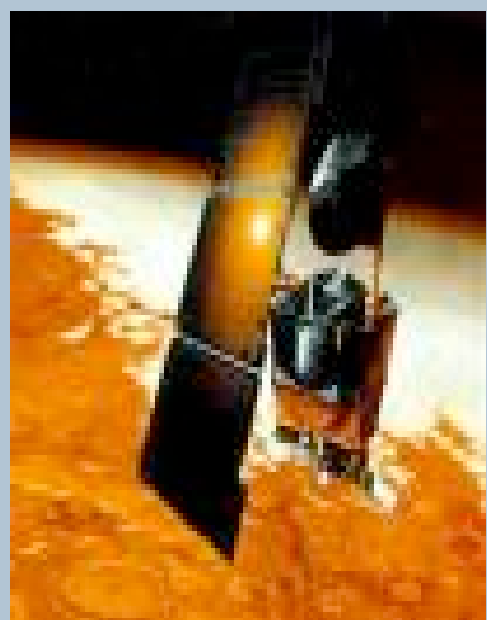
## The Value of Formal Methods



### Ariane 5

16 bit floating point from legacy Ariane 4 code was used with client code expecting 32 bit numbers, causing an uncaught overflow. As a result, the launcher was destroyed 40 seconds into the flight.

The launch cost of an Ariane 5 is \$180 million in 2000 U.S. Dollars.



### Mars Climate Orbiter

Orbiter software represented Force Time in Ns. Ground software represented Force Time in lbf s. Result: Loss of spacecraft.

Cost: \$327,600,000.



### Patriot Missile Failure

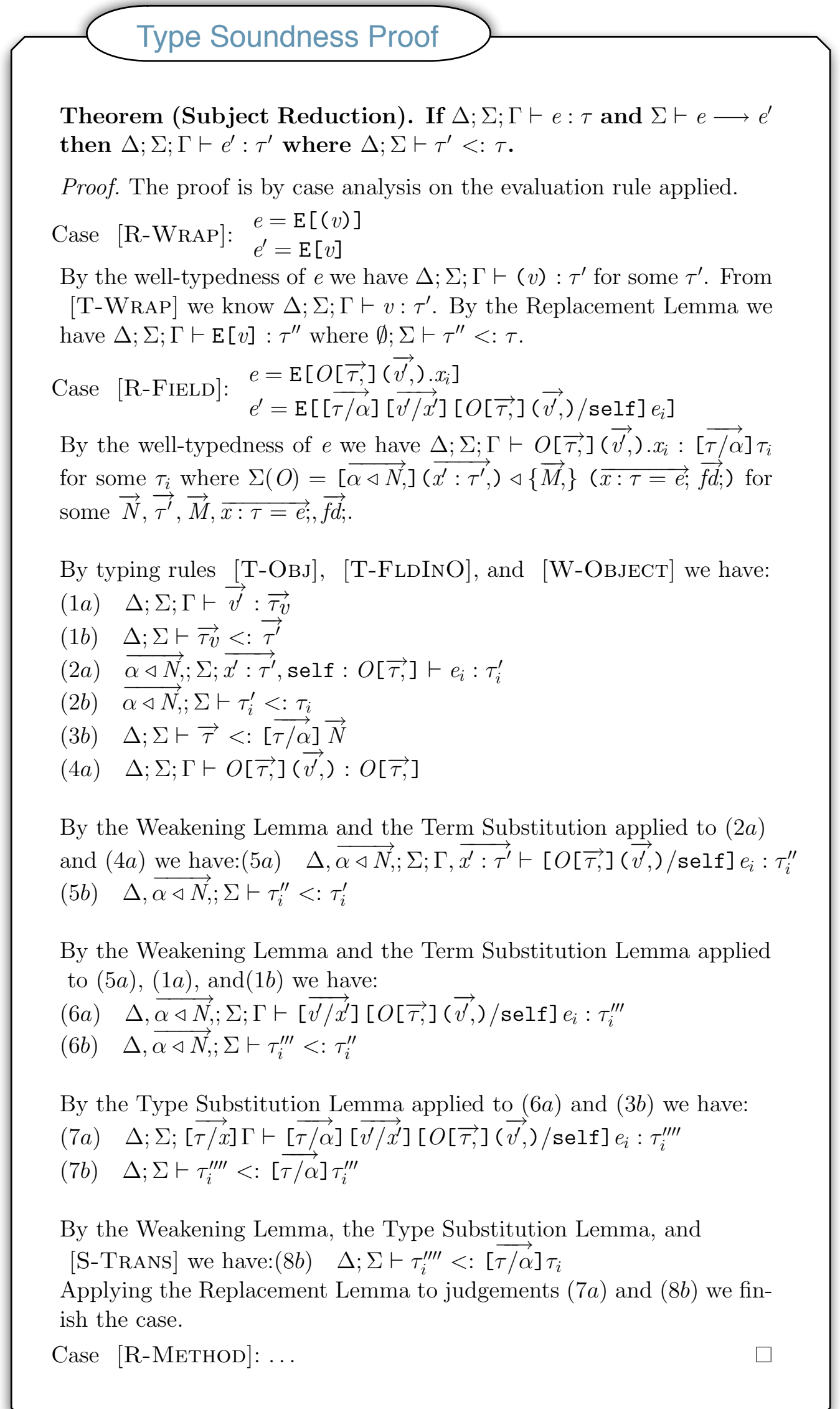
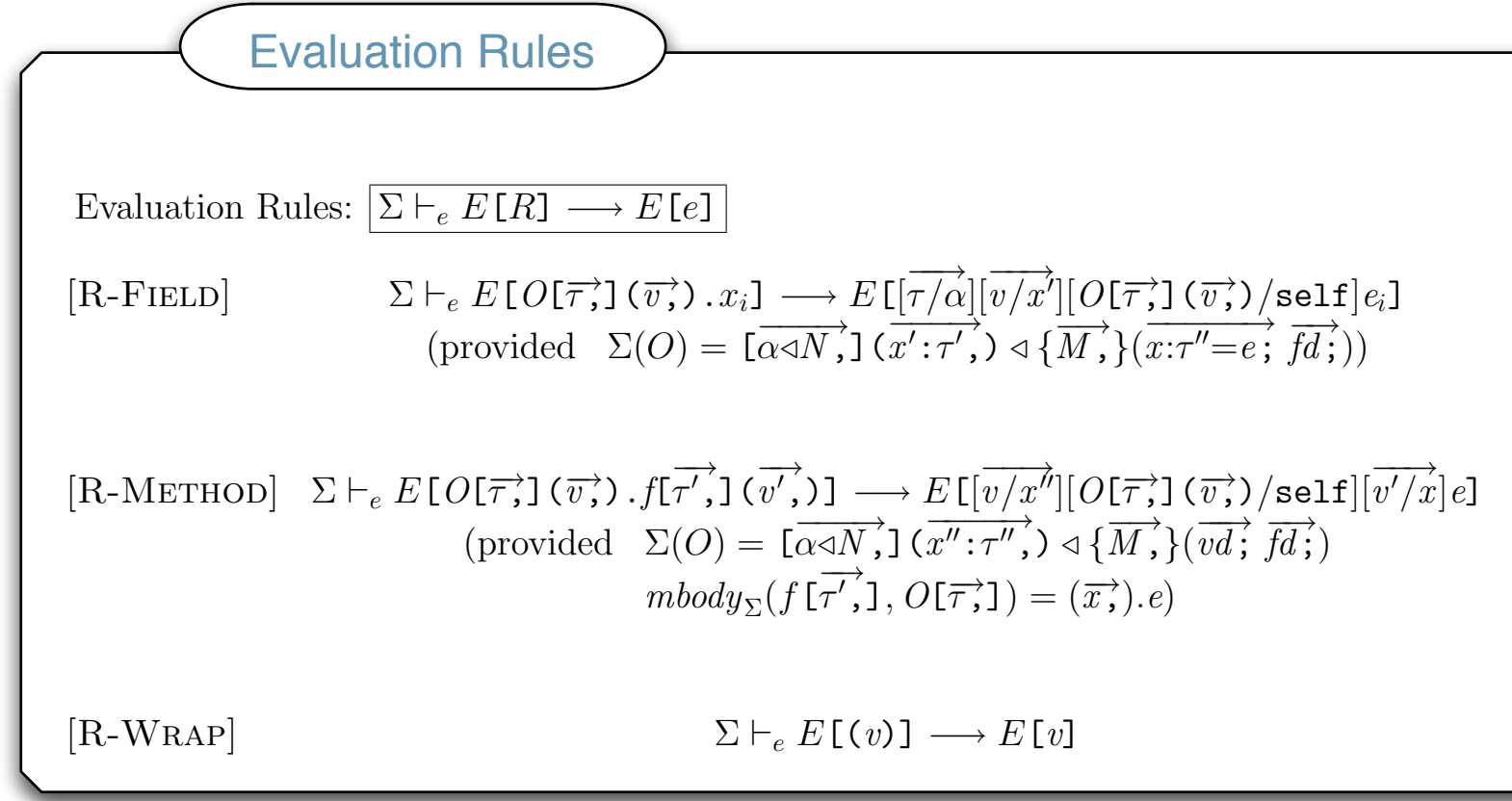
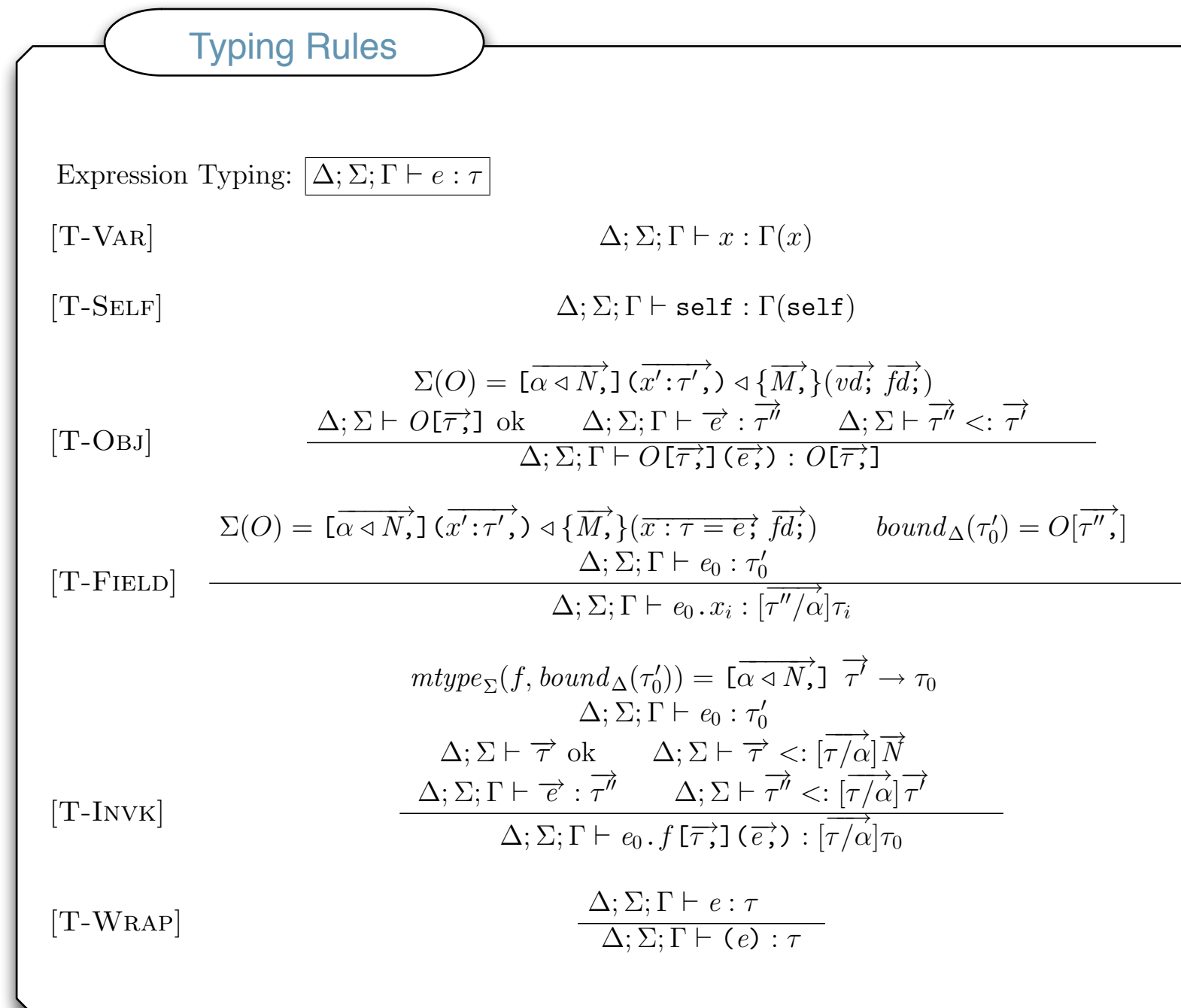
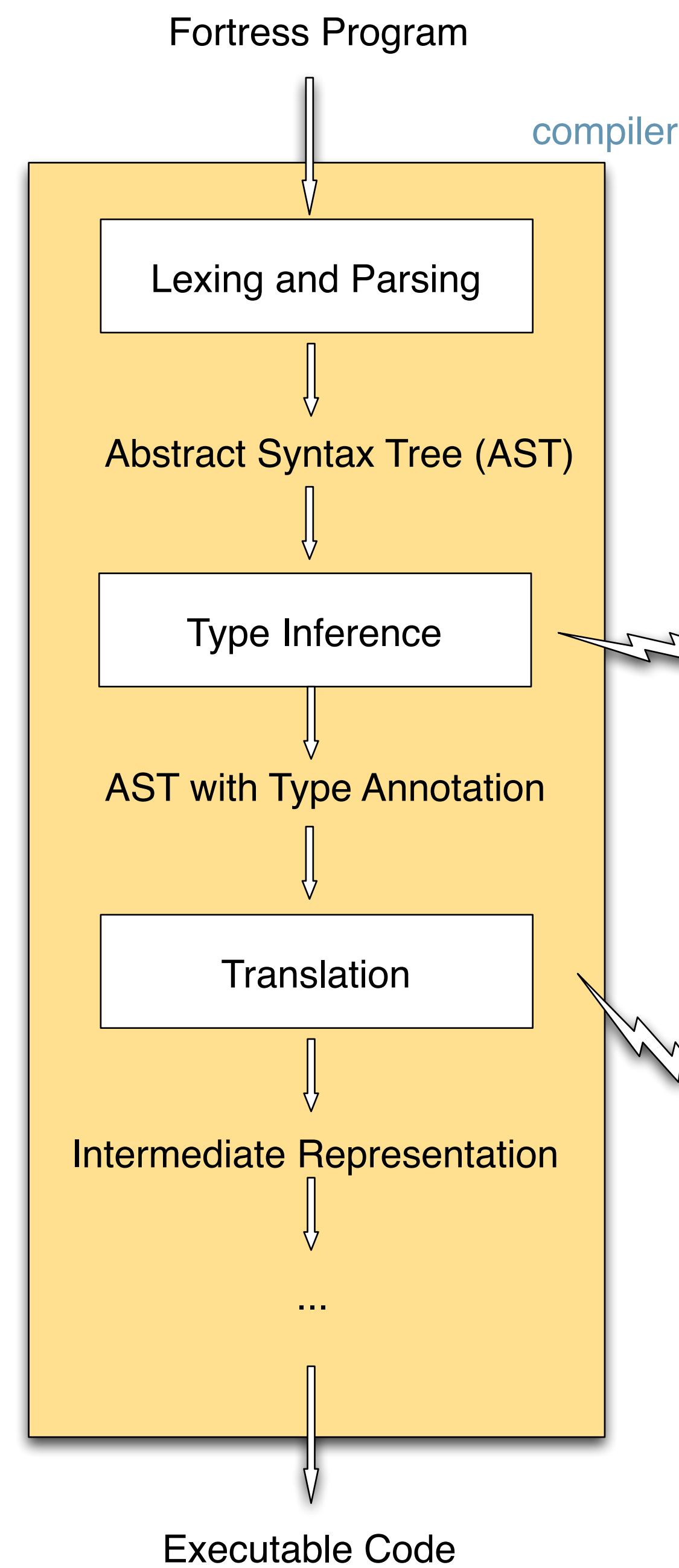
Accumulated rounding error in patriot missile software caused a missile to track its target incorrectly.

Result: SCUD missile was able to strike an army barrack, resulting in 28 Americans killed.

## Formalized Semantics

- Provides unambiguous specification for compiler writers
- Fewer insidious bugs
- More portable code

- Allows proofs of soundness and formal analysis



### Example Program in Fortress

```
object Main[]() traits {Object}
  myself:Main[] = self
  identity[](x:Object):Object = x
end

Main[]().identity[](Main[]().myself)
```

## Mechanized Semantics

- Tests soundness of language semantics

### Soundness of the Example Program

Suppose  $\Sigma = \{\text{Main} \mapsto \square \triangleleft \{\text{Object}\} \text{ (myself:Main} \square = \text{self; identity} \square(x:\text{Object}): \text{Object} = x;)\}$

If  $\emptyset; \Sigma; \emptyset \vdash \text{Main} \square(). \text{identity} \square(\text{Main} \square(). \text{myself}) : \text{Object}$  and  $\Sigma \vdash \text{Main} \square(). \text{identity} \square(\text{Main} \square(). \text{myself}) \longrightarrow^* \text{Main} \square(). \text{identity} \square(\text{Main} \square(). \text{myself})$  then  $\emptyset; \Sigma; \emptyset \vdash \text{Main} \square(). \text{identity} \square(\text{Main} \square(). \text{myself}) : \text{Object}$ .

