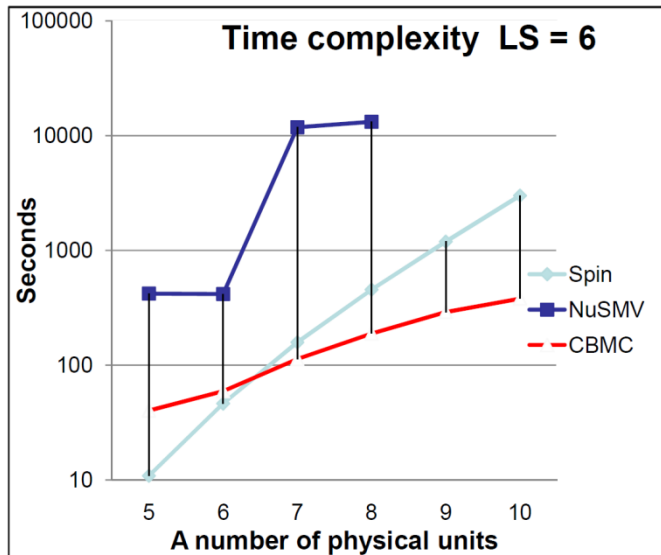


# **An Inductive Method for Verifying Properties of a Program**

Sungkeun Cho  
ROSAEC Workshop  
ROPAS, SNU

# Motivation

- MSR (Multi-Sector Read) function
  - Copy data from sectors of a flash memory to a buffer



Model Checking Performance for MSR \*

- To verify that MSR code works correctly with an arbitrary size of memory

---

\* Moonzoo Kim. Model Checking for the Practical C Program Analysis – Experience Reports. In *the 2<sup>nd</sup> ROSAEC workshop*. 2009.

# Hoare Triple

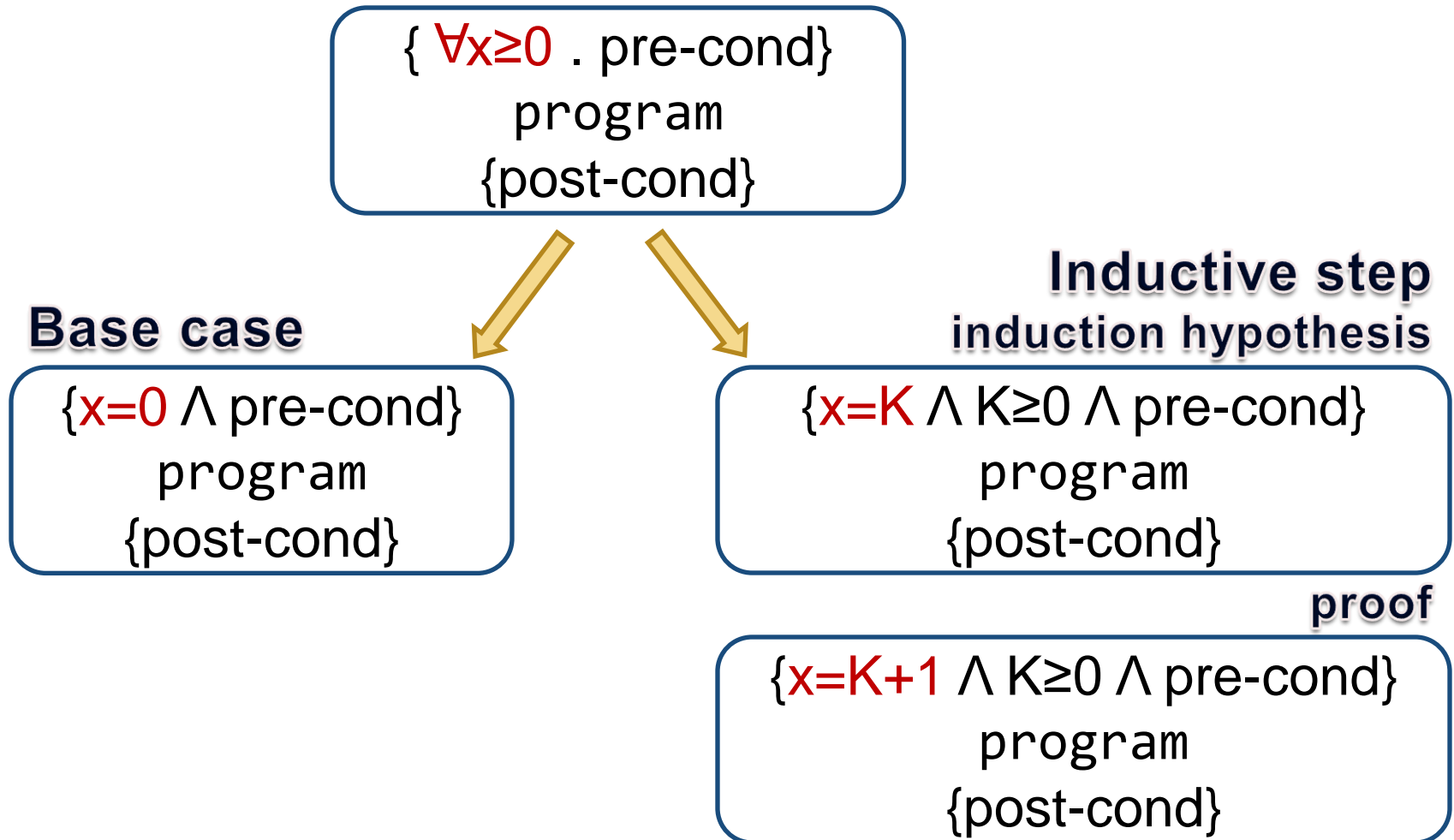
{pre-condition}  
program  
{post-condition}

if pre-condition is true  
and program executes



then post-condition is true

# An Inductive Method



# Example – While Loop

iteration number  
of while loop

$\{\forall x \geq 0 . \text{pre-cond}\}$   
`while(...){...}`  
 $\{\text{post-cond}\}$

**Base case**

$\{x=0 \wedge \text{pre-cond}\}$   
`while(...){...}`  
 $\{\text{post-cond}\}$

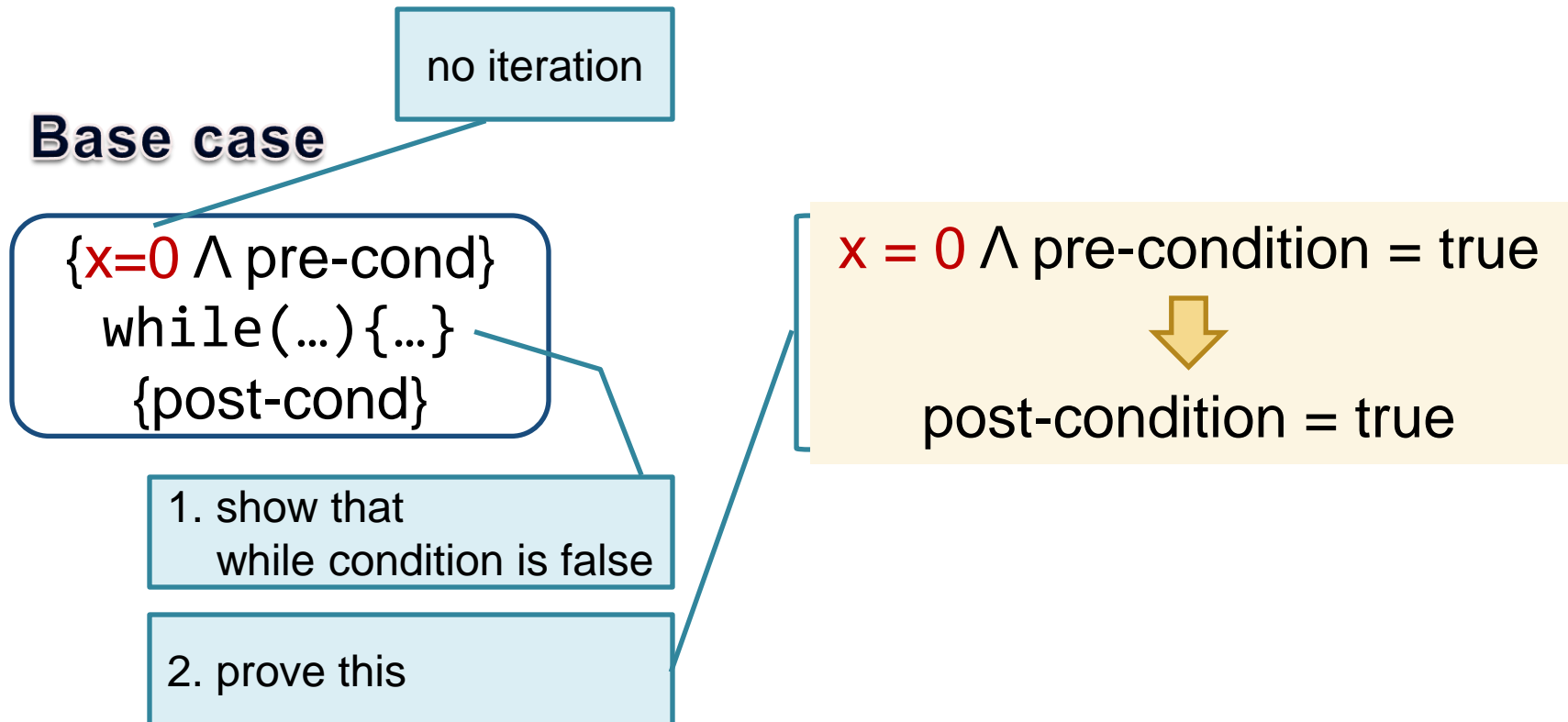
**Inductive step**  
induction hypothesis

$\{x=K \wedge K \geq 0 \wedge \text{pre-cond}\}$   
`while(...){...}`  
 $\{\text{post-cond}\}$

**proof**

$\{x=K+1 \wedge K \geq 0 \wedge \text{pre-cond}\}$   
`while(...){...}`  
 $\{\text{post-cond}\}$

# Example – While Loop



# Example – While Loop

**Inductive step**  
**induction hypothesis**

1. show that  
while condition is true

```
{x=K ∧ K≥0 ∧ pre-cond}  
while(...) { ... }  
{post-cond}
```

```
{x=K+1 ∧ K≥0 ∧ pre-cond}  
while(...) {  
  body;  
}  
{post-cond}
```

**proof**

```
{x=K+1 ∧ K≥0 ∧ pre-cond}  
while(...) { ... }  
{post-cond}
```

loop  
unrolling

2. prove this

3. prove this by  
induction hypothesis

```
{x=K+1 ∧ K≥0 ∧ pre-cond}  
body;  
{x=K ∧ K≥0 ∧ pre-cond}  
while(...) {  
  body;  
}  
{post-cond}
```

# Summary

- Achievement
  - The pre- and post-conditions of MSR
- Strength
  - Intuitive
    - Easy to apply
    - Easy to understand
- Weakness
  - Take a lot of time
  - Not trustworthy



# Future Work

- Mechanize the proof formally
  - Coq
    - Formal proof management
    - Mathematical definitions and theorems
  - Why tool
    - Software verification platform
    - Integrated with many provers
  - Frama-C
    - Extensible platform dedicated to source-code analysis of C software

**Thank you.**