

# Statická analýza v nástroji Facebook Infer zaměřená na detekci porušení atomičnosti

Dominik Harmim

Vedoucí: Prof. Ing. Tomáš Vojnar, Ph.D.

xharmi00@stud.fit.vutbr.cz

Vysoké učení technické v Brně, Fakulta informačních technologií



- **Atomicita** (provádění operací bez přerušení)
  - je vyžadována v **paralelních programech**,
  - porušení může mít **kritické následky**.

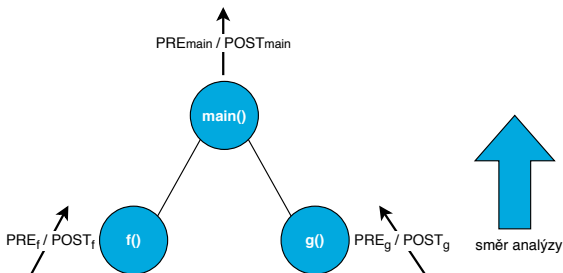
```
replace(a, b) {  
  if (contains(a)) {  
    i = index_of(a);  
    set(i, b);  
  }  
}
```

`contains` a `index_of` by měly  
být volány atomicky

- **Nedostatky současných analyzátorů** porušení atomicity:
  - vysoká míra falešných pozitiv,
  - rychlost,
  - škálovatelnost,
  - ...

- Volně šířený nástroj pro **statickou analýzu**.
- Používá **abstraktní interpretaci (Infer.AI)**.
- Analýza jednotlivých funkcí od listů stromů ke kořenům.
  - Počítání souhrnů funkcí (**summary**).
- Důraz na **škálovatelnost**.

```
main() {  
  f();  
  g();  
}
```



## Dvě fáze analýzy:

### ① Detekce atomických sekvencí

- Derivace množin funkcí volaných atomicky.

```
f() {  
  h1();  
  lock();  
  h2();  
  h3();  
  unlock();  
  h4();  
}
```

$(h2 \ h3) \rightarrow POST_f$

### ② Detekce porušení atomicity

- Porušení pro libovolnou dvojici, která se vyskytla za sebou v atomické sekvenci z 1. fáze.

```
g() {  
  h1();  
  h2();  
  h3();  
  h4();  
}
```

Porušení atomicity pro  $h2 \ h3$ .

## Současný stav:

- Implementace **detekce atomických sekvencí** (1. fáze).
  - Pro jazyk C se zámký typu **POSIX Threads (Pthreads)**.
  - Experimentální ověření.

## Budoucí cíle:

- Implementace **detekce porušení atomicity** (2. fáze).
  - Experimentální ověření.
- Žádost o začlenění do repositáře **Facebook Infer** (**Pull Request**).