Porovnání a experimentální vyhodnocení různých přístupů ke statické analýze

Tomáš Beránek

Vysoké učení technické v Brně - Fakulta informačních technologií
Božetěchova 2, 612 66 Brno
xberan46@stud.fit.vutbr.cz

30. ledna 2020

Obsah

- Motivace
- Existující přístupy ke statické analýze
- Nástroj Facebook Infer
- Nasazení Inferu na reálný software
- Přizpůsobení Inferu na kontrolu assertů
- Průběžná analýza Inferem při vývoji
- Odstranění zastavení analýzy

Motivace

- Proč statická analýza?

- Proč statická analýza?
  - Stále komplexnější software

- Proč statická analýza?
  - Stále komplexnější software
- Jaký nástroj zvolit?

- Proč statická analýza?
  - Stále komplexnější software
- Jaký nástroj zvolit?
  - Různé nástroje jsou vhodné pro různé softwary

- Proč statická analýza?
  - Stále komplexnější software
- Jaký nástroj zvolit?
  - Různé nástroje jsou vhodné pro různé softwary
  - Celá sada kooperujících nástrojů

- Jak nástroje integrovat do vývojového procesu?

- Jak nástroje integrovat do vývojového procesu?
  - Automatické spouštění

- Jak nástroje integrovat do vývojového procesu?
  - Automatické spouštění
  - Rychlé a přehledné zpřístupnění výsledků

- Jak nástroje integrovat do vývojového procesu?
  - Automatické spouštění
  - Rychlé a přehledné zpřístupnění výsledků
  - Průběžná analýza

- Jak nástroje integrovat do vývojového procesu?
  - Automatické spouštění
  - Rychlé a přehledné zpřístupnění výsledků
  - Průběžná analýza
  - Nízký počet falešných hlášení

Existující přístupy ke statické analýze

- Facebook
  - FB Infer na mobilních aplikacích v C++/Obj-C
  - Průběžná i celková analýza
  - Analýza pouze změněných funkcí a funkcí na nich závislých

Existující přístupy ke statické analýze

- Facebook
  - FB Infer na mobilních aplikacích v C++/Obj-C
  - Průběžná i celková analýza
  - Analýza pouze změněných funkcí a funkcí na nich závislých
- Red Hat

Existující přístupy ke statické analýze

- Facebook
  - FB Infer na mobilních aplikacích v C++/Obj-C
  - Průběžná i celková analýza
  - Analýza pouze změněných funkcí a funkcí na nich závislých
- Red Hat
- Honeywell
  - Kontrola assert maker

- Nelze prokázat absenci chyb v softwaru
- Lze detekovat celou řadu problémů
  - Úniky paměti, NULL dereference, ...
- Podporované jazyky
  - C, C++, Objective-C a Java
- Analýza odspodu nahoru
  - Možnost analýzy nedokončených projektů

- Složen z dílčích nezávislých analyzátorů
  - Paralelní analýza i na úrovni souborů
- Analýza probíhá ve dvou fázích
  - Fáze zachycení (angl. Capture)
  - Analyzační fáze

Nasazení Inferu na reálný software

- Dva základní přístupy k analýze
  - Jednorázová analýza
  - Průběžná analýza
- Každý přístup se potýká s jinými problémy

Nasazení Inferu na reálný software

- Problémy u jednorázové analýzy

- Problémy u jednorázové analýzy
  - Zpřístupnění překladových příkazů
    - Automaticky
    - Ručně

- Problémy u jednorázové analýzy
  - Zpřístupnění překladových příkazů
    - Automaticky
    - Ručně
  - Kompatibilita s vnitřním překladačem Inferu
    - Na úrovni překladových příkazů
    - Na úrovni zdrojových souborů

- Problémy u jednorázové analýzy
  - Zpřístupnění překladových příkazů
    - Automaticky
    - Ručně
  - Kompatibilita s vnitřním překladačem Inferu
    - Na úrovni překladových příkazů
    - Na úrovni zdrojových souborů
  - Velké množství hlášení
    - Vracení se ke starému kódu je neefektivní

Nasazení Inferu na reálný software

- Průběžná analýza

- Průběžná analýza
  - Částečně řeší problémy jednorázové analýzy

- Průběžná analýza
  - Částečně řeší problémy jednorázové analýzy
  - Automatizace procesu přináší další problémy:

- Průběžná analýza
  - Částečně řeší problémy jednorázové analýzy
  - Automatizace procesu přináší další problémy:
    - Ošetření falešných hlášení

- Průběžná analýza
  - Částečně řeší problémy jednorázové analýzy
  - Automatizace procesu přináší další problémy:
    - Ošetření falešných hlášení
    - Způsob hlášení výsledků

- Průběžná analýza
  - Částečně řeší problémy jednorázové analýzy
  - Automatizace procesu přináší další problémy:
    - Ošetření falešných hlášení
    - Způsob hlášení výsledků
    - Integrace do vývojového procesu

Kód firmy CAMEA

- 4 části v C,C++ a vhdl
- Dodatečné vytvoření sestavovacích specifikaci (make, cmake)
- Extrakce překladových příkazů z přiložené cmake specifikace
- Ruční úpravy kvůli nekompatibilitě s interním překladačem Inferu

Kodek CCSDS formátu

- Čistý jazyk C a jednoduchý Makefile
- Stále ve vývoji
- Snaha o nasazení Inferu do vývoje

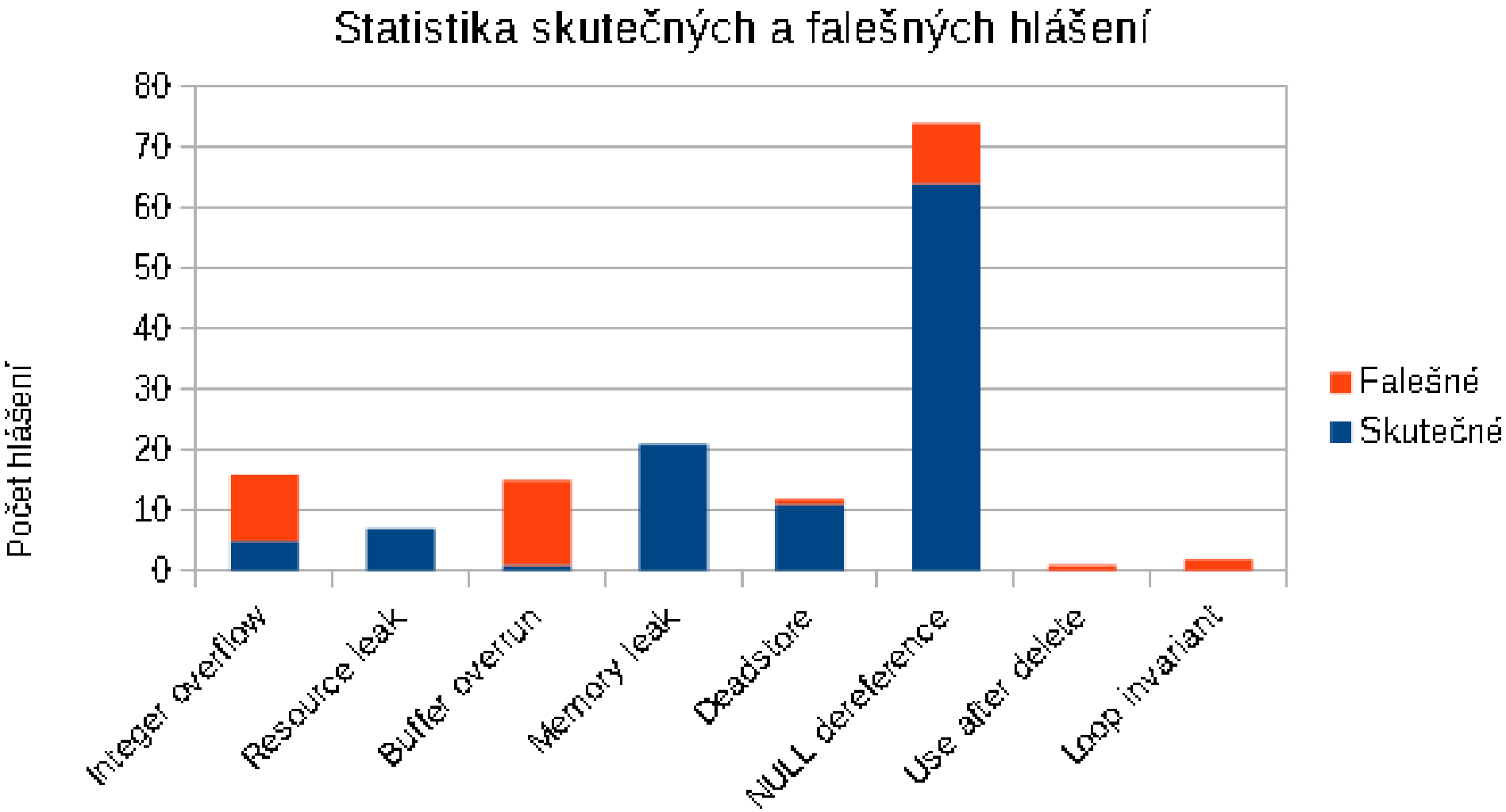
Jádro platformy Arrowhead

- Psáno v Javě (Maven)
- Problém při extrakci překladových příkazů
- Analýza po částech
- Nekompatibilita překladačů (11+ vs 8)

Ostatní analyzované projekty

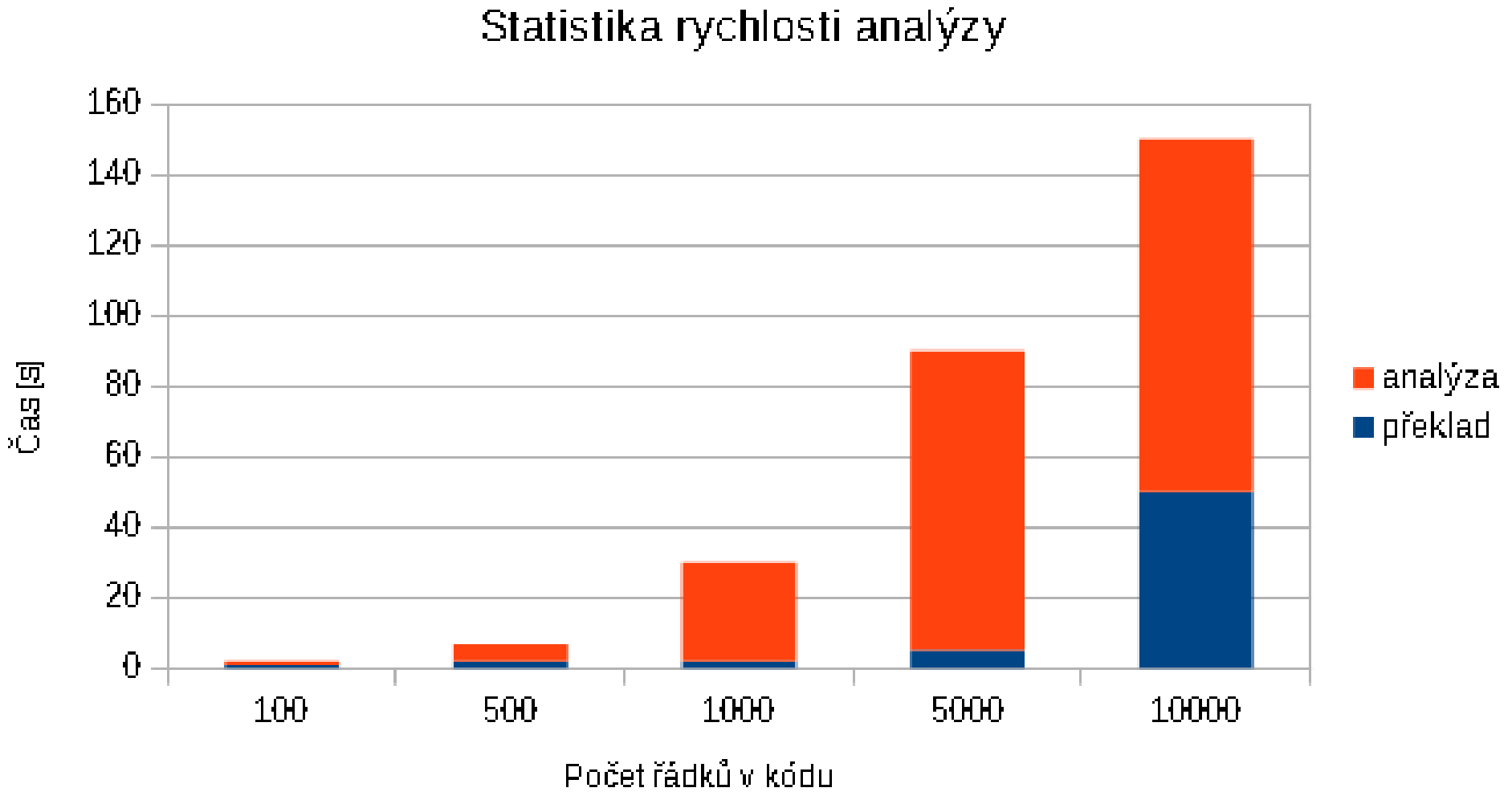
- Školní projekty
- Speciálně vytvořené testy

Výsledky ověření vlastností



pozn. zahrnuty i nedokončené nebo řádně neotestované projekty

Výsledky ověření vlastností



pozn. počet souborů výrazně ovlivňuje překladovou fázi

Přizpůsobení Inferu na kontrolu assertů

- Automatické generování assertů
- Požadavek od firmy Honeywell na snížení počtu falešných hlášení

Přizpůsobení Inferu na kontrolu assertů

- Automatické generování assertů
- Požadavek od firmy Honeywell na snížení počtu falešných hlášení
- Dvě úpravy:

Přizpůsobení Inferu na kontrolu assertů

- Automatické generování assertů
- Požadavek od firmy Honeywell na snížení počtu falešných hlášení
- Dvě úpravy:
  - Nahrazení typu chyby

Přizpůsobení Inferu na kontrolu assertů

- Automatické generování assertů
- Požadavek od firmy Honeywell na snížení počtu falešných hlášení
- Dvě úpravy:
  - Nahrazení typu chyby
  - Oprava upraveného assert makra

Průběžná analýza Inferem při vývoji

- Přístup k verzím -> integrace s Gitem
- Celková analýza vs analýza změn
- Okamžitá zpětná vazba
- Filtrace falešných hlášení
- Pre-commit hook
- Nutnost sledovat infer-out/
- Dodatečná celková analýza

Odstranění zastavení analýzy

- Analyzátor bi-abduction
- Uzavření místa výskytu do konstrukce if-else s předem neznámou podmínkou
- Možné vytvoření dalších chyb
- Potřeba vytvářet kopie zdrojových souborů
- Lze automatizovat

Děkuji za pozornost.