
Java PathFinder
Adam Bielański
Weryfikacja modelowa programów Javy.

# Plan

- Skąd ten pomysł?
- Początki weryfikacji w NASA
- Java PathFinder2
  - Główne elementy
  - Rozszerzenia
- Stan na dziś
- Jak można pomóc?

# Skąd ten pomysł?

- Misja Mars PathFinder (1997):
  - Koszt misji: **250 000 000 USD**
  - Radość spowodowana dead-lockiem: **Bezcenna**
  - Konsekwencje:  Utrata danych zbieranych przez kilka dni...

# Skąd ten pomysł?

- Misja DeepSpace 1 (1998):
  - Koszt misji: **152 000 000 USD**
  - Dead-lock w dniu spotkania z asteroidą wyłączył sondę na ok. 6 godzin
  - System był **prawie** zweryfikowany

# Początki weryfikacji w NASA

- Java PathFinder (1)
  - Tłumaczenie **źródeł** Javy do PROMELI za pomocą CommonLisp'a
  - Brak możliwości zweryfikowania bibliotek
  - Formułowanie asercji w kodzie Javy
  - Znalezione błędy w Remote Agent

# Java PathFinder2

- Weryfikacja **skompilowanego kodu** Javy
- Specjalna maszyna wirtualna
  - Niedeterminizm
  - Własne mechanizmy odśmiecania
  - Specyfikowanie 'atomowości'
  - Powtarzalna sterta
- Partial Order Reduction
  - Zapobieganie eksplozji stanów
  - 'Megakroki'

# Java PathFinder2
# Główne elementy

- Tworzenie abstrakcji programu
  - Budowanie abstrakcji dla każdej klasy
  - Dodawanie zmiennych zależnych od różnych klas
- Analiza statyczna – redukcja stanów.
- Analiza czasu wykonania:
  - Symulacja
  - Sterowanie weryfikacją
- Wykonywanie symboliczne

# Java PathFinder 2
# Rozszerzenia

- Heurystyki
  - Ograniczenie głębokości DFS
  - Preferowanie nieodwiedzonych gałęzi
- RTJS - Systemy czasu rzeczywistego
  - Utożsamianie stanów różniących się 'nieznacznie'
  - Asynchroniczne zdarzenia i obsługa tych zdarzeń
  - Zegar i timer'y
- Generowanie pozytywów i negatywów.

# Stan na dziś
# Java PathFinder 4

- Rozwijany jako open-source
- Dla większości standardowych bibliotek jest abstrakcja
- Nie ma modelowania czasu ani kosztów wykonania
- Jest częściowy plugin do Eclipse
- Wykonywanie symboliczne
- Rozszerzalność: Listener, MIJ, ChoiceGenerator

# Jak można pomóc?

- Plugin do Eclipse
- Abstrakcje bibliotek
- Poprawienie wykonywania symbolicznego
- Usunięcie wycofywanego interfejsu do debuggowania
- Refaktoryzacja – poprawienie enkapsulacji