

# Własności programów imperatywnych.

8 czerwca 2009

# Plan

- Logika Hoare'a
- Narzędzia Why, Caduceus, Krakatoa
- Dowody w Coqu

Trójki Hoare'a do dowodzenia poprawności częściowej:

$\{\alpha\} P \{\beta\}$  — jeśli przed wykonaniem programu  $P$  spełniony jest pre-warunek  $\alpha$ , to po wykonaniu programu  $P$  (o ile  $P$  się zatrzyma) spełniony jest post-warunek  $\beta$ .

Reguły wyprowadzania takich trójek, np:

[przypisanie]  $\{\alpha[t/x]\} x := t \{\alpha\}$

[pętla while] 
$$\frac{\{\phi \wedge b\} P \{\phi\}}{\{\phi\} \text{ while } b \text{ do } P \{\phi \wedge \neg b\}}$$

[sekwencja] 
$$\frac{\{\alpha\} P_1 \{\beta\} \quad \{\beta\} P_2 \{\gamma\}}{\{\alpha\} P_1; P_2 \{\gamma\}}$$

[osłabianie] 
$$\frac{\alpha \implies \alpha' \quad \{\alpha'\} P \{\beta'\} \quad \beta' \implies \beta}{\{\alpha\} P \{\beta\}}$$

Aby udowodnić, że  $\{\alpha\} x := t \{\beta\}$ , trzeba pokazać, że  $\alpha \implies \beta[t/x]$ .

Innymi słowy  $\beta[t/x]$  jest najłabszym pre-warunkiem dla programu  $x := t$  i post-warunku  $\beta$ .

Aby dowieść poprawności programu względem specyfikacji  $\{\alpha\} P \{\beta\}$ :

- oblicz najłabszy pre-warunek  $wp(P, \beta)$  dla programu  $P$  i danego post-warunku  $\beta$  i  $P$
- udowodnij że dany pre-warunek  $\alpha$  implikuje obliczony najłabszy pre-warunek  $wp(P, \beta)$  ( $\alpha \implies wp(P, \beta)$ )
- udowodnij pozostałe obowiązki dowodowe
- udowodnij terminację  $P$

# Why, Caduceus, Krakatoa

Autorzy (wszystkich trzech): J.C. Filliatre, C. Marche

- Why — narzędzie z własnym językiem (taki skromny ocaml ze specyfikacjami), generujące najłagodniejszy pre-warunek i obligacje dowodowe
- Caduceus — parser i tłumacz (front-end) z C do Why
- Krakatoa — parser i tłumacz (front-end) z Javy do Why

Why generuje obligacje dowodowe (back-end) dla:

- systemów wspomagania dowodzenia:  
Coq, PVS, Isabelle/HOL, HOL 4, HOL Light, Mizar
- automatycznych systemów dowodzących:  
Simplify, Alt-Ergo, Yices, Z3, CVC3

Możliwe podejście: jak cokolwiek udowodnimy obligacje to jest OK.