Verifica funzionale di programmi con Dafny

Lorenzo Quellerba

Univeristà degli Studi di Torino

June 2023

Dafny

- Dafny è un linguaggio di programmazione *object oriented* che supporta sia il paradigma imperativo che quello funzionale
- Supporta la specifica formale attraverso precondizioni, postcondizioni, invarianti, varianti e il *framing* della memoria
- La parte di dimostrazioen è gestita da Z3, un SMT solver
- Al termine del processo di verifica un programma Dafny può essere compilato in altri linguaggi tra cui C++, Go, Java
- Il programma finale scritto in Dafny ricade nel paradigma *correct by construction*

Dafny: funzionamento

Tripla di Hoare

$$\{P\}C\{Q\}$$

Se l'asserzione P è vera prima dell'esecuzione del comando C allora l'asserzione Q sarà vera al termine dell'esecuzione

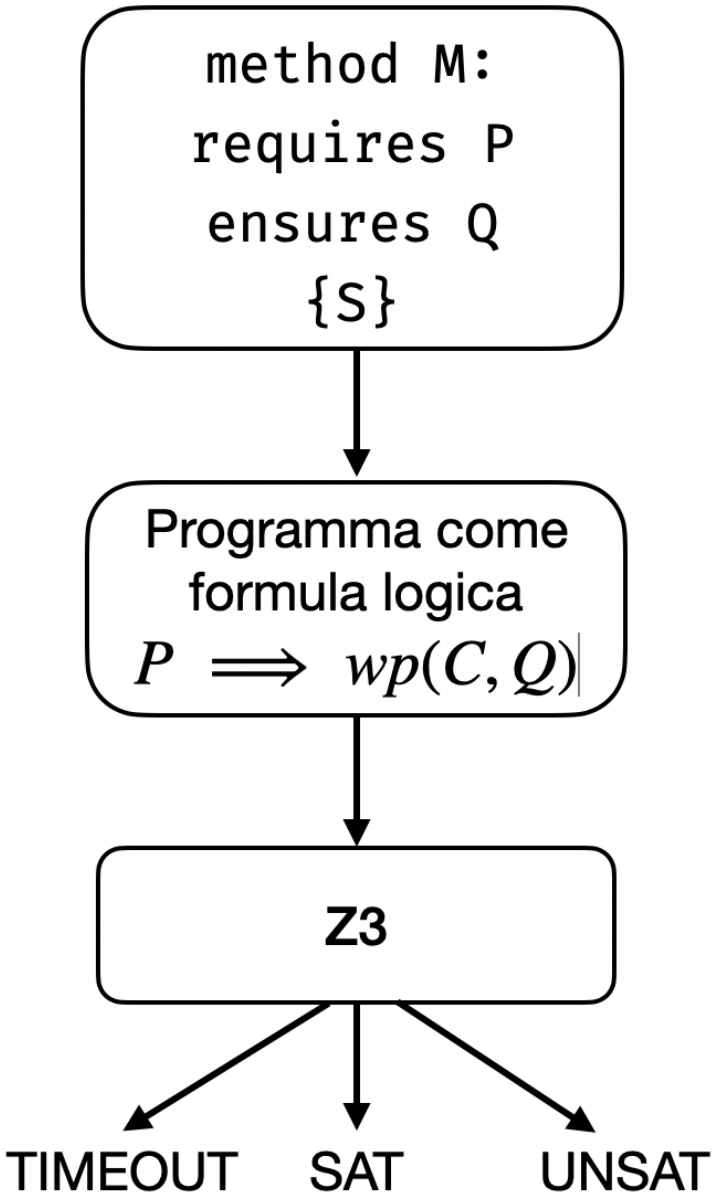
Predicate transformer semantics

La semantica dei *predicate transformer* è una riformulazione della logica di *Floyd-Hoare* che definisce una strategia completa per la costruzione di deduzioni valide

Weakest precondition

Dato un comando C e una postcondizione Q la *weakest precondition* (*wp*) è un predicato ϕ tale per cui per ogni precondizione P, $\{P\}C\{Q\}$ se e solo se $P \implies \phi$

Dafny: funzionamento



Caratteristiche del linguaggio

- Reference types e value types
- Generici
- predicati metodi funzioni classi
-

Albero binario di ricerca

Implementazione dell'albero binario di ricerca

BST: variabili d'istanza

Variabili d'istanza

BST: invariante di struttura

invariante

BST: costruttore

Costruttore

BST: inserimento

Inserimento

BST: ricerca

ricerca

BST: cancellazione

Cancellazione