Verifica funzionale di programmi con Dafny

Lorenzo Quellerba

Univeristà degli Studi di Torino

June 2023

Dafny

- Dafny è un linguaggio di programmazione che supporta sia il paradigma imperativo
- Supporta la verifica funzionale attraverso blabla
- Un programma Dafny può anche essere compilato in altri linguaggi tra cui

Figure: Logo

Verifica funzionale

Qua dentro accenni al problema della verifica funzionale (letteralmente al massimo la tripla di Hoare e i predicate transformer)

Dafny

Qua parli di Dafny

Albero binario di ricerca

Implementazione dell'albero binario di ricerca

Il rene

1. Il rene è un organo del corpo umano
2. È molto importante
3. Non puoi vivere senza entrambi ma con solo uno si

```
□□⟦S, Q⟧  =  □ℒ□⟦S, Q⟧ &&
□□⟦S, true⟧
```

2.9.1. The connection between □ℒ□ and □□

I argued in Section 2.8.0 that □□ and □□ are not the backward and forward formulations of the same function. But there is a way that □ℒ□ and □□ are. It turns out that, for every S, P, and Q, the following holds:

```
□□⟦S, P⟧ ==> Q  if and only
if  P ==> □ℒ□⟦S, Q⟧
```

I have written □□ and □ℒ□ as taking two arguments, a program statement and a predicate. For a fixed S, we can think of □□⟦S, _⟧ and □ℒ□⟦S, _⟧ as functions of a predicate. Whenever such functions satisfy the if-and-only-if relation above, at all. Similarly, if a function has a corresponding lower adjoint, then that lower adjoint is unique, but the function may not have an lower adjoint at all.

The functions of a Galois connection have many nice properties. One of these pertains to how the functions distribute over disjunction and conjunction. Every lower adjoint is *universally disjunctive* and every upper adjoint is *universally conjunctive*. For our functions □□ and □ℒ□, this means:

```
□□⟦S, P0 || P1 || P2 || …⟧ =
  □□⟦S, P0⟧ || □□⟦S, P1⟧ ||
□□⟦S, P2⟧ || …
```

and

```
□ℒ□⟦S, Q0 && Q1 && Q2 && …⟧ =
  □ℒ□⟦S, Q0⟧ && □ℒ□⟦S, Q1⟧
&& □ℒ□⟦S, Q2⟧ && …
```

where I have used the notations P0,

1. Primo elemento

1. Primo elemento
2. Secondo elemento

1. Primo elemento
2. Secondo elemento
3. Terzo elemento

1. Primo elemento
2. Secondo elemento
3. Terzo elemento
4. Quarto elemento

Ciao

Mondo

Titolo della slide

1. Vorrei questo nella prima
2. Anche questo nella prima

Titolo della slide

1. Questo nella seconda
2. Questo nella seconda