

簡單的 Hoare_Logic 驗證 C code 例子

Proof K

Formal Verification

在形式化的規範上
證明系統有期望的性質與描述

Formal?

用一組符號表示多個意思

Formal methods

- Model checking
- Logical Inference
- Others

今天演講著重在 Logical Inference

驗證流程

- 建立抽象模型
- 程式碼規範表示成模型上的規範
- 撰寫證明
- 檢查證明

建立抽象模型

用現有或自定義的公理化理論
描述要驗證的程式碼

現有的公理化理論

- Hoare Logic
- Linear Temporal Logic
- Computer Tree Logic
- others

程式碼規範表示成模型上的規範

將希望驗證的性質
描述成公理化理論中的
lemma 或 theorem

撰寫證明

寫證明步驟驗證 lemma 或 theorem

檢查證明

檢驗證明是否有推理錯誤的地方
如果沒有那就代表程式碼驗證完成
表示程式碼滿足給定的規範

驗證流程的自動化

使用定理證明工具

定理證明工具

又稱

Proof assistant

或

Proof checker

Coq
Isabelle/HOL
Lean

...

今天 Demo 使用
Isabelle/HOL

Isabelle/HOL 語法

Demo 時順便解說

Demo 使用的公理化理論

Hoare Logic

Hoare Logic

Charles Antony Richard Hoare

1969

Hoare triple

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

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

- C 為 command
- P 為未執行 C 前，對程式行為的斷言 (assertion)
- Q 為執行 C 後，對程式行為的斷言 (assertion)

Command

- SKIP
- $X := y$
- $C_0; \dots; C_n$
- IF P THEN Q ELSE R
- WHILE P DO C

Basic rule

Precondition strengthening

$$P \Rightarrow B, \{B\} C \{Q\}$$

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

Basic rule

Postcondition weakening

$$\{ P \} C \{ B \} , B \Rightarrow Q$$

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

SKIP

The skip axiom

$$\{P\}\text{SKIP}\{P\}$$

$X := y$

The Floyd assignment axiom

$$\{P\} X := y \{ \exists v. (X = y[v/X]) \wedge P[v/X] \}$$

The Hoare assignment axiom

$$\{P[y/X]\} X := y \{P\}$$

驗證 $x := y$

$\{P\} x := y \{Q\}$

Prove:

$P \Rightarrow Q[y/x]$

$C_0; \dots; C_n$

The sequencing rule

$\{P\} C_0 \{Q\}, \{Q\} C_1 \{R\}$

$\{P\} C_0 ; C_1 \{R\}$

IF P THEN Q ELSE R

The conditional rule

$\{F \wedge P\} Q \{B\}$, $\{F \wedge \sim P\} R \{B\}$

$\{F\}$ IF P THEN Q ELSE $R \{B\}$

WHILE P DO C

The WHILE-rule

$$\{ I \wedge P \} C \{ I \}$$

$$\{ I \} \text{ WHILE } P \text{ DO } C \{ I \wedge \sim P \}$$

驗證 WHILE P DO C

$\{ F \}$ WHILE P DO C $\{ Q \}$

Prove:

$$\begin{aligned} & F \Rightarrow I \\ & I \wedge \sim P \Rightarrow Q \\ & \{ I \wedge P \} C \{ I \} \end{aligned}$$

Demo

Url:

[https://github.com/KevinKu/Formal-
verification-of-simple-C-code](https://github.com/KevinKu/Formal-verification-of-simple-C-code)