C Timed Information Flow

June 8, 2016

Mikael Elkiær Christensen, michrill@student.aau.dk Mikkel Sandø Larsen, milars11@student.aau.dk

Department of Computer Science
Aalborg University
Denmark





Mikael & Mikkel

Introduction DLM

Coone

Inference

Constraint checking

Polyvariant functi

The CTIF Tool

Process

Time Policies

Evamples

Generalization

Introduction



Embedded devices / IoT

CTIF

Mikael & Mikkel

Introduction

DLM

Overvi

Inference

Constraint abo

Algorithm

Polyvariant functi evaluation

The CTIF Tool

Demonstration

Time Policies

F.......

Generalization

Estimated number of devices:

▶ 2006: 2 billion

▶ 2015: 15 billion

▶ 2020: 200 billion

Usage:

▶ 40.2 % Business/manufacturing

▶ 30.3 % Health care

▶ 8.3 % Retail

▶ 7.7 % Security



Arduino and Raspberry

CTIE

Mikael & Mikkel

Introduction

The CTIF Tool

Estimated sold units:

- ▶ Arduino 1.5 million (2013)¹
- Raspberry Pi 3 million (2014)²

Implications:

- More exposed devices
- More amateur implementations

http://medea.mah.se/2013/04/arduino-fag/

Dept. of Computer Science Aalborg University Denmark



Programmer's perspective

CTIF

Mikael & Mikkel

Introduction

DLM

Scone

Inference

Constraint check

Algorithm

Polyvariant function

The CTIF Tool

P . . .

Time Policies

Evamples

Generalization

Extension to C:

- Simple syntax
- ► Minimal intrusiveness
- Compiler errors
- ► (Visual aids)

Time policies

► Same characteristics as above



Mikael & Mikkel

Introductio

DLM

Scone

Inference

Constraint checking

Polyvariant function

evaluation The CTIF Tool

Process

Demonstration

Time Policies

Generalization

DLM



Abstract lattice

CTIF

Mikael & Mikkel

Introduction

DLM

Overview

Inference

Constraint checkin

Polyvariant function

The CTIF Tool

Demonstration

Time Policies

Generalization

 $\begin{array}{cccc}
 & T & & \\
 & L_1 & L_2 & \\
 & L_2 & L_2 & \\
 & L_1 & L_2 & \\$

23



Label policies

CTIF

Mikael & Mikkel

Introductio

DLM

Overview

Inforonce

Constraint checking

Algorithm
Polyvariant function

evaluation

The CTIF Tool

Demonstration

Time Policies

Examples

$$L_{1} = \{o_{1} \rightarrow r_{1}, r_{2}\} \quad L_{2} = \{o_{1} \rightarrow r_{1}; o_{2} \rightarrow r_{1}\}$$

$$L_{1} \sqcup L_{2} = \{o_{1} \rightarrow r_{1}; o_{2} \rightarrow r_{1}\}$$

$$L_{1} \sqcap L_{2} = \{o_{1} \rightarrow r_{1}, r_{2}\}$$

$$L_{2} \sqsubseteq L_{1} \wedge L_{1} \not\sqsubseteq L_{2}$$



Example lattice

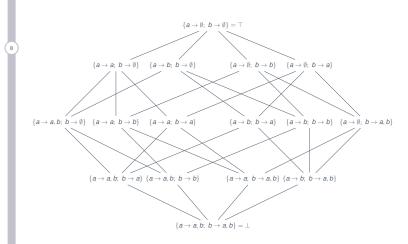
CTIF

Mikael & Mikkel

Overview

The CTIF Tool

Time Policies





Mikael & Mikkel

Introductio

_...

Overv

Scope

Inference

Constraint checking

Polyvariant function evaluation

The CTIF Tool

P IUCESS

Time Policies

Generalizatio

Run-time

- Principal hierarchy
- ► Label as first-class citizen
- ► Function call authority
- Run-time label checking

Integrity

- "Opposite" of privacy
- ► CIF and CBIF employ this



Mikael & Mikkel

Introductio

DLM

Scone

Inference

Constraint checking

Polyvariant functio

The CTIF Tool

Domonstration

Time Policies

Examples

Generalization

Inference



Constraint checking

CTIF

Mikael & Mikkel

ntroductio

0....

осоре

Inferen

Constraint checking

Polyvariant function

The CTIF Tool

Domenstration

Time Policies

Evamples

Generalizatio

Label types:

- ► Policy
- ▶ Variable
- Constant
- ► Composite labels (join/meet)
- ▶ Upper/lower bound

Output channel constraints:

- ► No simple check of reader sets
- ► Constraint for each argument, enabling inference



Algorithm

CTIF

Mikael & Mikkel

Introductio

_...

Overvie

Scope

Inference

Algorithm

Polyvariant functi

Polyvarian

evaluation

The CTIF Tool

Demonstration

Time Policies

Evamples

Generalization

```
Data: A set Q of constraints "L_1 \sqsubseteq L_2"
    foreach "L_1 \sqsubseteq L_2" \in Q do
           let Q' = Q \setminus \{ "L_1 \sqsubset L_2" \}
           Q := Q' \cup unjoin("L_1 \sqsubseteq L_2")
    foreach "L_1 \sqsubseteq L_2" \in Q do
           if L<sub>1</sub> is a variable label then
                  \operatorname{cub}(L_1) := \top
    checked:= false
    while ¬checked do
           checked:= true
           foreach "L_1 \sqsubseteq L_2" \in Q do
10
                  if novar(L_1) \not\sqsubseteq novar(L_2) then
11
                         if L₁ is a variable label then
12
                                \operatorname{cub}(L_1) := \operatorname{cub}(L_1) \cap \operatorname{novar}(L_2)
13
                                checked = false
14
                         else
15
                                FRROR
16
```

Algorithm 1: Label inference from constraint set

23



Polyvariant function evaluation

CTIF

Mikael & Mikkel

landara alta anti-

Introducti

DLM

Overv

acupe

merend

Algorithm

Polyvariant function

evaluation

The CTIF Tool Process

Demonstration

Time Policies

Examples Generalization

Example where inference fails

```
int foo(int {{p->p}} x);
p <- int foo(int x);
int bar(int y) { return foo(y); }</pre>
```

Alternative to function evaluation

- ► Evaluation dependent on each call
- ► Set of constraints based on parameters
- ► Downside: Evaluation of library functions



Mikael & Mikkel

Introductio

DLM

.

Scope

Inference

Constraint checkin

Polyvariant functi

evaluation The CTIF Tool

Process

Demonstration

Time Policies

Examples

Generalization

The CTIF Tool



Mikael & Mikkel

Introduction

DLM

Overvie

Inforono

IIIICICIICC

Constraint checking

Polyvariant functi

evaluation

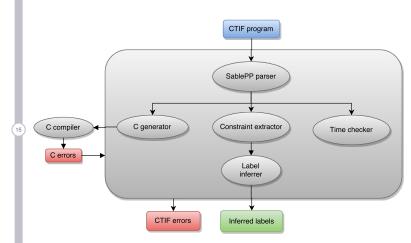
The CTIF Tool Process

Demonstration

Time Policies

_

Examples





Mikael & Mikkel

Introductio

DLM

Overvie

Inforonce

IIIIeieiice

Algorithm

Polyvariant function

evaluation
The CTIF Tool

Demonstration

Time Policies

Time Policies





Mikael & Mikkel

Introductio

DLM

Scope

Inference

Constraint check

Algorithm

Polyvariant function

The CTIF Tool

Process

Time Policies

amnles

Time Policies



u

All

23

Bill calculator

CTIF

Mikael & Mikkel

atroduction

DLM

0----

la fausa a s

Constraint cher

Algorithm

Polyvariant funct

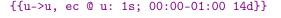
The CTIF Tool

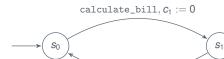
FIUCESS

Time Policies

Examples

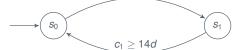
eneralization





calculate_bill, $c_1 := 0, (00 : 00 \le \tau_s < 01 : 00)$?

 $c_1 > 1s$



Dept. of Computer Science Aalborg University Denmark



Password checker

CTIF

Mikael & Mikkel

Introductio

Overview

Scope

Interence

Constraint checkin

Polyvariant function

evaluation

The CTIF Tool Process

Demonstration

Time Policies Examples

Generalization

 $\{\{pc-> 0 \ 10m * 3\}\}$ $\mathtt{get_users}, \mathit{C}_2 := 0$ S1 2 $(c_2 \ge 10m)$? get_users $s_{1,3}$ $(c_2 \ge 10m)$? S_{2,3} $(c_2 \ge 10m)^2$

Dept. of Computer Science Aalborg University Denmark

23



Mikael & Mikkel

Introductio

DLM

0----

Inference

Constraint checking

Algorithm

Polyvariant fund

The CTIF Tool

Pronoss

Demonstration

Time Policies

Examples







2 count

CTIF

Mikael & Mikkel

Introductio

DLM

Saana

Inference

0-------

Almorithm

Aigontiiiii

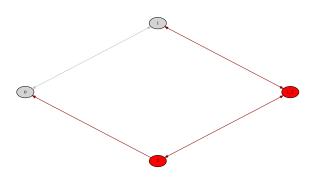
Polyvariant function evaluation

The CTIF Tool

Demonstration

Time Policies

Evamplee





Mikael & Mikkel

Introductio

DLM

0----

Inference

Constraint che

At in

Algoritimi

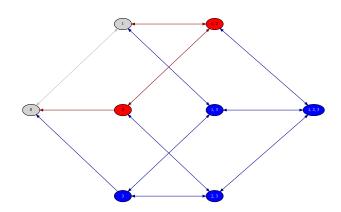
Polyvariant function

The CTIF Tool

Process

Time Policies

Evamplee





23

23

CTIF

Mikael & Mikkel

Introductio

DLM

Coone

Inference

Constraint of

Algorithm

Polyvariant fund

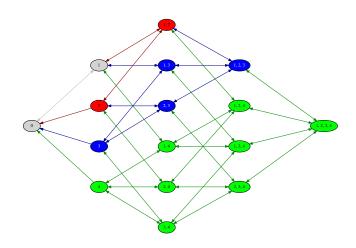
evaluation

The CTIF Tool

Demonstratio

Time Policies

Examples



Questions?

