Abstraktsete domeenide omaduspõhine testimine

Bakalaureusetöö

Simmo Saan

Tartu Ülikool, arvutiteaduse instituut

Juuni, 2018

Ülesehitus

Sissejuhatus

- Staatiline analüüs — programme ei käivitata
  - Vigade otsimine
  - Vigade puudumise tõestamine
- Abstraktne interpretatsioon
  - Ligikaudsed seisundid
  - Teooria garanteerib korrektsuse (ingl. *sound*)
- Analüsaatorites esineb vigu
  - Analüüus ja selle korrektsus rikutud

Sissejuhatus

- Staatiline analüüs — programme ei käivitata
  - Vigade otsimine
  - Vigade puudumise tõestamine
- Abstraktne interpretatsioon
  - Ligikaudsed seisundid
  - Teooria garanteerib korrektsuse (ingl. *sound*)
- Analüsaatorites esineb vigu
  - Analüüus ja selle korrektsus rikutud

Eesmärk

Goblint analüsaatori

- Domeenide omaduspõhine testimine
- Vigade tuvastamine

Intervallid

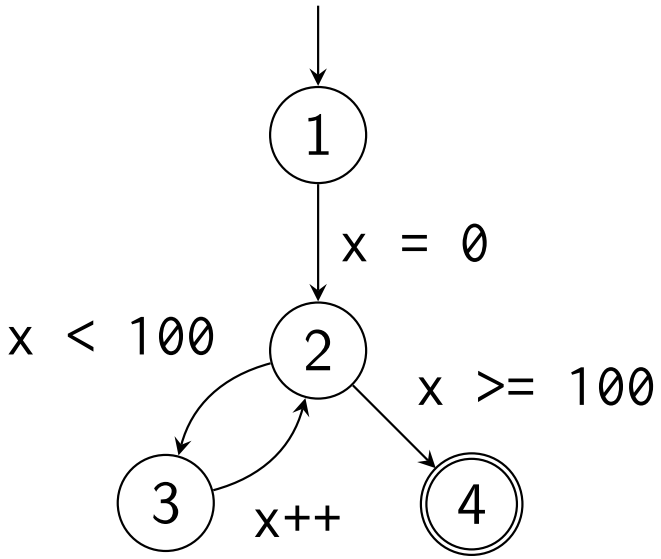
- Täisarvude staatiliseks analüüsiks saab kasutada **intervalle**
  - Näiteks $[0, 3]$, $[-1, 5]$, $[2, 2]$, $[1, +\infty]$, $[-\infty, +\infty]$
- Aritmeetilised tehted intervallidel
  - Näiteks liitmine $[0, 3] + [-1, 5] = [-1, 8]$

Intervallid

- Täisarvude staatiliseks analüüsiks saab kasutada **intervalle**
  - Näiteks $[0, 3]$, $[-1, 5]$, $[2, 2]$, $[1, +\infty]$, $[-\infty, +\infty]$
- Aritmeetilised tehted intervallidel
  - Näiteks liitmine $[0, 3] + [-1, 5] = [-1, 8]$
- Osalise järjestuse seos sisalduvuse kaudu
  - Näiteks $[2, 2] \sqsubseteq [0, 3] \sqsubseteq [-1, 5] \sqsubseteq [-\infty, +\infty]$
  - Kokkuleppeliselt väiksem tähendab täpsemat
- Ühendamise tehe ühendi kaudu
  - Näiteks $[0, 3] \sqcup [5, 7] = [0, 7]$
- Suurim intervall
  - $\top = [-\infty, +\infty]$

Näidisanalüüs intervallidega

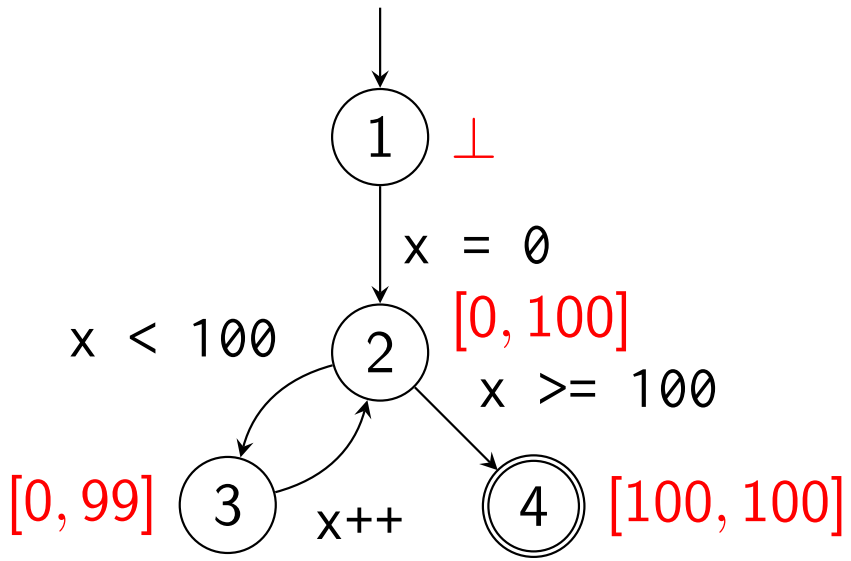
```
int x = 0;
while (x < 100)
    x++;
```



Näidisanalüüs intervallidega

```
int x = 0;
while (x < 100)
    x++;
```

Muutuja x väärtus



Täielikud võred

Domeen peab moodustama **täieliku võre**:

- Elementide hulk $\mathbb{D}$
- Osalise järjestuse seos $\sqsubseteq$
- Ülemise raja tehe $\sqcup$
- Alumise raja tehe $\sqcap$
- Suurim element $\top$
- Vähim element $\bot$

Domeenide omadused

Olgu $\mathbb{D}$ täielik võre, siis iga $a, b, c \in \mathbb{D}$ korral:

Domeenide omadused

Olgu $\mathbb{D}$ täielik võre, siis iga $a, b, c \in \mathbb{D}$ korral:

- $a \sqsubseteq a$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq c$, siis $a \sqsubseteq c$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq a$, siis $a = b$

Domeenide omadused

Olgu $\mathbb{D}$ täielik võre, siis iga $a, b, c \in \mathbb{D}$ korral:

- $a \sqsubseteq a$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq c$, siis $a \sqsubseteq c$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq a$, siis $a = b$

- $a \sqsubseteq a \sqcup b$ ja $b \sqsubseteq a \sqcup b$
- $a \sqcap b \sqsubseteq a$ ja $a \sqcap b \sqsubseteq b$
- kui $a \sqsubseteq c$ ja $b \sqsubseteq c$, siis $a \sqcup b \sqsubseteq c$
- kui $c \sqsubseteq a$ ja $c \sqsubseteq b$, siis $c \sqsubseteq a \sqcap b$

Domeenide omadused

Olgu $\mathbb{D}$ täielik võre, siis iga $a, b, c \in \mathbb{D}$ korral:

- $a \sqsubseteq a$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq c$, siis $a \sqsubseteq c$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq a$, siis $a = b$

- $a \sqsubseteq a \sqcup b$ ja $b \sqsubseteq a \sqcup b$
- $a \sqcap b \sqsubseteq a$ ja $a \sqcap b \sqsubseteq b$
- kui $a \sqsubseteq c$ ja $b \sqsubseteq c$, siis $a \sqcup b \sqsubseteq c$
- kui $c \sqsubseteq a$ ja $c \sqsubseteq b$, siis $c \sqsubseteq a \sqcap b$

- $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$
- $a \sqcup b = b \sqcup a$
- $a \sqcup a = a$
- $a \sqcup (a \sqcap b) = a$

- $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$
- $a \sqcap b = b \sqcap a$
- $a \sqcap a = a$
- $a \sqcap (a \sqcup b) = a$

Domeenide omadused

Olgu $\mathbb{D}$ täielik võre, siis iga $a, b, c \in \mathbb{D}$ korral:

- $a \sqsubseteq a$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq c$, siis $a \sqsubseteq c$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq a$, siis $a = b$

- $\bot \sqsubseteq a$
- $a \sqsubseteq \top$
- $a \sqcup \bot = a$
- $a \sqcap \top = a$

- $a \sqsubseteq a \sqcup b$ ja $b \sqsubseteq a \sqcup b$
- $a \sqcap b \sqsubseteq a$ ja $a \sqcap b \sqsubseteq b$
- kui $a \sqsubseteq c$ ja $b \sqsubseteq c$, siis $a \sqcup b \sqsubseteq c$
- kui $c \sqsubseteq a$ ja $c \sqsubseteq b$, siis $c \sqsubseteq a \sqcap b$

- $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$
- $a \sqcup b = b \sqcup a$
- $a \sqcup a = a$
- $a \sqcup (a \sqcap b) = a$

- $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$
- $a \sqcap b = b \sqcap a$
- $a \sqcap a = a$
- $a \sqcap (a \sqcup b) = a$

Domeenide omadused

Olgu $\mathbb{D}$ täielik võre, siis iga $a, b, c \in \mathbb{D}$ korral:

- $a \sqsubseteq a$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq c$, siis $a \sqsubseteq c$
- kui $a \sqsubseteq b$ ja $b \sqsubseteq a$, siis $a = b$

- $a \sqsubseteq a \sqcup b$ ja $b \sqsubseteq a \sqcup b$
- $a \sqcap b \sqsubseteq a$ ja $a \sqcap b \sqsubseteq b$
- kui $a \sqsubseteq c$ ja $b \sqsubseteq c$, siis $a \sqcup b \sqsubseteq c$
- kui $c \sqsubseteq a$ ja $c \sqsubseteq b$, siis $c \sqsubseteq a \sqcap b$

- $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$
- $a \sqcup b = b \sqcup a$
- $a \sqcup a = a$
- $a \sqcup (a \sqcap b) = a$

- $\bot \sqsubseteq a$
- $a \sqsubseteq \top$
- $a \sqcup \bot = a$
- $a \sqcap \top = a$

Samaväärsed:

1. $a \sqsubseteq b$
2. $a \sqcup b = b$
3. $a \sqcap b = a$

- $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$
- $a \sqcap b = b \sqcap a$
- $a \sqcap a = a$
- $a \sqcap (a \sqcup b) = a$

Omaduspõhine testimine ja Goblint analüsaator

Omaduspõhine testimine:

- QuickCheck
- Hea matemaatiliste tingimuste kontrollimiseks
- Omadused — predikaadid
- Generaatorid — juhuslikud

Omaduspõhine testimine ja Goblint analüsaator

Omaduspõhine testimine:

- QuickCheck
- Hea matemaatiliste tingimuste kontrollimiseks
- Omadused — predikaadid
- Generaatorid — juhuslikud

Goblint analüsaator:

- TÜ, TUM
- Mitmelõimelised C programmid
- Andmejooksud
- Kirjutatud OCaml-is

Goblinti domeenni signatuur

```
module type S =
sig
  type t (* domeeni elementide tüüp *)
  val equal: t -> t -> bool (* seos = *)
  val leq: t -> t -> bool (* seos ⊑ *)
  val join: t -> t -> t (* tehe ⊔ *)
  val meet: t -> t -> t (* tehe ⊓ *)
  val bot: unit -> t (* element ⊥ *)
  val is_bot: t -> bool
  val top: unit -> t (* element ⊤ *)
  val is_top: t -> bool
  val widen: t -> t -> t (* tehe ⨆ *)
  val narrow: t -> t -> t (* tehe ⨅ *)
end
```

Goblinti täiendamine

- Domeenidesse generaatorid:

```
val arbitrary: unit -> t QCheck.arbitrary
```

- Kõik omadused omaduspõhiste testidena
  - Näiteks ülemraja kommutatiivsus ($a \sqcup b = b \sqcup a$):

```
let join_comm = make ~name:"join comm" (pair arb arb)
      (fun (a, b) -> D.equal (D.join a b) (D.join b a))
```

  - `D` testitav domeen
  - `arb` selle generaator

QCheck'i väljund

```
generated error fail pass / total  time  test name
...
[✓]  300     0    0   10 /  100     0.0s trier: leq trans
[✓]  300     0    0    1 /  100     0.0s trier: leq antisym
[✓]  100     0    0  100 /  100     0.0s trier: join leq
[✗]    2     0    1    1 /  100     0.0s trier: join assoc
[✓]  100     0    0  100 /  100     0.0s trier: join comm
[✓]  100     0    0  100 /  100     0.0s trier: join idem
[✓]  100     0    0  100 /  100     0.0s trier: join abs
...
--- Failure ----------------------------------------------

Test trier: join assoc failed (91 shrink steps):

(0, 1, Not {3}([-63,63]))
```

Ülevaatlikud tulemused

Lähenemine	Võrdlemine	Testide arv		
		Kokku	Erindi teke	Mittekehtivad
Alt üles	`equal`	468	∼35	∼75
	`leq`	468	∼35	∼69
Ülalt alla	`equal`	27	0	∼12
	`leq`	27	0	∼12

Ülevaatlikud tulemused

Lähenemine	Võrdlemine	Testide arv		
		Kokku	Erindi teke	Mittekehtivad
Alt üles	`equal`	468	∼35	∼75
	`leq`	468	∼35	∼69
Ülalt alla	`equal`	27	0	∼12
	`leq`	27	0	∼12

Erindi tekkimise ja mittekehtimisel põhjuseid:

1. Viga domeeni implementeerimisel
2. Mittekehtimine teoreetilisel tasandil
3. Teadlik ja dokumenteeritud mittekehtimine
4. Sõltumine teistest probleemsetest omadustest/domeenidest

Trieri domeen

- Goblintis vaikimisi kasutusel
- Elemendid:
  - Üksikud täisarvud
  - Välistatud täisarvude hulgad (ingl. *exclusion set*)

Trieri domeen

- Goblintis vaikimisi kasutusel
- Elemendid:
  - Üksikud täisarvud
  - Välistatud täisarvude hulgad (ingl. *exclusion set*)
- Mittekehtiv ülemraja assotsiatiivsus

$$(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$$

näiteks argumentidel

$$a = 0, \quad b = 1, \quad c = \texttt{Not } \{3\}(\texttt{[-63,63]})$$

- Viga domeeni disainis

Kokkuvõte

Tehtud:

- Domeenide omaduste komplekt
- Goblinti täiendused: omadused ja generaatorid
- Goblinti domeenide testimine
- Tulemuste esmane analüüs

Kokkuvõte

Tehtud:

- Domeenide omaduste komplekt
- Goblinti täiendused: omadused ja generaatorid
- Goblinti domeenide testimine
- Tulemuste esmane analüüs

Järeldus

Omaduspõhist testimist on võimalik efektiivselt rakendada abstraktsetest domeenidest vigade leidmiseks.

Aitäh!

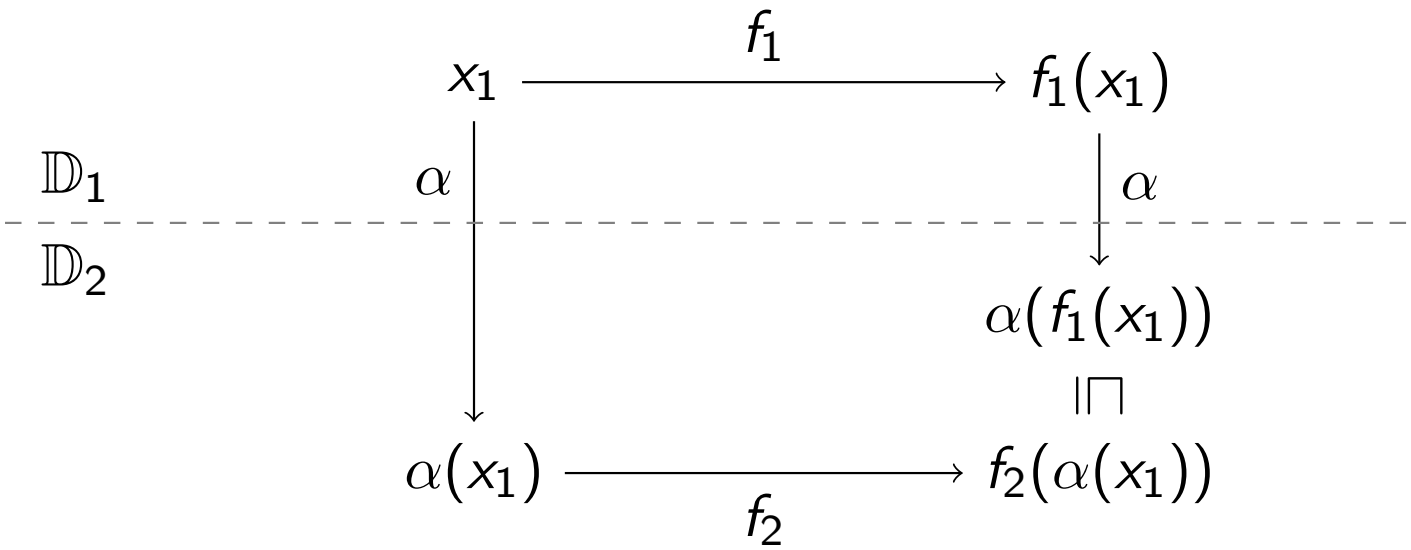
Domeenide omadused (2)

Programmianalüüsis:

- Laiendamise tehe $\sqcup$
  - $a \sqcup b \sqsubseteq a \sqcup b$
- Kitsendamise tehe $\sqcap$
  - $a \sqcap b \sqsubseteq a \sqcap b \sqsubseteq a$

Abstraktsiooni korrektsus:

- Abstraktsioonifunktsioon $\alpha : \mathbb{D}_1 \to \mathbb{D}_2$
- kui $a \sqsubseteq b$, siis $\alpha(a) \sqsubseteq \alpha(b)$
- $\alpha(f_1(x_1)) \sqsubseteq f_2(\alpha(x_1))$
  - f_1, f_2 vastavad monotoonsed tehted



Testitud täisarvude domeenid Goblintis