SAV 2023/24

Predikátová abstrakce – ilustrace

	1. dopředný běh s P_0	2. zpětný běh s substitucí implicitně	3. dopředný běh s $P_1 = \{a>0, a=0\}$
`int a=0;`	$\top$		
`read(&a);`	$\neg(a>0)$		
`int b=a+1;`	$\top$	$\equiv (a+1-1 \neq 0 \wedge a=0)$ $(a \neq 0 \wedge a=0)$ – SAT? ✗	$\top$
`if (a==0) {`	$\top$	$b-1 \neq 0 \wedge a=0$ – SAT? ✓	$\top$
`b=b-1;`	$\neg(a>0)$	$b-1 \neq 0$ – SAT? ✓	$\neg(a>0) \wedge a=0$
`if (b!=0)`	$\neg(a>0)$	$\top \wedge b \neq 0$ – SAT? ✓	$\neg(a>0) \wedge a=0$
`error();`	$\neg(a>0)$	$\top$	$\neg(a>0) \wedge a=0$ ✗
`}`			

Důkaz unsat:
$a=0 \wedge a \neq 0 \equiv \bot$
→ přidáme $a=0$, $a \neq 0$ (stačí $a=0$)

protipříklad nebyl nalezen!!!

- Předpoklad: počáteční mn-a predikátů $P_0 = \{a>0\}$
- žádná implicitní inicializace
- první běh, inicializace: konkr. stav:
  $\top \overset{?}{\Rightarrow} a>0$ ✗
  $\top \overset{?}{\Rightarrow} \neg(a>0)$ ✗
- první krok, první běh
  a) $wp(a>0, a:=0) \equiv 0>0 \equiv \bot$
  $\top$ ↑ aktuální stav $\overset{?}{\Rightarrow} \bot$ – wp(.) ✗

b) $wp(\neg(a>0), a:=0) \equiv \neg(0>0) = \top$

$\top \overset{?}{\Rightarrow} \top$ ✓

- průchod 1. podmínkou, 1. hranou:
  - a) $\top$ (↑ aktuální stav) $\wedge$ $a=0$ (↑ test) $\overset{?}{\Rightarrow}$ $a>0$ ×
  - b) $\top$ $\wedge$ $a=0$ $\overset{?}{\Rightarrow}$ $\neg(a>0)$ ✓
- zpětný chod přes $b = b-1$

  $wp(b \neq 0, b := b-1) \equiv b-1 \neq 0$

– nyní s explicitní substitucí ve zpětném běhu

1. běh s $P_0 = \{a > 0\}$

```
int a = 0;
read(&a);
int b = a+1;
if (a == 0) {
  b = b-1;
  if (b != 0)
    error()
}
```

Kód	1. běh	2. běh	3. dopředný běh
	$\top$		
int a = 0;	$\neg(a>0)$		
read(&a);	$\top$	$\wedge$ $(\exists b_1 : (\exists b_0 : b_0 \neq 0 \wedge b_0 = b_1 - 1) \wedge a = 0) \wedge b = a+1$ SAT ✓ ✗	$\top$
int b = a+1;	$\top$	$\wedge$ $(\exists b_0 : b_0 \neq 0 \wedge b_0 = b - 1) \wedge a = 0$ SAT? ✓	$b = a+1$
if (a == 0) {	$\neg(a>0)$	$\wedge$ $\exists b_0 : b_0 \neq 0 \wedge b_0 = b - 1$ SAT? ✓	$b = a+1 \wedge \neg(a>0) \wedge a = 0 \wedge b = 1 \wedge \neg(b=0)$
b = b-1;	$\neg(a>0)$	$\wedge$ $\top \wedge b \neq 0$ SAT? ✓	$\neg(b=a+1) \wedge \neg(a>0) \wedge a = 0 \wedge \neg(b=1) \wedge b = 0$
if (b != 0) error()	$\neg(a>0)$	$\top$	$\bot$ – unreachable !!!

2. běh

u existující hodnoty platí ... a spočte se každá ...

Důkaz nesplnitelnosti:

- $a = 0 \wedge b_1 = a+1 \Rightarrow b_1 = 1$
- $b_1 = 1 \wedge b_0 = b_1 - 1 \Rightarrow b_0 = 0$
- $b_0 = 0 \wedge b_0 \neq 0 \Rightarrow \bot$

přidáme všechny predikáty z důkazu

$P_1 = \{a > 0,\ a = 0,\ b = a+1,\ b = 1,\ b = b-1,\ b = 0,\ b \neq 0\}$

celý výraz $\equiv \bot$ výraz – negace $b = 0$

Predikátová abstrakce s Craigovými interpolanty

	1. běh s $J_1 = \{a>0\}$	interpolanty	
	$\top$	$\top$	
`int a = 0;`	$\neg(a>0)$	$\top$	
`read(&a);`	$\top$	$\top$	
`int b = a+1;`	$\top$	$b = a+1$	$b = a+1$
`if (a == 0) {`	$\neg(a>0)$	$b = 1$	$\neg(a>0) \wedge b = 1$
`b = b-1;`	$\neg(a>0)$	$b = 0$	$\neg(a>0) \wedge b = 0$
`if (b != 0)`	$\neg(a>0)$	F	× nedosažitelné (F)
`error();`			
`}`			

↑ nové predikáty pro konkrétní řádky

- formule nad cestou:

$\top \wedge$
$a_1 = 0 \wedge$
$[a_2 = ?] \wedge$
$b_1 = a_2 + 1 \wedge$
$a_2 = 0 \wedge$
$b_2 = b_1 - 1 \wedge$
$b_2 \neq 0$

- reprezentace read ve formuli by neměla být – mělo by tam být "$\top$"

φ / ψ – postupně posouvat hranici φ/ψ

Hledáme I:
- $\varphi \Rightarrow I$
- $\neg(\psi \wedge I)$
- I nad proměnnými sdílenými φ a ψ

sdílené prom.: b_1, a_2

sdíl. prom.: b_1

sdíl. prom.: b_2

celá formule φ – UNSAT