2017013569

11.

~~(1) ① $\{I\} \| F, C \vee P \to \{I, P\} \| F, C \vee P$~~

~~② $\{I\} \| F, C \vee \neg P \to \{I, \neg P\} \| F, C \vee \neg P$~~

~~if $I \not\models C$, P undefined in I~~

($C = C' \vee l$, $I \not\models C'$, l undef)

① 对当前I，∃一个C，C在I下unit，即C中除了一个literal未赋值外，其余的literal均为false → backtrack

② 好处：减少decide次数，提高效率

比如：$P_1 \vee P_2 \vee \neg P_3$，之前decide了 $\neg P_1, \neg P_2$，如果有unit-propagation：直接得到 P_3=false，

否则可能先decide P_3 再backtrack，效率低

(2)

① 回溯步骤不同：DPLL 使用backtrack，回退到上个decide

DPLL(T) 使用backjump

② 回溯后处理不同：DPLL(T) 会记录造成冲突的子式，并将其作为下的一个新clause（记忆学习）

而DPLL不会

③ 算法思想不同：DPLL只简单的回溯到上一个步骤，不做记录

DPLL(T) 则试图找到冲突根源，并且记录冲突产生的原因

扫描全能王 创建

2017013519

12.

(1)

① 用 $f_a(j)$ 替 $a[j]$

$a\langle i \triangleleft e\rangle[j] = e \land i \neq j \land f_a(j) \neq e$

② 分类讨论：

①：$i=j$

$e=e \land i\neq j \land f_a(j)\neq e \land i=j$ …①

（显然 $i\neq j$ 与 $i=j$ 矛盾）

②：$i\neq j$ $a[j]=e \land i\neq j \land f_a(j)\neq e$ …②

即 $f_a(j)=e \land i\neq j \land f_a(j)\neq e$

（显然有 $f_a(j)=e$ 与 $f_a(j)\neq e$ 矛盾）

∴ unsat

构造等价类：$\{\{i\},\{e\},\{j\},\{f_a(j)\}\}$

根据①，合并得 $\{\{i,j\},\{e\},\{f_a(j)\}\}$，

与 $i\neq j$ 矛盾，unsat

构造新价类 $\{\{i\},\{e\},\{j\},\{f_a(j)\}\}$

根据 $f_a(j)=e$，

合并得 $\{\{e,f_a(j)\},\{i\},\{j\}\}$

与 $f_a(j)\neq e$ 矛盾，unsat

(2) $\neg\phi = a\langle i \triangleleft e\rangle[j]\neq e \lor i=j \lor a[j]=e$，设 $\neg\phi = F$，只需证 F valid 即可

证明：

1	$I,\alpha \not\models F$	assumption
2	$I,\alpha \not\models a\langle i\triangleleft e\rangle[j]\neq e$	1, ∨
3	$I,\alpha \not\models i=j$	1, ∨
4	$I,\alpha \not\models a[j]=e$	1, ∨
~~5~~	~~$I,\alpha \models a\langle i\triangleleft e\rangle[j]=e$~~	
5	$I,\alpha \models i\neq j$	3, ¬
6	$I,\alpha \models a\langle i\triangleleft e\rangle[j]=a[j]$	5, r.o.w.2
7	$I,\alpha \models a\langle i\triangleleft e\rangle[j]=e$	2, ¬
8	$I,\alpha \models a[j]=a\langle i\triangleleft e\rangle[j]$	6, symm
9	$I,\alpha \models a[j]=e$	7, 8, trans
10	$\perp$	4, 9

∴ 有 $F=\neg\phi$ 为 valid 得证

因此有 ϕ unsat

13. 1. ~~假设程序的某个前后条件~~

① 秩函数为 $n+1-i$

~~$\downarrow n+1-i$~~ 从循环中仅一个 basic path:

$\{n+1-i \geq 0\}$

$\downarrow n+1-i$

$c_0: T := Y$

$c_1: Y := Y+X$

$c_2: X := T$

$c_3: i := i+1$

$\downarrow n+1-i$

VC 为:

$n+1-i \geq 0 \rightarrow wlp(c_0; c_1; c_2; c_3, n+1-i < n'+1-i')$ $[n/n'], [i/i']$

$wlp(c_3, n+1-i < n'+1-i')$

$= n+1-i-1 < n'+1-i'$

$wlp(c_2, n+1-i-1 < n'+1-i')$

$= n+1-i-1 < n'+1-i'$

$wlp(c_1, n+1-i-1 < n'+1-i')$

$= n+1-i-1 < n'+1-i'$

$wlp(c_0, n+1-i-1 < n'+1-i')$

$= n+1-i-1 < n'+1-i'$

根据 wlp 的 seq 规则, 只需 wlp 为 $n+1-i-1 < n+1-i$

最后 VC 为 $n+1-i \geq 0 \rightarrow n+1-i-1 < n+1-i$

$\because n+1-i-1 < n+1-i$ 恒为 true

∴ VC 成立, 终止

② 证明:

只需证 $\{i \geq 0 \wedge Y = fib(i) \wedge X = fib(i-1) \wedge i \neq n+1\}\ c_0; c_1; c_2; c_3$ $\{Y = fib(i) \wedge i \geq 0 \wedge X = fib(i-1)\}$ 有效

$wlp(c_3, I)$

$= wlp3 = Y = fib(i+1) \wedge i+1 \geq 0 \wedge X = fib(i)$

$wlp(c_2, wlp3)$

$= wlp2 = Y = fib(i+1) \wedge i+1 \geq 0 \wedge T = fib(i)$

$wlp(c_1, wlp2)$

$= wlp1 = Y+X = fib(i+1) \wedge i+1 \geq 0 \wedge T = fib(i)$

$wlp(c_0, wlp1)$

$= wlp0 = Y+X = fib(i+1) \wedge i+1 \geq 0 \wedge Y = fib(i)$

根据 wlp 的 seq 性质, 有 $wlp0 = wlp(c_0; c_1; c_2; c_3, I)$

要证 $\{I \wedge b\}\ c_0; c_1; c_2; c_3\ \{I\}$ 有效, 仅需证 $(I \wedge b) \rightarrow wlp0$ valid

⟸ 根据 fib 定义与 T_Z 性质, 可得:

$\begin{cases} i \geq 0 \Rightarrow i+1 \geq 1 \\ Y = fib(i) \wedge X = fib(i-1) \wedge i \geq 0 \Rightarrow Y+X = fib(i+1) \end{cases}$

∴ 有

$i \geq 0 \wedge Y = fib(i) \wedge X = fib(i-1) \wedge i \neq n+1 \Rightarrow Y+X = fib(i+1)$

$i \geq 0 \wedge Y = fib(i) \wedge X = fib(i-1) \wedge i \neq n+1 \Rightarrow i+1 \geq 0$

$i \geq 0 \wedge Y = fib(i) \wedge X = fib(i-1) \wedge i \neq n+1 \Rightarrow Y = fib(i)$

, 有 $(I \wedge b) \Rightarrow wlp(c_0; c_1; c_2; c_3, I)$, $\{I \wedge b\}\ c_0; c_1; c_2; c_3\ \{I\}$ valid

∴ 有 I 为循环不变式, 得证

13. ① 证明: $wlp(P_{fib}, X=fib(n))$ 2017013569

令内部循环为P_{while}

$= wlp(i:=1; X:=1; Y:=1; P_{while}, X=fib(n))$

$wlp(P_{while}, X=fib(n)) = i\geq 0 \wedge Y=fib(i) \wedge X=fib(i-1) = I$

$vc(P_{while}, X=fib(n))$

$$= \begin{cases} I\wedge\neg b \Rightarrow Q \\ I\wedge b \Rightarrow wlp(c_0;c_1;c_2;c_3, I) \end{cases}$$

$$= \begin{cases} i\geq 0 \wedge Y=fib(i) \wedge X=fib(i-1) \wedge i=n+1 \Rightarrow X=fib(n) \quad —① \\ i\geq 0 \wedge Y=fib(i) \wedge X=fib(i-1) \wedge i\neq n+1 \Rightarrow wlp(c_0;c_1;c_2;c_3, I) \quad —② \end{cases}$$

$wlp(Y:=1, I) = i\geq 0 \wedge 1=fib(i) \wedge X=fib(i-1) = wlp_{new2}$

$wlp(X:=1, wlp_{new2}) = i\geq 0 \wedge 1=fib(i) \wedge 1=fib(i-1) = wlp_{new1}$

$wlp(i:=1, wlp_{new1}) = 1\geq 0 \wedge 1=fib(1) \wedge 1=fib(0) = wlp_{new0}$

$vc(Y:=1, I) = \emptyset$

$vc(X:=1, wlp_{new2}) = \emptyset$

$vc(i:=1, wlp_{new1}) = \emptyset$

综上: 整体 $wlp = wlp(P_{fib}, X=fib(n)) = 1\geq 0 \wedge 1=fib(1) \wedge 1=fib(0)$

根据vc的seq规则: 整体vc为:

$$\begin{cases} true \Rightarrow 1\geq 0 \wedge 1=fib(1) \wedge 1=fib(0) \quad —① \\ i\geq 0 \wedge Y=fib(i) \wedge X=fib(i-1) \wedge i=n+1 \Rightarrow X=fib(n) \quad —② \\ i\geq 0 \wedge Y=fib(i) \wedge X=fib(i-1) \wedge i\neq n+1 \Rightarrow Y+X=fib(i+1) \wedge i+1\geq 0 \wedge Y=fib(i) \quad —③ \end{cases}$$

对①: 有$1\geq 0$, $1=fib(1)$, $1=fib(0)$均为true.
$true \Rightarrow true$ 成立

对②: $\because X=fib(i-1) \wedge i=n+1 \Rightarrow X=fib(n)$
$\therefore$ 有②成立

对③: $\because Y=fib(i) \wedge X=fib(i-1) \wedge i\geq 0 \Rightarrow Y+X=fib(i+1)$
又 $i\geq 0 \Rightarrow i+1\geq 0$
$Y=fib(i) \Rightarrow Y=fib(i)$, 有③成立

综上, 因为所有vc均成立,
有valid hoare三元组
$\{T\}P_{fib}\{X=fib(n)\}$成立

2017013569

14.

① (a) 终止于 $\sigma[x \mapsto 5]$，结果信号为 $\ominus$

(b) 终止于 $\sigma[x \mapsto 6]$，结果信号为 $\ominus$

(c) 终止于 $\sigma[x \mapsto 6]$，结果信号为 $\otimes$

②: a. invalid

a. $\sigma[x \mapsto 0]$ 经过 try (throw; x:=1) catch x:=2x+1，终止于 $\sigma[x \mapsto 1]$，

且结果信号为 $\ominus$，x=1 不满足 x=2，∴ invalid

b. valid: 对于 y<0，必定进入 while y≤0 do throw end 的循环，

并抛出异常，此时 y 不变，仍 <0，

之后执行 y:=y+1; throw，

y 变为 y_0+1，结果信号为 ⊥，

而对于 y_0 <0，y_0+1 ≤0 成立，

因此 valid

c. valid

如果一开始 z≤0，则不进入循环，结果信号为 $\ominus$，z≤0 符合

如果一开始 z≥1，则会在循环中抛出异常，并且抛出时 z 必 =1，符合 z=1

∴ valid

扫描全能王 创建

14. ③: 2017013569

(H-throw) $$\frac{}{\{P\}\ \text{throw}\ \{\bot\}\{P\}}$$

~~(H-try-catch)~~

(H-try-catch) $$\frac{\{P\}\,c_1\,\{Q_1\}\{R_1\} \qquad \{R_1\}\,c_2\,\{Q_2\}\{R_2\}}{\{P\}\ \text{try}\ c_1\ \text{catch}\ c_2\ \text{end}\ \{Q_1 \vee Q_2\}\ \{R_2\}}$$

证明: ~~wp(try fi)~~ X

设整体代码为 c_{full}

if X>0 then X:=0 else throw fi 为 c_{try}

X:=-1; throw 为 c_{catch}

推导树如下: (其中 R_a, R_b 为任意条件)

$$\frac{\dfrac{\dfrac{}{\{X>0\}X:=0\{X=0\}\{R_a\}} \quad \dfrac{}{\{X\le 0\}\text{throw}\{\bot\}\{X\le 0\}}}{\{T\}\ \text{if}\ X>0\ \text{then}\ X:=0\ \text{else throw fi}\ \{X=0\}\{X\le 0\}} \qquad \dfrac{\dfrac{}{\{X\le 0\}X:=-1\{X=-1\}\{R_b\}} \quad \dfrac{}{\{X=-1\}\text{throw}\{\bot\}\{X=-1\}}}{\{X\le 0\}\ X:=-1;\text{throw}\ \{\bot\}\{X=-1\}}}{\{T\}\ \text{try}\ c_{try}\ \text{catch}\ c_{catch}\ \text{end}\ \{X=0\}\ \{X=-1\}}$$

其中: P为T, Q_1为$X=0$, R_1为$X\le 0$, Q_2为$\bot$, R_2为$X=-1$

$\{P\}c_1\{Q_1\}\{R_1\}$ $\{R_1\}c_2\{Q_2\}\{R_2\}$

$Q_1 \vee Q_2$为$X=0$,

$\{P\}$ try c_1 catch c_2 end $\{Q_1\vee Q_2\}\{R_2\}$

综上, 该Hoare四元组 valid