

Sviluppo di Software Sicuro - S³ Analisi dei flussi informativi

Corso di Laurea Magistrale in
Sicurezza Informatica: Infrastrutture e Applicazioni
Università di Pisa – Polo di La Spezia
C. Montangero
Anno accademico 2009/10

Sommario

- Concetti introduttivi
- Comandi elementari
- Comandi composti
- Stabilità e terminazione
- Conclusioni

S³ 2009/10 – Flussi informativi

INTRODUZIONE

S3: SPARK - C.Montangero - Copyright 2010

3

Contesto

- Dato un blocco di comandi S
 - *contesto* = elenco alfabetico delle variabili usate
- I flussi informativi vengono *calcolati*
 - grazie a composizione di matrici booleane
 - 1 per vero, 0 per falso
 - indicizzate dalle variabili nel contesto
- A partire dai comandi elementari
- Convenzioni
 - Variabili di programma: maiuscole: A, B, ... X, W,...
 - Meta variabili: minuscole: v, t, ...

S3: SPARK - C.Montangero - Copyright 2010

4

Esempio

S: if W>0 then X:=Y+Z else Z:=2 end if;

- Ci interessa sapere:
 - cosa *può* essere modificato
 - cosa *può* essere conservato
 - cosa *può* influenzare che cosa (derives)
- Per esempio, in S:
 - X può essere modificato
 - X può essere conservato
 - X può dipendere da Y

S3: SPARK - C.Montangero - Copyright 2010

5

Matrice delle *definizioni* D^S

- Matrice diagonale
- $D^S_{v,v} = 1$ sse S *può* definire v
- Esempio

S': if W>0 then X:=Y+Z else Z:=2 end if;

	X	Y	Z	W
X	1	0	0	0
Y	0	0	0	0
Z	0	0	1	0
W	0	0	0	0

$D^{S'} =$

S3: SPARK - C.Montangero - Copyright 2010

6

Matrice delle var. *preservate* P^S

- Matrice diagonale
- $P^S_{v,v} = 1$ sse s può preservare il *valore iniziale* di v
- Esempio

```
S': if W>0 then X:=Y+Z else Z:=2 end if;
```

	X	Y	Z	W
X	1	0	0	0
Y	0	1	0	0
Z	0	0	1	0
W	0	0	0	1

S3: SPARK - C.Montangero - Copyright 2010

7

Matrice delle *ridefinizioni* R^S

- Non diagonale, in generale
- $R^S_{v,t} = 1$ sse il *valore finale* di t può dipendere dal *valore iniziale* di v

Esempio

```
S': if W>0 then X:=Y+Z else Z:=2 end if;
```

	X	Y	Z	W
X	1	0	0	0
Y	1	1	0	0
Z	1	0	1	0
W	1	0	1	1

S3: SPARK - C.Montangero - Copyright 2010

8

Preliminari

- Siano:
 - I la matrice identità (1 nella diagonale)
 - O la matrice nulla (tutti 0)
- Le operazioni logiche or, and vengono estese puntualmente alle matrici
- Con MN indichiamo il prodotto righe x colonne
 - or = somma, and = prodotto
 - $(MN)_{ij} = \text{or}_k (M_{ik} \text{ and } M_{kj})$
 - $(MN)_{ij} = 1$ sse esiste almeno una coppia di 1 con lo stesso indice nella riga e nella colonna

S3: SPARK - C.Montangero - Copyright 2010

9

Approccio

- Comandi elementari
 - null, assegnamento, chiamata procedura
 - matrici definite in base alla semantica dei comandi
 - In HIS, R è definita in funzione di matrici ausiliarie, ottenibili per analisi sintattica delle espressioni
- Comandi composti
 - approccio compositazionale
 - matrici definite in funzione delle matrici delle parti

S3: SPARK - C.Montangero - Copyright 2010

10

S³ 2009/10 – Flussi informativi

COMANDI ELEMENTARI

S3: SPARK - C.Montangero - Copyright 2010

11

Comandi elementari: null

- Possiamo porre:
- $D^{\text{null}} = \mathbb{O}$: null non modifica nulla
- $P^{\text{null}} = \mathbb{I}$: null non modifica nulla
- $R^{\text{null}} = \mathbb{I}$: null non modifica nulla
 - il valore finale di ogni variabile (può) dipende(re) dal suo valore iniziale

S3: SPARK - C.Montangero - Copyright 2010

12

Comandi elementari: procedure

- Possiamo sfruttare le annotazioni

```
procedure P(X : out Float; I: in Integer )
--# global in out Z;
--# derives X from I & Z from *,I;
```

- La dichiarazione definisce le matrici per P:
- Il contesto è dato dai parametri e dalle globali
- NB: le globali stanno anche nel contesto del chiamante

D	I	X	Z	P	I	X	Z	R	I	X	Z
I	0			I	1			I	1	1	1
X		1		X		0		X			
Z			1	Z			1	Z			1

S3: SPARK - C.Montangero - Copyright 2010

13

Comandi elementari: procedure (2)

- La chiamata associa argomenti e parametri
- Assumiamo {X,Y,Z,W} come contesto del chiamante

```
P(X,Y)
```

- Nelle tabelle, le colonne relative agli argomenti out vengono sostituite da quelle dei corrispondenti parametri
- Per le altre: solo gli out sono definiti, e quindi
 - in D, tutti 0
 - in P, tutti 1
 - in R, 1 sulla diagonale (valore finale = valore iniziale)
- non le formalizzeremo...

S3: SPARK - C.Montangero - Copyright 2010

14

Esempio

D	I	X	Z	P	I	X	Z	R	I	X	Z
I	0			I	1			I	1	1	1
X		1		X		0		X			
Z			1	Z			1	Z			1

matrici procedura

	X	I				X	I				X	I		
D	X	Y	Z	W	P	X	Y	Z	W	R	X	Y	Z	W
X	X				X					X				
I	Y				Y					Y				
Z					Z					Z				
W				0	W				1	W				1

matrici
chiamata:
solo contesto
chiamata

S3: SPARK - C.Montangero - Copyright 2010

15

Esempio

D	I	X	Z	P	I	X	Z	R	I	X	Z
I	0			I	1			I	1	1	1
X		1		X		0		X			
Z			1	Z			1	Z			1

matrici procedura

	X	I				X	I				X	I		
D	X	Y	Z	W	P	X	Y	Z	W	R	X	Y	Z	W
X	X	1			X	0				X				
I	Y		0		Y		1			Y	1	1	1	
Z				1	Z			1		Z			1	
W					0	W			1	W				1

matrici
chiamata

S3: SPARK - C.Montangero - Copyright 2010

16

Assegnamento

$v := e(\Sigma)$, dove Σ è l'insieme delle variabili che appaiono in e

- $D^v := e(\Sigma)_{i,i} = 1$ sse $i=v$
- $P^v := e(\Sigma)_{i,i} = 1$ sse $i \neq v$
- $R^v := e(\Sigma)_{i,j} = 1$ sse $(j=v \text{ e } i \text{ in } \Sigma) \text{ o } P_{i,j} = 1$
- Σ comprende gli argomenti di eventuali chiamate di funzioni
– no effetti collaterali

S3: SPARK - C.Montangero - Copyright 2010

17

Assegnamento: esempio

S1: $X := Y + Z$ $\Sigma = \{Y, Z\}$

- $D^{X:=Y+Z}_{i,i} = 1$ sse $i=X$
- $P^{X:=Y+Z}_{i,i} = 1$ sse $i \neq X$
- $R^{X:=Y+Z}_{i,j} = 1$ sse $(j=X \text{ e } i \text{ in } \{Y, Z\}) \text{ o } P_{i,j} = 1$

D	X	Y	Z	W	P	X	Y	Z	W	R	X	Y	Z	W
X	1				X					X				
Y					Y		1			Y	1	1		
Z					Z			1		Z	1		1	
W					W				1	W				1

S3: SPARK - C.Montangero - Copyright 2010

18

Assegnamento: esempio

S2: $W:=2*X \quad \Sigma = \{X\}$

- $D^{W:=2*X}_{i,i} = 1$ sse $i=W$
- $P^{W:=2*X}_{i,i} = 1$ sse $i \neq W$
- $R^{W:=2*X}_{i,j} = 1$ sse $(j=W \text{ e } i=X)$ o $P_{i,j} = 1$

D	X	Y	Z	W	P	X	Y	Z	W	R	X	Y	Z	W
X					X	1				X	1			1
Y					Y		1			Y		1		
Z					Z			1		Z			1	
W				1	W					W				

S3: SPARK - C.Montangero - Copyright 2010

19

S³ 2009/10 – Flussi informativi

COMANDI COMPOSTI

S3: SPARK - C.Montangero - Copyright 2010

20

Sequenza

$S' S''$

- Si compongono le matrici dei singoli blocchi
- $D^{S' S''} = D^{S'}$ or $D^{S''}$
- $P^{S' S''} = P^{S'}$ and $P^{S''}$
- $R^{S' S''} = R^{S'} R^{S''}$, infatti
 - $R^{S' S''}_{i,j} = \text{or}_k (R^{S'}_{i,k} \text{ and } R^{S''}_{k,j})$, infatti
 - $R^{S' S''}_{i,j} = 1$ sse esiste k tale che
 - j può dipendere da k , che può dipendere da i
 - ergo, sse j può dipendere da i

S3: SPARK - C.Montangero - Copyright 2010

21

Sequenza: esempio

$S = S1 \ S2 = X:=Y+Z; W:=2*X;$

- $D^S = D^{S1}$ or D^{S2}

X Y Z W		X Y Z W		X Y Z W	
X	1	X		X	1
Y		or Y		is Y	
Z		Z		Z	
W		W	1	W	1

- $P^S = P^{S1}$ and P^{S2}

X Y Z W		X Y Z W		X Y Z W	
X		X	1	X	
Y	1	and Y	1	is Y	1
Z	1	Z	1	Z	1
W	1	W		W	

S3: SPARK - C.Montangero - Copyright 2010

22

Sequenza: esempio

$S = S1 \ S2 = X:=Y+Z; W:=2*X;$

- $R^S = R^{S1} R^{S2}$

S1: X:=Y+Z					S2: W:=2*X				S1 S2			
X	Y	Z	W		X	Y	Z	W	X	Y	Z	W
X					1			1				
Y	1	1				1			1	1		1
Z	1		1				1		1		1	1
W				1								

- ricordatevi di S.
Tommaso

S3: SPARK - C.Montangero - Copyright 2010

23

Condizionale

$C = \text{if } e(\Sigma) \text{ then } S' \text{ else } S'' \text{ end if;}$

- $D^C = D^{S'} \text{ or } D^{S''}$
- $P^C = P^{S'} \text{ or } P^{S''}$
- Si deve tener conto della dipendenza da e
 - tutte le variabili definite in C dipendono anche dalle variabili in e
- $R = R^{e(\Sigma)} \text{ or } R^{S'} \text{ or } R^{S''}$, dove
 - $R^{e(\Sigma)}_{i,j} = 1$ sse $D_{j,j} = 1$ e i in Σ

S3: SPARK - C.Montangero - Copyright 2010

24

Condizionale : esempio

C': if W>0 then X:=Y+Z else Z:=2 end if;

- $D^{C'} = D^{X:=Y+Z} \text{ or } D^{Z:=2}$

X Y Z W

X 1

Y

Z

W

X

or Y

Z

W

X Y Z W

X 1

is Y

Z 1

W
- $R^{W>0}$

X Y Z W

X

Y

Z

W 1 1

Condizionale : esempio (2)

C': if W>0 then X:=Y+Z else Z:=2 end if;

- $R' = R^{X:=Y+Z} \text{ or } R^{Z:=2}$

R X:=Y+Z

X Y Z W

X

Y 1 1

Z 1 1

W

R Z:=2

X Y Z W

1

or 1

1

1

X Y Z W

1

1 1

1 1

1
- $R^{C'} = R^{e(\Sigma)} \text{ or } R'$

R'

X Y Z W

X 1

Y 1 1

Z 1 1

W

Re

X Y Z W

1

or

1 1

1 1

1 1 1

X Y Z W

1

1 1

1 1

1 1 1
- Esercizio: if then

Cicli

$W = \text{while } e(\Sigma) \text{ loop } S \text{ end loop};$

- $D^W = D^S$ (se si entra)
- $P^W = \mathbb{I}$ (se non si entra)
- R si ottiene per sviluppo del while con if then:

$W = \text{if } e(\Sigma) \text{ then } S \text{ W end if};$

S3: SPARK - C.Montangero - Copyright 2010

27

R in un ciclo

$W = \text{while } e(\Sigma) \text{ loop } S \text{ end loop};$

$W = \text{if } e(\Sigma) \text{ then } S \text{ W end if};$

$$\begin{aligned}
 R^W &= R^{e(\Sigma)} \text{ or } \mathbb{I} \text{ or } R^S R^W \\
 &= \mathbb{I}(R^{e(\Sigma)} \text{ or } \mathbb{I}) \text{ or } R^S (R^{e(\Sigma)} \text{ or } \mathbb{I} \text{ or } R^S R^W) \\
 &= \mathbb{I}(R^{e(\Sigma)} \text{ or } \mathbb{I}) \text{ or } R^S (R^{e(\Sigma)} \text{ or } \mathbb{I}) \text{ or } (R^S)^2 R^W \\
 &= \dots \\
 &= (R^{e(\Sigma)} \text{ or } \mathbb{I}) (\mathbb{I} \text{ or } R^S \text{ or } (R^S)^2 \text{ or } \dots) \\
 &= (R^{e(\Sigma)} \text{ or } \mathbb{I}) (R^S)^*
 \end{aligned}$$

dove $(R^S)^*$ è la chiusura riflessiva e transitiva di R^S

S3: SPARK - C.Montangero - Copyright 2010

28

e allora?

- La chiusura riflessiva e transitiva di R
 - si calcola in $O(n^3)$ – Teorema di Warshall – n variabili
- Esempio: GCD di C e D

```
while D/=0 loop R:=C rem D; C:=D; D:=R; end loop;
```

- Confronto Rs e Rw
- la var R può dipendere dal suo valore iniziale
 - se non si entra
- C pure, se si entra,
 - tramite D, dal secondo giro in poi
- $D = C \text{ rem } D$

	Re or I			Rs			Rs*=Rw		
	C	D	R	C	D	R	C	D	R
C	1			1	1		1	1	1
D	1	1	1	1	1	1	1	1	1
R			1						1

S3: SPARK - C.Montangero - Copyright 2010

29

Un paio di commenti

- La chiusura riflessiva e transitiva spesso uguale a R^{corpo}
- Se ci sono variabili immodificate in e , non è così:
- siano M, N i valori iniziali di C e D:

```
while D/=M loop R:=C rem D; C:=D; D:=R; end loop;
```

- sopra, Examiner non segnala errori (serve più semantica)
- Però può individuare errori legati al mancato aggiornamento della guardia: ad esempio

```
while D/=0 loop R:=M rem N; C:=D; D:=R; end loop;
```

- Nozione di *stabilità* della guardia:
 - se si entra nel ciclo, *non si termina*

S3: SPARK - C.Montangero - Copyright 2010

30

Flusso di un sottoprogramma

- Calcolabile per composizione
 - confronto con le annotazioni
 - errori se discrepanti
- Altri costrutti
 - per traduzione a quelli già visti
 - vincoli di SPARK essenziali
- Variabili composite
 - considerate globalmente
 - aggiornate se si aggiorna una parte (grana grossa)
 - vincoli SPARK essenziali
 - esempio: importazione solo al primo livello

S3: SPARK - C.Montangero - Copyright 2010

31

S³ 2009/10 – Flussi informativi

STABILITA' E TERMINAZIONE

S3: SPARK - C.Montangero - Copyright 2010

32

Stabilità di una guardia

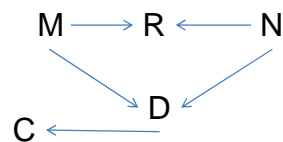
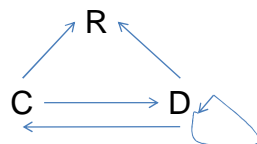
- Due passi:
 - stabilità delle variabili
 - stabilità della guardia
- Rappresentazione grafica della R (del corpo)
 - un arco orientato da i a j se $R_{ij} = 1$
 - il valore di i può contribuire al valore di j
 - solo le variabili del corpo

S3: SPARK - C.Montangero - Copyright 2010

33

Esempio - GCD

$R := C \text{ rem } D; C := D; D := R;$



$R := M \text{ rem } N; C := D; D := R;$

S3: SPARK - C.Montangero - Copyright 2010

34

Variabili stabili



- Una var è *stabile* se *non* è raggiungibile da un ciclo
 - di indice i , se i è la lunghezza del cammino per arrivarci
- A sinistra non ci sono variabili stabili
- A destra sono tutte stabili
 - M,N indice 0; R, D indice 1; C indice 2

S3: SPARK - C.Montangero - Copyright 2010

35

Guardia stabile

- Una variabile che compare nella guardia ma *non* nel corpo è stabile di indice 0
- La guardia è *stabile*
 - se tutte le sue variabili sono stabili

```
while D/=0 loop R:=C rem D; C:=D; D:=R; end loop;
```

```
while D/=0 loop R:=M rem N; C:=D; D:=R; end loop;
```

- La seconda guardia è stabile, la prima no.
- Nel secondo caso, Examiner segnala che c'è un problema
 - se si entra nel ciclo, perché la guardia non cambia

S3: SPARK - C.Montangero - Copyright 2010

36

Alcune osservazioni

- (si entra) e (guardia stabile) \Rightarrow non termina
 - vuol dire anche
- (si entra) e termina \Rightarrow (guardia non stabile)
 - ma non si può dedurre che
- (si entra) e (guardia non stabile) \Rightarrow termina
 - per questa ci vuole più semantica
 - funzione di terminazione

S3: SPARK - C.Montangero - Copyright 2010

37

S³ 2009/10 – Flussi informativi

CONCLUSIONI

S3: SPARK - C.Montangero - Copyright 2010

38

Valutazione

- Le verifiche sono efficienti
- Forniscono indicazioni utili sulla correttezza
 - ma non complete
- I messaggi di errore sono
 - semplici
 - utili per individuare i difetti
- Buon compromesso per software non critico

S3: SPARK - C.Montangero - Copyright 2010

39

S³ 2009/10 – Flussi informativi

PROSSIMO ARGOMENTO:

CONTRATTI

S3: SPARK - C.Montangero - Copyright 2010

40

Esercizio: if then

$C = \text{if } e(\Sigma) \text{ then } S' \text{ else null; end if;}$

- Si compongono le matrici dei singoli blocchi
- $D^C = D^{S'}$ or $D^{\text{null}} = D^{S'}$ or $\mathbf{O} = D^{S'}$
- $P^C = P^{S'}$ or $P^{\text{null}} = P^{S'}$ or $\mathbf{I} = \mathbf{I}$
- $R = R^{e(\Sigma)}$ or $R^{S'}$ or \mathbf{I}