Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2003–2004

docente: Stefano Ferrari

Soluzione del secondo compitino — 13.01.2004 — Versione C

valutazioni **1** (4) ____ **2** (5) ____ **3** (4) ____ **4** (7) ____ **5** (7) ____ **6** (7) ____

Cognome ______________________________

Nome ______________________________

Matricola ______________ **Firma** ______________

Esercizio 1

Siano dati i linguaggi L_1 e L_2:

- $L_1 = \{a,\ ab,\ bc\}$
- $L_2 = \{ab,\ 0,\ 1\}$

Descrivere i linguaggi:

a) $L_3 = L_1 \cup L_2$

b) $L_4 = L_1 L_2$

c) $L_5 = {L_1}^3$

d) $L_6 = L_1 {L_2}^*$

e) $L_7 = (L_1 L_2)^*$

f) $L_8 = {L_1}^* {L_2}^*$

Per quegli insiemi di cui sia troppo lungo (o impossibile) dare una descrizione estensionale, elencare almeno tre elementi, indicando le caratteristiche degli elementi che li compongono.

Soluzione

a) $L_3 = L_1 \cup L_2 = \{a,\ ab,\ bc,\ 0,\ 1\}$
Nota: L'elemento ab deve essere incluso solo una volta.

b) $L_4 = L_1 L_2 = \{aab,\ a0,\ a1,\ abab,\ ab0,\ ab1,\ bcab,\ bc0,\ bc1\}$

c) $L_5 = {L_1}^3$
L'insieme L_5 è formato dalle stringhe che si ottengono concatenando tre stringhe (qualsiasi) appartenenti a L_1. Poiché L_1 ha 3 elementi, possono essere formate $3^3 = 27$ stringhe come concatenazione di tre elementi di L_1. L'insieme $\{aabbc,\ bcabbc,\ ababc\}$ è un sottoinsieme di L_5.

d) $L_6 = L_1 {L_2}^*$
L'insieme L_6 è formato da stringhe che hanno un elemento di L_1 come prefisso e una concatenazione di un numero arbitrario (eventualmente nullo) di elementi di L_2 come suffisso. Poiché ${L_2}^*$ è composto da infiniti elementi, anche L_6 avrà infiniti elementi. L'insieme $\{a,\ ab001,\ bcabab0\}$ è un sottoinsieme di L_6.

e) $L_7 = (L_1 L_2)^*$
L'insieme L_7 è equivalente a ${L_4}^*$. Pertanto, anche L_7 è composto da infiniti elementi. L'insieme $\{\epsilon,\ ab0,\ a0a1bcab\}$ è un sottoinsieme di L_7.

f) $L_8 = {L_1}^* {L_2}^*$
Gli elementi dell'insieme L_8 sono il risultato della concatenazione di una stringa di ${L_1}^*$ con una stringa di ${L_2}^*$. Poiché sia ${L_1}^*$ che ${L_2}^*$ hanno infiniti elementi, anche L_8 avrà cardinalità infinita. L'insieme $\{\epsilon,\ ab0100ab,\ bcaba0010ab\}$ è un sottoinsieme di L_8.

Esercizio 2

Sia data la seguente grammatica, $G = \langle T, V, P, S \rangle$, definita su $A = \{a,\ b,\ c,\ d\}$:

- insieme dei simboli terminali, T: $T = A$
- insieme dei metasimboli, V: $V = \{K,\ H\}$

- insieme delle regole di produzione, P: $P = \{S ::= K,\ K ::= b|Hc,\ H ::= c|Ka|Hb\}$

Quali fra le seguenti stringhe vengono generate da G?

a) *cbbab*

b) *cbbcac*

c) *aaaaa*

d) *bacac*

e) *babbc*

Riportare la successione di regole da applicare per la generazione di tali stringhe e le stringhe parziali ottenute.

a)

cbbab	
	S
$S ::= K$	K
$K ::= b$	b

Non è possibile aggiungere altri simboli in quanto si è raggiunte una stringa senza metasimboli. La stringa *cbbab* non può essere generata da G: $cbbab \notin L(G)$.

b)

cbbcac	
	S
$S ::= K$	K
$K ::= Hc$	Hc
$H ::= Ka$	Kac
$K ::= Hc$	$Hcac$
$H ::= Hb$	$Hbcac$
$H ::= Hb$	$Hbbcac$
$H ::= c$	$cbbcac$

La stringa *cbbcac* è generata da G: $cbbcac \in L(G)$.

c)

aaaaa	
	S
$S ::= K$	K

Non esiste nessuna regola in G che permeta di ottenere a da K. La stringa *aaaaa* non può essere generata da G: $aaaaa \notin L(G)$.

d)

bacac	
	S
$S ::= K$	K
$K ::= Hc$	Hc
$H ::= Ka$	Kac
$K ::= Hc$	$Hcac$
$H ::= Ka$	$Kacac$
$K ::= b$	$bacac$

La stringa *bacac* è generata da G: $bacac \in L(G)$.

e)

babbc	
	S
$S ::= K$	K
$K ::= Hc$	Hc
$H ::= Hb$	Hbc
$H ::= Hb$	$Hbbc$
$H ::= Ka$	$Kabbc$
$K ::= b$	$babbc$

La stringa *babbc* è generata da G: $babbc \in L(G)$.

Esercizio 3

Sia dato il seguente automa a stati finiti, A, $A = \langle Q, \Sigma, \delta, q_0, F\rangle$:

- insieme degli stati, Q: $Q = \{q_0, q_1, q_2, q_3\}$
- alfabeto di input, Σ: $\Sigma = \{a, b, c, d, e\}$
- funzione di transizione δ:

	a	b	c	d	e
q_0	q_1	q_3	q_1	q_1	q_1
q_1	q_3	q_2	q_2	q_0	q_1
q_2	q_0	q_0	q_2	q_1	q_1
q_3	q_3	q_1	q_1	q_2	q_2

- stato iniziale, q_0
- insieme di stati finali, F: $F = \{q_1\}$

Indicare:

a) quattro stringhe accettate da A

b) quattro stringhe rifiutate da A

Soluzione

a) quattro stringhe accettate da A:

- ccce
- aaccd
- caab
- cabbd

b) quattro stringhe rifiutate da A:

- eeabd
- dbddac
- acda
- b

Esercizio 4

Costruire un automa a stati finiti deterministico che simuli lo stato di un serbatoio di 4 l di capacità. Il rifornimento può essere effettuato tramite una serie di rabbocchi da un litro ciascuno, o tramite un pieno, il quale porta la disponibilità di carburante a 4 l. Le attività del dispositivo che utilizza il serbatoio sono tali da comportare il consumo di 1 l per ogni attività.

L'automa deve modellare lo stato del serbatoio (cioè la quantità di carburante disponibile) utilizzando come input i simboli:

- r: (rabbocco) viene immesso un litro di carburante nel serbatoio.
- p: (pieno) viene immessa nel serbatoio una quantità tale da riempirlo.
- c: (consumo) viene utilizzato un litro di carburate.

Prestare particolare attenzione alla modellazione dei casi in cui si raggiunge uno stato fisicamente impossibile:

- tentativo di immettere una quantità di carburante superiore alla capacità del serbatoio;
- consumo di una quantità di carburante non disponibile.

Tali situazioni devono essere segnalate intrappolando l'automa in stati opportuni.

Soluzione

L'automa deve modellare un sistema fisico. L'insieme dei simboli di input modella quindi gli stimoli che il sistema riceve dall'esterno e gli stati descrivono le situazioni in cui il sistema viene a trovarsi.

Questo permette di vedere l'automa come un simulatore del sistema in esame. È quindi ragionevole pensare ad un automa che accetti le stringhe che rappresentano le sequenze di stimoli fisicamente realizzabili oppure quelle che rappresentano una sequenza di eventi di particolare interesse.

Nel caso in esame, sono date le seguenti informazioni:

- il serbatoio ha capacità massima 4 l e può essere riempito e svuotato a multipli di litro; poiché l'automa deve rappresentare lo stato del serbatoio, ci sono almeno cinque stati: $q_0, \ldots, q_4$ che rappresentano i litri di carburante presenti nel serbatoio (se l'automa si troverà nello stato q_i rappresenterà la presenza di i litri di carburante);
- bisogna rappresentare la situazione in cui si tenti consumare del carburante che non c'è: lo stato *a secco* servirà per rappresentare questa situazione;
- bisogna rappresentare la situazione in cui si tenti immettere nel serbatoio del carburante oltre la sua capacità: lo stato *trabocca* servirà per rappresentare questa situazione;
- quindi, l'insieme degli stati, Q, sarà:
  $Q = \{q_0, q_1, q_2, q_3, q_4, \textit{a secco}, \textit{trabocca}\}$
- alfabeto di input, Σ:
  $\Sigma = \{r, p, c\}$, secondo il significato dato di, rispettivamente, immissione di un litro di carburante, immissione (a seconda dello stato del serbatoio) di una quantità necessaria a portarlo nello stato q_4 (serbatoio pieno) e consumo di un litro di carburante.

Il comportamento dell'automa può essere descritto dalla tabella delle transizioni, $\delta : Q \times \Sigma \rightarrow Q$ riportata in Tabella 1.

Da notare che gli stati *a secco* e *trabocca*, una volta raggiunti, non possono più essere lasciati.

L'insieme degli stati finali, F, è $F = \{q_0, q_1, q_2, q_3, q_4\}$. In tal modo, l'automa accetterà tutte e sole le sequenze di simboli che rappresentano delle operazioni fisicamente possibili.

Lo stato iniziale, in mancanza di specifiche esplicite, può essere scelto arbitrariamente.

Esercizio 5

Sia data l'espressione regolare E, definita su $\Sigma = \{a, b, c\}$:

- $E = (b + c)^3 abc^*$

Quali fra le seguenti stringhe vengono descritte da E?

a) *bcbabccc*

b) *cccabccc*

c) *cccbab*

d) *ccaabc*

e) *bbbabcccc*

δ	r	p	c
q_0	q_1	q_4	*a secco*
q_1	q_2	q_4	q_0
q_2	q_3	q_4	q_1
q_3	q_4	q_4	q_2
q_4	*trabocca*	q_4	q_3
a secco	*a secco*	*a secco*	*a secco*
trabocca	*trabocca*	*trabocca*	*trabocca*

Tabella 1: Tabella delle transizioni dell'automa dell'esercizio 4

f) *baccacc*

g) *ccbab*

Soluzione

Le espressioni regolari denotano degli insiemi di stringhe. In tal senso, possiamo applicare l'operatore di relazione insiemistica $\subseteq$ alle espressioni regolari per indicare che l'insieme denotato da un'espressione contiene l'insieme denotato da una seconda espressione regolare. Per esempio, $E_1 \subseteq E_2$ significa che tutte le stringhe descritte da E_1 sono descritte anche da E_2.

Ricordando che l'espressione regolare s descrive l'insieme di stringhe composto dalla sola s, $\{s\}$, si può dimostrare che tale stringa viene descritta da un'espressione regolare E derivando una catena di inclusioni del tipo $s \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_k \equiv E$.

a) *bcbabccc*
$bcbabccc = (bcb)(ab)(ccc) \subseteq (b+c)^3ab(c)^3 \subseteq (b+c)^3abc^*$.

La stringa *bcbabccc* viene descritta da E.

b) *cccabccc*
$cccabccc = (ccc)(ab)(ccc) = (c)^3ab(c)^3 \subseteq (b+c)^3abc^*$.

La stringa *cccabccc* viene descritta da E.

c) *cccbab*
cccbab ha b come quarto simbolo. Le stringhe descritte da E devono avere una a come quarto simbolo, quindi *cccbab* non viene descritta da E.

d) *ccaabc*
ccaabc ha una a come terzo simbolo. Le stringhe descritte da E devono avere b o c come terzo simbolo, quindi *ccaabc* non viene descritta da E.

e) *bbbabcccc*
$bbbabcccc = (bbb)(ab)(cccc) = (b)^3(ab)(c)^4 \subseteq (b+c)^3ab(c)^*$.

La stringa *bbbabcccc* viene descritta da E.

f) *baccacc*
baccacc ha a come secondo simbolo. Le stringhe descritte da E devono avere b o c come secondo simbolo, quindi *baccacc* non viene descritta da E.

g) *ccbab*
$ccbab = (ccb)(ab)\epsilon \subseteq (b+c)^3ab(c)^*$.

La stringa *ccbab* viene descritta da E.

Esercizio 6

Indicare una espressione regolare definita su $\Sigma = \{a, b, c\}$ che descriva le seguenti stringhe:

- *aaabbb*
- *caaab*
- *cccaab*
- *caabcc*

ma non le seguenti:

- *baacbb*
- *bbbaabca*
- *ccababbb*
- *ccaabb*

Soluzione

Per individuare un'espressione regolare accettabile (che non sia banalmente l'unione delle quattro stringhe del primo gruppo) bisogna individuare delle regolarità nel primo insieme di stringhe che non siano presenti nel secondo insieme.

Si possono notare alcune caratteristiche comuni alle stringhe del primo gruppo:

- i simboli seguono sempre lo stesso ordine: ad un (eventuale) blocco di c segue un blocco di a, a cui segue un blocco di b, a cui, infine, segue un (eventuale) blocco di c;
- le b sono sempre presenti in un unico blocco e in numero dispari.

Queste proprietà sono sufficienti a discriminare il primo gruppo di stringhe dal secondo. Infatti:

- *baacbb*: non rispetta la sequenza c-a-b-c
- *bbbaabca*: non rispetta la sequenza c-a-b-c
- *ccababbb*: non rispetta la sequenza c-a-b-c
- *ccaabb*: il blocco di b ha lunghezza pari

Le proprietà summenzionate sono formalizzabili con le seguenti espressioni regolari:

- sequenza c-a-b-c: $c^*a^*b^*c^*$; l'obbligo di presenza di almeno una a e di una b può essere ottenuto con l'espressione $c^*aa^*bb^*c^*$, ma non è necessario ai fini della discriminazione dei gruppi;
- blocco dispari di b: $b(b^2)^*$.

Unendo le due espressioni, si ottiene $c^*a^*b(b^2)^*c^*$.

La soluzione proposta, non è tuttavia l'unica accettabile. Per esempio, anche $c^*a^2(ab^* + bc^*)$ risponde ai requisiti richiesti.