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 B

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:

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

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

b) $L_4 = L_1 L_2 = \{aa, abc, aaa, 0a, 0bc, 0aa, 1a, 1bc, 1aa, \}$

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 $\{a10, 110, 0a0\}$ 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 $\{a, 1bcaa, 0abca\}$ 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 $\{\epsilon, 0100a, a11\}$ 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 $\{\epsilon, a001abcaabc, bcaaa, 0110\}$ 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: $P = \{S ::= K,\ K ::= a|bH,\ H ::= d|bK|aH\}$

Quali fra le seguenti stringhe vengono generate da G?

a) *bbbad*

b) *abbcb*

c) *bbbb*

d) *baba*

e) *baabbd*

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

Soluzione

a)

bbbad	
	S
$S ::= K$	K
$K ::= bH$	bH
$H ::= bK$	bbK
$K ::= bH$	$bbbH$
$H ::= aH$	$bbbaH$
$H ::= d$	$bbbad$

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

b)

abbcb	
	S
$S ::= K$	K
$K ::= a$	a

Non è possibile aggiungere altri simboli, in quanto non ci sono metasimboli nella stringa generata fino a questo punto. La stringa *abbcb* non è generata da G: $abbcb \notin L(G)$.

c)

bbbb	
	S
$S ::= K$	K
$K ::= bH$	bH
$H ::= bK$	bbK
$K ::= bH$	$bbbH$
$H ::= bK$	$bbbbK$

Non è possibile eliminare il metasimbolo K. Pertanto, la stringa *bbbb* non è generata da G: $bbbb \notin L(G)$.

d)

baba	
	S
$S ::= K$	K
$K ::= bH$	bH
$H ::= aH$	baH
$H ::= bK$	$babK$
$K ::= a$	$baba$

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

e)

baabbd	
	S
$S ::= K$	K
$K ::= bH$	bH
$H ::= aH$	baH
$H ::= aH$	$baaH$
$H ::= bK$	$baabK$
$K ::= bH$	$baabbH$
$H ::= d$	$baabbd$

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

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_3	q_2	q_2	q_0	q_1
q_1	q_0	q_0	q_2	q_1	q_1
q_2	q_1	q_3	q_1	q_1	q_1
q_3	q_0	q_3	q_2	q_0	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:

- eeabd
- ccce
- aaccd
- cabbd

b) quattro stringhe rifiutate da A:

- dbddac
- acda
- caab
- cbeba

Esercizio 4

Un apparecchio per la riproduzione di videocassette è dotato dei seguenti tasti: *play*, *stop*, *fast forward (FFW)*, *rewind (RWD)* e *eject*. La pressione del tasto *play* attiva la normale riproduzione della cassetta inserita, mentre i tasti *FFW* e *RWD* attivano rispettivamente le modalità di avanzamento o arretramento rapido. Il tasto *stop* blocca qualsiasi attività del videoregistratore (*play*, *FFW*, e *RWD*), portandolo nello stato di riposo. Il tasto *eject*, infine, causa il rilascio della cassetta inserita. Una volta che la cassetta stata rilasciata, ogni successiva pressione di uno qualsiasi dei tasti non ha alcun effetto.

Modellare il comportamento di tale dispositivo tramite un automa a stati finiti deterministico, utilizzando come stati le modalità in cui il videoregistratore si trova ad operare e come simboli di input i tasti che l'utente preme.

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:

- alfabeto di input, Σ:
  $\Sigma = \{play,\ stop,\ FFW,\ RWD,\ eject\}$
- insieme degli stati, Q:
  $Q = \{riproduzione,\ avanzamento\ rapido,\ riavvolgimento\ rapido,\ riposo,\ rilascio\}$

La tabella delle transizioni, $\delta : Q \times \Sigma \to Q$ è quindi quella riportata in Tabella 1: ad ogni tasto corrisponde una modalità di funzionamento e sono permesse le transizioni da ogni stato ad un altro. L'unica eccezione è lo stato di rilascio della cassetta, che, una volta raggiunto, non può più essere lasciato. Il comportamento descritto in Tabella 1 non è comunque l'unico che che soddisfa le specifiche del problema. Alcune varianti saranno descritte nel seguito.

Ipotizzando di voler modellare le operazioni che possono essere eseguite nella riproduzione di una singola videocassetta, si può ragionevolmente porre *riposo* come stato iniziale. Ciò corrisponde alla situazione di cassetta inserita e videoregistratore inattivo. Analogamente, è ragionevole porre *rilascio* come unico stato finale: $F = \{rilascio\}$. Ciò equivale ad accettare tutte e sole le sequenze di azioni che terminano con il rilascio della cassetta.

Possono inoltre essere considerate altre varianti:

transizioni vincolate per poter passare da una modalità all'altra bisogna passare per lo stato *riposo*. Questo comportamento è descritto tramite la tabella delle transizioni riportata in Tabella 2.

transizioni obbligate per evitare brusche variazioni di velocità ai motori del videoregistratore, alcune transizioni forzano il passaggio allo stato di riposo. Questo comportamento è descritto tramite la tabella delle transizioni riportata in Tabella 3.

$F = Q$ ponendo tutti gli stati nell'insieme degli stati finali, l'automa accetta tutte le stringhe che modellano le sequenze di eventi fisicamente possiili.

stato iniziale fittizio aggiungendo uno stato iniziale fittizio, q_0, si modella la situazione in cui non si conosce la modalità in cui opera il videoregistratore all'inizio della simulazione. La tabella delle transizioni, $\delta : Q \times \Sigma \to Q$ si arricchisce con le seguenti transizioni: $\delta(q_0, play) = play$, $\delta(q_0, stop) = stop$, $\delta(q_0, FFW) = FFW$, $\delta(q_0, RWD) = RWD$ e $\delta(q_0, eject) = eject$.

Esercizio 5

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

- $E = a^2(ab)^*(c + ab)b^*$

δ	*play*	*stop*	*FFW*	*RWD*	*eject*
riproduzione	*riproduzione*	*riposo*	*avanzamento*	*riavvolgimento*	*rilascio*
avanzamento	*riproduzione*	*riposo*	*avanzamento*	*riavvolgimento*	*rilascio*
riavvolgimento	*riproduzione*	*riposo*	*avanzamento*	*riavvolgimento*	*rilascio*
riposo	*riproduzione*	*riposo*	*avanzamento*	*riavvolgimento*	*rilascio*
rilascio	*rilascio*	*rilascio*	*rilascio*	*rilascio*	*rilascio*

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

δ	*play*	*stop*	*FFW*	*RWD*	*eject*
riproduzione	*riproduzione*	*riposo*	*riproduzione*	*riproduzione*	*riproduzione*
avanzamento	*avanzamento*	*riposo*	*avanzamento*	*avanzamento*	*avanzamento*
riavvolgimento	*riavvolgimento*	*riposo*	*riavvolgimento*	*riavvolgimento*	*riavvolgimento*
riposo	*riproduzione*	*riposo*	*avanzamento*	*riavvolgimento*	*rilascio*
rilascio	*rilascio*	*rilascio*	*rilascio*	*rilascio*	*rilascio*

Tabella 2: Tabella delle transizioni per la variante "transizioni vincolate" dell'automa dell'esercizio 4

Quali fra le seguenti stringhe vengono descritte da E?

a) *aaababc*

b) *aaababababb*

c) *aaaacbb*

d) *aacb*

e) *abbbaac*

f) *aaabab*

g) *aacbbc*

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) *aaababc*
$aaababc = (aa)(abab)c\epsilon = a^2(ab)^2c\epsilon \subseteq a^2(ab)^*c\epsilon \subseteq a^2(ab)^*(c+ab)b^*$.

La stringa *aaababc* viene descritta da E.

b) *aaababababb*
$aaababababb = (aa)(abab)(ab)(bb) = a^2(ab)^2(ab)b^2 \subseteq a^2(ab)^*(ab)b^* \subseteq a^2(ab)^*(c+ab)b^*$.

La stringa *aaababababb* viene descritta da E.

c) *aaaacbb*
aaaacbb inizia con quattro a. L'espressione E non può descrivere stringhe che iniziano con più di tre a. Quindi *aaaacbb* non viene descritta da E.

d) *aacb*
$aacb = (aa)(c)(b) = a^2\epsilon(c)(b) \subseteq a^2\epsilon(c)b^* \subseteq a^2(ab)^*(c+ab)b^*$.

La stringa *aacb* viene descritta da E.

e) *abbbaac*
abbbaac inizia con *ab*. L'espressione E descrive stringhe che iniziano con due a. Quindi *abbbaac* non viene descritta da E.

f) $E = a^2(ab)^*(c+ab)b^*$

g) *aaabab*
$aaabab = (aa)(ab)(ab) = a^2(ab)(ab)\epsilon \subseteq a^2(ab)^*(c+ab)b^*$.

La stringa *aaabab* viene descritta da E.

h) *aacbbc*
aacbbc contiene due c. Poiché le stringhe descritte da E possono contenere solo una c, la stringa *aacbbc* non può essere descritta da E.

Esercizio 6

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

δ	*play*	*stop*	*FFW*	*RWD*	*eject*
riproduzione	*riproduzione*	*riposo*	*avanzamento*	*riavvolgimento*	*riposo*
avanzamento	*riproduzione*	*riposo*	*avanzamento*	*riposo*	*riposo*
riavvolgimento	*riproduzione*	*riposo*	*riposo*	*riavvolgimento*	*riposo*
riposo	*riproduzione*	*riposo*	*avanzamento*	*riavvolgimento*	*rilascio*
rilascio	*rilascio*	*rilascio*	*rilascio*	*rilascio*	*rilascio*

Tabella 3: Tabella delle transizioni per la variante "transizioni vincolate" dell'automa dell'esercizio 4

- *aaca*
- *accaaba*
- *cacaabbba*
- *cccabbaba*

ma non le seguenti:

- *aaacba*
- *cbcbaab*
- *ccccb*
- *caabbac*

Esercizio 6

Si può notare che le stringhe da descrivere hanno tutte la sottostringa *ca* a coprire il terzo e il quarto simbolo della stringa. Questa caratteristica può essere descritta tramite l'espressione regolare $(a+b+c)^2ca(a+b+c)^*$:

- due simboli qualsiasi come prefisso: $\underline{(a+b+c)^2}ca(a+b+c)^*$
- la stringa *ca* al terzo e quarto simbolo: $(a+b+c)^2\underline{ca}(a+b+c)^*$
- a seguire una stringa qualsiasi: $(a+b+c)^2ca\underline{(a+b+c)^*}$

Le stringhe da escludere non godono di questa proprietà:

- $aa\underline{ac}ba$
- $cb\underline{cb}aab$
- $ccc\underline{c}b$
- $ca\underline{ab}bac$

La soluzione proposta, non è tuttavia unica. Per esempio, anche $(a+c)^2ca(b^*a)^*$ risponde ai requisiti richiesti.