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 della seconda parte — 04.06.2004 — Versione A

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:

- $L_1 = \{y, 1, 2\}$
- $L_2 = \{x, 1, 2\}$

Descrivere i linguaggi:

a) $L_3 = L_1 \cap L_2$

b) $L_4 = L_1 \cup L_2$

c) $L_5 = L_1 L_2$

d) $L_6 = {L_1}^2$

e) $L_7 = L_1 {L_2}^*$

f) $L_8 = (L_1 L_2)^*$

g) $L_9 = {L_1}^* {L_2}^*$

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) $L_3 = L_1 \cap L_2 = \{1, 2\}$

b) $L_4 = L_1 \cup L_2 = \{y, 1, 2, x\}$

c) $L_5 = L_1 L_2 = \{yx, 1x, 2x, y1, 11, 21, y2, 12, 22\}$

d) $L_6 = {L_1}^2 = \{yy, y1, y2, 1y, 11, 12, 2y, 21, 22\}$

e) $L_7 = L_1 {L_2}^*$
L'insieme L_7 è formato da stringhe che hanno un elemento di L_1 seguito da una concatenazione di un numero arbitrario (eventualmente nullo) di elementi di L_2. Poiché ${L_2}^*$ è composto da infiniti elementi, anche L_7 avrà infiniti elementi. L'insieme $\{y, 11x, 2xxx\}$ è un sottoinsieme di L_7.

f) $L_8 = (L_1 L_2)^*$
L'insieme L_8 è equivalente a ${L_5}^*$. Pertanto, L_8 è composto da infiniti elementi. L'insieme $\{\epsilon, yx11, 21y2yx\}$ è un sottoinsieme di L_8.

g) $L_9 = {L_1}^* {L_2}^*$
Gli elementi dell'insieme L_9 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_9 avrà cardinalità infinita. L'insieme $\{\epsilon, y2y1, x11, yyy112x22\}$ è un sottoinsieme di L_9.

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: $P = \{S ::= K, K ::= d|Ha, H ::= c|Kd|Hb\}$

Quali fra le seguenti stringhe vengono generate da G?

a) *ddaba*

b) *ab*

c) *caba*

d) *cadada*

e) *bada*

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

Soluzione

a)

$ddaba$	
	S
$S ::= K$	K
$K ::= Ha$	Ha
$H ::= Hb$	Hba

Non esiste nessuna regola che permetta di ottenere il simbolo a dal metasimbolo H. La stringa *ddaba* non è quindi generata da G: $ddaba \notin L(G)$.

b)

ab	
	S
$S ::= K$	K

Non esiste nessuna regola che permetta di ottenere il simbolo b dal metasimbolo K. La stringa *ab* non è quindi generata da G: $ab \notin L(G)$.

c)

$caba$	
	S
$S ::= K$	K
$K ::= Ha$	Ha
$H ::= Hb$	Hba

Non esiste nessuna regola che permetta di ottenere il simbolo a dal metasimbolo H. La stringa *caba* non è quindi generata da G: $caba \notin L(G)$.

d)

$cadada$	
	S
$S ::= K$	K
$K ::= Ha$	Ha
$H ::= Kd$	Kda
$K ::= Ha$	$Hada$
$H ::= Kd$	$Kdada$
$K ::= Ha$	$Hadada$
$H ::= c$	$cadada$

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

e)

$bada$	
	S
$S ::= K$	K
$K ::= Ha$	Ha
$H ::= Kd$	Kda
$K ::= Ha$	$Hada$
$H ::= Hb$	$Hbada$

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

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_2	q_1	q_2	q_1
q_1	q_2	q_0	q_2	q_0	q_1
q_2	q_3	q_1	q_0	q_1	q_2
q_3	q_2	q_1	q_2	q_3	q_1

- 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:

- abdd
- bbcb
- caae
- db

b) quattro stringhe rifiutate da A:

- aaa
- edbac
- bacce
- d

Esercizio 4

Un ascensore opera in una palazzina di due piani.

L'ascensore è accessibile da tre punti: piano terra, primo piano, secondo piano. L'utente può chiamare l'ascensore premendo il pulsante di chiamata del piano a cui si trova. L'ascensore si porta direttamente al piano dove è stata effettuata la chiamata, ignorando eventuali chiamate che sopraggiungiungano nel frattempo.

Oltre alle chiamate dai piani, l'ascensore risponde ad un segnale d'allarme portandosi in posizione di sicurezza, al piano terreno. Dopo essersi portato in tale posizione, l'ascensore non risponde più alle chiamate, necessitando dell'intervento di un addetto per riprendere il funzionamento normale.

Modellare il comportamento dell'ascensore tramite un automa a stati finiti deterministico, dove gli stati rappresentano le posizioni in cui l'ascensore viene a trovarsi, e la stringa di input rappresenta i segnali che l'ascensore riceve.

Ipotizzare che non possano avvenire due chiamate contemporaneamente o durante il servizio ad un utente. Astrarre da condizioni legate alla dinamica, e considerare istantanei gli spostamenti fra i piani.

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:

- insieme degli stati, Q:
  $Q = \{q_t, q_1, q_2, q_s\}$
  per indicare, rispettivamente, il piano terra, il primo ed il secondo piano e, infine, la posizione di sicurezza;
- alfabeto di input, Σ:
  $\Sigma = \{T, 1, 2, A\}$
  per indicare, rispettivamente, la chiamata per il piano terra, per il primo ed il secondo piano e, infine il segnale d'allarme.

Dalle specifiche è possibile dedurre i seguenti comportamenti:

- l'ascensore va diretto al piano selezionato;
- se riceve un segnale di allarme, si porta nella posizione di sicurezza;
- una volta in posizione di sicurezza, non risponde più ai segnali.

Mancano invece specifiche riguardo allo stato finale ed allo stato iniziale. Si può ipotizzare che lo stato iniziale sia quello relativo al piano terra, e lo stato finale sia quello della posizione di sicurezza.

La tabella delle transizioni, $\delta : Q \times \Sigma \rightarrow Q$ può essere quella riportata in Tabella 1.

Esercizio 5

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

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

Quali fra le seguenti stringhe vengono descritte da E?

a) *abbbca*

b) *abbabb*

c) *accbbc*

d) *baaabb*

e) *abcabc*

f) *aaaacc*

g) *cccccc*

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 $s \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_k \equiv E$.

δ	T	1	2	A
q_t	q_t	q_1	q_2	q_s
q_1	q_t	q_1	q_2	q_s
q_2	q_t	q_1	q_2	q_s
q_s	q_s	q_s	q_s	q_s

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

a) *abbbca*
La stringa *abbbca* non può essere descritta da E perché le stringhe descritte da E non possono terminare per a.

b) *abbabb*
$abbabb = (abb)(a)(bb) = (abb)(a)(b^2) \subset (a+b+c)^*a(b+c)^2$.

La stringa *abbabb* viene descritta da E.

c) *accbbc*
La stringa *accbbc* non può essere descritta da E perché le stringhe descritte da E devono avere una come terz'ultimo simbolo.

d) *baaabb*
$baaabb = (baa)(a)(bb) = (baa)(a)b^2 \subset (a+b+c)^*a(b+c)^2$

La stringa *baaabb* viene descritta da E.

e) *abcabc*
$abcabc = (abc)(a)(bc) = (abc)(a)b^2 \subset (a+b+c)^*a(b+c)^2$

La stringa *abcabc* viene descritta da E.

f) *aaaacc*
$aaaacc = (aaa)(a)(cc) = a^3(a)c^2 \subset (a+b+c)^*a(b+c)^2$

La stringa *aaaacc* viene descritta da E.

g) *cccccc*
La stringa *cccccc* non può essere descritta da E in quanto una stringa di E ha a come terz'ultimo simbolo.

Esercizio 6

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

- *bbcbb*
- *bbccba*
- *bbcaaa*
- *bbcccbaa*

ma non le seguenti:

- *bbcbac*
- *bbcabc*
- *cbbaa*
- *abbcab*

Soluzione

Si può notare che le stringhe da includere hanno tutte *bbc* come prefisso. Inoltre, esse terminano eventualmente con una sequenza di a. Fra la sequenza iniziale, *bbc*, e la sequenza finale di a, possono esserci solo simboli b o c. Queste caratteristiche possono essere descritte dall'espressione regolare $b^2c(b+c)^*a^*$:

- *bbc* come prefisso: $\underline{b^2c}(b+c)^*a^*$;
- eventuale suffisso composto da una sequenza di a: $b^2c(b+c)^*\underline{a^*}$;
- ed eventuale sequenza di b e c nella parte centrale: $b^2c\underline{(b+c)^*}a^*$.

Nessuna delle stringhe del secondo gruppo viene descritta da tale espressione regolare:

- *bbcbac*: ha delle a, termina per c;
- *bbcabc*: ha delle a, termina per c;
- *cbbaa*: non inizia per *bbc*;
- *abbcab* non inizia per *bbc*.

Altre espressioni regolari che rispettano le specifiche del problema possono essere:

- $b^2(b+c)^*a^*$,
- $b(b+c)^*a^*$.

L'espressione regolare $(b+c)^*a^*$ non può essere ritenuta valida in quanto descrive anche la terza stringa da escludere.