Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2004–2005

docente: Stefano Ferrari

14.01.2005 — Soluzione del secondo compitino — vers. A

valutazioni **1** (4) ______ **2** (4) ______ **3** (4) ______ **4** (6) ______ **5** (6) ______ **6** (8) ______

Cognome ____________________

Nome ____________________

Matricola ____________________ **Firma** ____________________

Esercizio 1

Siano dati i linguaggi L_1 e L_2:

- $L_1 = \{ab, bc, c\}$
- $L_2 = \{a, b, c\}$

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) $L_8 = (L_1 L_2)^*$

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. In particolare, chiarire se la stringa vuota ϵ appartiene al linguaggio.

Soluzione

a) $L_3 = L_1 \cap L_2 = \{c\}$

b) $L_4 = L_1 \cup L_2 = \{ab, bc, c, a, b\}$

c) $L_5 = L_1 L_2 = \{aba, bca, ca, abb, bcb, cb, abc, bcc, cc\}$

d) $L_6 = {L_1}^2 = \{abab, bcab, cab, abbc, bcbc, cbc, abc, bcc, cc\}$

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 $\{ab, abbbbc, bccbcba\}$ 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 $\{\epsilon, aba, cabcb\}$ è un sottoinsieme di L_8.

Esercizio 2

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

- insieme dei simboli terminali, T: $T = \Sigma$
- insieme dei metasimboli, V: $V = \{K, H\}$
- insieme delle regole di produzione, P: $P = \{S ::= K,\ K ::= a|Hb|Hc,\ H ::= c|Kd|Hb\}$

Quali fra le seguenti stringhe vengono generate da G?

a) $ccdb$

b) $cabba$

c) $adcc$

d) cbc

e) $adcdbb$

Riportare la successione di regole da applicare per la generazione di tali stringhe e le stringhe parziali ottenute, spiegando perché non si possono ottenere le stringhe che eventualmente non risultassero appartenere al linguaggio generato da G.

Soluzione

a) *ccdb*

	S
$S ::= K$	K
$K ::= Hb$	Hb
$H ::= Kd$	Kdb
$K ::= Hc$	$Hcdb$
$H ::= c$	$ccdb$

La stringa *ccdb* è generata da G: $ccdb \in \mathcal{L}(G)$.

b) *cabba*

	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 *cabba* non è generata da G: $cabba \notin \mathcal{L}(G)$.

c) *adcc*

	S
$S ::= K$	K
$K ::= Hc$	Hc
$H ::= c$	cc

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

d) *cbc*

	S
$S ::= K$	K
$K ::= Hc$	Hc
$H ::= Hb$	Hbc
$H ::= c$	cbc

La stringa *cbc* è generata da G: $cbc \in \mathcal{L}(G)$.

e) *adcdbb*

	S
$S ::= K$	K
$K ::= Hb$	Hb
$H ::= Hb$	Hbb
$H ::= Kd$	$Kdbb$
$K ::= Hc$	$Hcdbb$
$H ::= Kd$	$Kdcdbb$
$K ::= a$	$adcdbb$

La stringa *adcdbb* è generata da G: $adcdbb \in \mathcal{L}(G)$.

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_2	q_1	q_2	q_3	q_1
q_1	q_1	q_2	q_1	q_2	q_1
q_2	q_3	q_0	q_3	q_0	q_3
q_3	q_3	q_2	q_1	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:
- *dabcc*
- *beac*
- *deccc*
- *dc*

b) quattro stringhe rifiutate da A:
- *babb*
- *dec*
- *adbbc*
- *da*

Esercizio 4

Modellare, tramite un automa a stati finiti deterministico, l'utilizzo di una maglietta.

La maglietta può essere sottoposta alle seguenti azioni: uso, lavaggio, asciugatura.

Una maglietta può essere utilizzata solo se è asciutta e pulita. L'azione di lavaggio rende una maglietta pulita e bagnata. L'azione di asciugatura rende la maglietta asciutta. L'uso rende la maglietta sporca.

Modellare un automa a stati finiti deterministico dove gli stati rappresentano le condizioni in cui una maglietta si può trovare (sia in termini di pulizia che di umidità), e la stringa di input rappresenta la sequenza di azioni che possono essere operate sulla maglietta.

Ipotizzare che non si possano verificare contemporaneamente più azioni. Modellare l'automa in modo che esso accetti solo le stringhe che descrivono un utilizzo accettabile (e igienico) della maglietta.

Stati e simboli riportati nel testo sono solo indicativi: possono essere modificati, ridotti ed estesi a secondo delle esigenze del progetto.

Soluzione

L'automa deve modellare un sistema fisico. L'insieme dei simboli di input modella quindi gli stimoli che il sistema riceve dall'esterno (o le azioni che esso subisce) 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: l'automa deve accettare le stringhe che rappresentano le sequenze di stimoli (o azioni) 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:
  $Q = \{p,\ s,\ b\}$
  dove p sta per "pulita e asciutta", s sta per "sporca" e b sta per "bagnata";
- alfabeto di input, Σ:
  $\Sigma = \{a,\ l,\ u\}$
  per indicare, rispettivamente, le azioni di asciugatura, di lavaggio e di utilizzo della maglietta.

Dalle specifiche è possibile dedurre i seguenti comportamenti:

- l'uso della maglietta quando è sporca o bagnata non è corretto;
- l'azione di lavaggio porta la maglietta nello stato b;
- l'utilizzo porta la maglietta nell stato s.

Per poter catturare le sequenze di azioni ritenute non corrette è necessario introdurre un nuovo stato, e ("errore"), dal quale, una volta raggiunto, l'automa non possa più uscirne.

Si può ipotizzare che lo stato iniziale sia quello relativo alla maglietta pulita ($q_0 = p$), e che gli stati finali siano tutti, escluso e ($F = \{p,\ s,\ b\}$).

In mancanza di specifiche, si può ipotizzare che asciugare una maglietta pulita non abbia alcun effetto, mentre asciugare una maglietta sporca sia un'azione non corretta. Allo stesso modo, si può pensare che lavare una maglietta bagnata non abbia alcun effetto e sia un'azione ammissibile.

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

Esercizio 5

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

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

Quali fra le seguenti stringhe vengono descritte da E?

a) *acbbcaaccb*

b) *cacccabcc*

c) *bbcacabb*

d) *acaabba*

e) *bbccbacccc*

f) *ccaaacb*

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) *acbbcaaccb*
$acbbcaaccb \subseteq (ac)(bbc)(a)(a)(cc)(b) \subseteq (ac + bbc + a)^3(a)(cc+b)^2 \subseteq (ac^* + b^*c)^3a(c^2+b)^2 \subseteq (ac^* + b^*c)^*a(b + c^2)^2$

La stringa *acbbcaaccb* viene descritta da E: $acbbcaaccb \in \mathcal{L}(E)$.

b) *cacccabcc*
$cacccabcc \subseteq (c)(accc)(a)(b)(cc) \subseteq (c +$

$\boldsymbol{\delta}$	a	u	l
p	p	s	b
b	p	e	b
s	e	e	b
e	e	e	e

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

$accc)^2(a)(b+cc)^2 \subseteq (b^*c+ac^*)^2a(b+c^2)^2 \subseteq (ac^*+b^*c)^*a(b+c^2)^2$

La stringa *cacccabcc* viene descritta da E: $cacccabcc \in \mathcal{L}(E)$.

c) *bbcacabb*
$bbcacabb \subseteq (bbc)(ac)(a)(bb) \subseteq (bbc+ac)^2(a)b^2 \subseteq (b^*c+ac)^2a(b+c^2)^2 \subseteq (ac^*+b^*c)^*a(b+c^2)^2$

La stringa *bbcacabb* viene descritta da E: $bbcacabb \in \mathcal{L}(E)$.

d) *acaabba*
Poiché E ha per suffisso l'espressione $a(b+c^2)^2$, tutte le stringhe descritte da E dovranno terminare con un stringa dell'insieme $\{abb, abcc, accb, acccc\}$.

La stringa *acaabba* non rispetta questa regola, quindi non può essere descritta da E: $acaabba \notin \mathcal{L}(E)$.

e) *bbccbacccc*
Poiché E ha per prefisso l'espressione $(ac^*+b^*c)^*$, nelle sottostringhe descritte da questa sottoespressione, tutte le occorrenze del simbolo b devono essere seguite da un simbolo c. Nella stringa *bbccbacccc*, il prefisso *bbcc* può essere descritto da $(ac^*+b^*c)^*$, il suffisso *acccc* può essere descritto da $a(b+c^2)^2$, ma il simbolo b rimanente ($bbcc\underline{b}acccc$) non può essere descritto in alcun modo da E.

Pertanto, la stringa *acaabba* non può essere descritta da E: $acaabba \notin \mathcal{L}(E)$.

f) *ccaaacb*
La stringa *ccaaacb* non ha un suffisso descrivibile da $a(b+c^2)^2$. Quindi essa non può essere descritta da E: $ccaaacb \notin \mathcal{L}(E)$.

Esercizio 6

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

- *bcbbccb*
- *aaabcabc*
- *abcaaabcbc*
- *cbbbcc*

ma non le seguenti:

- *accb*
- *cbbcbaaab*
- *aaabbb*
- *cabbc*

Soluzione

Si può notare che le stringhe da includere o sono composte esclusivamente da b e c (è il caso della prima e dell'ultima stringa), oppure contengono la sottostringa bc preceduta da sequenze di a di diversa lunghezza (è il caso della seconda e della terza stringa). Queste caratteristiche possono essere descritte dall'espressione regolare $(b+c)^*+(a^*bc)^*$:

- sequenze di b e c come prefisso: $\underline{(b+c)^*}+(a^*bc)^*$;
- sequenze di a seguite da bc: $(b+c)^*+\underline{(a^*bc)^*}$.

Nessuna delle stringhe del secondo gruppo viene descritta da tale espressione regolare, in quanto tutte possiedono almeno un simbolo a che non è seguito da bc.

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

- $a^*(b+c)^2(a+b)^2a^*(b+c)^*$,
- $(a^*+bc)^*+(b^*c^*+cb)^*$,
- $(b+c)^6b^*+(a^*bc)^*$,
- $(a^*bc+cb^*+b)^*$.