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 — 08.07.2004 — 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:

- $L_1 = \{a, b, z\}$
- $L_2 = \{x, y, z\}$

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) $L_3 = L_1 \cap L_2 = \{z\}$

b) $L_4 = L_1 \cup L_2 = \{a, b, z, x, y\}$

c) $L_5 = L_1 L_2 = \{ax, ay, az, bx, by, bz, zx, zy, zz\}$

d) $L_6 = {L_1}^2 = \{aa, ab, az, ba, bb, bz, za, zb, zz\}$

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 $\{b, azxx, zzyxz\}$ 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 $\{\epsilon, axbz, zzzyay\}$ 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 $\{\epsilon, baab, zyxx, baayyz\}$ 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: $P = \{S ::= K, K ::= d|Ha|Hc, H ::= c|Kd|Hb\}$

Quali fra le seguenti stringhe vengono generate da G?

a) *cdaba*

b) *ab*

c) *cadbc*

d) *ccdbba*

e) *cbada*

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

Soluzione

a) *cdaba*

	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 *cdaba* non è quindi generata da G: $cdaba \notin L(G)$.

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) *cadbc*

	S
$S ::= K$	K
$K ::= Hc$	Hc
$H ::= Kd$	$Kdbc$
$H ::= c$	$cadbc$

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

d) *ccdbba*

	S
$S ::= K$	K
$K ::= Ha$	Ha
$H ::= Hb$	Hba
$H ::= Hb$	$Hbba$
$H ::= Kd$	$Kdbba$
$K ::= Hc$	$Hcdbba$
$H ::= c$	$ccdbba$

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

e) *cbada*

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

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

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

- bc
- aab
- abdc
- dbacc

b) quattro stringhe rifiutate da A

- bcc
- aaab
- bbcad
- bad

Esercizio 4

Il sistema d'accesso di una banca è articolato su due porte (interna ed esterna).

Quando una delle due porte è aperta, l'altra viene bloccata. Quando entrambe le porte sono chiuse, il sistema le sblocca entrambe.

Modellare il comportamento di tale sistema tramite un automa a stati finiti deterministico, dove gli stati rappresentano le varie configurazioni di bloccaggio (*esterno*, *interno*, *libere*), e la stringa di input rappresenta la sequenza di eventi di apertura e chiusura delle porte delle porte (*aperta esterna*, *chiusa esterna*, *aperta interna*, *chiusa interna*).

Ipotizzare che non si possano aprire simultaneamente entrambe le porte. Ipotizzare inoltre, per semplicità di progetto, che gli eventi che non potrebbero fisicamente realizzarsi quando il sistema si trova in un dato stato abbiano l'effetto di far permanere il sistema in tale stato.

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 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:
  $Q = \{est, int, lib\}$
  per indicare, rispettivamente, il blocco della porta esterna, di quella interna o l'assenza di blocco ad entrambe le porte;
- alfabeto di input, Σ:
  $\Sigma = \{ae, ce, ai, ci\}$
  per indicare, rispettivamente, gli eventi di apertura e chiusura della porta esterna e di apertura e chiusura della porta interna.

Dalle specifiche è possibile dedurre i seguenti comportamenti:

- l'apertura di una porta blocca l'altra;
- se le porte sono entrambe chiuse, il blocco viene tolto ad entrambe.

Inoltre, per ragioni di semplicità progettuale, sono da escludere eventi simultanei e eventi fisicamente impossibili possono essere interpretati come eventi che non modificano lo stato in cui l'automa si trova. Mancano invece specifiche riguardo allo stato finale ed allo stato iniziale. Si può ipotizzare che sia lo stato iniziale che quello finale siano quello con entrambe le porte chiuse: $q_0 = lib$ e $F = \{lib\}$.

La tabella delle transizioni, $\delta : Q \times \Sigma \to Q$ può essere la seguente:

$\boldsymbol{\delta}$	ae	ce	ai	ci
est	est	est	est	lib
int	int	lib	int	int
lib	int	lib	est	lib

Ipotizzando uno stato *trap* per intrappolare l'automa qualora si verifichi un evento fisicamente impossibile, l'automa avrebbe il seguente comportamento:

$\boldsymbol{\delta}$	ae	ce	ai	ci
est	$trap$	$trap$	$trap$	lib
int	$trap$	lib	$trap$	$trap$
lib	int	$trap$	est	$trap$
$trap$	$trap$	$trap$	$trap$	$trap$

In tal caso avrebbe senso modificare la definizione di insieme degli stati finali in: $F = \{est, int, lib\}$. Ciò consentirebbe all'automa di accettare solo le sequenze di eventi che siano fisicamente realizzabili.

Esercizio 5

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

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

Quali fra le seguenti stringhe vengono descritte da E?

a) *aabbba*

b) *aabaababb*

c) *aabaabacb*

d) *abb*

e) *accab*

f) *baaabb*

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

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

b) *aabaababb*
$aabaababb = (aa)(b)(aa)(b)(a)(bb) = ((a^2)(b)(a^2)(b))(a)(b^2) \subset ((a^2)(b))^2(a)(b^2) \subset (a^2+b)^2(a)(b^2) \subset (a^2+b)^*(a)(b^2) \subset (a^2+b)^*a(b+c)^2$.

c) *aabaabacb*
$aabaabacb = (aa)(b)(aa)(b)(a)(cb) \subset ((a^2)(b))^2(a)(b+c)^2 \subset (a^2+b)^*(a)(b+c)^2$.

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

e) *accab*
La stringa *accab* non può essere descritta da E perché gli ultimi due simboli delle stringhe descritte da E devono essere scelti nell'nsieme $\{b, c\}$.

f) *baaabb*
$baaabb = (b)(aa)(a)(bb) = (b)(a^2)(a)(b^2) \subseteq (a^2+b)^2a(b+c)^2 \subseteq (a^2+b)^*a(b+c)^2$.

g) *cccccc*
La stringa *cccccc* non può essere descritta da E perché il terz'ultimo simbolo delle stringhe descritte da E deve essere a.

Esercizio 6

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

- *bbccaaa*
- *bbb*
- *bbcca*
- *bbbaa*

ma non le seguenti:

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

Soluzione

Si può notare che le stringhe da includere sono tutte composte da una sequenza di b seguita eventualmente da una sequenza di c, infine seguita da un'eventuale sequenza di a. Queste caratteristiche possono essere descritte dall'espressione regolare $b^*c^*a^*$:

- Sequenza iniziale di b come prefisso: $\underline{b^*}c^*a^*$;
- eventuale sequenza di c: $b^*\underline{c^*}a^*$;
- ed eventuale sequenza di a: $b^*c^*\underline{a^*}$.

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

- *bbcbac*: ha una c che inframezza la potenziale sequenza di b;
- *bbcabc*: dopo la sequenza *bbca* iniziale (che verrebbe descritta dall'espressione regolare considerata) inizia una nuova sequenza bc;
- *cbbaa*: antepone c alla sequenza di b;
- *abbcab*: antepone a alla sequenza di b iniziale.

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

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