



UNIVERSITÀ DEGLI STUDI
DI MILANO

CORSO DI LAUREA IN SICUREZZA DEI SISTEMI E DELLE RETI
INFORMATICHE

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006

docente: Stefano FERRARI

22.06.2006 — Soluzione della seconda parte — versione 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 :

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

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) $L_6 = L_1^3$
- e) $L_7 = L_1^* L_2^*$
- f) $L_8 = (L_2 L_1)^*$

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) $L_3 = L_1 \cap L_2 = \emptyset$
Gli insiemi L_1 e L_2 non hanno elementi in comune, quindi la loro intersezione è vuota.
Nota: L'insieme vuoto \emptyset è diverso dall'insieme costituito dalla sola stringa vuota, $\{\epsilon\}$.
- b) $L_4 = L_1 \cup L_2 = \{a, ab, b, bc, c\}$
- c) $L_5 = L_1 L_2 = \{aab, ac, bab, bc, bcab, bcc\}$

d) Il linguaggio $L_6 = L_1^3$ ha 27 elementi. L'insieme $\{aaa, aab, bcbbc, bcbca, bcbcb, bcbcbc\}$ è un sottoinsieme di L_6 .

e) $L_7 = L_1^* L_2^*$
L'insieme L_7 è dato dalle stringhe formate come concatenazione di un numero arbitrario (eventualmente nullo) di elementi di L_1 seguito da una concatenazione di un numero arbitrario (eventualmente nullo) di elementi di L_2 . Poiché sia L_1^* che L_2^* sono composti da infiniti elementi, anche L_7 avrà infiniti elementi. L'insieme $\{\epsilon, aabc, cabcab, bcc\}$ è un sottoinsieme di L_7 .

f) $L_8 = (L_1 L_2)^*$
L'insieme L_8 è formato dalla concatenazione di un numero arbitrario (eventualmente nullo) di stringhe composte da un elemento di L_1 e da un elemento di L_2 . Pertanto, L_8 è composto da infiniti elementi. L'insieme $\{\epsilon, bcab, aabbabbcab\}$ 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, $P: P = \{S ::= H, K ::= a|cH|dH, H ::= b|aK|cH\}$

Quali fra le seguenti stringhe vengono generate da G ?

- a) $acadb$

- b) $ccab$
- c) $cccaa$
- d) $acaab$
- e) $adca$

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)

$S ::= H$	S
$H ::= aK$	H
$K ::= cH$	aK
$H ::= aK$	acH
$K ::= dH$	$acaK$
$H ::= b$	$acadH$
	$acadb$

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

b)

$H ::= cH$	S
$H ::= cH$	cH
$H ::= aK$	ccH
	$ccaK$

Non esiste regola che permetta di ottenere il simbolo b dal metasimbolo K .

La stringa $ccab$ non è generata da G : $ccab \notin \mathcal{L}(G)$.

c)

$S ::= H$	S
$H ::= cH$	H
$H ::= cH$	cH
$H ::= cH$	ccH
$H ::= aK$	$cccH$
$K ::= a$	$cccaK$
	$cccaa$

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

d)

$H ::= aK$	S
$K ::= cH$	aK
$H ::= aK$	acH
$K ::= a$	$acaK$
	$acaa$

La stringa generata non coincide con la stringa data, $acaab$, e non può essere ulteriormente estesa, per mancanza di metasimboli.

La stringa $acaab$ non è generata da G : $acaab \notin \mathcal{L}(G)$.

e)

$H ::= aK$	$adca$
$K ::= dH$	S
$H ::= cH$	aK
$H ::= aK$	adH
	$adcH$
	$adcaK$

Non è possibile eliminare il metasimbolo K senza aggiungere un altro simbolo.

La stringa $adca$ non è generata da G : $adca \notin \mathcal{L}(G)$.

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_1	q_1	q_1	q_3	q_1
q_1	q_3	q_0	q_1	q_2	q_3
q_2	q_1	q_3	q_2	q_0	q_0
q_3	q_3	q_2	q_0	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 :

- $daaade$
- $daba$
- $edde$
- cba

- b) quattro stringhe rifiutate da A :

- $deba$
- dbb
- aac
- $dddec$

Esercizio 4

Modellare, tramite un automa a stati finiti deterministico, il funzionamento di una lavapiatti.

Una lavapiatti è dotata di uno sportello che permette l'accesso al cestello e di un pulsante di attivazione. Nel normale funzionamento, l'utente apre lo sportello, inserisce i piatti da lavare, chiude lo sportello e attiva la lavapiatti. Al termine del ciclo di lavaggio, l'utente svuota il cestello.

Il cestello della lavapiatti ha una capienza massima di cinque piatti, ma in fase di lavaggio, può sopportare il peso solo di quattro piatti.

Attivare la lavapiatti senza aver chiuso lo sportello non ha effetti, così come cercare di aprire lo sportello con la lavapiatti in funzione (un dispositivo di blocco impedisce tale operazione).

Ipotizzare che non si possano verificare contemporaneamente più azioni. Modellare l'automata in modo che esso accetti solo le stringhe che descrivono il funzionamento normale della lavapiatti. In particolare, individuare possibili situazioni fisicamente irrealizzabili o pericolose e formalizzarle in modo che l'automata rifiuti le successioni di azioni che porterebbero la lavapiatti in tali situazioni.

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

Soluzione

L'automata 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'automata come un simulatore del sistema in esame: l'automata 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.

La macchina che deve essere descritta dall'automata è composta da alcuni sottosistemi, responsabili di particolari funzioni: il cestello, lo sportello e il pulsante di attivazione. L'insieme di stati in cui la lavapiatti può trovarsi sono descritti dalle combinazioni possibili dei suoi sottosistemi.

Lo stato in cui si trova il cestello può essere

descritto dal volume di carico, o, meglio, dal numero di piatti caricati (da 0 a 5). Lo sportello può essere aperto o chiuso, quindi due stati sono sufficienti per descrivere tale sottosistema. Infine, la lavapiatti può essere attiva o a riposo: anche questa situazione può essere descritta da due stati.

Quindi lo stato della lavapiatti potrebbe essere descritto da $6 \times 2 \times 2 = 24$ stati. Tuttavia, le specifiche consentono di ridurre il numero di stati necessari. La lavapiatti non può essere attiva e con lo sportello aperto. Quindi, le combinazioni degli stati dei sottosistemi sportello e pulsante di attivazione possono essere ridotti a 3: sportello aperto, sportello chiuso (ma lavapiatti a riposo) e lavapiatti attiva (con sportello chiuso).

Inoltre le specifiche dicono che se la lavapiatti non può sopportare un lavaggio con un carico equivalente a 5 camicie, quindi deve essere previsto anche uno stato di errore.

Quindi, l'insieme degli stati, Q , può quindi essere:

$$Q = \{a_0, a_1, a_2, a_3, a_4, a_5, c_0, c_1, c_2, c_3, c_4, c_5, l_0, l_1, l_2, l_3, l_4, \text{errore}\}$$

dove la prima lettera indica lo stato relativo allo sportello ed al pulsante di attivazione (a per sportello aperto, c per sportello chiuso, e l per lavaggio), mentre il numero in pedice indica lo stato del cestello, espresso in camicie caricate.

Lo stato *errore* è tale per cui una volta raggiunto non lo si possa più lasciare. Questa caratteristica formalizza il fatto che la situazione di errore è irreversibile, cioè non esiste una sequenza di azioni che permetta di riassorbire una situazione non accettabile.

Le azioni che possono essere effettuate sono:

- l'inserimento di un piatto;
- l'estrazione di un piatto;
- l'apertura dello sportello;
- la chiusura dello sportello;
- la attivazione della lavapiatti;
- lo spegnimento della lavapiatti.

Le specifiche non chiariscono cosa succeda se si cerca di prelevare un piatto non presente nel cestello. Si può ipotizzare che questa azione non abbia conseguenze. Allo stesso modo, si può ipotizzare che il tentativo di aprire lo sportello

quando esso sia già aperto, o di chiuderlo quando esso sia già chiuso, non abbia alcun effetto.

L'insieme dei simboli, Σ , può essere:

$$\Sigma = \{i, s, a, c, o, t\}$$

dove i rappresenta l'inserimento di un piatto, s l'estrazione dal cestello di un piatto, a e c rappresentano rispettivamente l'apertura e la chiusura dello sportello, e , infine, o e t rappresentano rispettivamente l'attivazione e lo spegnimento della lavapiatti.

L'insieme dei simboli può essere esteso aggiungendo un simbolo che rappresenti l'evento di terminazione della operazione di lavaggio. Tuttavia, tale evento può in prima battuta essere rimpiazzato dall'operazione di spegnimento manuale (t).

Si può inoltre ipotizzare che il tentativo di caricare o scaricare il cestello a sportello chiuso causi un errore irreversibile e quindi comporti la transizione dell'automa nello stato *errore*.

Ogni sequenza di azioni che non comporti il raggiungimento dello stato *errore* rappresenta il normale funzionamento della lavapiatti. Pertanto, qualsiasi sequenza di simboli che non porti nello stato *errore* deve venire accettata, e, quindi, tutti gli stati tranne *errore* compongono l'insieme degli stati finali, F .

Si può ipotizzare che lo stato iniziale sia quello relativo alla lavapiatti scarica, spenta e con lo sportello chiuso, c_0 .

Con le ipotesi fatte, dovrebbero essere accettate, per esempio, le seguenti sequenze di azioni: *aicot*, *aiicasco*, *ototai*. Al contrario, verrebbero rifiutate, tra le altre, le seguenti sequenze di azioni: *i*, *aici*, *aiiii*, *aiiiiico*. Va notato che aggiungendo un qualsiasi suffisso ad una stringa rifiutata, si ottiene sempre una stringa rifiutata: se una certa sequenza di azioni porta in uno stato non accettabile, qualsiasi sequenza di azioni ad essa successiva non può renderla accettabile.

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

Una variante possibile può essere individuata osservando che le operazioni sullo sportello (apertura e chiusura) sono mutuamente esclusive. Pertanto, potrebbero essere sostituite da una singola azione di apertura/chiusura il cui effetto sarebbe quello di aprire lo sportello se chiuso, e di chiuderlo se aperto. Analogamente, anche le operazioni di attivazione e spegnimento della lavastoviglie potrebbero essere modellate da una singola azione.

Un'altra variante possibile riguarda l'insieme degli stati finali, F . Se F fosse ristretto allo stato iniziale (cioè lavapiatti scarica, disattiva e con lo sportello chiuso) si modellerebbero le sequenze di azioni tali da riportare la lavapiatti nella situazione di "riposo" e pronta per essere nuovamente utilizzata.

Esercizio 5

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

$$\bullet E = (a + bc)^2(ba^* + c)^*$$

Quali fra le seguenti stringhe vengono descritte da E ?

- a) *aaa*
- b) *bcabca*
- c) *aabbacac*
- d) *bccabb*
- e) *aabbcc*
- f) *bcabacc*

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

Osserviamo innanzitutto l'espressione regolare E è la concatenazione di due sottoespressioni: $E_1 = (a+bc)^2$ e $E_2 = (ba^*+c)^*$. Quindi, le stringhe descritte da E dovranno obbligatoriamente avere un suffisso descritto da E_2 eventualmente preceduto da un prefisso descritto da E_1 (poiché E_1 descrive anche la stringa vuota). Questa premessa semplificherà la spiegazione delle soluzioni di seguito riportate.

δ	i	s	a	c	o	t
a_0	a_1	a_0	a_0	c_0	a_0	a_0
a_1	a_2	a_0	a_1	c_1	a_1	a_1
a_2	a_3	a_1	a_2	c_2	a_2	a_2
a_3	a_4	a_2	a_3	c_3	a_3	a_3
a_4	a_5	a_3	a_4	c_4	a_4	a_4
a_5	errore	a_4	a_5	c_5	a_5	a_5
c_0	errore	errore	a_0	c_0	l_0	c_0
c_1	errore	errore	a_1	c_1	l_1	c_1
c_2	errore	errore	a_2	c_2	l_2	c_2
c_3	errore	errore	a_3	c_3	l_3	c_3
c_4	errore	errore	a_4	c_4	l_4	c_4
c_5	errore	errore	a_5	c_5	errore	c_5
l_0	errore	errore	l_0	l_0	l_0	c_0
l_1	errore	errore	l_1	l_1	l_1	c_1
l_2	errore	errore	l_2	l_2	l_2	c_2
l_3	errore	errore	l_3	l_3	l_3	c_3
l_4	errore	errore	l_4	l_4	l_4	c_4
errore	errore	errore	errore	errore	errore	errore

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

a) aaa

Il prefisso aa può essere descritto da E_1 , ma la rimanente sottostringa, a , non può essere descritta da E_2 (il simbolo a dovrebbe essere preceduto da almeno un simbolo b).

La stringa aaa non viene descritta da E : $aaa \notin \mathcal{L}(E)$.

b) $bcabca$

Il prefisso bca può essere descritto da E_1 , ma la rimanente sottostringa bca non può essere descritta da E_2 (anche qui, il simbolo a dovrebbe essere preceduto da almeno un simbolo b).

La stringa $bcabca$ non viene descritta da E : $bcabca \notin \mathcal{L}(E)$.

c) $aabbacac$

Il prefisso aa può essere descritto da E_1 , ma la rimanente sottostringa $bbacac$ non può essere descritta da E_2 : il penultimo simbolo, a , dovrebbe essere preceduto da almeno un simbolo b , invece è preceduto da c .

La stringa $aabbacac$ non viene descritta da E : $aabbacac \notin \mathcal{L}(E)$.

d) $bccabb$

Il prefisso bcc non può essere descritto da E_1 in quanto presenta un simbolo c non preceduto da un simbolo b .

La stringa $bccabb$ non viene descritta da E : $bccabb \notin \mathcal{L}(E)$.

e) $aabbcc$

$$aabbcc \subseteq (a)(a)(b)(b)(c)(c) \subseteq (a+bc)(a+bc)(ba^*)(ba^*)(c)(c) \subseteq (a+bc)^2(ba^*+c)(ba^*+c)(ba^*+c) \subseteq (a+bc)^2(ba^*+c)^4 \subseteq (a+bc)^2(ba^*+c)^*$$

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

f) $bcabacc$

$$bcabacc \subseteq (bc)(a)(ba)(c)(c) \subseteq (bc+a)^2(ba^*)(c)(c) \subseteq (a+bc)^2(ba^*+c)(ba^*+c)(ba^*+c) \subseteq (a+bc)^2(ba^*+c)^3 \subseteq (a+bc)^2(ba^*+c)^*$$

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

Esercizio 6

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

- $cbcaabb$
- $abbabbb$
- $bcaabbb$

- *cccabab*

ma non le seguenti:

- *bbabbca*
- *abbaba*
- *abbaabbc*
- *acaacb*

Soluzione

Si può notare che tutte le stringhe da includere contengono solo due simboli a , eventualmente separati da simboli b . I rimanenti simboli sono solo b o c e si trovano nella parte iniziale delle stringhe. Questa caratteristica può essere descritta dall'espressione regolare $(b + c)^*ab^*a$. Nessuna delle stringhe del secondo gruppo viene descritta da tale espressione regolare:

- *bbabbca*: ha una c fra le due a ;
- *abbaba*: ha tre simboli a ;
- *abbaabbc*: ha tre simboli a ;
- *acaacb*: ha tre simboli a (e le prime due a sono intervallate da c).

Altre espressioni regolari che rispettano le specifiche:

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

Una descrizione alternativa può essere ricavata notando che tutte le stringhe da includere terminano con b e sono lunghe 7 simboli, mentre l'unica stringa da escludere che termina per b hanno lunghezza 6. Pertanto, l'espressione $(a + b + c)^6b$ soddisfa i requisiti. Analogo ragionamento può essere fatto per motivare l'espressione regolare $(a + b + c)^5(a + b)^2$.