Università degli Studi di Milano

Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2007–2008 docente: Stefano Ferrari

13.02.2008 — Soluzione del secondo compitino — 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:

- $L_1 = \{x, y\}$
- $L_2 = \{c, cx, cy\}$

Descrivere i linguaggi:

a) $L_3 = L_1 \cap L_2$

b) $L_4 = L_1 \cup L_2$

c) $L_5 = L_2 L_1$

d) $L_6 = {L_1}^2$

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

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) $L_3 = L_1 \cap L_2 = \emptyset$
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) $L_4 = L_1 \cup L_2 = \{c, cx, cy, x, y\}$

c) $L_5 = L_2 L_1 = \{cx, cxx, cxy, cy, cyx, cyy\}$

d) $L_6 = L_1^2 = \{xx, xy, yx, yy\}$

e) $L_7 = L_2^* L_1^*$
L'insieme L_7 è dato dalle stringhe formate come concatenazione di un numero arbitrario (eventualmente nullo) di elementi di L_2 seguito da una concatenazione di un numero arbitrario (eventualmente nullo) di elementi di L_1. Poiché sia ${L_1}^*$ che ${L_2}^*$ sono composti da infiniti elementi, anche L_7 avrà infiniti elementi. L'insieme $\{\epsilon, xxy, ccxccx, cx\}$ 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 $\{\epsilon, ycx, xcxcxycxc\}$ 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: $P = \{S ::= K,\ K ::= d|aH|bH,\ H ::= a|bK|cH\}$

Quali fra le seguenti stringhe vengono generate da G?

a) *acbac*

b) *accbd*

c) *abbca*

d) *bbaad*

e) *bcbaa*

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)

	acbac
	S
$S ::= K$	K
$K ::= aH$	aH
$H ::= cH$	acH
$H ::= bK$	$acbK$
$K ::= aH$	$acbaH$
$H ::= cH$	$acbacH$

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

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

b)

	accbd
	S
$S ::= K$	K
$K ::= aH$	aH
$H ::= cH$	acH
$H ::= cH$	$accH$
$H ::= bK$	$accbK$
$K ::= d$	$accbd$

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

c)

	abbca
	S
$S ::= K$	K
$K ::= aH$	aH
$H ::= bK$	abK
$K ::= bH$	$abbH$
$H ::= cH$	$abbcH$
$H ::= a$	$abbca$

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

d)

	bbaad
	S
$K ::= bH$	bH
$H ::= bK$	bbK
$K ::= aH$	$bbaH$
$H ::= a$	$bbaa$

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

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

e)

	bcbaa
	S
$S ::= K$	K
$K ::= bH$	bH
$H ::= cH$	bcH
$H ::= bK$	$bcbK$
$K ::= aH$	$bcbaH$
$H ::= a$	$bcbaa$

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

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_0	q_0	q_0	q_3
q_1	q_1	q_1	q_2	q_3	q_1
q_2	q_2	q_2	q_1	q_1	q_2
q_3	q_2	q_3	q_1	q_1	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

Esercizio 4

a) quattro stringhe accettate da A:

- ebabd
- bcad
- deac
- eccc

b) quattro stringhe rifiutate da A:

- bcda
- ecca
- eba
- aabdd

Esercizio 4

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

La batteria è utilizzata per immagazzinare energia durante la fase di carica, energia che può poi essere utilizzata per compiere lavoro durante la fase d'uso. La batteria può essere in carica (quando inserita in un apposito carica-batteria), in uso (quando inserita in un utensile) oppure a riposo. Con il susseguirsi dei cicli di carica e di uso, la batteria subisce un degrado della sua capacità di accumulare energia.

Ipotizzare che la batteria nuova contenga energia pari a quattro ore d'uso e che la quantità d'energia accumulata in un'ora di carica sia pari all'energia consumata durante un'ora d'uso. Quando è a riposo, l'energia accumulata non subisce variazioni.

Per ogni sessione di carica, la carica massima accumulabile è minore della carica accumulata alla fine dell'ultima sessione di carica (o all'inizio di

una sessione d'uso). In particolare, la carica accumulabile diminuisce della carica corrispondente ad un'ora d'uso.

Quando la carica accumulata dalla batteria è completamente esaurita, la batteria non può più essere ricaricata.

Per sessione di carica si intendono dei periodi di tempo durante i quali la batteria è posta in carica (o a riposo) senza essere in uso. Analogamente, per sessione d'uso si intendono dei periodi di tempo durante i quali la batteria è posta in uso (o a riposo) senza essere in carica.

Ipotizzare che non si possano verificare contemporaneamente più azioni e che le azioni abbiano effetto immediato. Modellare l'automa in modo che esso accetti solo le stringhe che descrivono il normale (e sicuro) utilizzo della batteria. In particolare, individuare possibili situazioni fisicamente irrealizzabili o pericolose e formalizzarle in modo che l'automa rifiuti le successioni di azioni che porterebbero l'uso della batteria 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'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 o le proprietà del sistema stesso.

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.

Lo stato della batteria si può descrivere attraverso tre sottostati (o proprietà): la carica accumulata, la carica accumulabile e la condizione in cui si trova (riposo, uso, carica). Il valore della carica accumulata e di quella accumulabile è misurabile in ore, e precisamente può valere da 0 a 4 ore (solo valori interi). Considerando che la carica accumulata non può essere superiore alla carica accumulabile e che se la carica accumulata vale 0 (batteria esaurita) il valore corrispondente agli altri sottostati è indifferente, gli stati possibili sono i seguenti: Con queste considerazioni l'insieme degli stati, Q, è:

$$\begin{aligned} Q \;=\; & \{R_{44}, R_{34}, R_{24}, R_{14}, R_{33}, R_{23}, R_{13}, R_{22}, \\ & R_{12}, R_{11}, U_{44}, U_{34}, U_{24}, U_{14}, U_{33}, U_{23}, \\ & U_{13}, U_{22}, U_{12}, U_{11}, C_{44}, C_{34}, C_{24}, C_{14}, \\ & C_{33}, C_{23}, C_{13}, C_{22}, C_{12}, C_{11}, E\} \end{aligned}$$

dove la lettera indica la situazione (riposo, uso, carica), il primo numero le ore di carica accumulata e il secondo numero le ore di carica accumulabili. Lo stato E indica invece la batteria esaurita.

Le azioni che possono essere compiute sulla batteria sono:

- porre la batteria a riposo,
- porre la batteria sotto carica,
- porre la batteria in uso.

Inoltre, deve essere considerato il trascorrere del tempo. Poiché le specifiche descrivono eventi della durata di un'ora, è naturale modellare il tempo con simboli che rappresentano un periodo di tempo della durata di un'ora.

L'alfabeto, Σ, sarà quindi: $\Sigma = \{r, u, c, t\}$. I simboli indicheranno rispettivamente il porre la batteria a riposo, in uso o in carica, mentre t indicherà il trascorrere di un'ora di tempo.

L'effetto del tempo è relativamente semplice da descrivere: se la batteria è in carica, la carica accumulata aumenterà fino a raggiungere la carica accumulabile; se la batteria è in uso, la carica accumulata diminuirà fino all'esaurimento; se, infine, la batteria è a riposo, la carica accumulata non viene modificata. In ogni caso, il tempo non influisce sulla carica accumulabile.

L'effetto delle altre azioni, invece, è un po' più complesso perché può agire sulla carica accumulabile. In particolare, l'interruzione di una sessione di carica fissa come nuova carica accumulabile la carica al momento accumulata.

Le specifiche non chiariscono cosa succeda se si cerca di mettere a riposo (o in carica, o in uso) la batteria quando questa sia già a risposo (o in carica, o in uso). Si può ipotizzare che questa azione non abbia conseguenze. Allo stesso modo, si può ipotizzare che prolungare il tempo di carica non abbia effetto, una volta raggiunta la carica pari a quella accumulabile.

Si può invece ragionevolmente ipotizzare che il tentativo di utilizzare o caricare una batteria esaurita non rappresenti il corretto uso della batteria; pertanto tale comportamento può essere catturato attraverso un opportuno stato errore (*err*).

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

Si può ipotizzare che lo stato iniziale sia quello relativo alla batteria carica al massimo e a riposo: R_{44}.

Con le ipotesi fatte, dovrebbero essere accettate, per esempio, le seguenti sequenze di azioni: *uttctttr* (stato finale R_{33}), *utttctut* (stato finale U_{12}), *cttttutrutttr* (stato finale E). Al contrario, verrebbero rifiutate, tra le altre, le seguenti sequenze di azioni: *uttttttt*, *utttctutt*. 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

δ	r	u	c	t
R_{44}	R_{44}	U_{44}	C_{44}	R_{44}
R_{34}	R_{34}	U_{34}	C_{34}	R_{34}
R_{24}	R_{24}	U_{24}	C_{24}	R_{24}
R_{14}	R_{14}	U_{14}	C_{14}	R_{14}
R_{33}	R_{33}	U_{33}	C_{33}	R_{33}
R_{23}	R_{23}	U_{23}	C_{23}	R_{23}
R_{13}	R_{13}	U_{13}	C_{13}	R_{13}
R_{22}	R_{22}	U_{22}	C_{22}	R_{22}
R_{12}	R_{12}	U_{12}	C_{12}	R_{12}
R_{11}	R_{11}	U_{11}	C_{11}	R_{11}
U_{44}	R_{44}	U_{44}	C_{44}	U_{34}
U_{34}	R_{34}	U_{34}	C_{34}	U_{24}
U_{24}	R_{24}	U_{24}	C_{24}	U_{14}
U_{14}	R_{14}	U_{14}	C_{14}	E
U_{33}	R_{33}	U_{33}	C_{33}	U_{23}
U_{23}	R_{23}	U_{23}	C_{23}	U_{13}
U_{13}	R_{13}	U_{13}	C_{13}	E
U_{22}	R_{22}	U_{22}	C_{22}	U_{12}
U_{12}	R_{12}	U_{12}	C_{12}	E
U_{11}	R_{11}	U_{11}	C_{11}	E
C_{44}	R_{44}	U_{44}	C_{44}	C_{44}
C_{34}	R_{33}	U_{33}	C_{34}	C_{44}
C_{24}	R_{22}	U_{22}	C_{24}	C_{34}
C_{14}	R_{11}	U_{11}	C_{14}	C_{24}
C_{33}	R_{33}	U_{33}	C_{33}	C_{33}
C_{23}	R_{22}	U_{22}	C_{23}	C_{33}
C_{13}	R_{11}	U_{11}	C_{13}	C_{23}
C_{22}	R_{22}	U_{22}	C_{22}	C_{22}
C_{12}	R_{11}	U_{11}	C_{12}	C_{22}
C_{11}	R_{11}	U_{11}	C_{11}	C_{11}
E	E	err	err	E
err	err	err	err	err

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

non accettabile, qualsiasi sequenza di azioni ad essa successiva non può renderla accettabile.

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

Le specifiche rendono possibili diverse semplificazioni. Prima tra tutte, per diminuire il numero di stati dell'automa, la diminuzione della carica accumulabile massima: passando da 4 a 3 ore, il numero di stati diminuisce considerevolmente. Un'altra semplificazione consiste nel rilassare la specifica relativa all'effetto memoria: in tal caso, la capacità accumulabile non diminuisce con l'uso, e l'automa si riduce ad un semplice contatore (incremento se in carica, decremento se in uso).

Esercizio 5

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

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

Individuare, motivando le risposte, quali fra le seguenti stringhe vengono descritte da E:

a) *bcaaacb*

b) *ccaabbb*

c) *abaccb*

d) *abbbccb*

e) *aabbccb*

f) *abccab*

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

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

a) *bcaaacb*
Nessuna stringa descritta da E_1 può aver b come primo simbolo, e, pertanto, neanche E può descrivere una stringa che inizi per b.

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

b) *ccaabbb*
$ccaabbb = (cca)(ab)(bb) \subseteq (c^*a)(ab)(b^2) \subseteq (c^*a + ab)^2(b^2 + c^*b)^*$

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

c) *abaccb*
$abaccb = (ab)(a)(ccb) \subseteq (ab)(c^*a)(c^*b) \subseteq (ab)(c^*a)(b^2 + c^*b) \subseteq (c^*a + ab)^2(b^2 + c^*b)^*$

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

d) *abbbccb*
Tutti i simboli b presenti nelle stringhe descritte da E_1 possono essere presenti solo se preceduti da un simbolo a. Nella stringa considerata, dopo i primi due simboli ab è presente una sequenza di b che non possono essere generati da E_1.

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

e) *aabbccb*
$aabbccb = (a)(ab)(b)(ccb) \subseteq (c^*a)(ab)(c^*b)(c^*b) \subseteq (c^*a)(ab)(b^2 + c^*b)(b^2 + c^*b) \subseteq (c^*a + ab)^2(b^2 + c^*b)^*$

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

f) *abccab*
$abccab = (ab)(cca)(b) \subseteq (ab)(c^*a)(c^*b) \subseteq (c^*a + ab)^2(b^2 + c^*b)^*$

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

Esercizio 6

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

- *baaaacaa*
- *bcccbabc*
- *aacaacac*
- *ccbca*

ma non le seguenti:

- *accbacba*
- *ccabab*
- *aacbacb*
- *bcbccba*

Le stringhe da descrivere terminano per a o per c, mentre quelle da escludere terminano per a o per b. Quindi, una opportuna regola per distinguere le stringhe che terminano per a potrebbe fornire l'espressione regolare cercata. Si può notare che le stringhe da descrivere che terminano per a, hanno come simbolo precedente alla sequenza di a il simbolo c (*baaaacaa*, *ccbca*), mentre nelle stringhe da escludere è il simbolo b a precedere il simbolo a (*accbacba*, *bcbccba*) Questa caratteristica può essere descritta dall'espressione regolare ca^*, che ha anche la proprietà di descrivere il solo simbolo c e può quindi essere utilizzata per descrivere il suffisso delle stringhe da descrivere. Pertanto, l'espressione regolare $(a+b+c)^*ca^*$ descrive tutte le stringhe del primo insieme ed esclude le stringhe del secondo insieme:

- *accbacba*: termina con a, ma tale simbolo non è preceduto da un simbolo c;
- *ccabab*: non termina né per a, né per c;
- *aacbacb*: non termina né per a, né per c;
- *bcbccba*: termina con a, ma tale simbolo non è preceduto da un simbolo c.

Altre espressioni regolari che rispettano le specifiche:

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