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

19.07.2006 — 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) $L_6 = {L_2}^3$

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) $L_3 = L_1 \cap L_2 = \emptyset$
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) $L_6 = L_2^3 = \{ababab, ababc, abcab, abcc, cabab, cabc, ccab, ccc\}$

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) dielementi di L_2. Poiché sia ${L_1}^*$ che ${L_2}^*$ sono composti da infiniti elementi, anche L_7 avrà infiniti elementi. L'insieme $\{\epsilon, bbbcbc, ababab, abcbab\}$ 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 $\{\epsilon, bab, bcaabbabaab\}$ 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) $acaab$

b) $acadb$

c) $cccaa$

d) *ccab*

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)

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

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: $acaab \notin \mathcal{L}(G)$.

b)

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

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

c)

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

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

d)

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

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

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

e)

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

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_3	q_0	q_1	q_2	q_3
q_1	q_1	q_1	q_1	q_3	q_1
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:

- *abec*
- *daaa*
- *daabbb*
- *cbebeb*

b) quattro stringhe rifiutate da A:

- *dea*
- *aaade*
- *beee*
- *dbbacd*

Esercizio 4

Modellare, tramite un automa a stati finiti deterministico, il funzionamento di un forno a microonde.

Il forno a microonde è dotato di uno sportello che permette l'accesso al piano interno e di un pulsante di attivazione. Nel normale funzionamento, l'utente apre lo sportello, pone il cibo da scaldare sul piano interno, chiude lo sportello e attiva il forno. Al termine del ciclo di irradiazione, l'utente svuota il forno.

Il piano interno è dotato di un sensore che rileva la presenza (o l'assenza) dell'oggetto da scaldare.

Attivare il forno senza aver chiuso lo sportello non ha effetti, così come attivarlo a forno vuoto. L'apertura dello sportello durante la fase di irradiazione, causa la terminazione dell'irradiazione.

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

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.

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

Lo stato in cui si trova il piano interno può essere descritto dalla presenza o dall'assenza di peso ad esso applicato, cioè, semplificando, dal fatto che il forno sia pieno o sia vuoto; quindi, due stati sono necessari per descrivere questo sottosistema. Lo sportello può essere aperto o chiuso, quindi due stati sono sufficienti per descrivere tale sottosistema. Infine, il forno può essere attiva o a riposo: anche questa situazione può essere descritta da due stati.

Quindi lo stato del forno potrebbe essere descritto da $2 \times 2 \times 2 = 8$ stati. Tuttavia, le specifiche consentono di ridurre il numero di stati necessari. Il forno non può essere attivo e con lo sportello aperto. Lo stesso vale per il piano interno e l'attivazione: il forno non irraggia, se è vuoto. Ciò permette di eliminare alcuni stati e di ridurre a 5 il numero di stati necessari (quelli possibili). È inoltre opportuno aggiungere uno stato *errore* per formalizzare le situazioni impossibili.

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

$$Q = \{apr, avr, cpi, cpr, cvr, errore\} \quad (1)$$

dove la prima lettera indica lo stato relativo allo sportello (a per "aperto", c per "chiuso"), la seconda al piano interno (p per "pieno', v per "vuoto") e la terza al pulsante di attivazione (i per "irraggiamento", r per "riposo").

Le azioni che possono essere effettuate sono:

- l'inserimento di un piatto di cibo;
- l'estrazione di un piatto di cibo;
- l'apertura dello sportello;
- la chiusura dello sportello;
- la attivazione del dispositivo irradiante;
- lo spegnimento del dispositivo irradiante;

Le specifiche chiariscono che se si apre lo sportello durante la fase di irradiazione, tale attività cessa.

Non viene invece specificato quale deve essere il comportamento dell'automa per azioni quali il tentativo di aprire lo sportello quando esso sia già aperto, o di chiuderlo quando esso sia già chiuso Si può ipotizzare che azioni del genere non abbiano alcun effetto.

Azioni fisicamente impossibili, quali l'inserimento di un piatto di cibo quando lo sportello è chiuso, o il tentativo di inserire più di un piatto, devono invece essere rilevate e proibite. Tali

azioni devono quindi portare l'automa nello stato *errore*. Questo stato deve essere 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.

L'insieme dei simboli, Σ, può essere:

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

dove i e s rappresentano rispettivamente l'inserimento e l'estrazione di un piatto, a e c rappresentano rispettivamente l'apertura e la chiusura dello sportello, o e t rappresentano rispettivamente l'attivazione e lo la disattivazione del dispositivo di irradiazione, e, infine, il simbolo r rappresenta l'evento di terminazione della operazione di riscaldamento del cibo.

L'evento r potrebbe in prima battuta essere rimpiazzato dall'operazione di spegnimento manuale (t).

Ogni sequenza di azioni che non comporti il raggiungimento dello stato *errore* rappresenta il normale funzionamento del forno a microonde. 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 al forno vuoto, spento e con lo sportello chiuso, *cvr*.

Con le ipotesi fatte, dovrebbero essere accettate, per esempio, le seguenti sequenze di azioni: *aicor*, *acacac*, *oooaicots*. Al contrario, verrebbero rifiutate, tra le altre, le seguenti sequenze di azioni: *i*, *aici*, *aiiii*, *aiiiico*. 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, $\delta : Q \times \Sigma \to Q$ 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 si attivazione e spegnimento del dispositivo di irradiazione 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 forno vuoto, disattivo e con lo sportello chiuso) si modellerebbero le sequenze di azioni tali da riportare il forno nella situazione di "riposo" e pronto per essere nuovamente utilizzato.

Esercizio 5

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

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

Quali fra le seguenti stringhe vengono descritte da E?

a) *bac*

b) *cbbbca*

c) *abccab*

d) *bcabbcc*

e) *abcbaac*

f) *bcbcbcbbc*

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: $E_1 = (a+bc)^2$ 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	r
apr	$errore$	avr	apr	cpr	apr	apr	apr
avr	apr	avr	avr	cvr	apr	avr	avr
cpi	$errore$	$errore$	apr	cpi	cpi	cpr	cpr
cpr	$errore$	$errore$	apr	cpr	cpi	cpr	cpr
cvr	$errore$	$errore$	avr	cvr	cvr	cvr	cvr
$errore$	$errore$	$errore$	$errore$	$errore$	$errore$	$errore$	$errore$

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

a) *bac*
Il prefisso *ba* non può essere descritto da E_1 (il simbolo b dovrebbe essere seguito da un simbolo c).

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

b) *cbbbca*
Il prefisso c non può essere descritto da E_1 (il simbolo c dovrebbe essere preceduto da un simbolo b).

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

c) *abccab*
Il prefisso *abc* può essere descritto da E_1, ma la rimanente sottostringa *cab* 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 *abccab* non viene descritta da E: $abccab \notin \mathcal{L}(E)$.

d) *bcabbcc*
$bcabbcc = (bc)(a)(b)(b)(c)(c) \subseteq (bc + a)^2(ba^*)(ba^*)(c)(c) \subseteq (bc + a)^2(ba^* + c)^4 \subseteq (a + bc)^2(ba^* + c)^*$

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

e) *abcbaac*
$abcbaac = (a)(bc)(baa)(c) \subseteq (a + bc)^2(ba^2)(c) \subseteq (a + bc)^2(ba^*)(c) \subseteq (a + bc)^2(ba^* + c)^2 \subseteq (a + bc)^2(ba^* + c)^*$

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

f) *bcbcbcbbc*
$bcbcbcbbc = (bc)(bc)(b)(c)(b)(b)(c) \subseteq (a + bc)(a + bc)(ba^*)(c)(ba^*)(ba^*)(c) \subseteq (a + bc)^2(ba^* + c)^5 \subseteq (a + bc)^2(ba^* + c)^*$

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

Esercizio 6

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

- *bccbccc*
- *acabbcc*
- *aaabcbc*
- *cabbccc*

ma non le seguenti:

- *ccbccab*
- *bccbbcca*
- *bccbcb*
- *babbabc*

Soluzione

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

- *ccbccab*: ha una a fra le due b;
- *bccbbcca*: ha tre simboli b;
- *bccbcb*: ha tre simboli b;
- *babbac*: ha tre simboli b (e le prime due b sono intervallate da a).

Altre espressioni regolari che rispettano le specifiche:

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

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