Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2003–2004

docente: Stefano Ferrari

03.02.2004 — Soluzione della seconda parte — Versione A

Esercizio 1

Siano dati i linguaggi L_1 e L_2:

- $L_1 = \{0, 1, 2\}$
- $L_2 = \{x, 1, a\}$

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) $L_6 = {L_2}^2$

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) $L_3 = L_1 \cap L_2 = \{1\}$

b) $L_4 = L_1 \cup L_2 = \{0, 1, 2, x, a\}$
Nota: L'elemento 1 deve essere incluso solo una volta.

c) $L_5 = L_1 L_2 = \{0x, 01, 0a, 1x, 11, 1a, 2x$ $21, 2a\}$

d) $L_6 = {L_2}^2$
L'insieme L_6 è formato dalle stringhe che si ottengono concatenando due stringhe (qualsiasi) appartenenti a L_2. Poiché L_2 ha 3 elementi, possono essere formate $3^2 = 9$ stringhe come concatenazione di due elementi di L_2:
$L_6 = \{xx, x1, xa, 1x, 11, 1a, ax, a1, aa\}$.

e) $L_7 = {L_1}^* L_2$
L'insieme L_7 è formato da stringhe che hanno un elemento di L_2 prefissato da una concatenazione di un numero arbitrario (eventualmente nullo) di elementi di L_1. Poiché ${L_1}^*$ è composto da infiniti elementi, anche L_7 avrà infiniti elementi. L'insieme $\{x, 12210a, 001021\}$ 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 $\{\epsilon, 0x112x, 212x0a11\}$ 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 $\{\epsilon, 02011, a1xaa, 22011axx\}$ 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: $P = \{S ::= K,\ K ::= d|Hb,\ H ::= a|Kc|Hb\}$

Quali fra le seguenti stringhe vengono generate da G?

a) dcb

b) $dbcba$

c) $abbb$

d) $abbcb$

e) $bbad$

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

Soluzione

a) *dcb*

	S
$S ::= K$	K
$K ::= Hb$	Hb
$H ::= Kc$	Kcb
$K ::= d$	dcb

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

b) *dbcba*

	S
$S ::= K$	K

Non esiste nessuna regola che permetta di ottenere il simbolo a dal metasimbolo K. La stringa *dbcba* non è quindi generata da G: $dbcba \notin L(G)$.

c) *abbb*

	S
$S ::= K$	K
$K ::= Hb$	Hb
$H ::= Hb$	Hbb
$H ::= Hb$	$Hbbb$
$H ::= a$	$abbb$

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

d) *abbcb*

	S
$S ::= K$	K
$K ::= Hb$	Hb
$H ::= Kc$	Kcb
$K ::= Hb$	$Hbcb$
$H ::= Hb$	$Hbbcb$
$H ::= a$	$abbcb$

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

e) *bbad*

	S
$S ::= K$	K
$K ::= d$	d

Non è possibile aggiungere altri simboli alla stringa generata, in quanto non ci sono altri metasimboli nella stringa parziale. La stringa *bbad* non è quindi generata da G: $bbad \notin L(G)$.

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

Soluzione

a) quattro stringhe accettate da A:

- aab
- bccd
- ceaa
- db

b) quattro stringhe rifiutate da A:

- aaa
- badd
- dabc
- b

Esercizio 4

Un robot autonomo deve circolare su un pista di colore bianco con il bordo destro di colore verde e il bordo sinistro di colore blu. Una banda rossa (larga quanto la pista) contraddistingue l'arrivo. Il robot è dotato di un sensore in grado di percepire il colore della pista sottostante.

Modellare il comportamento del robot tramite un automa a stati finiti deterministico, dove gli stati rappresentano le manovre che il robot deve eseguire (*curva a destra*, *curva a sinistra*, *avanti diritto* e *fermo*) e i valori letti dal sensore (*rosso*, *bianco*, *verde* e *blu*) rappresentano la stringa di input.

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:
  $Q = \{\textit{vaga per il campo}, \textit{evita il bordo}, \textit{fermo}\}$
- alfabeto di input, Σ:
  $\Sigma = \{\textit{rosso}, \textit{bianco}, \textit{nero}\}$

Dalle specifiche è possibile dedurre i seguenti comportamenti:

- se il robot si trova sul bianco, deve continuare ad esplorare il campo;
- se si trova sul rosso, è sul bordo e deve riportarsi all'interno del campo;
- se si trova sul nero, deve fermarsi (ha raggiunto l'obiettivo).

In assenza di specifiche, si può ipotizzare che una volta incontrato il colore nero, il robot si fermi anche se il sensore rileva altri colori. Quindi, i comportament precedenti sono validi per tutti gli stati, ad eccezione di quando il robot è fermo. Tale comportamento può essere descritto tramite la tabella delle transizioni, $\delta : Q \times \Sigma \to Q$ è riportata in Tabella 1.

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

In assenza di esplicite specifiche, sono legittime le seguenti assunzioni:

- tutti gli stati sono finali ($F = Q$): non ci sono sequenze di simboli di input che rappresentano una situazione fisicamente impossibile o che causano un comportamento non lecito
- il robot inizia a funzionare dopo essere stato posto sulla pista: si esclude che il primo colore che il sensore rileva sia qualcosa di diverso dal bianco (*vaga per il campo* è lo stato iniziale).

Possono inoltre essere considerate altre varianti:

stato iniziale fittizio si aggiunge all'automa di cui sopra uno stato che non rappresenta nessuna manovra. È uno stato (non finale) q_0 con le seguenti transizioni:
$\delta(q_0, \textit{rosso}) = \textit{evita il bordo}$,
$\delta(q_0, \textit{bianco}) = \textit{vaga per il campo}$,
$\delta(q_0, \textit{nero}) = \textit{fermo}$.

$F = \{\textbf{\textit{fermo}}\}$ l'automa accetta solo le sequenze che condurrebbero il robot alla regione nera. Con questa variante si può aggiungere uno stato *errore* che catturi l'automa se dopo un simbolo *nero* venga presentato un simbolo diverso.

Esercizio 5

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

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

Quali fra le seguenti stringhe vengono descritte da E?

a) *bcabcacaa*

b) *aaabcaccc*

c) *acac*

d) *bbaaaacac*

e) *bcaccaa*

f) *bcbcaaccc*

g) *aaaaccc*

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,

$\boldsymbol{\delta}$	*rosso*	*bianco*	*nero*
vaga per il campo	*evita il bordo*	*vaga per il campo*	*fermo*
evita il bordo	*evita il bordo*	*vaga per il campo*	*fermo*
fermo	*fermo*	*fermo*	*fermo*

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

$\{s\}$, 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) *bcabcacaa*
$bcabcacaa = (bcabc)(ac)(aa) \subseteq (bc+a)^3ac(a)^2 \subseteq (bc+a)^3ac(a+c)^2 \subseteq (bc+a)^*ac(a+c)^2$.

La stringa *bcabcacaa* viene descritta da E.

b) *aaabcaccc*
$aaabcaccc = (aaabc)(ac)(cc) \subseteq (bc+a)^4ac(c)^2 \subseteq (bc+a)^4ac(a+c)^2 \subseteq (bc+a)^*ac(a+c)^2$.

La stringa *aaabcaccc* viene descritta da E.

c) *acac*
$acac = (ac)(ac) \subseteq ac(a+c)^2 \subseteq (bc+a)^*ac(a+c)^2$.

La stringa *acac* viene descritta da E.

d) *bbaaaacac*
La stringa *bbaaaacac* inizia per una doppia b. Tale sottostringa non può essere descritta da E.

e) *bcaccaa*
La stringa *bcaccaa* ha *cc* come sottostringa composta dal terz'ultimo e quart'ultimo simbolo ($bca\underline{cc}aa$). Essa non può essere quindi descritta da E in quanto E richiede che la sottostringa nella posizione indicata sia *ac* ($(bc+a)^*\underline{ac}(a+c)^2$).

f) *bcbcaaccc*
$bcbcaaccc = (bcbca)(ac)(cc) \subset (bc+a)^3ac(c)^2 \subset (bc+a)^3ac(a+c)^2 \subseteq (bc+a)^*ac(a+c)^2$.

La stringa *bcbcaaccc* viene descritta da E.

g) *aaaaccc*
$aaaaccc = (aaa)(ac)(cc) = a^3ac(c)^2 \subset (bc+a)^3ac(a+c)^2 \subseteq (bc+a)^*ac(a+c)^2$.

La stringa *aaaaccc* viene descritta da E.

Esercizio 6

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

- *caaabcbb*
- *ccc*
- *cbbbbb*
- *caaaacbbb*

ma non le seguenti:

- *acaabbbc*
- *baacca*
- *acac*
- *cbba*

Soluzione

Si può notare che le stringhe da descrivere iniziano tutte per c. Inoltre, se in tali stringhe sono presenti dei simboli a, essi sono immediatamente seguenti alla c iniziale. Questa caratteristica può essere descritta dall'espressione regolare $ca^*(b+c)^*$:

- c'è una c iniziale: $\underline{c}a^*(b+c)^*$
- eventualmente seguita da una sequenza di a: $c\underline{a^*}(b+c)^*$
- e da una qualsiasi combinazione di b e c: $ca^*\underline{(b+c)^*}$

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

- *acaabbbc*: non ha la c iniziale
- *baacca*: non ha la c iniziale
- *acac*: non ha la c iniziale
- $cbb\underline{a}$: la a non è immediatamente seguente la c.

La soluzione proposta, non è tuttavia unica. Per esempio, anche $ca^*(b+c)^2b^*$ risponde ai requisiti richiesti.