Antwoorden Languages & Machines (Oefening 2)

1. Originele grammatica G (uit opgave 4.4 van het boek):

$$G = \begin{cases} S & \to & A\,B \mid B\,C\,S \\ A & \to & a\,A \mid C \\ B & \to & b\,B \mid \lambda \\ C & \to & c\,C \mid \lambda \end{cases}$$

G_1: (nieuw startsymbool, S_0, niet recursief maken)

$$G_1 = \begin{cases} S_0 & \to & A\,B \mid B\,C\,S \\ S & \to & A\,B \mid B\,C\,S \\ A & \to & a\,A \mid C \\ B & \to & b\,B \mid \lambda \\ C & \to & c\,C \mid \lambda \end{cases}$$

G_2: (non-contracting maken door null-regels te elimineren).
De null regels zijn: $\{C, B, A, S, S_0\}$

$$G_2 = \begin{cases} S_0 & \to & A \mid B \mid C \mid S \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid B\,C\,S \mid \lambda \\ S & \to & A \mid B \mid C \mid S \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid B\,C\,S \\ A & \to & a\,A \mid a \mid C \\ B & \to & b\,B \mid b \\ C & \to & c\,C \mid c \end{cases}$$

G_3: (chain rules elimineren).
De niet-triviale kettingen zien er als volgt uit:

$$\begin{array}{rcl} chain(S) & = & \{A, B, C, S\} \\ chain(S_0) & = & \{A, B, C, S, S_0\} \end{array}$$

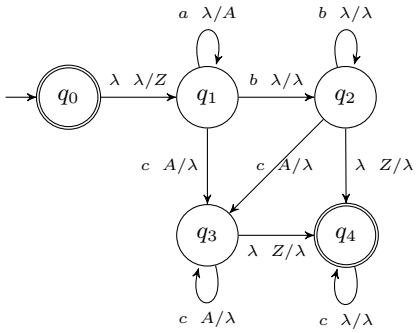
$$G_3 = \begin{cases} S_0 & \to & a\,A \mid a \mid c\,C \mid c \mid b\,B \mid b \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid B\,C\,S \mid \lambda \\ S & \to & a\,A \mid a \mid c\,C \mid c \mid b\,B \mid b \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid B\,C\,S \\ A & \to & a\,A \mid a \mid c\,C \mid c \\ B & \to & b\,B \mid b \\ C & \to & c\,C \mid c \end{cases}$$

G_4: (rechterkanten fatsoeneren)

$$G_4 = \begin{cases} S_0 & \to & X\,A \mid a \mid Z\,C \mid c \mid Y\,B \mid b \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid U\,S \mid \lambda \\ S & \to & X\,A \mid a \mid Z\,C \mid c \mid Y\,B \mid b \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid U\,S \\ A & \to & X\,A \mid a \mid Z\,C \mid c \\ B & \to & Y\,B \mid b \\ C & \to & Z\,C \mid c \\ X & \to & a \\ Y & \to & b \\ Z & \to & c \\ U & \to & B\,C \end{cases}$$

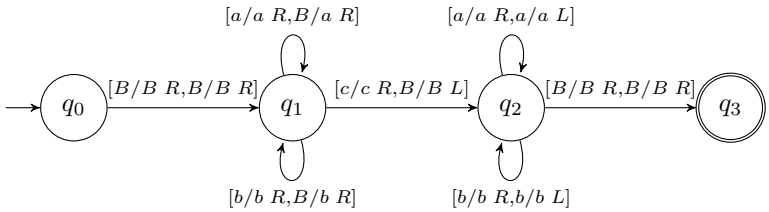
2. $L = \{a^i\, b^*\, c^j \mid j \geq i \geq 0\}$

   (a) Een deterministische PDA voor L:



   Er wordt eerst een Z op de stack gezet, om later te testen dat de stack (bijna) leeg is. In q_1 worden a's gelezen, en geteld op de stack. Dan kan er een willekeurig aantal b's volgen, die verder niet hoeven te worden geteld. Na de eerste c vanaf q_1 of q_2 springen we naar q_3. Hier worden net zoveel c's gelezen als er a's waren. Als de stack leeg is springen we naar q_4. Daar mogen nog meer c's volgen. De automaat is deterministisch, omdat er vanuit geen enkele toestand overlappende transities mogelijk zijn.

3. (a)



   (b) Er wordt eerst een maximaal woord $w \in \{a, b\}^*$ van tape 1 naar tape 2 gekopieerd. Na een c wordt gecheckt of het resterende woord w^R op tape 1 matcht met het omgekeerde woord op tape 2. De berekening is:

$[q_0; *BaabcbaaB; *BBBBB]$
$[q_1; B * aabcbaaB; B * BBBB]$
$[q_1; Ba * abcbaaB; Ba * BBB]$
$[q_1; Baa * bcbaaB; Baa * BB]$
$[q_1; Baab * cbaaB; Baab * B]$
$[q_2; Baabc * baaB; Baa * bB]$
$[q_2; Baabcb * aaB; Ba * abB]$
$[q_2; Baabcba * aB; B * aabB]$
$[q_2; Baabcbaa * B; *BaabB]$
$[q_3; BaabcbaaB*; B * aabB]$

De TM termineert in de accepterende toestand q_3, dus het *aabcbaa* wordt geaccepteerd.

(c) Deze TM termineert altijd (na 1 pass over het woord op tape 1), dus hij beslist deze taal.

(d) Deze TM is deterministisch, want het symbool op tape 1 bepaalt uniek welke transitie wordt genomen.

Voorbeeldtoets: uitwerkingen

1. (a) (i) Gesloten:

$$\underbrace{\underbrace{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}_{\det \neq 0} \cdot \underbrace{\begin{bmatrix} e & f \\ g & h \end{bmatrix}}_{\det \neq 0}}_{\det \neq 0}$$

$(\det M_1 M_2 = \det M_1 . \det M_2)$.

(ii) Eenheidselement: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

(iii) Inverse:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{\det \begin{bmatrix} a & b \\ c & d \end{bmatrix}} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

alle berekeningen in $\mathbb{Z}_{11}$,

dus $\frac{1}{\det \begin{bmatrix} a & b \\ c & d \end{bmatrix}} = (\underbrace{ad - bc}_{\neq 0})^{-1} \pmod{11}$, dus inverse bestaat.

(iv) Associativiteit: geldt voor matrixvermenigvuldiging, dus hoeft niet nader onderzocht te worden.

(b). $\det \begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix} = 10 - 18 = -8 = 3$

$11 = 3.3 + 2$
$3 = 1.2 + 1 \Rightarrow 1 = 3 - 1.2 = 3 - 1.(11 - 3.3)$
$= 4.3 - 1.11$

$\Rightarrow 3^{-1} = 4$.

dus $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}^{-1} = 4 \cdot \begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 20 & -24 \\ -12 & 8 \end{bmatrix}$

$= \begin{bmatrix} 9 & 9 \\ 10 & 8 \end{bmatrix}$ controle $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 9 & 9 \\ 10 & 8 \end{bmatrix} = \begin{bmatrix} 78 & 66 \\ 77 & 67 \end{bmatrix}$

$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

(c) Bepaal het aantal matrices met determinant nul:

$ad - bc = 0 \Rightarrow ad = bc$

$d \in \{1, \to 10\}$, dan $a = bcd^{-1}$

met $b, c \in \mathbb{Z}_{11}$ geeft dit $11 \times 11 \times 10 =$ **1210** mogelijkheden

$d = 0$, dan $a \in \mathbb{Z}_{11}$, $\begin{cases} (b,c) = (0,c) \to 11 \text{ mogelijkheden} \\ (b,0) \to 10 \text{ "} \\ ((0,0) \text{ niet dubbel tellen}) \end{cases}$

in totaal $11 \cdot 21 =$ **231**

Samen geeft dit: 1441 mogelijkheden.

Het aantal elementen van G is dus:

$11^4 - 1441 = 14641 - 1441 = 13200$.

2. $165 = 3 \cdot 5 \cdot 11$, $U(st) = U(s) \oplus U(t)$ indien $ggd(s,t) = 1$.

$$U(165) \sim U(3) \oplus U(5) \oplus U(11)$$
$$\sim U(15) \oplus U(11)$$
$$\sim U(33) \oplus U(5)$$
$$\sim U(3) \oplus U(55)$$

(b) p priem $\Rightarrow U(p) \sim \mathbb{Z}_{p-1}$

dus $U(165) \sim U(3) \oplus U(5) \oplus U(11)$
$\sim \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{10}$

$(a,b,c) \in \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{10}$

$|(a,b,c)| = kgv(|a|, |b|, |c|)$

$((a,b,c))^{20} = (a^{20}, b^{20}, c^{20}) = (0,0,0)$

$\downarrow \quad \downarrow \quad \downarrow$

$\in \mathbb{Z}_2 \quad \in \mathbb{Z}_4 \quad \in \mathbb{Z}_{10}$ (optelling)

dus $a^{20} = \underbrace{(a + \ldots + a)}_{20\times} = 0$ etc.

$U(165)$ is dus niet cyclisch.

3. $S = \{a \mid a \in \mathbb{Z},\ 2|a \text{ of } 3|a\}$.

$2 \in S$, $3 \in S$ maar $2+3 = 5 \notin S \Rightarrow$ geen deelring.

4. $p(x) = 1 + x + x^3 + x^4 + x^5$

a. $(x^3 + ax^2 + bx + c)(x^2 + dx + e)$

$= x^5 + x^4(a+d) + x^3(ad + b + e) + x^2(ae + bd + c)$
$+ x(be + cd) + ce$

x^0: $ce = 1 \Rightarrow \boxed{c = 1 \quad e = 1}$

x^1: ~~$ae + bd + c = 1 \Rightarrow \quad a +$~~

$be + cd = 1 \Rightarrow \quad b + d = 1 \Rightarrow d = 1 - b = 1 + b$

x^2 $ae + bd + c = 0 \Rightarrow \quad a + b + b^2 + 1 = 0$

$\Rightarrow \quad a + 1 = 0 \qquad (b + b^2 = b + b = 0).$

$\Rightarrow \boxed{a = 1}$

x^4: ~~ad~~ $a + d = 1$, $a = 1 \Rightarrow \boxed{d = 0} \Rightarrow \boxed{b = 1}$

x^3: $ad + b + e = \quad 1 + 1 = 0 \neq 1$

Conclusie: ontbinding niet mogelijk.

b. 2-3 ontbinding niet mogelijk,
$p(0) = p(1) = 1$, dus 1-4 ontbinding ook niet mogelijk, dus $p(x)$ irreducibel.

c. $p(x)$ irreducibel $\Rightarrow \langle p(x) \rangle$ maximaal ideaal $\Rightarrow \mathbb{Z}_2[x]/\langle p(x) \rangle$ lichaam.

d. $F = \{ ax^4 + bx^3 + cx^2 + dx + e + \langle p(x) \rangle \mid a, b, c, d, e \in \mathbb{Z}_2 \}$

dus $|F| = 2^5 = 32$.

(e) $\dim_{\mathbb{Z}_2}(\mathbb{F}) = 5$, basis $1, x, x^2, x^3, x^4$.

(f) $\mathbb{Z}_2 \subset \mathbb{K} \subset \mathbb{F}$

$\underbrace{\qquad}_{d} \quad \underbrace{\qquad}_{e}$

$\dim_{\mathbb{Z}_2}(\mathbb{K}) = d \Rightarrow |\mathbb{K}| = 2^d$.

als $\dim_{\mathbb{K}} \mathbb{F} = e$ dan $de = 5$,

immers: $\dim_{\mathbb{K}} \mathbb{F} = e \Rightarrow |\mathbb{K}|^e = |\mathbb{F}| \Rightarrow$

$(2^d)^e = 2^5 \Rightarrow de = 5$

(g) $de = 5 \Rightarrow d = 1$ of $d = 5$

$d = 1 \Rightarrow \mathbb{K} = \mathbb{Z}_2$

$d = 5 \Rightarrow \mathbb{K} = \mathbb{F}$.

8| $3^{20} = 3^{2^4} \cdot 3^{2^2}$

Compute

$3^{2^0} = 3 \pmod 5$

$3^{2^1} = (3^{2^0})^2 = 9 = 4 \pmod 5$

$3^{2^2} = (3^{2^1})^2 = 16 = 1 \pmod 5$

$3^{2^3} = (3^{2^2})^2 = 1^2 = 1 \pmod 5$

$3^{2^4} = (3^{2^3})^2 = 1^2 = 1 \pmod 5$

$\Rightarrow 3^{20} = 3^{2^4} \cdot 3^{2^2} = 1 \cdot 1 = 1 \pmod 5$

Alternatively, $\langle 3 \rangle = \{3^1, 3^2, 3^3, 3^4\}$ so
$3^1 = 3$, $3^2 = 4$, $3^3 = 2$, $3^4 = 1$

$|\langle 3 \rangle| = 4$ and $3^{20} = (3^4)^5 = 1 \pmod 5$
$3^4 = 1$, as 4 is order of group!

9| $n = 55 = 5 \cdot 11$, that means $|U_{55}| = 4 \cdot 10 = 40 = r$.
To decode M, need e^{-1} in $\mathbb{Z}_r$, so 7^{-1} in $\mathbb{Z}_{40}$.

Euclid: $40 = 5 \cdot 7 + 5$
$7 = 1 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

$\Rightarrow 1 = 5 - 2 \cdot 2 = 40 - 5 \cdot 7 - 2(7 - 5) = 40 - 5 \cdot 7 - 2(7 - 40 + 5 \cdot 7)$
$= 3 \cdot 40 + (-17)7$

$\Rightarrow 7^{-1} = -17 = 40 - 17 = 23 \pmod{40}$

9| vervolg

Now $C = 2$, need to compute $2^{23} \pmod{55}$

$23 = 2^4 + 2^2 + 2^1 + 2^0$

$2^{2^0} = 2$

$2^{2^1} = 4$

$2^{2^2} = 16$

$2^{2^3} = (16)^2 = 256 = 36$

$2^{2^4} = (36)^2 = 1.296 = 31 \pmod{55}$

$\Rightarrow 2^{23} = 31 \cdot 16 \cdot 4 \cdot 2 = 62 \cdot 64$

$= 7 \cdot 9 = 63 = 8 \pmod{55}$

$\Rightarrow h = 8$