1 Answers Languages & Machines (Test Exam 2)

1. Original grammar G (assignment 4.4 from the book):

$$G = \left\{ \begin{array}{lcl} S & \to & A\,B \mid B\,C\,S \\ A & \to & a\,A \mid C \\ B & \to & b\,B \mid \lambda \\ C & \to & c\,C \mid \lambda \end{array} \right.$$

G_1: (add new start symbol, S_0, making it non-recursive)

$$G_1 = \left\{ \begin{array}{lcl} S_0 & \to & A\,B \mid B\,C\,S \\ S & \to & A\,B \mid B\,C\,S \\ A & \to & a\,A \mid C \\ B & \to & b\,B \mid \lambda \\ C & \to & c\,C \mid \lambda \end{array} \right.$$

G_2: (make it non-contracting, by eliminating null-rules).
The null-rules are: $\{C, B, A, S, S_0\}$

$$G_2 = \left\{ \begin{array}{lcl} S_0 & \to & A \mid B \mid C \mid S \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid B\,C\,S \mid \lambda \\ S & \to & A \mid B \mid C \mid S \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid B\,C\,S \\ A & \to & a\,A \mid a \mid C \\ B & \to & b\,B \mid b \\ C & \to & c\,C \mid c \end{array} \right.$$

G_3: (eliminate the chain rules).
The non-trivial chains are:

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

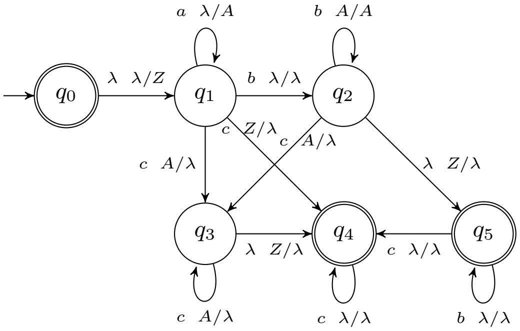
$$G_3 = \left\{ \begin{array}{lcl} S_0 & \to & a\,A \mid a \mid c\,C \mid c \mid b\,B \mid b \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid B\,C\,S \mid \lambda \\ S & \to & a\,A \mid a \mid c\,C \mid c \mid b\,B \mid b \mid A\,B \mid B\,C \mid B\,S \mid C\,S \mid B\,C\,S \\ A & \to & a\,A \mid a \mid c\,C \mid c \\ B & \to & b\,B \mid b \\ C & \to & c\,C \mid c \end{array} \right.$$

G_4: (bring the right-hand sides in the proper shape)

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

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

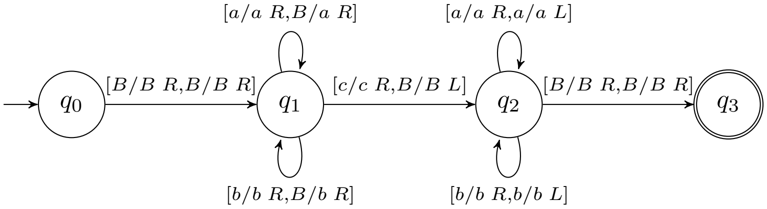
(a) This is a quite difficult exercise. Please try hard first, and convince yourself that your PDA is correct and deterministic. A deterministic PDA for L is:



First a Z is pushed on the stack, to be able to test later that the stack is empty (so we have read sufficiently many c's). In q_1 the a's are read and counted on the stack. Then an arbitrary number of b's is read in q_2, q_5, but these don't need to be counted. As long as there are A's on the stack, we still need to read c's in q_3, also popping A's. After a Z, we can still read any numbers of b's (q_5) and then c's (q_4).

The automaton is deterministic since there are no overlapping rules from the same state. The automaton is slightly complicated, since we should allow for having 0 a's and/or 0 b's and/or 0 c's.

3. (a)



(b) We first copy a maximal word $w \in \{a, b\}^*$ from tape 1 to tape 2. After a c, we check if the remaining word (supposedly w^R) on tape 1 indeed matches the reverse of the word on tape 2. The concrete computations is:

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

The TM terminates in the accepting state q_3, so the word *aabcbaa* is accepted.

(c) This TM will terminate for all inputs (even with 1 pass over the word on tape 1), so it indeed *decides* the language.

(d) This TM is deterministic, since the state and the symbol on tape 1 decide uniquely which transition will be taken. (of course, you may have defined a non-deterministic TM yourself).

2 Answers Algebra (Test Exam 2

4. V has four elements, S_3 has six elements, V can only be isomorphic to a subgroup of S_n if four divides the number of elements in S_n.

   All nonzero elements of V have order 2. Take $H = \{\epsilon, (12), (34), (12)(34)\}$. Corresponding isomorphism: $\phi((0,0)) = \epsilon$, $\phi((1,0)) = (12)$, $\phi((0,1)) = (34)$, $\phi((1,1)) = (12)(34)$.

5. (a) $Z(G)$ is a subgroup of G if for all $h_1, h_2 \in Z(G)$ also $h_1h_2 \in Z(G)$ and $h \in Z(G)$ implies that $h^{-1} \in Z(G)$. If $h_1, h_2 \in Z(G)$ then for all $g \in G$:

   $$h_1h_2g = h_1gh_2 = gh_1h_2 \quad hg = gh \Rightarrow g = h^{-1}gh \Rightarrow gh^{-1} = h^{-1}g.$$

   (b) Take:

   $$g_1 = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

   The only matrices that commute with g_1 are diagonal matrices:

   $$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

   Now take:

   $$g_2 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$$

   The only diagonal matrices that commute with g_2 are diagonal matrices of the form:

   $$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$$

   (c) Define $\phi : Z(G) \to \mathbb{R}$ by

   $$\phi(\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}) = a$$

   Check that this defines an ismorphism.

6. (a) $p(a) \neq 0$ for all $a \in \mathbb{Z}_5$, and $\deg p(x) = 3$, so $p(x)$ is irreducible.

   (b) The ideal I is generated by an irreducible polynomial and is therefore maximal in $\mathbb{Z}_5[x]$, therefore $\mathbb{Z}_5[x]/I$ is a field.

   (c) All elements of $\mathbb{F}$ are of the form

   $$a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + I \quad a_i \in \mathbb{Z}_5.$$

   It follows that $\mathbb{F}$ has 5^5 elements.

   (d) Long division of $p(x)$ by $2x + 3$ yields:

   $$p(x) = (3x^2 + 4x + 4)(2x + 3) + 4.$$

   And therefore the inverse is given by:

   $$3x^2 + 4x + 4 + I.$$

   (e) $x^3 + 3x + 2$ is also irreducible and of degree 3 and hence $\mathbb{Z}_5[x]/ < x^3 + 3x + 2 >$ is a field of 5^5 elements. Since fields of the same number of elements are isomorphic, the statement follows.

7. For each edge of the square we can choose from five colors. This yields that there are 5^4, i,e, 625 ways to paint the square. However, there are four rotations and four reflections that reduce the number of different possibilities.

   Since the square is made of iron wire, we can take D_4 as the group of symmetries. Then:

$$|\mathrm{Fix}(R_0)| = 625 \quad |\mathrm{Fix}(R_{90})| = 5 \quad |\mathrm{Fix}(R_{180})| = 25 \quad |\mathrm{Fix}(R_{270})| = 5$$

   and

$$|\mathrm{Fix}(H)| = 5^3 = 125 \quad |\mathrm{Fix}(V)| = 5^3 = 125 \quad |\mathrm{Fix}(D)| = 5^2 = 25 \quad |\mathrm{Fix}(D')| = 5^2 = 25$$

   Using Burnside's theorem it follows that the number of orbits, that is the number of different colorings is:

$$\frac{1}{8}(625 + 5 + 25 + 5 + 125 + 125 + 25 + 25) = 120.$$

8. $$\alpha = (15)(234) = (15)(24)(23).$$

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

$|\langle 3 \rangle| = 4$ and $3^{20} = (\underbrace{3^4}_{=1})^5 = 1 \pmod 5$

, 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 $2^{23} \pmod{55}$

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

$$2^{2^0} = 2$$

$$2^{2^1} = 4$$

$$2^{2^2} = 16$$

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

$$2^{2^4} = (36)^2 = 1.296 = 31 \qquad (\text{mod } 55)$$

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

$$= 7 \cdot 9 = 63 = 8 \qquad (\text{mod } 55)$$

$\Rightarrow k = 8$