# Tutorial 1: Solutions

**Exercise 1:**

1. There exists a word $\varepsilon$ such that for all words $w$, $\varepsilon * w = w = w * \varepsilon$, which one ?
2. Given $k \in \{1, \dots, n + n'\}$, what is the $k^{th}$ letter of the word $w * w'$ ?
3. Prove that concatenation is associative, which means that given three words $w$, $w'$, and $w''$, we have $(w * w') * w'' = w * (w' * w'')$. What is the 'key' argument?
4. Prove that concatenation is *cancelative* that is to say for all words $w$, $w'$, and $w''$, we have

$$w * w' \;=\; w * w'' \quad \Rightarrow \quad w' \;=\; w'' \qquad \text{and} \qquad w' * w \;=\; w'' * w \quad \Rightarrow \quad w' \;=\; w'' \,.$$

**Solution:** Given a word $w = w_1 \cdots w_n$, we write $|w| = n$ for the size of $w$.

1. If $\varepsilon * w = w$, then $|\varepsilon * w| = |\varepsilon| + |w| = |w|$, so $|\varepsilon| = 0$.

   The only word of length 0 is the empty word. We easily check that it satisfies the required equations.

$$\varepsilon = \text{the empty word}$$

2. Let $k \in \{1, \dots, n + n'\}$, then $(w * w')_k = \begin{cases} w_k & \text{if } 1 \le k \le n \\ w'_{k-n} & \text{if } n + 1 \le k \le n + n' \end{cases}$

3. We want to prove that $(w * w') * w'' = w * (w' * w'')$. To prove that two words are equal, we need:

   - to prove that they have the same length,
   - then prove that for every $k$ smaller than the length, the $k$-th letter is the same.

   First step: $|(w * w') * w''| = n + n' + n'' = |w * (w' * w'')|$.

   Second step: Let $1 \le k \le n + n' + n''$, we need to prove that $((w * w') * w'')_k = (w * (w' * w''))_k$. We proceed by case disjunction. In each case, we compute separately $((w * w') * w'')_k$ and $(w * (w' * w''))_k$ using the formula of question 2), and check that they are equal.

   (a) Case $1 \le k \le n$.

$$\begin{aligned} ((w * w') * w'')_k &= (w * w')_k && \text{because } 1 \le k \le n + n' \\ &= w_k && \text{because } 1 \le k \le n \end{aligned}$$

$$(w * (w' * w''))_k = w_k \qquad \text{because } 1 \le k \le n$$

(b) Case $n+1 \leq k \leq n+n'$.

$$\begin{aligned}((w * w') * w'')_k &= (w * w')_k && \text{because } 1 \leq k \leq n+n' \\ &= w'_{k-n} && \text{because } n+1 \leq k \leq n+n'\end{aligned}$$

$$\begin{aligned}(w * (w' * w''))_k &= (w' * w'')_{k-n} && \text{because } n+1 \leq k \leq n+n'+n'' \\ &= w'_{k-n} && \text{because } 1 \leq k-n \leq n'\end{aligned}$$

(c) Case $n+n'+1 \leq k \leq n+n'+n''$.

$$((w * w') * w'')_k = w''_{k-n-n'} \qquad \text{because } n+n'+1 \leq k \leq n+n'+n''$$

$$\begin{aligned}(w * (w' * w''))_k &= (w' * w'')_{k-n} && \text{because } n+1 \leq k \leq n+n'+n'' \\ &= w''_{k-n-n'} && \text{because } n'+1 \leq k-n \leq n'+n''\end{aligned}$$

4. - Assume $w * w' = w * w''$. We want to prove that $w' = w''$.
   First, note that $|w * w'| = |w| + |w'| = |w * w''| = |w| + |w''|$. Thus, we have $|w'| = |w''|$.
   Let us write $n = |w|$ and $n' = |w'| = |w''|$.
   Let $k \in \{1, \ldots, n'\}$, we want to show that $w'_k = w''_k$.

   $$\begin{aligned}w'_k &= (w * w')_{k+n} && \text{because } n+1 \leq k+n \leq n+n' \\ &= (w * w'')_{k+n} && \text{because } w' = w'' \\ &= w''_k && \text{because } n+1 \leq k+n \leq n+n'\end{aligned}$$

   - Assume $w' * w = w'' * w$. By the same reasoning, $|w'| = |w''|$.
   Using the same notations, for $k \in \{1, \ldots, n'\}$, we have:

   $$w'_k = (w' * w)_k = (w'' * w)_k = w''_k$$

**Exercise 2:**

1. Propose a definition for the concatenation $L * L'$ of two languages $L$ and $L'$ over $\Sigma$

2. Prove that $*$ is associative, that is to say, for all $A$, $B$, and $C$ languages over $\Sigma$ we have:

$$(A * B) * C \quad = \quad A * (B * C)$$

3. Prove that $*$ distributes over $\cup$, that is to say, for all $A$, $B$, and $C$ languages over $\Sigma$:

$$A * (B \cup C) = (A * B) \cup (A * C) \quad \text{and} \quad (B \cup C) * A = (B * A) \cup (C * A)$$

4. (a) Prove that for all $A$, $B$, and $C$ languages over $\Sigma$ we have:

$$A * (B \cap C) \subseteq (A * B) \cap (A * C) \quad \text{and} \quad (B \cap C) * A \subseteq (B * A) \cap (C * A)$$

   (b) Find a counter-example proving that the converse inclusions do not hold.

5. Recall that $\Sigma$ is identified with the words of length 1. Complete the following sentences:

(a) For $n \in \mathbb{N}$ (pay a special attention to the case $n = 0$), the language $\Sigma^n$ is the set of $\cdots$

(b) The language

$$\bigcup_{n \geqslant 0} \Sigma^n$$

is the set of $\cdots$

6. (a) Find three nonempty languages $A$, $B$, and $C$ such that $A \neq B$ but $A * C = B * C$.

   (b) Give a sufficient condition on $A$ and $B$ such that for all nonempty language $C$, we have $A * C \neq B * C$.

**Solution:**

1. $L * L' = \{w * w' \mid w \in L \text{ and } w' \in L'\}$

2. This is an equality between two sets: we proceed by double inclusion.

   - $(A * B) * C \quad \subseteq \quad A * (B * C)$:
     Assume $w \in (A * B) * C$. By definition, $w$ is of the form $w = w' * \gamma$ with $w' \in A * B$ and $\gamma \in C$. Since $w' \in A * B$, by definition again, $w' = \alpha * \beta$ with $\alpha \in A$ and $\beta \in B$. So, $w = (\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$ using the result of exercise 1, question 3. Then $w \in A * (B * C)$ since $\alpha \in A$ and $\beta * \gamma \in B * C$.
   - $A * (B * C) \quad \subseteq \quad (A * B) * C$:
     Assume $w \in (A * B) * C$. By unfolding the definitions, $w = \alpha * (\beta * \gamma)$, with $\alpha \in A$, $\beta \in B$, $\gamma \in C$. Using Ex.1, q.3, we have $w = (\alpha * \beta) * \gamma$. Therefore $w \in (A * B) * C$.

3. We show $A * (B \cup C) = (A * B) \cup (A * C)$ by double inclusion.

   $\subseteq$: Let $w \in A * (B \cup C)$, i.e., $w = \alpha * w'$ with $\alpha \in A$ and $w' \in B \cup C$. We reason by case disjunction:
   – either $w' \in B$, in which case $w \in A * B \subseteq (A * B) \cup (A * C)$.
   – or $w' \in C$, in which case $w \in A * C \subseteq (A * B) \cup (A * C)$.
   In both cases, we have proved $w \in (A * B) \cup (A * C)$.

   $\supseteq$: Let $w \in (A * B) \cup (A * C)$. We reason by case disjunction:
   – either $w \in A * B$, in which case $w = \alpha * \beta$ with $\alpha \in A$ and $\beta \in B \subseteq B \cup C$. So $w \in A * (B \cup C)$; – or $w \in A * C$, in which case $w = \alpha * \gamma$ with $\alpha \in A$ and $\gamma \in C \subseteq B \cup C$. So $w \in A * (B \cup C)$. In both cases, we have $w \in A * (B \cup C)$.

   Same reasoning for $(B \cup C) * A = (B * A) \cup (C * A)$.

   $\subseteq$: Let $w \in (B \cup C) * A$, i.e., $w = w' * \alpha$ with $\alpha \in A$ and $w' \in B \cup C$.
   Then either $w' \in B$ or $w' \in C$, and in both cases $w \in (B * A) \cup (C * A)$.

   $\supseteq$: Let $w \in (B * A) \cup (C * A)$.
   Then either $w \in B * A$ or $w \in C * A$, and in both cases $w \in (B \cup C) * A$.

4. a)
   - Assume $w \in A * (B \cap C)$.
     Then we have $w = \alpha * w'$ such that $\begin{cases} \alpha \in A & (1) \\ w' \in B & (2) \\ w' \in C & (3) \end{cases}$.
     By (1) and (2) we obtain $w \in A * B$, and by (1) and (3) we obtain $w \in A * C$.
     Therefore, $w \in (A * B) \cap (A * C)$.

- $(B \cap C) * A \subseteq (B * A) \cap (C * A)$: same reasoning.

4. b) We want to prove that there exist languages $A, B, C$ such that $(A * B) \cap (A * C) \not\subseteq A * (B \cap C)$. Let us take the one letter alphabet $\Sigma = \{a\}$.

Take $\begin{cases} A = \{a, \varepsilon\} \\ B = \{a\} \\ C = \{aa\} \end{cases}$

Then $A * B = \{aa, a\}$ and $A * C = \{aaa, aa\}$, so $(A * B) \cap (A * C) = \{aa\}$.
But $B \cap C = \varnothing$, so $A * (B \cap C) = \varnothing$.
Thus, $(A * B) \cap (A * C) \ \not\subseteq\ A * (B \cap C)$.

For the other counter example, we can just take the same languages $A, B$ and $C$, and check that $(B * A) \cap (C * A) \not\subseteq (B \cap C) * A$.

5. Given a language $L$, we define $L^n = \underbrace{L * \ldots * L}_{n \text{ times}}$.
By convention, we choose $L^0 = \{\varepsilon\}$. (The reason for this choice is that $\{\varepsilon\}$ is the neutral element for the $*$ operation on languages. Thus, we get the inductive formula $L^{n+1} = L^n * L$ even for $n = 0$).
Thus:

(a) The language $\Sigma^n$ is the set of all words of length $n$.

(b) The language $\bigcup_{n \geq 0} \Sigma^n$ is the set of all words on $\Sigma$: $\bigcup_{n \geq 0} \Sigma^n = \Sigma^*$.

6. a) Let us take the alphabet $\Sigma = \{a, b\}$. We give three counter-examples, there are many others.

$$\begin{array}{lll} A_1 = \{a, \varepsilon\} & A_2 = \{a, ab\} & A_3 = \Sigma^* \\ B_1 = \{\varepsilon\} & B_2 = \{a, aabba, abb\} & B_3 = \Sigma^* \setminus \{ab\} \\ C_1 = \{a\}^* & C_2 = \Sigma^* & C_3 = \{\varepsilon, ab\} \end{array}$$

*Remark: $B_1$ **is** a non-empty language, since it contains one element, the empty word. The only empty language is $\varnothing$.*

We can check that:

- $A_1 * C_1 = B_1 * C_1 = \{a\}^*$.
- $A_2 * C_2 = B_2 * C_2 = \{aw \mid w \in \Sigma^*\}$.
- $A_3 * C_3 = B_3 * C_3 = \Sigma^*$.

6. b) Some possible conditions:

- *"The smallest word(s) of $A$ and the smallest word(s) of $B$ have different sizes."*
  Written formally: $\min_{w \in A} |w| \ \neq\ \min_{w \in B} |w|$.
- *"The words of $A$ and $B$ begin with different letters."*
  Formally: for all $w = w_1 \cdots w_n \in A$, for all $w' = w'_1 \cdots w'_{n'} \in B$, $w_1 \neq w'_1$.
- $A \cap B = \varnothing$ (proving that this condition works is a bit difficult! Hint: look at the words of minimum length in $A, B$ and $C$).
  Try it yourself before reading the following. Take $a \in A, b \in B, c \in C$ with minimum length if their respective sets. Then $a * c$ has minimal length in $A * C$ and $b * c$ has minimum length in $B * C$.

First case : $|a * c| \leq |b * c|$. Then if $a * c \in B * C$, then we have equality, otherwise $b * c$ does not have minimum length. Then $a * c = b' * c'$ for some $b' \in B, c' \in C$. We have $|c'| \geq |c|$ since $c$ has minimum length. Then

$$|b'| + |c'| = |b' * c'| = |a * c| = |b * c| \leq |b| + |c| = |a| + |c|$$

and using minimality of the length

$$|a| = |b'| \qquad \text{and} \qquad |c'| = |c|$$

and finally we get $a = b'$ and $c = c'$. We get $a \in B$ which is a contradiction.

Second case : $|a * c| > |b * c|$. If $b * c \in A * C$ we get a contradiction with the minimality of $a * c$.

In both cases we saw that there is a elements that is in one of the sets and not the other one. Then $A * C \neq B * C$.

**Exercise 3:**

1. Suppose that $\Sigma = \{0, 1\}$. Give a finite rewriting system $\mathcal{P}$ such that for all words $w \in \{0, 1\}^*$:
   - if some 0 occurs in $w$, then $w \to^* 0$
   - $w \to^* 1$ in all other cases.
2. Suppose that $\Sigma = \{0, \dots, n-1\}$ for $n \in \mathbb{N} \setminus \{0\}$. Give a rewriting system $\mathcal{P}$ such that for all words $w \in \{0, \dots, n-1\}^*$ of length $\ell$, we have $w \to^* k \in \{0, \dots, n-1\}$, the word of length 1 whose unique letter is the sum of the letter of $w$ modulo $n$, i.e.

$$k \quad = \quad (w_1 + \cdots + w_\ell) \mod n\,.$$

**Solution:**

1. Take $\mathcal{P} = \{00 \to 0, 01 \to 0, 10 \to 0, 11 \to 1, \varepsilon \to 1\}$.
2. Take $\mathcal{P} = \{pq \to (p + q \bmod n) \mid p, q \in \Sigma\} \cup \{\varepsilon \to 0\}$.

**Exercise 4:** Given two nonempty sets $A$ and $B$, define a bijection between $\mathfrak{P}(A \times B)$ and $(\mathfrak{P}(B))^A$.
**Solution:** We define the following map

$$\begin{array}{rccc} \varphi: & \mathfrak{P}(A \times B) & \longrightarrow & (\mathfrak{P}(B))^A \\ & X & \longmapsto & a \mapsto \{b \mid (a, b) \in X\} \end{array}$$

Thus, given $X \subseteq A \times B$, $\varphi(X)$ is a function from $A$ to $\mathfrak{P}(B)$ defined as $\varphi(X)(a) = \{b \mid (a, b) \in X\}$. To show that $\varphi$ is bijective, we prove that the following map is the inverse of $\varphi$:

$$\begin{array}{rccc} \psi: & (\mathfrak{P}(B))^A & \longrightarrow & \mathfrak{P}(A \times B) \\ & f & \longmapsto & \{(a, b) \mid b \in f(a)\} \end{array}$$

- Let $X \subseteq A \times B$.

$$\begin{aligned} \psi \circ \varphi(X) &= \{(a, b) \mid b \in \varphi(X)(a)\} \\ &= \{(a, b) \mid (a, b) \in X\} \\ &= X \end{aligned}$$

- Let $f : A \to \mathfrak{P}(B)$. We want to show $\varphi \circ \psi(f) = f$, i.e., $(\varphi \circ \varphi(f))(a) = f(a)$ for all $a \in A$. So, assume $a \in A$.

$$\begin{aligned}(\varphi \circ \psi(f))(a) &= \{b \mid (a,b) \in \psi(f)\} \\ &= \{b \mid b \in f(a)\} \\ &= f(a)\end{aligned}$$