Discrete Mathematics in Computer Science

M. Helmert, G. Röger
S. Eriksson
University of Basel
Computer Science
Fall Semester 2023

Exercise Sheet 6

Due: Monday, November 6, 2023, 4pm

Please carefully read the exercises FAQ on ADAM!

Note: Submissions that are exclusively created with LaTeX will receive a bonus mark. Please submit only the resulting PDF file.

Exercise 6.1 (1 mark)

Consider the partial function $\mathbb{N}_0 \nrightarrow \mathbb{N}_0$ with

$f(1) = 0$ and

$f(n) = f(n-1) + 3$ for $n > 1$.

Specify the domain of definition and the image of f.

Exercise 6.2 (2 marks)

Specify a partial function $f : \{0, 1, 2, 3, 4, 5\} \nrightarrow \{u, v, w, x, y, z\}$ which satisfies *all* of the following properties:

(i) $|\text{img}(f)| = 4$ (ii) $3 \notin \text{dom}(f)$

(iii) $f^{-1}[\{v, x, z\}] = \{0, 1, 4, 5\}$ (iv) $f|_{\{0,1,2\}}$ is a total function

You can specify your function either by listing the mapping explicitly or by drawing the graph.

Exercise 6.3 (2 marks)

Show with an example that there are sets A, B, C and functions $f : A \to B$ and $g : B \to C$ such that $g \circ f$ is injective but g is not injective.

Exercise 6.4 (2 marks)

Let A be a non-empty set and $f : A \to B$ be a function such that there are functions

- $g : B \to A$ with $g(f(x)) = x$ for all $x \in A$ and
- $h : B \to A$ with $f(h(y)) = y$ for all $y \in B$.

Show that f must be bijective.

Exercise 6.5 (3 marks)

As a preparation for this exercise, read the short description about the enigma machine provided as a separate instruction file.

We consider an enigma machine over the alphabet $\Sigma = \{\texttt{A}, \texttt{B}, \texttt{C}, \texttt{D}, \texttt{E}\}$ with a plugboard, two rotors and a reflector. We describe the internal connections with "positions" $\{1, 2, 3, 4, 5\}$. Informally we can think of them as positions on a disk, with 1 being the topmost position and positions increasing clockwise.

The plugboard has a fixed wiring that maps the alphabet to output positions with the following function $P = \{\texttt{A} \mapsto 1, \texttt{B} \mapsto 2, \texttt{C} \mapsto 3, \texttt{D} \mapsto 4, \texttt{E} \mapsto 5\}$. Furthermore, it allows for plugging pairs of letters together, with the effect that those pairs switch position, resulting in mapping C. For example if C maps letter `A` to `C` then `A` is mapped to plugboard output $P(C(\texttt{A})) = 3$.
Afterwards the signal flows through a left rotor L, followed by right rotor R and the reflector U and then back through R, L and the plugboard. The mappings by L, R and U are all given as permutations of the positions. While the reflector is static, the actually applied mapping of the rotors depends on their current rotation n and j. We define R_0 and L_0 to be the permutation induced by the non-rotated placement of the rotors. Representing a rotation of a rotor by one position by permutation $\rho = \{1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 5, 5 \mapsto 1\}$, the actually applied permutation of the right rotor after n rotations can now be described by $R_n = \rho^{-n} \circ R_0 \circ \rho^n$. The definition is analogous for the left rotor and j rotations.
Given $P, C, L_0, R_0, U, \rho, n$ and j the encoding of the next letter is overall defined as the permutation

$$C^{-1} \circ P^{-1} \circ L_j^{-1} \circ R_n^{-1} \circ U \circ R_n \circ L_j \circ P \circ C.$$

We consider the following configuration of the enigma machine:

- The plugboard connects letter `A` and `D`, as well as letters `B` and `C`.
- $L_0 = \{1 \mapsto 4, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 5, 5 \mapsto 3\}$
- $R_0 = \{1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 5, 5 \mapsto 1\}$
- $U = \{1 \mapsto 5, 2 \mapsto 3, 3 \mapsto 2, 4 \mapsto 4, 5 \mapsto 1\}$

(a) Specify $P \circ C$.

(b) Specify R_1.

(c) Encode the word `ED`, assuming that for encoding the first letter both L and R are in their initial placement (i.e. $n = j = 0$), and for encoding the second letter rotor R has been rotated once (i.e. $n = 1, j = 0$).

Submission rules:
Upload a single PDF file (ending in .pdf). Put the names of all group members on top of the first page. Make sure your PDF has size A4 (fits the page size if printed on A4). There is a template that satisfies these requirements available on ADAM.