Exercise 1. Promela and Spin (12 Marks \textit{bonus})

Figure 1 shows a simple production robot with one arm that picks up blanks arriving on a feed belt and transports them to a deposit belt. The file \texttt{production-cell-one-arm.pml} (downloadable from the website) contains a simple Promela model of this production robot.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{production-cell-one-arm.png}
\caption{Simplified production robot with one arm}
\end{figure}

\textbf{a.} (4 Marks) Specify the following properties in LTL (using variables and labels available in the model). Not all of the properties may be satisfied by the model. Verify them with Spin and state whether the model satisfies the properties. Also state whether you think that the properties are system requirements, domain knowledge (environment assumptions), or software specification.

---

\textsuperscript{1}this means that by doing this exercise it is possible to achieve >100\% of points.
i. There are never two blanks on the table

ii. Always if there is a plate on the table, there must eventually be a blank on the deposit belt.

iii. If property i holds, then also property ii holds.

iv. Always if the arm is moving to the deposit belt, it will eventually arrive at the deposit belt without being at the table before that, unless it is again moving to the table. Also, always if the arm is moving to the table, it will eventually arrive at the table without being at the deposit belt before that, unless it is again moving to the deposit belt.

v. If property i holds, then iv holds.

b. (8 Marks) (Disclaimer: We did not actually create a solution for this task ourselves and we know that creating such a model will be challenging and time-consuming. Therefore, we will also give points to partial solutions—if they are accompanied by a short text, possibly with diagrams, max. 2 pages, that explains what you did and what problems you encountered.)

Extend the model to represent a production robot with two arms and a press as shown in Fig. 2. Model the controller as two parallel processes that communicate via a synchronous channel. One controller should be responsible for controlling armA and another should be responsible for controlling the press and armB. Specify also additional LTL properties, e.g., that armA must not release the blank into the press before it arrived at the press.

![Diagram of the production robot with two arms, a press, and two controllers](image)

Figure 2: Production robot with two arms, a press, and two controllers

---

2Note: In Promela, you can use the `#define` directive to define a subformula that you reuse in other formulae.
Exercise 2. Büchi Automata (3 Marks)
Give Büchi automata that describe all infinite words over $\Sigma = \{a, b, c\}$

a. that contain at least one $a$.

b. where an $a$ is never immediately followed by a $b$.

c. that can contain at least one $a$ and one $b$, but then has an infinite sequence of $c$s.

Exercise 3. Nested Depth-First Search (3 Marks)
Figure 3 shows a Büchi Automaton without transition labels. Describe in which order the outer (blue) and inner (red) depth-first searches of the nested depth-first search algorithm visit the states of this automaton. Assume that if a state has more than one outgoing transition, the transitions will be explored in the order as indicated by the numbers (1 and 2) that label some of the transitions in Fig. 3.

Use a notation like “b0, b1, r5, r6, b3, . . . , bx – report cycle!” to describe in which order the blue and red depth-first searches mark a state with the number as shown in the figure as blue/red and whether in the end a cycle is reported.

Figure 3: Example Büchi Automaton without transition labels

Exercise 4. Büchi Automata Product Construction (6 Marks)

a. Create two Büchi automata over the alphabet $\Sigma = \{a, b\}$ that accept the following languages.

i. All words that contain at least two $a$s.

ii. All words where an $a$ is always eventually followed by a $b$.

b. Create a Büchi automaton accepting the intersection of these languages.