Solutions to Exercises 1

Exercise 1 (Sheffer Stroke)**.** Any logical constant and connector can be simulated with Sheffer strokes. In fact:

$$\begin{aligned}
\neg\varphi \quad & \equiv \varphi \uparrow \varphi \\
1 \equiv \varphi \uparrow \neg\varphi \quad & \equiv \varphi \uparrow (\varphi \uparrow \varphi) \\
0 \equiv \neg 1 \quad & \equiv (\varphi \uparrow (\varphi \uparrow \varphi)) \uparrow (\varphi \uparrow (\varphi \uparrow \varphi)) \\
\varphi_0 \land \varphi_1 \equiv \neg(\varphi_0 \uparrow \varphi_1) \quad & \equiv (\varphi_0 \uparrow \varphi_1) \uparrow (\varphi_0 \uparrow \varphi_1) \\
\varphi_0 \lor \varphi_1 \equiv (\neg\varphi_0 \uparrow \neg\varphi_1) & \equiv ((\varphi_0 \uparrow \varphi_0) \uparrow (\varphi_1 \uparrow \varphi_1)) \\
\varphi_0 \to \varphi_1 \equiv \neg\varphi_0 \lor \varphi_1 \quad & \equiv (((\varphi_0 \uparrow \varphi_0) \uparrow (\varphi_0 \uparrow \varphi_0)) \uparrow (\varphi_1 \uparrow \varphi_1))
\end{aligned}$$

Exercise 2 (Decision Procedure for SAT)**.** First we rewrite the formulas using only the allowed symbols:

1. $((a \to b) \to a) \to a \equiv \neg(\neg(\neg a \lor b) \lor a) \lor a$
2. $\neg(a \land b) \to (\neg a \lor \neg b) \equiv \neg\neg(a \land b) \lor (\neg a \lor \neg b)$
3. $((\neg a \to b) \land (a \to b)) \to b \equiv \neg((\neg\neg a \lor b) \land (\neg a \lor b)) \lor b$

Then we derive $\neg F \vdash 0$ (we collapse sequences of Simp):

1.

$$\dfrac{\dfrac{\dfrac{\neg(\neg(\neg(\neg a \lor b) \lor a) \lor a) \quad \neg(\neg(\neg(\neg a \lor b) \lor a) \lor a)}{(\neg(\neg(\neg(\neg 0 \lor b) \lor 0) \lor 0)) \lor (\neg(\neg(\neg(\neg 1 \lor b) \lor 1) \lor 1))}\text{CA (on a)}}{0 \lor (\neg(\neg(\neg b \lor 1) \lor 1))}\textsc{Simp}}{\neg(\neg(\neg b \lor 1) \lor 1)}\textsc{Simp}$$

Note that, if we are being pedantic, we cannot simplify further as the simplification rules only cover cases where a literal is on the left.

$$\dfrac{\dfrac{\dfrac{\neg(\neg(\neg b \lor 1) \lor 1) \quad \neg(\neg(\neg b \lor 1) \lor 1)}{(\neg(\neg(\neg 0 \lor 1) \lor 1)) \lor (\neg(\neg(\neg 1 \lor 1) \lor 1))}\text{CA (on b)}}{0 \lor 0}\textsc{Simp}}{0}\textsc{Simp}$$

2.

$$\dfrac{\dfrac{\dfrac{\neg\,(\neg\neg(a \land b) \lor (\neg a \lor \neg b)) \quad \neg\,(\neg\neg(a \land b) \lor (\neg a \lor \neg b))}{(\neg\,(\neg\neg(0 \land b) \lor (\neg 0 \lor \neg b))) \lor (\neg\,(\neg\neg(1 \land b) \lor (\neg 1 \lor \neg b)))}\text{CA (on a)}}{0 \lor (\neg\,(\neg\neg b \lor \neg b))}\textsc{Simp}}{\neg\,(\neg\neg b \lor \neg b)}\textsc{Simp}$$

$$\dfrac{\dfrac{\neg\,(\neg\neg b \lor \neg b) \quad \neg\,(\neg\neg b \lor \neg b)}{(\neg\,(\neg\neg 0 \lor \neg 0)) \lor (\neg\,(\neg\neg 1 \lor \neg 1))}\,\text{CA (on b)}}{0}\,\textsc{Simp}$$

3.

$$\dfrac{\dfrac{\neg\,(\neg((\neg\neg a \lor b) \land (\neg a \lor b)) \lor b) \quad \neg\,(\neg((\neg\neg a \lor b) \land (\neg a \lor b)) \lor b)}{(\neg\,(\neg((\neg\neg 0 \lor b) \land (\neg 0 \lor b)) \lor b)) \lor (\neg\,(\neg((\neg\neg 1 \lor b) \land (\neg 1 \lor b)) \lor b))}\,\text{CA (on a)}}{\neg\,(\neg(b \land 1) \lor b) \lor \neg\,(\neg b \lor b)}\,\textsc{Simp}$$

$$\dfrac{\dfrac{\neg\,(\neg(b \land 1) \lor b) \lor \neg\,(\neg b \lor b) \quad \neg\,(\neg(b \land 1) \lor b) \lor \neg\,(\neg b \lor b)}{(\neg\,(\neg(0 \land 1) \lor 0) \lor \neg\,(\neg 0 \lor 0)) \lor (\neg\,(\neg(1 \land 1) \lor 1) \lor \neg\,(\neg 1 \lor 1))}\,\text{CA (on b)}}{0}\,\textsc{Simp}$$

Exercise 3 (if-then-else)**.**

1. Let's first express f1 and f2 as propositional formulas. **if** x **then** y **else** z means that when x is true then y is true and when x is not true z is true. In propositional logic this becomes $(x \to y) \land (\neg x \to z)$. By repeating the process and reducing them to CNF, we get the following formulas for f1 and f2:

$$\begin{aligned}
\text{f1(a, b, c)} &\equiv ((a \lor b) \to (((b \land \neg a) \to (b \land c)) \land (\neg(b \land \neg a) \to (\neg b \land c)))) \land (\neg(a \lor b) \to c) \\
&\equiv (\neg(a \lor b) \lor ((\neg(b \land \neg a) \lor (b \land c)) \land ((b \land \neg a) \lor (\neg b \land c)))) \land ((a \lor b) \lor c) \\
&\equiv (\neg a \lor \neg b) \land c
\end{aligned}$$

$$\begin{aligned}
\text{f2(a, b, c)} &\equiv (c \to (a \to \neg b) \land (\neg a \to 1)) \land (\neg c \to 0) \\
&\equiv (\neg c \lor (\neg a \lor \neg b) \land (a \lor 1)) \land (c \lor 0) \\
&\equiv (\neg a \lor \neg b) \land c
\end{aligned}$$

which proves that they do always produce the same output. One could also have computed the truth tables of each formula and check that they were equal.

2. Since $a \uparrow b \equiv$ **if** (**if** a **then** b **else false**) **then false else true**, and any formula can be written with Sheffer strokes, any formula can also be written only using **if then else**.

   By noting that $\varphi \equiv$ **if** a **then** $\varphi[a := 1]$ **else** $\varphi[a := 0]$ where $a \in \text{FV}(\varphi)$ and by applying the identity recursively we can express any formula with **if then else** with only one variable in the condition. The proof goes by induction on the number of variables in the formula, and by noting that if φ has n variables and $a \in \text{FV}(\varphi)$, then $\varphi[a := 0]$ and $\varphi[a := 1]$ contain only $n - 1$ variables.

Exercise 4 (Propositional Tautologies)**.** Remember that for any formulas P, Q, and R, the formula $P \rightarrow Q \rightarrow R$ is parsed as $P \rightarrow (Q \rightarrow R)$ and is equivalent to $(P \wedge Q) \rightarrow R$.

1. If $P \wedge Q$ is true, then so is Q.
2. We consider two cases. If $P \rightarrow Q$ holds, then we are done, otherwise we have $P \wedge \neg Q$, and we are done as well.
3. Counterexample: $P = \top$, $Q = \bot$, $R = \bot$.
4. Counterexample: $P = \top$, $Q = \top$, $R = \bot$.
5. If R and $\neg R$ are true, then we have a contradiction and Q is true as well.
6. A formula always implies itself: $(P \rightarrow Q) \rightarrow (P \rightarrow Q)$.
7. (Peirce's law) We consider two cases. If P is true, then the whole formula is true. Otherwise, $(P \rightarrow Q)$ is true, meaning the implication $((P \rightarrow Q) \rightarrow P)$ is false. This makes the whole formula true as well.
8. Counterexample: $P = \top$, $Q = \bot$.
9. Assume $(\neg Q \rightarrow \neg P)$ and P are true. Assume now (by contradiction) that Q is false. Then, we would have that P is false, which is a contradiction. Therefore Q is true and so is the whole formula.
10. Counterexample: $P = \top$, $Q = \top$, $R = \bot$.
11. Assume the three disjunctions are true. We want to show that P is true as well. Consider the first two disjunctions (the third one is not needed). In either of them, if the left-hand-side (P) is true, then we are done. Otherwise, it means their right-hand-sides Q and $\neg Q$ are both true, which is a contradiction.
12. Counterexample: $P = \top$, $Q = \bot$.
13. Assume $\neg(P \wedge Q)$ and P are both true. If Q is true as well, then, we have $P \wedge Q$ is true, which is a contradiction. Therefore Q is false, which is what we needed to prove.

1 Transition Systems and Invariants

Exercise 5 (Special Invariants)**.**

1. S is an inductive invariant. It is the largest among all invariants.

   Solution: We have $S \subseteq S$, $I \subseteq S$, and for every $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$, $s' \in S$. Therefore, S is an inductive invariant.

   Moreover, S is the largest among all invariants because any invariant needs to be a subset of S.

2. $\mathit{Reach}(M)$ is an inductive invariant.

   Solution: First, we have $\mathit{Reach}(M) \subseteq S$ and $I \subseteq \mathit{Reach}(M)$.

   Then, we want to show that for all $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$, if $s \in \mathit{Reach}(M)$, then $s' \in \mathit{Reach}(M)$

   Let $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$. Assume $s \in \mathit{Reach}(M)$. By definition of Reach, there exists a trace $(s_0, a_0, s_1, \ldots, a_n, s_n) \in \mathit{Traces}(M)$ such that $s_n = s$. By definition of Traces, we also have $(s_0, a_0, s_1, \ldots, a_n, s, a, s') \in \mathit{Traces}(M)$, which proves that $s' \in \mathit{Reach}(M)$.

3. $\mathit{Reach}(M)$ is the smallest of all possible invariants.

   Solution: By definition, any invariant is a superset of $\mathit{Reach}(M)$.

Exercise 6 (Closure of Invariants)**.**

1. union

   Solution: Let P_1 and P_2 be two invariants, i.e. $\mathit{Reach}(M) \subseteq P_1$, and $\mathit{Reach}(M) \subseteq P_2$. We have $\mathit{Reach}(M) \subseteq P_1 \cup P_2$, therefore $P_1 \cup P_2$ is also an invariant.

2. intersection

   Solution: Let P_1 and P_2 be two invariants, i.e. $\mathit{Reach}(M) \subseteq P_1$, and $\mathit{Reach}(M) \subseteq P_2$. We have $\mathit{Reach}(M) \subseteq P_1 \cap P_2$, because every state in $\mathit{Reach}(M)$ belongs to both P_1 and P_2 by assumption. Therefore $P_1 \cap P_2$ is also an invariant.

3. complement with respect to S

   Solution: Let P be an invariant, i.e. $\mathit{Reach}(M) \subseteq P$. We don't necessarily have $S \setminus \mathit{Reach}(M) \subseteq P$. For instance, we can make a machine where $\mathit{Reach}(M) = \emptyset$ (no initial states), with S a non-empty set of states, and define $P = \emptyset$.

4. operation $f : 2^S \to 2^S$ defined by $f(X) = \mathit{Reach}(M) \cup (S \setminus X)$

   Solution: For any set X (not just invariants), we have $\mathit{Reach}(M) \subseteq f(X)$, therefore $f(X)$ is an invariant.

Answer the same questions about all *inductive invariants* of M.

1. union

   Solution: Let P_1 and P_2 be two inductive invariants. We show that $P_1 \cup P_2$ is also an inductive invariant.

   First, we have $I \subseteq P_1 \cup P_2$ (because e.g. $I \subseteq P_1$).

   Second, let $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$. Assume $s \in P_1 \cup P_2$. We consider two cases. If $s \in P_1$, we use the fact that P_1 is an inductive invariant to conclude that $s' \in P_1$, and therefore $s' \in P_1 \cup P_2$. The second case is similar.

2. intersection

   Solution: Let P_1 and P_2 be two inductive invariants. We show that $P_1 \cap P_2$ is also an inductive invariant.

   First, we have $I \subseteq P_1 \cap P_2$ (because elements of I are both in P_1 and in P_2).

   Second, let $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$. Assume $s \in P_1 \cap P_2$, i.e. $s \in P_1$, and $s \in P_2$. Since P_1 is an inductive invariant, we deduce that $s' \in P_1$, and similarly since P_2 is an inductive invariant, we deduce that $s' \in P_2$. Therefore $s' \in P_1 \cap P_2$.

3. complement with respect to S

   Solution: Same counter-example as above.

4. operation $f : 2^S \to 2^S$ defined by $f(X) = \mathit{Reach}(M) \cup (S \setminus X)$

   Solution: When X is an inductive invariant, $f(X)$ is not necessarily an inductive invariant. Consider a machine with two states $S = \{s_1, s_2\}$ and no initial state. Let there be a transition from s_1 to s_2 (with some letter), and no other transitions. The set $X = \{s_2\}$ is an inductive invariant. However, $f(X) = \{s_1\}$ is not (because of the transition from s_1 to s_2).

2 Relations

Exercise 7 (Relation Identities)**.** In the solutions, some equivalences are easier to read from bottom to top (and some from top to bottom).

1. $(X \bullet r_1) \bullet r_2 = X \bullet (r_1 \circ r_2)$

Solution: Let $z \in A$. We have:

$$\begin{aligned} z \in (X \bullet r_1) \bullet r_2 &\Leftrightarrow \exists y \in X \bullet r_1.\ (y,z) \in r_2 \\ &\Leftrightarrow \exists y \in A.\ y \in X \bullet r_1 \wedge (y,z) \in r_2 \\ &\Leftrightarrow \exists y \in A.\ \exists x \in X.\ (x,y) \in r_1 \wedge (y,z) \in r_2 \\ &\Leftrightarrow \exists x \in X.\ \exists y \in A.\ (x,y) \in r_1 \wedge (y,z) \in r_2 \\ &\Leftrightarrow \exists x \in X.\ (x,z) \in r_1 \circ r_2 \\ &\Leftrightarrow z \in X \bullet (r_1 \circ r_2) \end{aligned}$$

2. $(r \cup s) \circ t = (r \circ t) \cup (s \circ t)$

   Solution: Let $x, z \in A$. We have:

$$\begin{aligned} (x,z) \in (r \cup s) \circ t &\Leftrightarrow \exists y \in A.\ (x,y) \in r \cup s \wedge (y,z) \in t \\ &\Leftrightarrow \exists y \in A.\ ((x,y) \in r \vee (x,y) \in s) \wedge (y,z) \in t \\ &\Leftrightarrow \exists y \in A.\ ((x,y) \in r \wedge (y,z) \in t) \vee ((x,y) \in s \wedge (y,z) \in t) \\ &\Leftrightarrow (\exists y \in A.\ (x,y) \in r \wedge (y,z) \in t) \vee (\exists y \in A.\ (x,y) \in s \wedge (y,z) \in t) \\ &\Leftrightarrow (x,z) \in r \circ t \vee (x,z) \in s \circ t \\ &\Leftrightarrow (x,z) \in (r \circ t) \cup (s \circ t) \end{aligned}$$

3. $(r \cap s) \circ t = (r \circ t) \cap (s \circ t)$

   Solution: A counterexample:
   $r = \{(0,1)\}$, $s = \{(0,2)\}$ and $t = \{(1,0),(2,0)\}$.

   We have $(r \cap s) \circ t = \emptyset$, while $(r \circ t) \cap (s \circ t) = \{(0,0)\}$.

4. $(r_1 \circ r_2)^{-1} = (r_2^{-1} \circ r_1^{-1})$

   Solution: Let $x, z \in A$. We have:

$$\begin{aligned} (z,x) \in (r_1 \circ r_2)^{-1} &\Leftrightarrow (x,z) \in r_1 \circ r_2 \\ &\Leftrightarrow \exists y \in A.\ (x,y) \in r_1 \wedge (y,z) \in r_2 \\ &\Leftrightarrow \exists y \in A.\ (y,x) \in r_1^{-1} \wedge (z,y) \in r_2^{-1} \\ &\Leftrightarrow \exists y \in A.\ (z,y) \in r_2^{-1} \wedge (y,x) \in r_1^{-1} \\ &\Leftrightarrow (z,x) \in r_2^{-1} \circ r_1^{-1} \end{aligned}$$

5. $X \bullet r = ran(\Delta_X \circ r)$

Solution: Let $y \in A$. We have:

$$\begin{aligned}
y \in X \bullet r &\Leftrightarrow \exists x \in X.\ (x, y) \in r \\
&\Leftrightarrow \exists x \in A.\ x \in X \wedge (x', y) \in r \\
&\Leftrightarrow \exists x \in A.\ \exists x' \in A.\ x = x' \wedge x \in X \wedge (x', y) \in r \\
&\Leftrightarrow \exists x \in A.\ \exists x' \in A.\ (x, x') \in \Delta_X \wedge (x', y) \in r \\
&\Leftrightarrow \exists x \in A.\ (x, y) \in \Delta_X \circ r \\
&\Leftrightarrow y \in ran(\Delta_X \circ r)
\end{aligned}$$

6. If $r_1 \subseteq r_1'$ then $r_1 \circ r_2 \subseteq r_1' \circ r_2$ and $r_2 \circ r_1 \subseteq r_2 \circ r_1'$.

   Solution: Let $x, z \in A$. We have:

$$\begin{aligned}
(x, z) \in r_1 \circ r_2 &\Leftrightarrow \exists y \in A.\ (x, y) \in r_1 \wedge (y, z) \in r_2 \\
&\Rightarrow \exists y \in A.\ (x, y) \in r_1' \wedge (y, z) \in r_2 \text{ because } r_1 \subseteq r_1' \\
&\Leftrightarrow (x, z) \in r_1' \circ r_2
\end{aligned}$$

   Also,

$$\begin{aligned}
(x, z) \in r_2 \circ r_1 &\Leftrightarrow \exists y \in A.\ (x, y) \in r_2 \wedge (y, z) \in r_1 \\
&\Rightarrow \exists y \in A.\ (x, y) \in r_2 \wedge (y, z) \in r_1' \text{ because } r_1 \subseteq r_1' \\
&\Leftrightarrow (x, z) \in r_2 \circ r_1'
\end{aligned}$$

7. If $r_1 \subseteq r_1'$ then $r_1 \cup r_2 \subseteq r_1' \cup r_2$ and $r_2 \cup r_1 \subseteq r_2 \cup r_1'$.

   Solution: Let $x, y \in A$. We have:

$$\begin{aligned}
(x, y) \in r_1 \cup r_2 &\Leftrightarrow (x, y) \in r_1 \vee (x, y) \in r_2 \\
&\Rightarrow (x, y) \in r_1' \vee (x, y) \in r_2 \text{ because } r_1 \subseteq r_1' \\
&\Leftrightarrow (x, y) \in r_1' \cup r_2
\end{aligned}$$

   Also,

$$\begin{aligned}
(x, y) \in r_2 \cup r_1 &\Leftrightarrow (x, y) \in r_2 \vee (x, y) \in r_1 \\
&\Rightarrow (x, y) \in r_2 \vee (x, y) \in r_1' \text{ because } r_1 \subseteq r_1' \\
&\Leftrightarrow (x, y) \in r_2 \cup r_1'
\end{aligned}$$

Exercise 8 (Transitive relations)**.**

$$\begin{aligned}
r \circ r \subseteq r &\Leftrightarrow \forall x, z \in A.\ (x, z) \in r \circ r \Rightarrow (x, z) \in r \\
&\Leftrightarrow \forall x, z \in A.\ (\exists y \in A. (x, y) \in r \wedge (y, z) \in r) \Rightarrow (x, z) \in r \\
&\Leftrightarrow \forall x, z \in A.\ \forall y \in A.\ ((x, y) \in r \wedge (y, z) \in r) \Rightarrow (x, z) \in r \\
&\Leftrightarrow \forall x, y, z \in A.\ ((x, y) \in r \wedge (y, z) \in r) \Rightarrow (x, z) \in r \\
&\Leftrightarrow \text{r is transitive}
\end{aligned}$$

Exercise 9 (Symmetric relations)**.** First, since the composition of two symmetric relations is symmetric, we can show by induction on $n \geq 0$ that for any symmetric relation r, r^n is symmetric.

Second, taking the union of symmetric relations gives a symmetric relation, which means that for any symmetric relation r, r^* is also symmetric (using the previous point).

We can establish that $r \cup r^{-1}$ is a symmetric relation, and using the second point, that $(r \cup r^{-1})^*$ is also symmetric.

Finally, let $x, t \in A$. We have:

$$\begin{aligned}
(x, t) \in r^{-1} \circ (r \cup r^{-1})^* \circ r &\Leftrightarrow \exists y \in A.\ \exists z \in A.\ (x, y) \in r^{-1} \wedge (y, z) \in (r \cup r^{-1})^* \wedge (z, t) \in r \\
&\Leftrightarrow \exists z \in A.\ \exists y \in A.\ (t, z) \in r^{-1} \wedge (z, y) \in (r \cup r^{-1})^* \wedge (y, x) \in r \\
&\Leftrightarrow (t, x) \in r^{-1} \circ (r \cup r^{-1})^* \circ r
\end{aligned}$$

To go from the first to the second line, we use the fact that $(r \cup r^{-1})^*$ is symmetric.

Exercise 10 (Transitive closure)**.**

(i) $(r \cup r^{-1})^*$ is an equivalence relation,

Solution: We have three things to prove:

1. (Reflexivity) Let $x \in A$. We have $(x, x) \in (r \cup r^{-1})^*$ because $\triangle_A \subseteq (r \cup r^{-1})^*$.
2. (Symmetry) As seen in the previous section, $(r \cup r^{-1})^*$ is symmetric.
3. (Transitive) Let $(x, y) \in (r \cup r^{-1})^*$ and $(y, z) \in (r \cup r^{-1})^*$. By definition, there exist $n, m \geq 0$ such that $(x, y) \in (r \cup r^{-1})^n$ and $(y, z) \in (r \cup r^{-1})^m$. Therefore $(x, z) \in (r \cup r^{-1})^n \circ (r \cup r^{-1})^m = (r \cup r^{-1})^{n+m}$. This shows that $(x, z) \in (r \cup r^{-1})^*$.

(ii) if s is an equivalence relation containing r, then $(r \cup r^{-1})^* \subseteq s$.

Solution: Let s be an equivalence relation containing r. We prove by induction over $n \in \mathbb{N}$ that $(r \cup r^{-1})^n \subseteq s$.

1. (Case $n = 0$) $(r \cup r^{-1})^0 = \triangle_A \subseteq s$ because s is reflexive.
2. (Case $n = n' + 1$) Assume by induction that $(r \cup r^{-1})^{n'} \subseteq s$. We know that $r \subseteq s$, and that s is symmetric, therefore $r^{-1} \subseteq s$. Thus, we also have: $r \cup r^{-1} \subseteq s$.
   Finally, we have $(r \cup r^{-1})^n = (r \cup r^{-1})^{n'} \circ (r \cup r^{-1}) \subseteq s \circ s \subseteq s$ (because s is transitive), which concludes the proof.

3 Finite State Machines with Boolean Variables

Exercise 11 (Finite State Machines with Boolean Variables)**.** No. We can establish the following inductive invariant of the configurations of the FSM:

$$\begin{aligned} P = \{((x,y),m) \mid & (x \geq 1 \Rightarrow m(B)) \wedge \\ & (y \geq 1 \Rightarrow m(A)) \wedge \\ & ((x,y) = (3,2) \Rightarrow m(C)) \wedge \\ & ((x,y) = (2,3) \Rightarrow \neg m(C) \wedge \\ & (x,y) \neq (3,3)\} \end{aligned}$$