80-310/610 Logic and Computation

Exercise Set 1

Kevin T. Kelly

Read Van Dalen 1.1-1.2 and the Appendix up to the discussion of "satisfaction" (check the table of contents). The syntax of propositional logic is, admittedly, pretty straightforward, but the underlying ideas aren't so trivial and will show up repeatedly elsewhere in computer science and philosophy. This is a chance to get them right. The exercises invite you to draw some general morals that will apply to applications you confront repeatedly in the future.

Let U be a set of objects. Let $B \subseteq U$. Let $f_1, \ldots, f_n$ be functions defined on U that take finitely many arguments. Say that C is **inductive** (with base $B \subseteq U$ and **generation operations** $f_1, \ldots, f_n$) if and only if:

1. $B \subseteq C$;
2. if $x_1, \ldots, x_{k_i} \in C$ then $f_i(x_1, \ldots, x_{k_i}) \in C$.

Let C^* denote the intersection of all inductive sets (relative to $B, f_1, \ldots, f_n$). Then C^* is sometimes called the **inductive closure** of B under $f_1, \ldots, f_n$ or is said to be **inductively defined** by $B, f_1, \ldots, f_n$. It is immediate that C^* is a subset of each inductive set, since C^* is just the intersection of all such sets. An immediate consequence of this trivial observation is the non-trivial **principle of induction** on an inductively defined set C^*. Let Φ be a property of objects in U.

If

(a) for each $b \in B$, $\Phi(b)$;

(b) for each $x_1, \ldots, x_{k_i} \in C^*$, if $\phi(x_1)$ and $\ldots$ and $\phi(x_n)$ then $\phi(f_i(x_1, \ldots, x_{k_i}))$

Then for all $x \in C^*$, $\Phi(x)$.

Notice that the hypothesis just says that $\{x \in U : \Phi(x)\}$ is inductive. Hence, $C^* \subseteq \{x \in U : \Phi(x)\}$, so each $x \in C^*$ satisfies Φ. That's all there is to the principle of induction! Induction on the natural numbers is just a special case:

Exercise 1 *Show that the natural numbers are inductively definable with base $B = \{0\}$ and derive the usual principle of induction on the natural numbers.*

Solution. *Formation rule is: $f(n) = n + 1$. Induction becomes: If $\Phi(0)$ and if $\Phi(n)$ then $\Phi(n + 1)$ then for all $n \in N$ $\Phi(n)$.*

Strong induction on the natural numbers is the principle:

(a) $\Phi(0)$ and

(b) for each n, (for each $m < n$, $\Phi(m)$) implies $\Phi(n)$,

implies that for all $n, \Phi(n)$.

Exercise 2 *Prove that the induction principle is equivalent to the strong induction principle. Hint: when you instantiate the induction principle to prove strong induction, choose the property Φ in the induction principle as follows:*

$$\Psi(n) \textit{ if and only if for each } m \leq n, \textit{ not-}\Phi(m).$$

Solution: *Assume the induction principle. Suppose that $\Phi(0)$ and that for each n, the statement (for each $m < n$, $\Phi(m)$) implies $\Phi(n)$. Let $\Psi(n)$ be defined as "for all $m \leq n$, $\Phi(m)$. Then $\Psi(0)$. Suppose that $\Psi(n)$. Then by hypothesis, $\Psi(n+1)$. So by induction, for all n, $\Psi(n)$. So for all n, $\Phi(n)$.*

Conversely, assume the strong induction principle. Assume that $\Phi(0)$ and that for each n, $\Phi(n)$ implies $\Phi(n+1)$. Let n be given and suppose that for all $m < n$, $\Phi(m)$. If $n = 0$, $\Phi(0)$ is immediate by hypothesis. If $n > 0$, then we have $\Phi(n-1)$. By hypothesis, $\Phi(n)$. So for each n, the statement (for each $m < n$, $\Phi(m)$) implies $\Phi(n)$. So by strong induction, for each n, $\Phi(n)$. $\dashv$

Exercise 3 *Prove that: if $n \geq 5$ then:*

$$\textit{if } n \geq 5 \textit{ then } 2^n > n^2.$$

Hint: sometimes it is necessary to prove a lemma by induction before proving the main result.

Why are you allowed to start the proof with base case = 5 when the principle of induction starts with base case 0? Hint: fiddle with the choice of Φ in the principle of induction.

Solution: *In the base case, $2^5 = 32 > 25 = 5^2$. Next:*

$$\begin{array}{rcll} 2^{n+1} & = & 2 \cdot 2^n & \\ & > & 2n^2 & \textit{by induction hypothesis} \\ & > & n^2 + 2n + 1 & \textit{by the following lemma} \\ & = & (n+1)^2. & \end{array}$$

For the lemma, show by induction that for each $n \geq 3$, $n^2 > 2n + 1$. In the base case, $9 > 7$. Next:

$$\begin{array}{rcll} (n+1)^2 + 1 & = & n^2 + 2n + 2 & \\ & > & (2n+1) + 2n + 2 & \textit{by induction hypothesis} \\ & = & 4n + 3 & \\ & > & 2n + 2 & \\ & = & 2(n+1) + 1 & \end{array}$$

In Van Dalen's definition of PROP*, the basic set B is the set of atomic propositions $\{p_i : i \in N\}$ and the generation operations are, of course:

$$f_\wedge(x, y) \quad = \quad (x \wedge y);$$

$$\begin{aligned} f_\vee(x, y) &= (x \vee y); \\ f_\neg(x) &= (\neg x); \\ &\vdots \end{aligned}$$

Incidentally, what is U in the case of PROP*? Is U inductive?

The characterization of inductively defined sets "from above" by taking the intersection of all inductive sets makes the principle of induction transparent and makes it easy to show that an object $x \in C^*$. It's harder to show that something in U is not in C^* (look carefully at Van Dalen's example). Also, it seems a bit bizarre to define the natural numbers with an infinite intersection of infinite sets including gods, potatoes, and who-knows-what, just to throw all the rubbish away again? One natural alternative is to just iterate the generation operators by defining:

$$\begin{aligned} C^0 &= B; \\ C^{n+1} &= C^n \cup \{f_i(x_1, \ldots x_{k_i}) : i \leq n \text{ and } x_1, \ldots, x_{k_i} \in C^n\}; \\ C_* &= \bigcup_i C^i. \end{aligned}$$

Van Dalen claims it is easy to prove the following.

Exercise 4 (The way up is the way down (Heraclitus)) *Prove that $C^* = C_*$. Hint: use induction on C^* on one side and induction on N on the other.*

Solution *Suppose that $x \in C^*$. In the base case, suppose that $x \in B$. Then $x \in C^0$, so $x \in C_*$. Next, suppose that $x_1, \ldots, x_{k_i} \in C^*$. Then, by the induction hypothesis, for for each such x_i, there is some j such that $x_i \in C^j$. Let $m = \max_{i \leq n} \min_j x_i \in C^j$. Then $x_1, \ldots, x_{k_i} \in C^m$. Then $x \in C^{m+1} \subseteq C^*$.*

Conversely, suppose that $x \in C_*$. In the base case, suppose that $x \in C^0$. Then x is in each inductive set and, hence, is in C^*. Next, suppose that $x \in C^{n+1}$. Then there exist $x_1, \ldots, x_{k_i} \in C^n$ such that $x = f_i(x_1, \ldots, x_{k_i})$. By the induction hypothesis, $x_1, \ldots, x_{k_i} \in C^*$. So each inductive set contains $x_1, \ldots, x_{k_i} \in C^*$. Since each inductive set is closed under f_i, each inductive set also contains x, so $x \in C^*$.

Say that a **formation sequence** for x (relative to $B, f_1, \ldots, f_n$) is a finite sequence τ of elements of U such that for each x occurring in τ, $x = f(y_1, \ldots, y_k)$, where f is a generation operation and $y_1, \ldots, y_k$ occur earlier than x in τ.

Exercise 5 *Prove that $x \in C^*$ if and only if x has a formation sequence. Hint: use the preceding result and prove that $x \in C_*$ if and only if x has a formation sequence.*

Solution *By induction on N. If $x \in C^0$ then x has a formation sequence namely, (x). Suppose that $x \in C^{n+1}$. Then there exist $x_1, \ldots, x_{k_i} \in C^m$ such that $f(x_1, \ldots, x_{k_i}) = x$. Each x_i has a formation sequence, by induction hypothesis. Concatenate all of these formation sequences and add x to the end. The result is a formation sequence.*

Converse by induction on N. Suppose that x has a formation sequence of length 1. Then $x \in B$ so $x \in C^0 \subseteq C_*$. Suppose that x has a formation sequence of length $n+1 > 1$. Then there exist $x_1, \ldots, x_{k_i}$ occurring in the formation sequence earlier than

x such that $f(x_1, \ldots, x_{k_i}) = x$. Each x_i is in C_* by induction hypothesis. Since there are finitely many, there is some m such that each x_i is in C^m. Hence, $x = f(x_1, \ldots, x_{k_i})$ is in $C^{m+1} \subseteq C_*$.

Recursion is an obvious and attractive way of defining functions on C^*. One defines the value of the function on elements of B and then defines the function on x as a function of the values assigned to $x_1, \ldots, x_n$ when $f(x_1, \ldots, x_n) = x$. For example, on the natural numbers:

$$\begin{aligned} f(0) &= 1; \\ f(n+1) &= 2 \cdot 2^n. \end{aligned}$$

But there is a catch. Functions must have unique values for objects (independently of the way the objects are described) but if it is possible for the generation operators to produce the same object by distinct paths, recursion may yield two distinct values of a function on the same argument. Say that C^* is **freely generated** if and only if

1. each of the generation operators is injective (1-1);
2. the respective ranges of the generation operators are pair-wise disjoint;
3. no generation operator produces a value in B.

Exercise 6 *The* **palindromes** *on alphabet A are the strings on A that are invariant under reversal: e.g., "wait and wait".*

Let $A = \{0, 1\}$ and present formation rules that freely generate the set P of palindromes on A (don't forget the empty string $()$).

(*) Come up with generation rules for the palindromes under which the palindromes are not freely generated and witness that fact with an example. What if there were parentheses, as in PROP?

(*) Show how definition by recursion can yield inconsistent results when the palindromes are not freely generated.

Solution. *To freely generate P, let P be the least set X closed under:*

1. $(), (0), (1) \in X$;

2. *if $\sigma \in X$ then $0\sigma0, 1\sigma1 \in X$.*

To non-freely generate P, add the formation rule:

(c) *if $\sigma \in X$ then $\sigma\sigma \in X$.*

A witnessing example is 00 which could have been $(0()0)$ or $(0)(0)$.

A mis-defined recursive function would be:

$$\begin{aligned} \mathit{flip}(()) &= (); \\ \mathit{flip}(n\sigma n) &= (1-n)\sigma(1-n); \\ \mathit{flip}(\sigma\sigma) &= \sigma\sigma. \end{aligned}$$

Then $\mathit{flip}(00) = (11) \neq (00) = \mathit{flip}(00)$, which is a contradiction.

Be sure to look at van Dalen's proof of the existence and uniqueness of a recursively defined function in the Appendix.

Exercise 7 *Define rank and sub-palindrome for palindromes. Use van Dalen's examples for PROP as a guide. Let* $()$ *have rank 0. Instead of drawing trees, identify a tree with the set of is paths.*

Solution.

$$\begin{aligned} rank(()) &= 0; \\ rank((a)) &= 0; \\ rank(x\sigma x) &= 1 + rank(\sigma). \end{aligned}$$

$$\begin{aligned} sub(()) &= \{()\}; \\ sub((a)) &= \{(), (a)\}; \\ sub(x\sigma x) &= sub(\sigma) \cup \{(x\sigma x)\}; \end{aligned}$$

It's OK if they don't count $()$ *as a sub-palindrome of* (a).