Theory of Computation — Pete Manolios
Notes on induction — Jan 21, 2016

In response to a request for more information on induction, I prepared these notes. Read them if you are interested, but this is not required for the course. The notation I use differs from the notation you will see in the book we are using for the course. Being exposed to various notational conventions is a good thing, but may lead to confusion, so if something is not clear, please ask!

1 Initial Notation and Definitions

$\mathbb{N}$ and ω both denote the natural numbers, *i.e.*, $\{0, 1, \ldots\}$. The ordered pair whose first component is i and whose second component is j is denoted $\langle i, j\rangle$. $[i..j]$ denotes the closed interval $\{k \in \mathbb{N} : i \leq k \leq j\}$; parentheses are used to denote open and half-open intervals, *e.g.*, $[i..j)$ denotes the set $\{k \in \mathbb{N} : i \leq k < j\}$.

R is a *binary relation* on set S if $R \subseteq S \times S = \{\langle x, y\rangle : x, y \in S\}$. We abbreviate $\langle s, w\rangle \in R$ by sRw. A function is a relation such that xRy and xRw implies $y = w$.

Function application is sometimes denoted by an infix dot "." and is left associative. That is, $f.x$ is the unique y such that xfy. This allows us to use the curried version of a function when it suits us, *e.g.*, we may write $f.x.y$ instead of $f(x, y)$. That is, $f.x.y$ is really $(f.x).y$, where f is a function of one argument that returns $f.x$, a function of one argument.

From highest to lowest binding power, we have: parentheses, function application, binary relations (*e.g.*, sBw), equality ($=$) and membership ($\in$), conjunction ($\wedge$) and disjunction ($\vee$), implication ($\Rightarrow$), and finally, binary equivalence ($\equiv$). Spacing is used to reinforce binding: more space indicates lower binding.

$\langle Qx : r : b\rangle$ denotes a quantified expression, where Q is the quantifier, x the bound variable, r the range of x (**true** if omitted), and b the body. We sometimes write $\langle Qx \in X : r : b\rangle$ as an abbreviation for $\langle Qx : x \in X \quad \wedge \quad r : b\rangle$, where r is **true** if omitted, as before.

Cardinality of a set S is denoted by $|S|$. $\mathcal{P}(S)$ denotes the powerset of S.

A function from $[0..n)$, where n is a natural number, is called a *finite sequence* or an *n-sequence*.

What are numbers as mathematical objects? von Neumann proposed the following: $0 = \emptyset, 1 = \{0\}, 2 = \{0, 1\}, \ldots$, so $n = [0..n)$. Thus an n-sequence is a function from n.

An *ω-sequence* is a function from ω. We may sometimes refer to ω-sequences as infinite sequences, but as we will see there are infinite sequences that are "longer" than ω-sequences.

When we write $x \in \sigma$, for a sequence σ, we mean that x is in the range of σ.

2 Binary Relations

Let B, C be binary relations on set S. $B|_A$ denotes B *left-restricted* to the set A, *i.e.*, $B|_A = \{\langle x, y\rangle : xBy \quad \wedge \quad x \in A\}$.

Some important definitions follow.

- B is *reflexive* if $\langle \forall x \in S :: xBx\rangle$.
- B is *irreflexive* if $\langle \forall x \in S :: \neg(xBx)\rangle$.
- B is *transitive* if $\langle \forall x, y, z \in S :: xBy \quad \wedge \quad yBz \quad \Rightarrow \quad xBz\rangle$.
- B is a *preorder* (also called a *quasi-order*) if it is reflexive and transitive.
- The identity relation, B^0, is $\{\langle x, x\rangle : x \in S\}$.
- The *composition* of B and C is denoted $B;C$ and is the set $\{\langle b, c\rangle : \langle \exists x :: bBx \quad \wedge \quad xCc\rangle\}$.
- For all natural numbers i, B^{i+1} is $B^i; B$.

Exercise 1 *Prove the following.*

1. *B is reflexive iff $B^0 \subseteq B$.*
2. *$B^1 = B$.*
3. *B is transitive iff $B^2 \subseteq B$.*

We now continue with the definitions.

- B is *symmetric* if $\langle \forall x, y \in S :: xBy \quad \Rightarrow \quad yBx\rangle$.
- A preorder that is also symmetric is an *equivalence relation*.
- B is *asymmetric* if $\langle \forall x, y \in S :: xBy \quad \Rightarrow \quad \neg(yBx)\rangle$.
- B is *antisymmetric* if $\langle \forall x, y \in S :: xBy \quad \wedge \quad yBx \quad \Rightarrow \quad x = y\rangle$.
- A preorder that is antisymmetric is a *partial order*.
- If B is a partial order, $\langle S, B\rangle$ is a *poset*.
- The *inverse* of B is denoted B^{-1} and is $\{\langle x, y\rangle : yBx\}$.

Exercise 2 *Prove the following.*

1. *B is symmetric iff $B^{-1} \subseteq B$.*
2. *B is antisymmetric iff $B \cap B^{-1} \subseteq B^0$.*

If B is an equivalence relation, for each $x \in S$, it induces an *equivalence class* $[x]_B = \{y : xBy\}$. The *quotient* S/B is $\{[x]_B : x \in S\}$.

Exercise 3 *Prove the following.*

1. *If B is an equivalence relation, then $[x]_B$ and $[y]_B$ are either identical or disjoint.*
2. *If C is a preorder, then*
   (a) $B = \{\langle x, y\rangle : xCy \quad \wedge \quad yCx\}$ *is an equivalence relation.*
   (b) $\langle S/B, \preccurlyeq\rangle$ *is a poset, where $\preccurlyeq$ is defined as follows:*
   $[x]_B \preccurlyeq [y]_B \qquad \equiv \qquad xCy.$

We now continue with the definitions.

- B is *total* (also called *linear* or *connected*) if $\langle \forall x, y \in S :: xBy \quad \vee \quad yBx\rangle$.
- A *total order* is a partial order that is total.
- If B is a total order, $\langle S, B\rangle$ is a *toset*.
- An α-sequence $\langle a_0, a_1, a_2, \ldots\rangle$, where $\alpha \in \omega \quad \vee \quad \alpha = \omega$, is *decreasing* in B if $\langle \forall i : i+1 \ \in \ \alpha : a_{i+1} B a_i\rangle$.
- B is *terminating* (also called *well-founded*) if there is no decreasing ω-sequence in B.
- If B is terminating, then $\langle S, B\rangle$ is a *well-founded structure*.
- The *strict part* of a relation B is $\{\langle x, y\rangle : xBy \quad \wedge \quad x \neq y\}$.
- B is a *strict partial order* if it is the strict part of some partial order. Strict total orders are defined in an analogous way.
- A *well order* is a strict total order that is well-founded.
- If B is a well order, $\langle S, B\rangle$ is a *woset*.
- For $T \subseteq S$:
  - If $(m \in T \quad \wedge \quad \langle \forall x \in T :: xBm \quad \Rightarrow \quad x = m\rangle)$, then m is a *minimal* element of T (under B).
  - If $(m \in T \quad \wedge \quad \langle \forall x \in T :: mBx \quad \vee \quad m = x\rangle)$, then m is the *least* element of T (under B).
  - If $(m \in S \quad \wedge \quad \langle \forall x \in T :: mBx \quad \vee \quad m = x\rangle)$, then m is a *lower bound* of T (under B).
  - The notions of *maximal*, *greatest*, and *upper bound* are defined dually, *e.g.*, m is a maximal element of T under B iff m is a minimal element of T under B^{-1}.

Exercise 4 *Prove the following.*

1. *B is total iff $B \cup B^{-1} = S \times S$.*
2. *B is a strict partial order iff it is irreflexive and transitive.*
3. *If $\prec$ is a strict partial order and $x \preccurlyeq y \quad \equiv \quad x \prec y \quad \vee \quad x = y$ then $\preccurlyeq$ is a partial order.*
4. *If $\preccurlyeq$ is a preorder and $x \prec y \quad \equiv \quad x \preccurlyeq y \quad \wedge \quad \neg(y \prec x)$ then $\prec$ is a strict partial order.*
5. *B is a strict total order iff*
   (a) *B is irreflexive.*
   (b) *B is transitive.*
   (c) $\langle \forall x, y \in S :: xBy \quad \vee \quad yBx \quad \vee \quad x = y \rangle$.
6. *B is a well order iff it is well-founded and* $\langle \forall x, y \in S :: xBy \quad \vee \quad yBx \quad \vee \quad x = y \rangle$.

Exercise 5 *Let $\prec$ be a strict partial order on S. Prove the following.*

1. *Prove that $\langle S, \prec \rangle$ is a well-founded structure iff all non-empty subsets of S have a minimal element under $\prec$.*
2. *Prove that $\langle S, \prec \rangle$ is a woset iff all non-empty subsets of S have a least element.*

Given a set U (the "universe"), $X \subseteq U$, and a property P which is satisfied by some subsets of U, the P-sets, we say that C is the P-closure of X if C is the least P-set which includes X. If the P-sets include U and are closed under arbitrary intersections, we say that the P-sets of U form a *closure system*. If the P-sets of U form a closure system, then the P-closure of X always exists. It is $\cap\{Y \subseteq U : X \subseteq Y \quad \wedge \quad Y \text{ is a } P\text{-set}\}$.

Exercise 6 *Prove the following, where $U = S \times S$.*

1. *The reflexive relations form a closure system.*
2. *The irreflexive relations do not form a closure system.*
3. *The symmetric relations form a closure system.*
4. *The asymmetric relations do not form a closure system.*
5. *The antisymmetric relations do not form a closure system.*
6. *The transitive relations form a closure system.*

We can therefore speak of the reflexive closure, or the symmetric closure, or the transitive closure, or the reflexive, transitive closure, etc. B^+ denotes the transitive closure of B and B^* denotes the reflexive, transitive closure of B. This same notation is used in regular languages.

3 Induction

Mathematical induction works because the natural numbers (with the usual ordering) are a well-founded: if some property fails to hold for all naturals, it fails for some minimal n, but holds for all smaller numbers, which is exactly what we prove doesn't happen. We can extend this idea to more general sets. The *principle of well-founded induction* states: If $\langle W, \prec\rangle$ is a well-founded structure,

$$\text{(WFI)} \quad \langle \forall w \in W :: P.w\rangle \equiv \langle \forall w \in W :: \langle \forall v : v \prec w : P.v\rangle \Rightarrow P.w\rangle$$

Exercise 7 *Show that (weak) mathematical induction is a special case of well-founded induction.*

Exercise 8 *Show that strong mathematical induction (course of values induction) is a special case of well-founded induction.*

Proof Note that if $W = \omega$ and $\prec = <$, we have the principle of strong mathematical induction. Letting $\prec$ be $\{\langle n, n+1\rangle : n \in \omega\}$ gives us mathematical induction. $\square$

Theorem 1 *Let $\prec$ be a binary relation on W.* WFI *holds iff $\prec$ is terminating.*

Proof First, note that $\langle \forall w \in W :: P.w\rangle \quad \Rightarrow \quad \langle \forall w \in W :: \langle \forall v : v \prec w : P.v\rangle \Rightarrow P.w\rangle$.

Now, suppose that WFI holds and let $P.x$ denote that any decreasing sequence starting at x is finite. Then establishing $\langle \forall w \in W :: \langle \forall v : v \prec w : P.v\rangle \Rightarrow P.w\rangle$ is easy and $\prec$ is terminating.

Suppose that WFI does not hold, then (by the note above) we have $\langle \forall w \in W :: \langle \forall v : v \prec w : P.v\rangle \Rightarrow P.w\rangle$, but not $\langle \forall w \in W :: P.w\rangle$. Consider the set $X = \{x \in W : \neg P.x\}$. We know that X is non-empty. If $\prec$ is terminating then it has a minimal element, m, but this is a contradiction, as $\langle \forall v : v \prec m : P.v\rangle \Rightarrow P.m$ holds, but since $\neg P.m$, $\neg\langle \forall v : v \prec m : P.v\rangle$, which is $\langle \exists v : v \prec m : \neg P.v\rangle$, so $v \in X$ and $v \prec m$, contradicting the minimality of m, thus $\prec$ is not terminating. $\square$

Exercise 9 *Prove that if a relation is well-founded iff its transitive closure is well-founded.*

Exercise 10 *Prove that if a relation $\prec$ on S is well-founded, then so is $\prec_n$ on n-tuples of elements from S, where n is a positive natural number and $\prec_n$, the* lexicographic *version of $\prec$, is defined as follows: $\prec_1 = \prec$ and for $n > 1$, $\langle x_n, x_{n-1}, \ldots, x_1\rangle \prec_n \langle y_n, y_{n-1}, \ldots, y_1\rangle$ iff $x_n \prec y_n$ or ($x_n = y_n$ and $\langle x_{n-1}, \ldots, x_1\rangle \prec_{n-1} \langle y_{n-1}, \ldots, y_1\rangle$).*

Exercise 11 *Is the dictionary order well-founded?*

Induction on wosets is called *well-ordered induction* or *transfinite induction.*

Any well-founded relation can be extended to a well-ordered relation.

It turns out, that as a consequence of the *axiom of choice*, which states: the cartesian product of a non-empty family of non-empty sets is non-empty, we have that for any set S, there is a relation $\prec$ s.t. $\langle S, \prec\rangle$ is a woset. Note the remarkable consequence: we can well-order any set and can thus apply induction to any set.

Any woset is order isomorphic to an ordinal. This is an indication of why fundamental questions about termination are really questions about ordinals.

4 Recursion

Induction can be used to justify recursive definitions. The principle of well-founded recursion states that if:

1. $\langle W, \prec\rangle$ is a well-founded structure; and
2. g is a binary function that maps any $w \in W$ and any function from $\{v : v \prec w\}$ to W into W.

Then, the following is satisfied by exactly one function on W.

$$f.x = g(x, \{\langle y, f.y\rangle : y \prec x\})$$

Exercise 12 *Prove the principle of the well-founded recursion.*

5 ACL2s

If you are interested in how induction and recursion are used in the context of a theorem prover, let me know and I can give you some pointers and exercises to play around with. You can start by installing ACL2s.