Induction and Coinduction

(cribbed from Andy Gordon)

November 5, 2015

Let U be some universal set and $F : 2^U \to 2^U$ be a monotone function. Induction and co-induction are dual proof principles that derive from the definition of a set to be the least or greatest solution, respectively, of equations of the form $X = F(X)$. First some definitions.

0.1 FIXPOINTS, F-CLOSED AND F-DENSE SETS

A function $F : 2^U \to 2^U$ is *monotone* if $X \subseteq Y$ implies $F(X) \subseteq F(Y)$.
A *fixpoint* of F is a solution of the equation $X = F(X)$.
A set $X \subseteq U$ is *F-closed* iff $F(X) \subseteq X$.
A set $X \subseteq U$ is *F-dense* iff $X \subseteq F(X)$.
$\mu X.F(X) \triangleq \bigcap\{X \mid F(X) \subseteq X\}$.
$\nu X.F(X) \triangleq \bigcup\{X \mid X \subseteq F(X)\}$.

LEMMA 0.2.

(1) $\mu X.F(X)$ is the least F-closed set.
(2) $\nu X.F(X)$ is the greatest F-dense set.

Proof. We prove (2); (1) follows by a dual argument. Since $\nu X.F(X)$ contains every F-dense set by construction, we need only show that it is itself F-dense, for which the following lemma suffices.

If every X_i is F-dense, so is the union $\bigcup_i X_i$.

Since $X_i \subseteq F(X_i)$ for every i, $\bigcup_i X_i \subseteq \bigcup_i F(X_i)$. Since F is monotone, $F(X_i) \subseteq F(\bigcup_i X_i)$ for each i. Therefore $\bigcup_i F(X_i) \subseteq F(\bigcup_i X_i)$, and so we have $\bigcup_i X_i \subseteq F(\bigcup_i X_i)$ by transitivity, that is, $\bigcup_i X_i$ is F-dense. □

THEOREM 0.3 (TARSKI).

(1) $\mu X.F(X)$ is the least fixpoint of F.
(2) $\nu X.F(X)$ is the greatest fixpoint of F.

Proof. Again we prove (2) alone; (1) follows by a dual argument. Let $\overline{\nu} = \nu X.F(X)$. We have $\overline{\nu} \subseteq F(\overline{\nu})$ by Lemma 0.2. So $F(\overline{\nu}) \subseteq F(F(\overline{\nu}))$ by monotonicity of F. But then $F(\overline{\nu})$ is F-dense, and therefore $F(\overline{\nu}) \subseteq \overline{\nu}$. Combining the inequalities we have $\overline{\nu} = F(\overline{\nu})$; it is the greatest fixpoint because any other is F-dense, and hence contained in $\overline{\nu}$. □

We obtain two dual methods for defining sets and dual proof principles associated with these definitions.

0.4 INDUCTION AND COINDUCTION

$\mu X.F(X)$, the least solution of $X = F(X)$, is the set *inductively defined* by F.
$\nu X.F(X)$, the greatest solution of $X = F(X)$, is the set *co-inductively defined* by F.
Principle of induction: If X is F-closed then $\mu X.F(X) \subseteq X$.
Principle of co-induction: If X is F-dense then $X \subseteq \nu X.F(X)$.

EXAMPLE 0.5. Mathematical induction is a special case. Suppose there is an element $\mathtt{0} \in U$ and an injective function $\mathtt{succ} : U \to U$. If we define a monotone function $F_{\mathbb{N}} : 2^U \to 2^U$ by

$$F_{\mathbb{N}}(X) \triangleq \{\mathtt{0}\} \cup \{\mathtt{succ}\, x \mid x \in X\}$$

and set $\mathbb{N} \triangleq \mu X.F_{\mathbb{N}}(X)$, the associated principle of induction is that $\mathbb{N} \subseteq X$ if $F_{\mathbb{N}}(X) \subseteq X$, which is to say that $\mathbb{N} \subseteq X$ if

- $\mathtt{0} \in X$ and
- $x \in X$ implies $\mathtt{succ}\, x \in X$.

Think of X as a predicate on the natural numbers ($P(n)$ is true if $n \in X$). Then this says $\forall n \in \mathbb{N} \,.\, P(n)$ if

- $P(\mathtt{0})$ and
- $P(n)$ implies $P(n+1)$. □

EXAMPLE 0.6. Induction on syntax is again just a special case. In fact, the above example $F_{\mathcal{T}}$ corresponds exactly to the syntax of naturals in TAPL. For another example, consider boolean expressions, generated by the following function

$$F_{\mathcal{T}}(X) \triangleq \{\mathtt{true}, \mathtt{false}\} \cup \{\mathtt{if}\, x_1\, \mathtt{then}\, x_2\, \mathtt{else}\, x_3 \mid x_1, x_2, x_3 \in X\}.$$

The set of terms is $\mathcal{T} = \mu X.F_{\mathcal{T}}(X)$. The associated principle of induction is that $\mathcal{T} \subseteq X$ if $F_{\mathcal{T}}(X) \subseteq X$, which is to say that $\mathcal{T} \subseteq X$ if

- $\mathtt{true} \in X$ and
- $\mathtt{false} \in X$ and
- $x_1, x_2, x_3 \in X$ implies $\mathtt{if}\, x_1\, \mathtt{then}\, x_2\, \mathtt{else}\, x_3 \in X$.

Think of X as a predicate on terms ($P(\mathtt{t})$ is true if $\mathtt{t} \in X$). Then this says $\forall \mathtt{t} \in \mathcal{T} \,.\, P(\mathtt{t})$ if

- $P(\mathtt{true})$ and
- $P(\mathtt{false})$ and
- $P(x_1) \wedge P(x_2) \wedge P(x_3)$ implies $P(\mathtt{if}\, x_1\, \mathtt{then}\, x_2\, \mathtt{else}\, x_3)$. □

EXAMPLE 0.7. Induction on the derivation of evaluation is another special case. Induction on the derivation of typing is another special case. □

1 Strong Versions

The definitions given previously are in fact a bit weaker than one wants. For example, when showing that $P(n)$ implies $P(n+1)$ one would like to be able to assume that $n \in \mathbb{N}$. This is not justified by the principle induction as outlined so far. In this section we show that such assumptions can be justified using a stronger formulation of (co)induction.

PROPOSITION 1.1. *Let U be an arbitrary universal set and let $F : 2^U \to 2^U$ be some monotone function. If $\overline{\mu} \triangleq \mu X.F(X)$ and $\overline{\nu} \triangleq \nu X.F(X)$ we have:*

$$\begin{aligned}
\overline{\mu} &= \mu X.F(X) \cap \overline{\mu} && (\mu.\mathrm{I})\\
&= \mu X.F(X \cap \overline{\mu}) && (\mu.\mathrm{II})\\
&= \mu X.F(X \cap \overline{\mu}) \cap \overline{\mu} && (\mu.\mathrm{III})\\
\overline{\nu} &= \nu X.F(X) \cup \overline{\nu} && (\nu.\mathrm{I})\\
&= \nu X.F(X \cup \overline{\nu}) && (\nu.\mathrm{II})\\
&= \nu X.F(X \cup \overline{\nu}) \cup \overline{\nu} && (\nu.\mathrm{III})
\end{aligned}$$

Proof. We prove the results for $\overline{\nu}$; the proofs for $\overline{\mu}$ are dual. Make the following definitions.

$$\begin{aligned}
\overline{\nu}_1 &\triangleq \nu X.F(X) \cup \overline{\nu}\\
\overline{\nu}_2 &\triangleq \nu X.F(X \cup \overline{\nu})\\
\overline{\nu}_3 &\triangleq \nu X.F(X \cup \overline{\nu}) \cup \overline{\nu}
\end{aligned}$$

We must show that each $\overline{\nu}_i$ equals $\overline{\nu}$. Since $\overline{\nu} \subseteq F(\overline{\nu})$ it follows by coinduction that $\overline{\nu} \subseteq \overline{\nu}_i$ for each i. The reverse inclusions take a little more work.

$\overline{\nu}_2 \subseteq \overline{\nu}$**.** Since $\overline{\nu}$ is a fixpoint of F, which is monotone, we have $\overline{\nu} = F(\overline{\nu}) \subseteq F(\overline{\nu}_2 \cup \overline{\nu})$. Now $\overline{\nu}_2 \subseteq F(\overline{\nu}_2 \cup \overline{\nu})$ so $\overline{\nu}_2 \cup \overline{\nu} \subseteq F(\overline{\nu}_2 \cup \overline{\nu})$, and therefore $\overline{\nu}_2 \cup \overline{\nu} \subseteq \overline{\nu}$ by coinduction. Hence $\overline{\nu}_2 \subseteq \overline{\nu}$.

$\overline{\nu}_1 \subseteq \overline{\nu}_2$**.** We have $\overline{\nu}_1 = F(\overline{\nu}_1) \cup \overline{\nu} = F(\overline{\nu}_1) \cup F(\overline{\nu}) \subseteq F(\overline{\nu}_1 \cup \overline{\nu})$. So $\overline{\nu}_1 \subseteq \nu X.F(X \cup \overline{\nu})$.

$\overline{\nu}_3 \subseteq \overline{\nu}_2$**.** We have $\overline{\nu}_3 = F(\overline{\nu}_3 \cup \overline{\nu}) \cup \overline{\nu} = F(\overline{\nu}_3 \cup \overline{\nu}) \cup F(\overline{\nu}) = F(\overline{\nu}_3 \cup \overline{\nu})$ since $F(\overline{\nu}) \subseteq F(\overline{\nu}_3 \cup \overline{\nu})$. Hence $\overline{\nu}_3 \subseteq \nu X.F(X \cup \overline{\nu})$. □

(μ.III) and (ν.III) justify the following strong version of induction and coinduction.

1.2 STRONG (CO)INDUCTION (WHERE $\overline{\mu} = \mu X.F(X)$ AND $\overline{\nu} = \nu X.F(X)$)

Strong induction: If $F(X \cap \overline{\mu}) \cap \overline{\mu} \subseteq X$ then $\overline{\mu} \subseteq X$.
Strong co-induction: If $X \subseteq F(X \cup \overline{\nu}) \cup \overline{\nu}$ then $\overline{\nu} \subseteq X$.

EXAMPLE 1.3. For numbers, our strong induction yields $\mathbb{N} \subseteq X$ if $\{\mathtt{0}\} \cup \{\mathtt{succ}\, x \in \mathbb{N} \mid x \in X \wedge x \in \mathbb{N}\} \subseteq X$. Written another way, we can conclude that $\mathbb{N} \subseteq X$ if

- $\mathtt{0} \in X$ and
- $\mathtt{succ}\, x \in X$ for every x such that $x \in \mathbb{N} \cap X$ and $\mathtt{succ}\, x \in \mathbb{N}$.

Compare to the previous formulation:

- $\mathtt{0} \in X$ and
- $\mathtt{succ}\, x \in X$ for every x such that $x \in X$.

In practice it is often handy to assume that x is in $\overline{\mu}$ (here $\mathbb{N}$) and to only have to prove $F(X) \subseteq X$ when $F(X)$ is also in $\overline{\mu}$. □