Inducción estructural.

Fernando Schapachnik[1]

[1]Departamento de Computación, FCEyN,
Universidad de Buenos Aires, Buenos Aires, Argentina

Algoritmos y Estructuras de Datos II,
primer cuatrimestre de 2015

(2) Repaso

- ¿Qué significa *inferir*? Obtener una conclusión a partir de un conjunto de premisas.
- Pero no siempre esa conclusión es cierta: diferenciamos entre inferencias válidas e inválidas.
- Ojo: cuando decimos *inválidas* nos referimos a que no son válidas como forma de demostración, es decir, que lo que se infiere de ellas necesita ser validado por otros mecanismos.
- Algunas inferencias válidas:
  - Modus Ponens (o deducción): $p \Rightarrow q, p \vdash q$
  - Modus Tollens: $p \Rightarrow q, \neg q \vdash \neg p$
- Algunas inferencias inválidas:
  - Abducción: $p \Rightarrow q, q \vdash p$
  - Generalización inductiva: $P(i), P(i+1) \dots P(i+k) \vdash (\forall n)\ P(n)$

(3) Repaso

- Sin embargo, hay forma de hacer la inducción correctamente, ie, de manera tal de que sea una inferencia válida.
- Ya la conocíamos de Álgebra I:
- Inducción completa:
  $P(0), (\forall n)\ (P(n) \Rightarrow P(n+1)) \vdash (\forall n)\ P(n)$
- Inducción global:
  $P(0), (\forall n)\ [((\forall k < n)\ P(k)) \Rightarrow P(n)] \vdash (\forall n)\ P(n)$
- La inducción completa es una instancia particular de la inducción estructural.
- O dicho de otra manera: la inducción estructural es una generalización de la inducción completa para otros tipos de datos más allá de los $\textsc{Nat}$.

(4) Inducción estructural

- Llamemos $g_1, \ldots, g_k$ a los generadores del tipo T que no toman como parámetro una instancia de T.
- Llamemos $g_{k+1}, \ldots, g_n$ a los que sí toman una instancia de T.
- Si logramos probar el caso base: $P(g_1) \wedge \ldots \wedge P(g_k)$
- ...y el paso inductivo:
  $(\forall i : t)\, [P(i) \;\Rightarrow\; P(g_{k+1}(i))] \wedge \ldots \wedge (\forall i : t)\, [P(i) \;\Rightarrow\; P(g_n(i))]$
- Entonces podemos concluir: $(\forall i : t)\ P(i)$
- Atención: notar que para simplificar no escribimos los otros parámetros que toman los generadores.
- Podemos pensar que la aridad de g_j es $t \times t_j \rightarrow t$ (donde t_j podría ser una tupla).
- Entonces, la forma correcta del paso inductivo sería:

⚠ $(\forall i : t)\ [P(i) \;\Rightarrow\; (\forall e : t_{k+1})\ P(g_{k+1}(i, e))] \wedge \ldots \wedge$
$(\forall i : t)\ [P(i) \;\Rightarrow\; (\forall e : t_n)\ P(g_n(i, e))]$

- ¿Y si g toma más de un t? $\rightarrow$ Lo veremos en la práctica.

(5) Secuencias

- Probemos que en toda secuencia de $\textsc{Nat}$ el mínimo está acotado superiormente por el promedio.
- Para simplificar la demo vamos a pedir además que la secuencia sea decreciente.
- Formalmente:
  $(\forall s : \mathit{secu}(\mathit{nat}))\ \neg\text{vacía?}(s) \wedge_{\mathrm{L}} \text{decreciente}(s)$
  $\Rightarrow_{\mathrm{L}} \mathit{mín}(s) \leq \mathit{prom}(s)$
- ¿Cuál es el predicado que queremos probar para toda secuencia?
  $P(s) \equiv \neg\text{vacía?}(s) \wedge_{\mathrm{L}} \text{decreciente}(s) \Rightarrow_{\mathrm{L}} \mathit{mín}(s) \leq \mathit{prom}(s)$
- Queremos probar que $(\forall s : \mathit{secu}(\mathit{nat}))\ P(s)$.
- ¿Cuál es el caso base?: $P(<>)$
- ¿Y el paso inductivo?:
  $(\forall s : \mathit{secu}(\mathit{nat}))\ [P(s)\ \Rightarrow\ (\forall a : \mathit{nat})\ P(a \bullet s)]$
- ¿Sería equivalente utilizar
  $[(\forall s : \mathit{secu}(\mathit{nat}))\ P(s)]\ \Rightarrow$
  $[(\forall s : \mathit{secu}(\mathit{nat}), \forall a : \mathit{nat})\ P(a \bullet s)]$? ¡NO! ¿Por qué?

(6) Secuencias (caso base)

- Probemos el caso base: $P(<>)$
- Es decir,
  $\neg$vacía?$(<>) \wedge_{\mathrm{L}}$ decreciente$(<>) \Rightarrow_{\mathrm{L}}$ *mín*$(<>) \leq$ *prom*$(<>)$.
- Pero el antecedente da *false* (¿por qué? por primer axioma de vacía?()), haciendo a la implicación verdadera.
- Veamos ahora el paso inductivo.

(7) Secuencias (paso inductivo)

- Queremos probar que
  $(\forall s : secu(nat))\ [P(s) \ \Rightarrow \ (\forall a : nat)\ P(a \bullet s)]$
- Lo primero que podemos hacer, es "olvidarnos" del cuantificador universal y trabajar sin suponer ninguna característica sobre s.
- Tenemos una implicación. Si el antecedente es falso la implicación es verdadera. Veamos qué pasa cuando el antecedente es verdadero.
- Supongamos que vale el antecedente. Esto es, que vale $\neg\text{vacía?}(s) \wedge_{\mathrm{L}} \text{decreciente}(s) \Rightarrow_{\mathrm{L}} \mathit{mín}(s) \leq \mathit{prom}(s)$. Ojo: a esta altura no suponemos que vale para toda s, sólo para una en particular.
- En ese marco queremos probar que $(\forall a : nat)\ P(a \bullet s)$.
  Expandiendo P:
  $(\forall a : nat)\ [\neg\text{vacía?}(a \bullet s) \wedge_{\mathrm{L}} \text{decreciente}(a \bullet s) \Rightarrow_{\mathrm{L}} \mathit{mín}(a \bullet s) \leq \mathit{prom}(a \bullet s)]$.

(8) Secuencias (paso inductivo, cont.)

- Queremos probar que $(\forall a : nat)\ [\neg \text{vacía?}(a \bullet s) \wedge_{\mathrm{L}} \text{decreciente}(a \bullet s) \Rightarrow_{\mathrm{L}} \mathit{mín}(a \bullet s) \leq \mathit{prom}(a \bullet s)]$.
- De nuevo, una implicación adentro de un cuantificador. Podemos proceder como antes y notar que el antecedente puede ser verdadero o falso. Si fuese falso, la implicación se hace verdadera. Analicemos el caso donde el antecedente es verdadero y veamos qué pasa con el consecuente.
- Si s es vacía, nos queda $\mathit{mín}(a \bullet <>) \leq \mathit{prom}(a \bullet <>)$ que trivialmente vale.
- Ie, ahora queremos probar que $\mathit{mín}(a \bullet s) \leq \mathit{prom}(a \bullet s)$ cuando s no es vacía.
- ¿Me creen (en este caso, donde $a \bullet s$ es decreciente) que $\mathit{prom}(s) \leq \mathit{prom}(a \bullet s)$? Hay que demostrarlo igual.

(9) Secuencias (paso inductivo, cont.)

⚠ El planteo de una propiedad auxiliar que se demostrará luego se llama lema:

$$(\forall t : \mathit{secu}(\mathit{nat}), x : \mathit{nat})\ [\neg \text{vacía?}(t) \wedge_{\mathrm{L}} \text{decreciente}(t) \wedge x \geq \mathit{prim}(t) \Rightarrow_{\mathrm{L}} \mathit{prom}(t) \leq \mathit{prom}(x \bullet t)]$$

- Por el lema, sabemos que vale $\mathit{prom}(s) \leq \mathit{prom}(a \bullet s)$. Además, como suponíamos que valía $P(s)$ y s no es vacía y es decreciente (al serlo $a \bullet s$), podemos usar que $\mathit{mín}(s) \leq \mathit{prom}(s)$.
- Además (otro lema), $\mathit{mín}(a \bullet s) \leq \mathit{mín}(s)$.
- Juntando, $\mathit{mín}(a \bullet s) \leq \mathit{mín}(s) \leq \mathit{prom}(s) \leq \mathit{prom}(a \bullet s)$, de donde concluimos lo que queríamos, que era que $\mathit{mín}(a \bullet s) \leq \mathit{prom}(a \bullet s)$. $\square$

⚠ ¿Y cómo probamos los lemas? ¡También por inducción estructural!

(10) Secuencias (paso inductivo, cont.)

- Repasemos: ¿cómo plantemos el paso inductivo?
- Queríamos probar que
  $(\forall s : \mathit{secu}(\mathit{nat}))\ [P(s) \Rightarrow (\forall a : \mathit{nat})\ P(a \bullet s)]$

⚠ Dentro del paso inductivo, $P(s)$ se llama hipótesis inductiva y $(\forall a : \mathit{nat})\ P(a \bullet s)$ tesis inductiva.

⚠ Pensar a la inducción estructural de forma mecánica (eg, “el método de la rayita”) no sirve para nada.

(11) Fundamento teórico

- $\prec$ define un orden parcial sobre el conjunto A ssi $\prec$ es reflexiva, antisimétrica y transitiva. Si se quita la reflexividad se habla de un *orden parcial débil (o irreflexivo)*. $<$ es un orden parcial débil en $\mathbb{N}$.
- $\prec$ define un orden total sobre el conjunto A ssi define un orden parcial y además tiene comparabilidad (o tricotomía) $((\forall a, b \in A)\ a \prec b \vee b \prec a)$. $\leq$ es un orden total en $\mathbb{N}$.
- Decimos que $\prec$ define un buen orden sobre el conjunto A (o equivalentemente, que tiene un orden bien fundado) ssi $\prec$ es un orden total sobre A y cada subconjunto no vacío X de A tiene un elemento que es mínimo de acuerdo a $\prec$.
- (Nota: se podría usar orden parcial y obtener una definición sutilmente distinta, pero no nos vamos a complicar.)

(12) Principio de inducción bien fundada

- Principio de inducción bien fundada: si $\prec$ define un buen orden sobre el conjunto A, P es un predicado sobre A y se cumplen:
  1. P vale para todos los elementos mínimos de A de acuerdo a $\prec$, y
  2. para todo $a \in A$, cuando vale $P(b)$ para todos los $b \in A | b \prec a$, entonces vale $P(a)$,

  entonces, $(\forall a \in A)\ P(a)$
- Demostración:
  - Supongamos que $\prec$ define un orden bien fundado sobre A, que P cumple (1) y (2) pero que no vale para todos los elementos de A.
  - Como $\prec$ es un orden bien fundado, el conjunto $\{a \in A | \neg P(a)\}$ tiene un elemento mínimo, que llamaremos m.
  - Si m es un mínimo para A, entonces contradice (1).
  - Si no lo es, entonces tiene predecesores. Como m era el mínimo elemento que no cumplía P, todos sus predecesores sí lo cumplen. Pero eso contradice (2). $\square$

(13) Principio de inducción bien fundada (cont.)

- Miremos la regla 2:

  (2) para todo $a \in A$, cuando vale $P(b)$ para todos los $b \in A | b \prec a$, entonces vale $P(a)$,

  nos pide que P valga para todos los anteriores.
- Supongamos que tenemos A es numerable y por ende tenemos la noción de $\prec$-antecesor por un paso.
- Lema: si P vale para el $\prec$-antecesor por un paso de $a \in A$, entonces P vale para todos sus $\prec$-antecesores.
- Demostración: contrarrecíproco, trivial por inclusión de los $\prec$-antecesores por un paso en los $\prec$-antecesores.
- Entonces, en el caso numerable, podemos reformular el paso (2) así:

  (2) para todo $a \in A$, cuando vale $P(a\text{“}-1\text{”})$, entonces vale $P(a)$
- O, equivalentemente:

  (2) para todo $a \in A$, cuando vale $P(a)$, entonces vale $P(a\text{“}+1\text{”})$
- (Estamos usando el “-1” y el “$+1$” en sentido figurado.)

(14) Construcción de órdenes bien fundados

- Una forma de construir órdenes bien fundados para un conjunto infinito (pero numerable) es establecer un mapeo con los naturales.
- $f : A \to \mathbb{N}$
- $x \prec_f y$ ssi $f(x) \leq f(y)$
- Lema: $\prec_f$ es un orden bien fundado sobre A.
- Si A fue definido de manera inductiva, f se puede definir así:
  1. Si x es elemento base de A, $f(x) = 0$.
  2. Si x se construye a partir de los elementos $x_1, \ldots, x_n$, entonces $f(x) = 1 + \max(f(x_1), \ldots, f(x_n))$.
- Notar el caso de los racionales: densos, pero numerables.

(15) Vualá

- Ya tenemos todo lo que necesitamos para utilizar la inducción estructural sobre TADs.
- Dado que las instancias de un TAD son numerables, podemos usar la transparencia anterior para construirnos órdenes bien fundados.
- También podemos usar el lema anterior para utilizar la forma sencilla del paso (2) (por lo mismo, son numerables).

(16) Repaso

- Vimos
  - Un repasito de las formas de inducción que conocíamos de Álgebra.
  - El esquema general de la inducción sobre TADs.
  - Un ejemplo sobre secuencias, donde identificamos:
    - el caso base,
    - el paso inductivo, con su hipótesis inductiva y su tesis inductiva,
    - lemas.
  - Los fundamentos teóricos (ie, por qué funciona).
- Quedan para la práctica (¡no se la pierdan!).
  - Casos más complejos.
  - Propiedades que involucran condicionales.
  - Errores comunes, y en particular, suponer lo que se quiere demostrar.
- Empiecen a mirar la práctica 2.

(17) Bibliografía

- Ciesielski, K. Set Theory for the Working Mathematician. Cambridge, England: Cambridge University Press, 1997.
- Mendelson, Elliott, Introduction to Mathematical Logic. D. Van Nostrand Company, Inc., 1965.