Verificación Formal PCIC, 2021-1
Definiciones Inductivas

Favio E. Miranda Perea
Facultad de Ciencias UNAM

26 de octubre de 2020

1. Objetos y Juicios

Las nociones fundamentales en la clase de definiciones inductivas que trataremos son objetos y juicios.

- Objetos: se consideran como primitivos y previamente dados. Por ejemplo números, árboles, tipos, valores, etc.
- Juicios: Un juicio es una afirmación acerca de un objeto particular cumple cierta propiedad o bien que dos o más objetos pertenecen a una relación. Por ejemplo:

n Nat	n es un número natural
$n = m + k$	n es la suma de m con k
t asa	t es un árbol sintáctico
$3 + 4 * 5$ ExpAr	$3 + 4 * 5$ es una expresión aritmética válida
0.1234 float	0.1234 es un valor flotante
"aba" pal	"aba" es una cadena palíndrómo
T type	T es un tipo
$e : T$	La expresión e tiene tipo T
$e \to e'$	la expresión e se reduce a e'
$e \Downarrow v$	la expresión e se evalua al valor v.

Por lo general usaremos notación infija de la forma $s\ P$ para expresar que s cumple el juicio P o notación infija, cuando el juicio involucra a dos objetos, como $n = k, e : T, e \to e'$. Obsérvese que los juicios son esencialmente predicados en lógica, escritos de manera postfija, por ejemplo en lugar de $P(s)$ escribimos $s\ P$.

2. Reglas de Inferencia

Una regla de inferencia es un esquema de la forma

$$\frac{J_1 \;\; J_2 \ldots J_n}{J}$$

donde J_i, J son juicios.

Ya hemos manejado esta clase de reglas en lógica. Los juicios $J_1 \dots J_n$ son las *premisas* y J es la *conclusión* de la regla. Si no hay premisas la regla es un *axioma*. Algunos ejemplos son:

$$\frac{}{0\ \mathsf{Nat}} \qquad \frac{n\ \mathsf{Nat}}{suc(n)\ \mathsf{Nat}}$$

$$\frac{}{1\ \mathsf{impar}} \qquad \frac{n\ \mathsf{impar}}{suc(suc(n))\ \mathsf{impar}}$$

$$\frac{n\ \mathsf{par} \quad m\ \mathsf{par}}{n+m\ \mathsf{par}} \qquad \frac{n\ \mathsf{par} \quad m\ \mathsf{impar}}{n+m\ \mathsf{impar}}$$

$$\frac{p\ \mathsf{varp}}{p\ \mathsf{form}} \qquad \frac{\varphi\ \mathsf{form} \quad \psi\ \mathsf{form}}{\varphi \vee \psi\ \mathsf{form}}$$

$$\frac{\varphi\ \mathsf{true} \quad \psi\ \mathsf{true}}{\varphi \wedge \psi\ \mathsf{true}} \qquad \frac{\varphi\ \mathsf{true}}{\varphi \vee \psi\ \mathsf{true}}$$

3. Definiciones Inductivas

Una regla de inferencia $\dfrac{J_1 \ \ J_2 \dots J_n}{J}$ es inductiva si al menos uno de los juicios J_i es de la misma forma que el juicio J, es decir, ambos se refieren a la misma propiedad o relación.

Una definición inductiva es un conjunto finito de reglas de inferencia donde al menos una de ellas es inductiva. Por ejemplo considérese la siguiente definición de árboles binarios no etiquetados.

- *void* es un árbol binario.
- Si t, s son árboles binarios entonces $nodo(t, s)$ es un árbol binario.
- Son todos.

Esta definición inductiva corresponde a la siguiente definición mediante reglas de inferencia:

$$\frac{}{void\ \mathsf{btree}} \qquad \frac{t\ \mathsf{btree} \quad s\ \mathsf{btree}}{nodo(t,s)\ \ \mathsf{btree}}$$

Mas adelante puntualizaremos a que corresponde, en la definición por reglas de inferencia, la cláusula *son todos* en la definición original.

Como otro ejemplo veamos la definición inductiva del tipo de datos list_A de listas cuyos elementos son objetos de un conjunto o tipo A, definido aquí por el juicio $x\ A$:

$$\frac{}{nil\ \ \mathsf{list}_A} \qquad \frac{x\ A \quad \ell\ \ \mathsf{list}_A}{(a:\ell)\ \ \mathsf{list}_A}$$

El siguiente ejemplo es de un clásico lenguaje libre de contexto definido mediante la siguiente gramática en forma BNF

$$M ::= \varepsilon \mid (M) \mid MM$$

Esta definición puede reescribirse mediante reglas de inferencia como sigue:

$$\frac{}{\varepsilon\ M}(m1) \qquad \frac{s\ M}{(s)\ M}(m2) \qquad \frac{s_1\ M \quad s_2\ M}{s_1 s_2\ M}(m3)$$

En resumen:

- Las definiciones inductivas nos sirven para definir relaciones de manera mecánica.
- Es importante notar que no todas las relaciones pueden definirse mediante una definición inductiva. Por ejemplo la relación de ser una lista infinita.

4. Derivaciones

- Para mostrar que una instancia de una relación definida inductivamente es válida basta mostrar una derivación de dicha instancia.
- Una derivación es una composición o encadenamiento de reglas de inferencia a partir de axiomas la cual termina con la instancia que se quiere demostrar.
- Una derivación tiene una estructura de árbol donde la derivación de las premisas de una regla son los hijos de un nodo que representa una instancia de dicha regla.
- Dichos árboles se suelen desarrollar con la raíz hasta abajo.

Veamos un par de ejemplos:

- $\mathsf{suc}(\mathsf{suc}(\mathsf{suc}\,0)))\ \mathsf{Nat}$

$$\dfrac{\dfrac{\dfrac{}{0\ \mathsf{Nat}}}{\mathsf{suc}(0)\ \mathsf{Nat}}}{\mathsf{suc}(\mathsf{suc}(0))\ \mathsf{Nat}}}{\mathsf{suc}(\mathsf{suc}(\mathsf{suc}(0)))\ \mathsf{Nat}}$$

- $nodo(nodo(void, void), void)\ \mathsf{btree}$

$$\frac{\dfrac{void\ \mathsf{btree} \quad void\ \mathsf{btree}}{nodo(void,void)\ \mathsf{btree}} \qquad void\ \mathsf{btree}}{nodo(nodo(void, void), void)\ \mathsf{btree}}$$

Existen dos formas principales para construir derivaciones de un juicio dado:

- *Encadenamiento hacia adelante o construcción de abajo hacia arriba*: se inicia con los axiomas siendo la meta el juicio deseado. En este caso se mantiene un conjunto de juicios derivables que inicialmente es vacío, extendiendolo con la conclusión de cualquier regla cuyas premisas ya están en el conjunto. El proceso termina cuando el juicio deseado entra al conjunto. Este es un método indirecto en el sentido de que no se toma en cuenta el juicio meta al decidir como proceder en cada paso. Si el juicio es derivable entonces la aplicación exhaustiva del proceso terminará eventualmente con la conclusión deseada, en caso contrario es imposible en general decidir cuando parar en la construcción del conjunto y concluir que el juicio no es derivable.

- *Encadenamiento hacia atrás o construcción de arriba hacia abajo*: Se inicia con el juicio deseado buscando encadenar reglas hasta terminar en axiomas. Esta búsqueda mantiene una serie de metas actuales que son juicios cuyas derivaciones se buscan. Inicialmente este conjunto contiene únicamente el juicio deseado. En cada etapa se elimina un juicio del conjunto de metas y consideramos todas las reglas cuya conclusión es dicho juicio. Para cada regla agregamos sus premisas al conjunto de metas. El proceso termina cuando el conjunto de metas es vacío. Si el juicio es derivable eventualmente terminará este proceso. Sin embargo en el caso contrario, no hay en general un algoritmo para decidir que el juicio no es derivable.

5. Inducción

La gran mayoría de las demostraciones en este curso se harán usando inducción estructural sobre alguna definición inductiva, dicho principio puede resumirse como sigue:
Suponga que una propiedad o relación A está definida inductivamente por un conjunto de reglas de inferencia S_A. Para mostrar que una segunda propiedad P es válida para todos los elementos x de A basta probar que para cualquier regla que pertenezca a S_A, digamos

$$\frac{x_1\ A \ldots x_n\ A}{x\ A}$$

se cumple que:

$$\textit{Si } P \textit{ es válida para } x_1, \ldots, x_n \textit{ entonces } P \textit{ es válida para } x.$$

Es decir, basta mostrar que cada regla

$$\frac{x_1\ P \ldots x_n\ P}{x\ P}$$

obtenida al sustituir A por P en las reglas de S_A, es una regla válida.

Observemos que las reglas de S_A que son axiomas corresponden a los casos base de la inducción mientras que las otras reglas corresponden a pasos inductivos donde las premisas corresponden a la hipótesis de inducción.

Algunos ejemplos específicos son:

- Números naturales Nat: el principio usual de inducción para naturales es el siguiente:
  - Base de la inducción: probar $P(0)$
  - Hipótesis de inducción (H.I.): suponer $P(x)$
  - Paso inductivo: probar, usando la H.I., que $P(\mathsf{suc}(x))$

  lo cual en forma de reglas corresponde a :

$$\frac{}{0\ P} \qquad \frac{n\ P}{\mathsf{suc}(n)\ P}$$

- Listas list_A:

- Base de la inducción: probar $P(nil)$
- H.I. suponer $a\ inA$ y $P(\ell)$
- Paso inductivo: probar, usando la H.I., $P((a:\ell))$

lo cual en forma de reglas corresponde a :

$$\frac{}{nil\ P} \qquad \frac{a\ A \quad \ell\ P}{(a:\ell)\ P}$$

- Árboles binarios sin etiquetas btree:

  - Base de la inducción: probar $P(void)$.
  - H.I. suponer $P(t), P(s)$
  - Paso inductivo: probar $P(nodo(t,s))$

  lo cual en forma de reglas corresponde a :

$$\frac{}{void\ P} \qquad \frac{t\ P \quad s\ P}{nodo(s,t)\ P}$$

6. Reglas derivables y admisibles

Es importante observar que el número de reglas en una definición inductiva debe ser mínimo, esto facilitará las pruebas inductivas al haber menos casos que verificar en el paso inductivo. Respecto a este punto una vez que se tiene un conjunto de reglas primitivas o básicas Φ debemos distinguir otras clases de reglas, las derivables y las admisibles.

- *Reglas derivables*: Una regla $\mathcal{R}$ es derivable respecto a un conjunto de reglas básicas Φ si y sólo si $\mathcal{R}$ puede obtenerse usando las reglas primitivas de Φ, es decir si se sigue de una derivación parcial de reglas de Φ. Formalmente, la regla

$$\frac{J_1 \ldots J_n}{K}$$

es derivable si al suponer válidos los juicios $J_1, \ldots, J_k$ podemos concluir el juicio K mediante reglas de Φ. Por ejemplo la regla

$$\frac{s\ M}{((s))\ M}$$

es derivable con respecto a $\Phi_M = \{(m1), (m2), (m3)\}$ porque se tiene la siguiente derivación parcial que utiliza la regla $(m2)$ dos veces.

$$\frac{\dfrac{s\ M}{(s)\ M}}{((s))\ M}$$

- *Reglas admisibles* Una regla es admisible respecto a Φ si y sólo si el hecho de que sus premisas sean derivables a partir de Φ implica que su conclusión también es derivable a partir de Φ. Es decir, la regla

$$\frac{J_1 \dots J_n}{K}$$

es admisible si cada vez que podemos derivar $J_1 \dots J_n$ entonces necesariamente derivaremos K.
Puede observarse que una regla admisible no cambia el contenido del lenguaje, es decir, no genera mas cadenas. Por ejemplo la regla

$$\frac{()s\ M}{s\ M}$$

es admisible con respecto a Φ_M pues si derivamos $()s\ M$ entonces usamos la regla $(m3)$ necesariamente pero esto implica que tuvimos que derivar primero $s\ M$ que es lo que necesitabamos para probar la admisibilidad de la regla.

Obsérvese que una regla derivable es admisible mas no al revés. La regla anterior no es derivable pues no tenemos en las reglas primitivas una regla que elimine expresiones.
En contraste la siguiente regla

$$\frac{(s)\ M}{s\ M}$$

no es admisible con respecto a Φ_M pues podemos derivar por ejemplo $()()\ M$ pero no $)(\ M$.

Para afianzar los conceptos veamos unos ejemplos con números pares e impares. Las reglas primitivas son:

$$\frac{}{0\ \mathsf{par}}\ (0p) \qquad \frac{n\ \mathsf{par}}{suc(n)\ \mathsf{impar}}\ (si) \qquad \frac{n\ \mathsf{impar}}{suc(n)\ \mathsf{par}}\ (sp)$$

Por cierto, esta es una definición inductiva simultánea, estamos definiendo dos juicios par e impar al mismo tiempo dependiendo uno del otro.
Se deja como ejercicio verificar que la siguiente regla es derivable

$$\frac{n\ \mathsf{par}}{suc(suc(n))\ \mathsf{par}}\ (ssp)$$

Además la siguiente regla es admisible pero no derivable:

$$\frac{suc(n)\ \mathsf{impar}}{n\ \mathsf{par}}\ (invsi)$$

Veamos por qué: no es derivable pues no hay una regla que pase de impar a par eliminando una aplicación de sucesor. Es admisible pues si derivamos $suc(n)$ impar necesariamente fue mediante la regla (si) de manera que también derivamos n par.

Debemos enfatizar que las nociones de derivabilidad y admisibilidad dependen siempre de un conjunto fijo de reglas primitivas Φ. Al cambiar éste los conceptos pueden cambiar de igual forma.

7. Formalización con puntos fijos

Considérese nuevamente la definición de números naturales

$$\frac{}{0\ \mathsf{Nat}}\ (0n) \qquad \frac{n\ \mathsf{Nat}}{suc(n)\ \mathsf{Nat}}\ (sn)$$

Es claro que el conjunto de números naturales N es cerrado bajo estas reglas, pero también lo es el conjunto de enteros, de racionales y de reales. Entonces ¿Qué conjunto están definiendo las reglas? Esto es de gran importancia para poder justificar formalmente la definición así como los principios de inducción correspondientes. La idea es que un conjunto de reglas Φ va a definir al conjunto más pequeño cerrado bajo ellas. Esto corresponde al caso "son todos" dado en la definición por cláusulas.

A continuación formalizamos estas observaciones mediante el uso de puntos fijos en conjuntos.

Definición 1 *Formalmente una regla de inferencia*

$$\frac{a_1\ X \ldots a_n\ X}{a\ X}\ (\mathcal{R})$$

es un par $\mathcal{R} = \langle \mathcal{P}, a\rangle$ *donde* $\mathcal{P} = \{a_1, \ldots, a_n\}$ *son las premisas y* a *es la conclusión de* $\mathcal{R}$.

Por ejemplo $\Phi_{\mathsf{Nat}} = \{\langle \varnothing, 0\rangle, \langle n, suc(n)\rangle\}$ es una definición inductiva de Nat donde $\langle \varnothing, 0\rangle$ corresponde a la regla $(0n)$ y $\langle n, suc(n)\rangle$ a la regla (sn).

Definición 2 *Sean* Φ *un conjunto de reglas de inferencia y* B *un conjunto cualquiera. Definimos la aplicación de* Φ *a* B*, denotada* $\widehat{\Phi}(B)$*, como:*

$$\widehat{\Phi}(B) = \{x \mid \exists H\ (H, x) \in \Phi \wedge H \subseteq B\}$$

Es decir, $\widehat{\Phi}(B)$ *es el conjunto de todas aquellas conclusiones de instancias de reglas de* Φ *tales que las premisas respectivas pertenecen a* B.

Por ejemplo si $B = \{3, 6, 10\}$ entonces $\widehat{\Phi}_{\mathsf{Nat}}(B) = \{0, suc(3), suc(6), suc(10)\}$.

Es facil ver que $\widehat{\Phi}$ es un operador monótono, es decir, se cumple que si $A \subseteq B$ entonces $\widehat{\Phi}(A) \subseteq \widehat{\Phi}(B)$.

Definición 3 *Un conjunto* B *es* Φ*-cerrado si* $\widehat{\Phi}(B) \subseteq B$*. Es decir que para cualquier instancia* $\langle H, x\rangle$ *de una regla de* Φ*, si* $H \subseteq B$ *entonces* $x \in B$.

La siguiente definición es correcta.

Definición 4 *Sea* $\Phi = \{\mathcal{R}_1, \ldots, \mathcal{R}_n\}$ *una definición inductiva. El conjunto definido por* Φ *es el conjunto* Φ*-cerrado más pequeño con respecto a la inclusión. Es decir, el conjunto*

$$S(\Phi) = \bigcap\{B \mid B\ es\ \Phi - cerrado\}$$

Si Φ_X *define a un juicio* X *entonces definimos* $X = S(\Phi_X)$*. Es decir* $w\ X$ *significa* $w \in S(\Phi_X)$.

La definición anterior no es adecuada computacionalmente, pues la intersección es díficil de calcular al tener que calcular todos los conjuntos Φ-cerrados. En su lugar usamos una definición por aproximaciones observando que X es el mínimo conjunto que cumple $\widehat{\Phi}(X) = X$. Es decir, X es el mínimo punto fijo del operador $\widehat{\Phi}$.

Dejamos como ejercicio mostrar que ambas definiciones de X son equivalentes.
La ventaja de la segunda definición es que el punto fijo puede calcularse iterativamente como sigue:

$$\begin{aligned} X_0 &= \varnothing \\ X_{n+1} &= \widehat{\Phi}(X_n) \\ X &= \textstyle\bigcup_{i=0}^{\infty} X_i \end{aligned}$$

En el caso de nuestra definición de Nat se tiene:

$$\begin{aligned} X_0 &= \varnothing \\ X_1 &= \widehat{\Phi}(X_0) = \widehat{\Phi}(\varnothing) = \{0\} \\ X_2 &= \widehat{\Phi}(X_1) = \{0, suc(0)\} \\ &\vdots \\ X_{n+1} &= \widehat{\Phi}(X_n) = \{0, suc(0), \ldots, suc^n(0)\} \\ &\vdots \end{aligned}$$

De modo que

$$\mathsf{Nat} = \{0, suc(0), \ldots, suc^n(0), suc^{n+1}(0), \ldots\}$$

Obsérvese que X_1 es el conjunto de conclusiones de instancias de axiomas de Φ y que en general X_{n+1} es el conjunto de conclusiones de instancias de reglas de Φ cuyas premisas pertenecen a X_n. Más aún, se tiene que

$$X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq X_{n+1} \subseteq \ldots$$