Capítulo 2

El lenguaje de demostración Isa

Este capítulo describe los elementos básicos del lenguaje de demostración Isar (*Intelligible semi–automated reasoning*).

2.1 Panorama de la sintaxis (simplificada) de Isar

Nota 2.1.1 (Representación de lemas (y teoremas))**.**

- Un **lema** (o **teorema**) comienza con una **etiqueta** seguida por algunas **premisas** y una **conclusión**.
- Las premisas se introducen con la palabra **assumes** y se separan con **and**.
- Cada premisa puede etiquetarse para referenciarse en la demostración.
- La conclusión se introduce con la palabra **shows**.

Nota 2.1.2 (Gramática (simplificada) de las demostraciones en Isar)**.**

demostración	::=	**proof** método declaración* **qed**
	|	**by** método
declaración	::=	**fix** variable+
	|	**assume** proposición+
	|	(**from** hecho+)? **have** proposición+ demostración
	|	(**from** hecho+)? **show** proposición+ demostración
proposición	::=	(etiqueta**:**)? cadena
hecho	::=	etiqueta
método	::=	-
	|	**this**
	|	**rule** hecho
	|	**simp**
	|	**blast**
	|	**auto**
	|	**induct** variable
	|	...

La declaración **show** demuestra la conclusión de la demostración mientras que la declaración **have** demuestra un resultado intermedio.

2.2 Razonamiento proposicional

Nota 2.2.1 (Regla de introducción de la conjunción)**.**

$$(conjI)\ \frac{P \qquad Q}{P \wedge Q}$$

Lema 2.2.2 (Ejemplo de introducción de conjunción con razonamiento progresivo)**.**
$P, Q \vdash P \wedge (Q \wedge P)$.

Demostración: Estamos suponiendo

$$P \tag{2.1}$$

y

$$Q \tag{2.2}$$

De 2.2 y 2.1, por introducción de la conjunción, se tiene

$$Q \wedge P \tag{2.3}$$

De 2.1 y 2.3, por introducción de la conjunción, se tiene $P \wedge (Q \wedge P)$.

□

lemma *conj2*:
 assumes *p*: P **and** *q*: Q
 shows $P \wedge (Q \wedge P)$
proof −
 from *q p* **have** *qp*: $Q \wedge P$ **by** (*rule conjI*)
 from *p qp* **show** $P \wedge (Q \wedge P)$ **by** (*rule conjI*)
qed

Nota 2.2.3 (Razonamiento progresivo y regresivo)**.**

- Isabelle soporta *razonamiento progresivo*. La anterior demostración es una muestra.
- Isabelle soporta *razonamiento regresivo*. La siguiente demostración es una muestra.

Lema 2.2.4 (Ejemplo de introducción de la conjunción con razonamiento regresivo)**.**
$P, Q \vdash P \wedge (Q \wedge P)$

Demostración: Estamos suponiendo

$$P \tag{2.4}$$

y

$$Q \tag{2.5}$$

Para demostrar el lema, por introducción de la conjunción, basta probar

$$P \tag{2.6}$$

y

$$Q \wedge P \tag{2.7}$$

La condición 2.6 se tiene por la hipótesis 2.4. Para demostrar la condición 2.7, por introducción de la conjunción, basta probar

$$Q \tag{2.8}$$

y

$$P \tag{2.9}$$

La condición 2.8 se tiene por la hipótesis 2.5 y la condición 2.9 se tiene por la hipótesis 2.4.

□

lemma
 assumes *p*: P **and** *q*: Q
 shows $P \wedge (Q \wedge P)$
proof (*rule conjI*)

from p **show** P **by** *this*
next
 show $Q \wedge P$
 proof (*rule conjI*)
  from q **show** Q **by** *this*
 next
  from p **show** P **by** *this*
 qed
qed

Nota 2.2.5 (El método *this*)**.** El método *this* demuestra el objetivo usando el hecho actual (es decir, el de la cláusula **from**).

Nota 2.2.6 (Reglas de eliminación de la conjunción)**.**

$$(conjunct1)\ \frac{P \wedge Q}{P} \qquad (conjunct2)\ \frac{P \wedge Q}{Q}$$

Nota 2.2.7 (Regla de introducción de la implicación)**.**

$$(impI)\ \frac{\begin{array}{c} P \\ \hline Q \end{array}}{P \longrightarrow Q}$$

Lema 2.2.8 (Ejemplo de razonamiento híbrido)**.** *Sean a y b dos números naturales. Si* $0 < a$ *y* $a < b$*, entonces* $a * a < b * b$

lemma
 fixes *a b* :: *nat*
 shows $0 < a \wedge a < b \longrightarrow a * a < b * b$
proof (*rule impI*)
 assume *x*: $0 < a \wedge a < b$
 from *x* **have** *za*: $0 < a$ **by** (*rule conjunct1*)
 from *x* **have** *ab*: $a < b$ **by** (*rule conjunct2*)
 from *za ab* **have** *aa*: $a{*}a < a{*}b$ **by** *simp*
 from *ab* **have** *bb*: $a{*}b < b{*}b$ **by** *simp*
 from *aa bb* **show** $a{*}a < b{*}b$ **by** *arith*
qed

Nota 2.2.9 (Modus ponens)**.**

$$(mp)\ \frac{P \longrightarrow Q \qquad P}{Q}$$

Nota 2.2.10 (Reglas de introducción de la disyunción)**.**

$$(disjI1)\ \frac{P}{P \vee Q} \qquad (disjI2)\ \frac{Q}{P \vee Q}$$

Nota 2.2.11 (Regla de eliminación de la disyunción)**.**

$$(disjE)\ \frac{P \vee Q \qquad \begin{array}{c} P \\ \hline R \end{array} \qquad \begin{array}{c} Q \\ \hline R \end{array}}{R}$$

Lema 2.2.12 (Razonamiento por casos)**.**
$A \vee B, A \longrightarrow C, B \longrightarrow C \vdash C$

lemma
 assumes *ab*: $A \vee B$ **and** *ac*: $A \longrightarrow C$ **and** *bc*: $B \longrightarrow C$
 shows C
proof −
 note *ab*
 moreover {
  assume *a*: A
  from *ac a* **have** C **by** (*rule mp*) }
 moreover {
  assume *b*: B
  from *bc b* **have** C **by** (*rule mp*) }
 ultimately show C **by** (*rule disjE*)
qed

Nota 2.2.13 (Resumen de reglas proposicionales)**.**

TrueI	$True$
FalseE	$False \Longrightarrow P$
conjI	$[\![P; Q]\!] \Longrightarrow P \wedge Q$
conjunct1	$P \wedge Q \Longrightarrow Q$
conjE	$[\![P \wedge Q; [\![P; Q]\!] \Longrightarrow R]\!] \Longrightarrow R$
disjI1	$P \Longrightarrow P \vee Q$
disjI2	$Q \Longrightarrow P \vee Q$
disjE	$[\![P \vee Q; P \Longrightarrow R; Q \Longrightarrow R]\!] \Longrightarrow R$
notI	$(P \Longrightarrow False) \Longrightarrow \neg P$
notE	$[\![\neg P; P]\!] \Longrightarrow R$
impI	$(P \Longrightarrow Q) \Longrightarrow P \longrightarrow Q$
impE	$[\![P \longrightarrow Q; P; Q \Longrightarrow R]\!] \Longrightarrow R$
mp	$[\![P \longrightarrow Q; P]\!] \Longrightarrow Q$
iff	$(P \longrightarrow Q) \longrightarrow (Q \longrightarrow P) \longrightarrow P = Q$
iffI	$[\![P \Longrightarrow Q; Q \Longrightarrow P]\!] \Longrightarrow P = Q$
iffD1	$[\![Q = P; Q]\!] \Longrightarrow P$
iffD2	$[\![P = Q; Q]\!] \Longrightarrow P$
iffE	$[\![P = Q; [\![P \longrightarrow Q; Q \longrightarrow P]\!] \Longrightarrow R]\!] \Longrightarrow R$
ccontr	$(\neg P \Longrightarrow False) \Longrightarrow P$
classical	$(\neg P \Longrightarrow P) \Longrightarrow P$
exlude_middle	$\neg P \vee P$
disjCI	$(\neg Q \Longrightarrow P) \Longrightarrow P \vee Q$
impCE	$[\![P \longrightarrow Q; \neg P \Longrightarrow R; Q \Longrightarrow R]\!] \Longrightarrow R$
iffCE	$[\![P = Q; [\![P; Q]\!] \Longrightarrow R; [\![\neg P; \neg Q]\!] \Longrightarrow R]\!] \Longrightarrow R$
notnotD	$\neg \neg P \Longrightarrow P$
swap	$[\![\neg P; \neg R \Longrightarrow P]\!] \Longrightarrow R$

Nota 2.2.14 (Referencia de reglas de inferencia)**.** Más información sobre las reglas de inferencia se encuentra en la sección 2.2 de Isabelle's Logics: HOL.

2.3 Atajos de Isar

Nota 2.3.1 (Atajos de Isar)**.** Isar tiene muchos atajos, como los siguientes:

this	(éste)	= el hecho probado en la declaración anterior
then	(entonces)	= **from this**
hence	(por lo tanto)	= **then have**
thus	(de esta manera)	= **then show**
with hecho+	(con)	= **from** hecho+ **and** *this*
.	(por ésto)	= **by** *this*
..	(trivialmente)	= **by** regla (donde Isabelle adivina la regla)

Nota 2.3.2 (Razonamiento acumulativo)**.** Una sucesión de hechos que se van a usar como premisa en una declaración puede agruparse usando **moreover** (además) y usarse en la declaración usando **ultimately** (finalmente).

Lema 2.3.3 (Ejemplo de uso de atajos y razonamiento acumulativo)**.**
$A \wedge B \vdash B \wedge A.$

lemma $A \wedge B \longrightarrow B \wedge A$
proof $(rule\ impI)$
assume ab: $A \wedge B$
hence B **by** $(rule\ conjunct2)$
moreover from ab **have** A **..**
ultimately show $B \wedge A$ **by** $(rule\ conjI)$
qed

2.4 Cuantificadores universal y existencial

Nota 2.4.1 (Reglas del cuantificador universal)**.**

$$(allI)\ \frac{\bigwedge x.\ P\ x}{\forall x.\ P\ x} \qquad (allE)\ \frac{\forall x.\ P\ x \qquad \dfrac{P\ x}{R}}{R}$$

En la regla *allI* la nueva variable se introduce mediante la palabra **fix**.

Lema 2.4.2 (Ejemplo con cuantificadores universales)**.**
$\forall x.\ P \longrightarrow Q\ x \vdash P \longrightarrow (\forall x.\ Q\ x)$

lemma
assumes a: $\forall\ x.\ P \longrightarrow Q\ x$

shows $P \longrightarrow (\forall\ x.\ Q\ x)$
proof $(rule\ impI)$
assume p: P
show $\forall\ x.\ Q\ x$
proof $(rule\ allI)$
fix x
from a **have** pq: $P \longrightarrow Q\ x$ **by** $(rule\ allE)$
from $pq\ p$ **show** $Q\ x$ **by** $(rule\ mp)$
qed
qed

Nota 2.4.3 (Reglas del cuantificador existencial)**.**

$$(exI)\ \frac{P\ x}{\exists\, x.\ P\ x} \qquad (exE)\ \frac{\exists\, x.\ P\ x \qquad \bigwedge x.\ \dfrac{P\ x}{Q}}{Q}$$

En la regla *exE* la nueva variable se introduce mediante la declaración
'**obtain** ... **where** ... **by** (*rule exE*)'.

Lema 2.4.4 (Ejemplo con cuantificador existencial y demostración progresiva)**.**
$\exists\, x.\ P \wedge Q(x) \vdash P \wedge (\exists\, x.\ Q(x))$

lemma
assumes e: $\exists\ x.\ P \wedge Q(x)$
shows $P \wedge (\exists\ x.\ Q(x))$
proof $-$
from e **obtain** x **where** f: $P \wedge Q(x)$ **by** $(rule\ exE)$
from f **have** p: P **by** $(rule\ conjunct1)$
from f **have** q: $Q(x)$ **by** $(rule\ conjunct2)$
from q **have** eq: $\exists\ x.\ Q(x)$ **by** $(rule\ exI)$
from $p\ eq$ **show** $P \wedge (\exists\ x.\ Q(x))$ **by** $(rule\ conjI)$
qed

Lema 2.4.5 (Ejemplo con cuantificador existencial y demostración progresiva automática)**.**

$\exists\, x.\ P \wedge Q(x) \vdash P \wedge (\exists\, x.\ Q(x))$

lemma
assumes e: $\exists\ x.\ P \wedge Q(x)$
shows $P \wedge (\exists\ x.\ Q(x))$
proof $-$

from e **obtain** x **where** f: $P \wedge Q(x)$ **..**
from f **have** p: P **..**
from f **have** q: $Q(x)$ **..**
from q **have** eq: $\exists\ x.\ Q(x)$ **..**
from p eq **show** $P \wedge (\exists\ x.\ Q(x))$ **..**
qed

Lema 2.4.6 (Ejemplo con cuantificador existencial y demostración regresiva)**.**
$\exists x.\ P \wedge Q(x) \vdash P \wedge (\exists x.\ Q(x))$

lemma
assumes e: $\exists\ x.\ P \wedge Q(x)$
shows $P \wedge (\exists\ x.\ Q(x))$
proof (*rule conjI*)
show P
proof $-$
from e **obtain** x **where** p: $P \wedge Q(x)$ **by** (*rule exE*)
from p **show** P **by** (*rule conjunct1*)
qed
show $\exists\ y.\ Q(y)$
proof $-$
from e **obtain** x **where** p: $P \wedge Q(x)$ **by** (*rule exE*)
from p **have** q: $Q(x)$ **by** (*rule conjunct2*)
from q **show** $\exists\ y.\ Q(y)$ **by** (*rule exI*)
qed
qed

Definición 2.4.7 (Ejemplo de definición existencial)**.** *El número natural x divide al número natural y si existe un natural k tal que* $k \times x = y$*. Se representa por* $x \mid y$*.*

definition *divide* :: *nat* $\Rightarrow$ *nat* $\Rightarrow$ *bool* (- | - [*80,80*] *80*) **where**
$x \mid y \equiv \exists\ k.\ k{*}x = y$

Nota 2.4.8 (Ejemplo de activación automática de regla de simplificación)**.** La definición de `divide` se añade a las reglas de simplificación.

declare *divide-def* [*simp*]

Lema 2.4.9 (Transitividad de la divisibilidad)**.** *Sean a, b y c números naturales. Si a es divisible por b y b es divisible por c, entonces a es divisible por c.*

lemma *divide-trans*:

```
  fixes a b c :: nat
  assumes ab: a | b and bc: b | c
  shows a | c
proof simp
  from ab obtain m where m: m*a = b by auto
  from bc obtain n where n: n*b = c by auto
  from m n have m*n*a = c by auto
  thus ∃ k. k*a = c by (rule exI)
qed
```

Nota 2.4.10 (Método *auto*)**.** En el lema anterior es la primera vez que se usa el método automático (**by** *auto*).

Lema 2.4.11 (CNS de divisibilidad)**.** *Sean a y b dos números naturales. Entonces a es divisible por b syss el resto de dividir a entre b es cero.*

```
lemma CNS-divisibilidad:
  (a | b) = (b mod a = 0)
by auto
```

2.5 Razonamiento ecuacional

Nota 2.5.1 (Elementos para el razonamiento ecuacional)**.** El razonamiento ecuacional se realiza de manera más concisa usando la combinación de **also** (además) y **finally** (finalmente).

Lema 2.5.2 (Ejemplo de razonamiento ecuacional)**.** *Si $a = b$, $b = c$ y $c = d$, entonces $a = d$.*

```
lemma
  assumes 1: a = b and 2: b = c and 3: c = d
  shows a = d
proof –
  have a = b by (rule 1)
  also have ... = c by (rule 2)
  also have ... = d by (rule 3)
  finally show a = d .
qed
```

Nota 2.5.3 (Demostración automática con la maza)**.** El lema anterior puede demostrarse automáticamente con la maza ("sledgehammer").

lemma
 assumes *1*: $a = b$ **and** *2*: $b = c$ **and** *3*: $c = d$
 shows $a = d$
proof $-$
 show $a{=}d$ **by** $(metis\ 1\ 2\ 3)$
qed