Isar (Big) Operational Semantics

(goals, assumptions) Isar (goals, assumptions)

[g, a] proof - ⇓ [g, a]

[g, a] proof ⇓ [g', a']

[g, a] proof (method) ⇓ [g', a']

proof (prove)
proof (state)
proof (chain)

$P \xrightarrow{\Delta} P'$

P, P' = program
Δ = label describing the semantic configuration both before & after the transition

[g, a, c] have P [P, a, c] 11

$$\frac{[g,a,c]\ C_1 \Downarrow [g',a',c'] \quad [g',a',c']\ C_2 \Downarrow [g'',a'',c'']}{[g,a,c]\ C_1 ; C_2 \Downarrow [g'',a'',c'']}$$

assumes rule + shows + || sequential

5

[{}, {}, {}] lemma assumes: n1 "A_1" [n1, {}, {n2}]
g a c
shows: n2 "A_2"

g a c
[{}, {}, {}] have <prop> proof ⇓ [{}, {}, prop + c]

[g, a, c] <proof> ⇓ [g', a', c']

[g, a, c] proof - [g, a, c] 4

[g, a, c] by method ⇓ [g', a', c'] 1

9 [{}, {}, {}] assumes n1: "A_1" [{}, {}, {n1}]

10 [{}, {}, {}] shows n2: "A_2" [{A_2}, {}, {}]

[g, a, c] from e_1 e_2 … e_n ⇓ [g, a + [e_1 … e_n], c] 3

[{}, {}, {}] and n3: "A_3" … "A"
[{}, {}, {n3}]

[g, a, c] show "prop" ["prop", a, c] 2

[g, a, c] assume e1: $prop_1$ … e_n: $prop_n$ [g, a, c + [e_1, … e_n] + [this]] 7

[[[A_1 … A_n] ⇒ P]], [[A_1 … A_n]], c] show P [P, [[A_1 … A_n]], c] 8

[{}, {}, {}] lemma assumes "A" shows "A" ⇓ [A, A]   [A, A] by (simp add: n1) ⇓ [{}, {}, {}]

[{}, {}, {}] lemma assumes "A" shows n3: "A" | by (simp add: n1) ⇓ [{}, {}, {n3}]

assumes n1: "A"

[{},{},{}] lemma shows n2: "A" ["A", {}, "A"] | ["A", {}, "A"] proof - ["A", {}, "A"] | ["A", {}, "A"] from n1 ["A", n1=>"A", n1=>"A"] | ["A", "A", "A"] shows "A" ["A", "A", "A"] | ["A", "A", "A"] by assumption [{}, {}, {n2}]

[{},{},{}] lemma assumes n1: "A" shows n6: "A" | proof - | from n1 | show "A" | by assumption [{}, {}, {n6}]

5 4 3 2 1

lemma shows

[{},{},{}] n7: "A=>A" [{A=>A, {}, {}] | [A=>A, {}, {}] proof - [A=>A, {}, {}] | [A=>A, {}, {}] assume e1: "A" [A=>A, {e1}, {}] | [A=>A, e1, {}] from e1 [A=>A, {}, {e1}] | [A=>A, {}, {e1}] from e1 [A=>A, {e1}, {e1}] | [A=>A, A, e1] show "A" [A, A, e1] | [A, A, e1] by assumption [{}, {}, {n7}]

[{}, {}, {}] lemma shows n7: "A=>A" proof - assume e1: "A" from e1 show "A" by assumption [{}, {}, {n7}]

10 4 7 3 8 1