Proof Styles

Stylised has been renamed to semi-structured!

What is a proof?

Assume the following facts are true:

(1) A person is happy if all of their children are rich.
(2) Someone is a supervillain if at least one of their parents is a supervillain.
(3) All supervillains are rich.

Show that:

All supervillains are happy.

(state any additional assumptions that you make)

Need an extra assumption:

(4) A supervillain is also a person.

Given:

(1) $\forall x.[\ \mathit{person}(x) \wedge \forall y.[\ \mathit{childof}(y,x) \longrightarrow \mathit{rich}(y)\ ] \longrightarrow \mathit{happy}(x)\ ]$

(2) $\forall x.[\ \exists y.[\ \mathit{childof}(x,y) \wedge \mathit{supervillain}(y)\ ] \longrightarrow \mathit{supervillain}(x)\ ]$

(3) $\forall x.[\ \mathit{supervillain}(x) \longrightarrow \mathit{rich}(x)\ ]$

(4) $\forall x.[\ \mathit{supervillain}(x) \longrightarrow \mathit{person}(x)\ ]$

To show:

(α) $\forall x.[\ \mathit{supervillain}(x) \longrightarrow \mathit{happy}(x)\ ]$

Now, this can be proven.

(1) $\forall x.[\ \mathit{person}(x) \wedge \forall y.[\ \mathit{childof}(y,x) \longrightarrow \mathit{rich}(y)\ ] \longrightarrow \mathit{happy}(x)\ ]$	(given)
(2) $\forall x.[\ \exists y.[\ \mathit{childof}(x,y) \wedge \mathit{supervillain}(y)\ ] \longrightarrow \mathit{supervillain}(x)\ ]$	(given)
(3) $\forall x.[\ \mathit{supervillain}(x) \longrightarrow \mathit{rich}(x)\ ]$	(given)
(4) $\forall x.[\ \mathit{supervillain}(x) \longrightarrow \mathit{person}(x)\ ]$	(given)
(5) Gru	$\forall$I const
(6) $\mathit{supervillain}(\mathit{Gru})$	(ass)
(7) $\mathit{person}(\mathit{Gru})$	$\forall{\to}$E(6, 4)
(8) Agnes	$\forall$I const
(9) $\mathit{childof}(\mathit{Agnes},\mathit{Gru})$	(ass)
(10) $\mathit{childof}(\mathit{Agnes},\mathit{Gru}) \wedge \mathit{supervillain}(\mathit{Gru})$	$\wedge$I(9, 6)
(11) $\exists y.[\ \mathit{childof}(\mathit{Agnes},y) \wedge \mathit{supervillain}(y)\ ]$	$\exists$I(10)
(12) $\mathit{supervillain}(\mathit{Agnes})$	$\forall{\to}$E(2, 11)
(13) $\mathit{rich}(\mathit{Agnes})$	$\forall{\to}$E(3, 12)
(14) $\mathit{childof}(\mathit{Agnes},\mathit{Gru}) \longrightarrow \mathit{rich}(\mathit{Agnes})$	$\to$I(9, 13)
(15) $\forall y.[\ \mathit{childof}(y,\mathit{Gru}) \longrightarrow \mathit{rich}(y)\ ]$	$\forall$I(8, 14)
(16) $\mathit{person}(\mathit{Gru}) \wedge \forall y.[\ \mathit{childof}(y,\mathit{Gru}) \longrightarrow \mathit{rich}(y)\ ]$	$\wedge$I(7, 15)
(17) $\mathit{happy}(\mathit{Gru})$	$\forall{\to}$E(1, 16)
(18) $\mathit{supervillain}(\mathit{Gru}) \longrightarrow \mathit{happy}(\mathit{Gru})$	$\to$I(6, 17)
(19) $\forall x.[\ \mathit{supervillain}(x) \longrightarrow \mathit{happy}(x)\ ]$	$\forall$I(5, 18)

Semi-Structured Proofs

Given:

* (1) $\forall x.[\ person(x) \land \forall y.[\ childof(y,x) \longrightarrow rich(y)\ ] \longrightarrow happy(x)\ ]$

(2) $\forall x.[\ \exists y.[\ childof(x,y) \land supervillain(y)\ ] \longrightarrow supervillain(x)\ ]$

(3) $\forall x.[\ supervillain(x) \longrightarrow rich(x)\ ]$

(4) $\forall x.[\ supervillain(x) \longrightarrow person(x)\ ]$

To show:

(α) $\forall x.[\ supervillain(x) \longrightarrow happy(x)\ ]$

Proof:

Take arb. Gru

(ass1) $sv(Gru)$

* (5) $p(Gru) \land \forall y.[\ childof(y, Gru) \rightarrow rich(y)\ ] \rightarrow happy(Gru)$ — from (1)

(6) $p(Gru)$ — from (ass1) and (…)

Take arb. Edith

(ass2) $childof(Edith, Gru)$

(7) $sv(Edith)$ — from (ass2) (ass1) and (…)

(8) $rich(Edith)$ — from (7) and (3)

(9) $\forall y.[\ childof(y, Gru) \rightarrow rich(y)\ ]$ — from (ass2), (8) and Edith arb.

(10) $happy(Gru)$ — from (5), (6), (9)

Thus (α) holds — from (ass1), (10) and Gru arb.

…opoulou & Wheelhouse (DoC) Reasoning about Programs

Comparing the Proof Styles

(1) **Free-Form Proofs:**

- (+) short to develop
- (+) might highlight the intuition
- (−) error prone

(2) **Natural Deduction Proofs:**

- (+) total confidence in the proof
- (−) very lengthy
- (−) layout sometimes (often?) difficult
- (−) intuition may be lost in the detail

(3) **Stylised Proofs:**

- (+) structure of argument made explicit
- (+) few errors
- (−) errors *are* still possible

Aims of a Proof

Aim	Free-Form	Natural Deduction	Stylised
prove only valid	X	✓	≈
easily read at time	X	≈	✓
easily read later	X	≈	✓
others can check	X	✓	✓
highlight intuitions	✓	X	≈

Semi-Structured Proofs: Rules

Rule 1. write out and name each given formula.

Rule 2. write out and name each formula to be shown.

Rule 3. plan out the proof and name intermediate results.

Rule 4. justify each step of the proof.

Rule 5. vary the size of each step as appropriate.

Making the plan and the Justifications

To prove P:	If $P = Q \wedge R$	then	prove Q and R.	($\wedge$I)
	If $P = Q \vee R$	then	prove either Q or R	($\vee$I)
	If $P = Q \longrightarrow R$	then	assume Q and prove R.	($\longrightarrow$I)
	If $P = \neg Q$	then	prove that $Q \longrightarrow \mathit{false}$.	($\neg$I)
	If $P = \forall x.\ Q(x)$	then	take arbitrary c and show $Q(c)$.	($\forall$I)
	If $P = \exists x.\ Q(x)$	then	find some c and show $Q(c)$.	($\exists$I)
	otherwise...		try proving that $\neg P \longrightarrow \mathit{false}$.	(PC)

After proving P:	If $P = Q \wedge R$	then	Q and R hold	($\wedge$E)
	If $P = Q \vee R$	then	proceed with case analysis	($\vee$E)
	If $P = (Q \longrightarrow R) \wedge Q$	then	R also holds	($\longrightarrow$E)
	If $P = \forall x.\ Q(x)$	then	$Q(c)$ holds for *any* c.	($\forall$E)
	If $P = \exists x.\ Q(x)$	then	$Q(c)$ holds for *some* c.	($\exists$E)
	If $P = \mathit{false}$	then	*any* Q holds.	($\perp$E)
	If $P = \neg Q$	then	$Q \longrightarrow \mathit{false}$ holds	($\neg$E)
	otherwise...		apply any lemma,	(LEM)
			or any logical equivalence.	(EQV)

[NB: in this context = stands for "has the form"]

Examples

$A \to C$

Given: (A) $\forall x \exists y. [\, friend(x, y) \to happy(x) \,]$

To show: (C) $\forall x. [\, \forall y.\ friend(x, y) \to happy(x) \,]$

Proof take x_1 arb.

$\longrightarrow$ (1) $\forall y.\ friend(x_1, y)$

need to show $happy(x_1)$

for some choice of y_1 for y

$\longrightarrow$ (2) $friend(x_1, y_1) \to happy(x_1)$ from (A)

$\longrightarrow$ (3) $friend(x_1, y_1)$ from (1)

Therefore

(4) $happy(x_1)$ from (2) and (3)

Thus we've shown

(5) $\forall y.\ friend(x_1, y) \to happy(x_1)$

Since x_1 was arb. then (C) follows from (5)

Given:

(1) $\forall x.[\ dragon(x) \land \forall y.[\ childof(y,x) \longrightarrow fly(y)\ ] \longrightarrow happy(x)\ ]$ (given)

(2) $\forall x.[\ green(x) \land dragon(x) \longrightarrow fly(x)\ ]$ (given)

(3) $\forall x.[\ \exists y.[\ parentof(y,x) \land green(y)\ ] \longrightarrow green(x)\ ]$ (given)

(4) $\forall x.\forall y.[\ childof(x,y) \land dragon(y) \longrightarrow dragon(x)\ ]$ (given)

(5) $\forall x.\forall y.[\ childof(y,x) \longrightarrow parentof(x,y)\ ]$ (given)

To show:

(α) $\forall x.[\ dragon(x) \longrightarrow (green(x) \longrightarrow happy(x))\ ]$

Proof:

take arb. dragon Smaug

(ass1) dragon (Smaug)

(ass2) green (Smaug)

need to show happy (Smaug)

(6) $\forall x. \forall y. [parentof(y,x) \land green(y) \rightarrow green(x)]$ from (3)

(7) $\forall x. \forall y. [childof(x,y) \land green(y) \rightarrow green(x)]$ from (6) and (5)

(8) $\forall x. [childof(x, Smaug) \rightarrow green(x)]$ from (7) and (ass2)

(9) $\forall x. [childof(x, Smaug) \rightarrow dragon(x)]$ from (4) and (ass1)

(10) $\forall x. (childof(x, Smaug) \rightarrow dragon(x) \land green(x))$ from (9) and (8)

(11) $\forall x. [childof(x, Smaug) \rightarrow fly(x)]$ from (10) and (2)

(12) happy(Smaug) follows from (1), (ass1) and (11)

Thus (α) holds from (ass1) (ass2) (12) Smaug arb.