

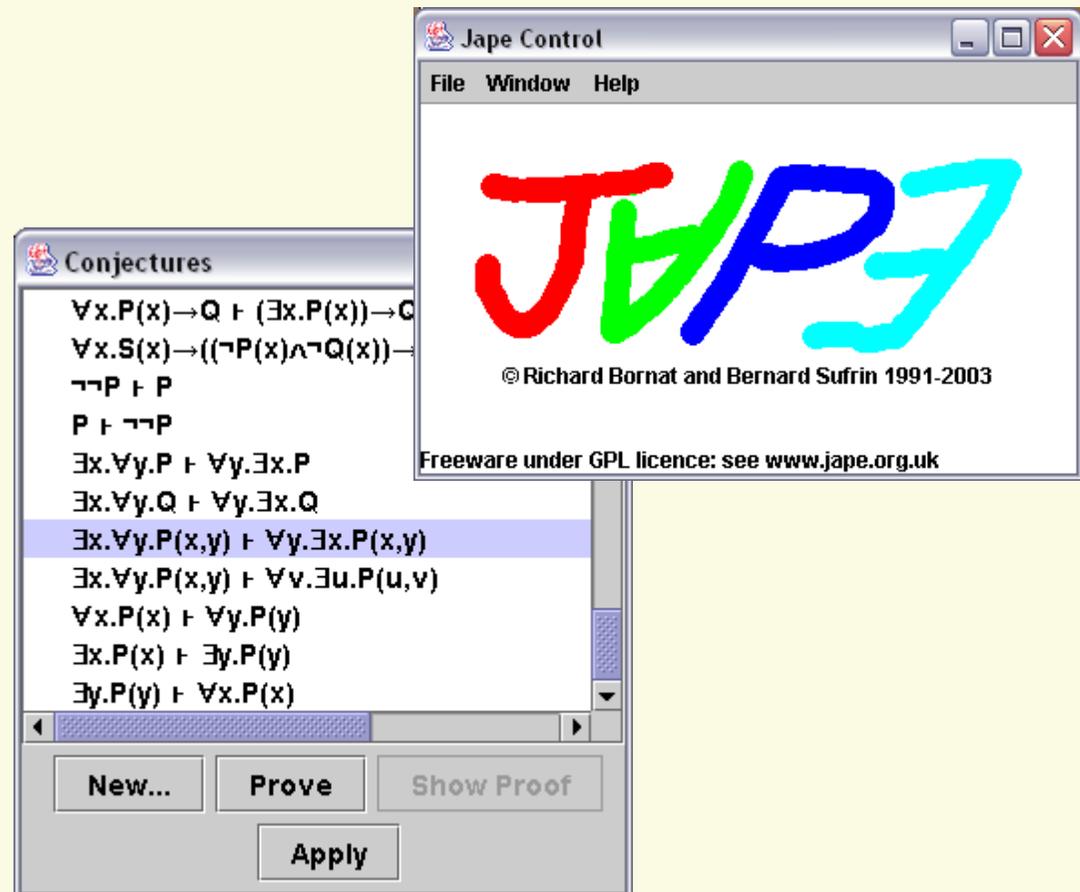
A spiral-bound notebook with a light brown, textured cover. The spiral binding is on the left side. The text is centered on the cover.

Jape

Just another proof editor

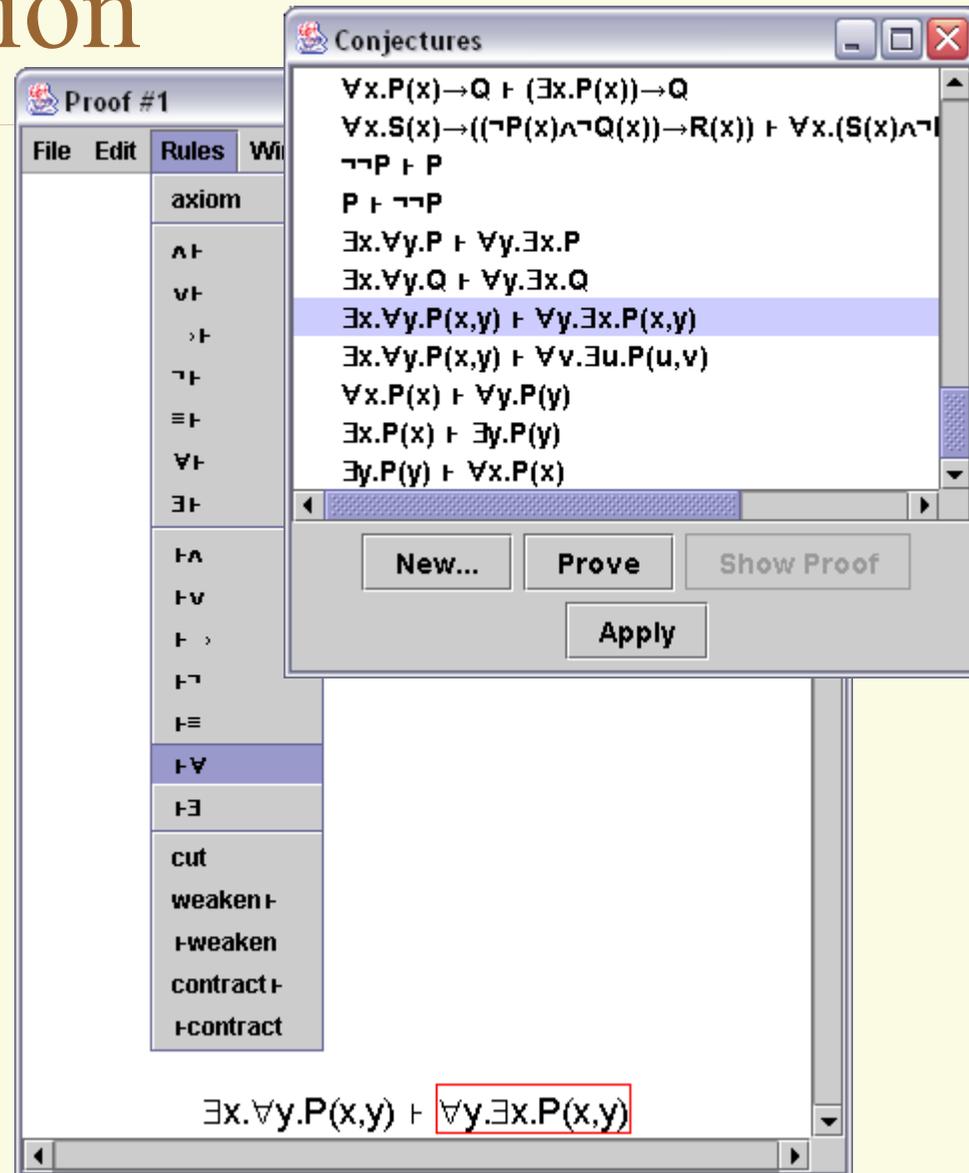
Jape – Just another proof editor

- Jape ist ein System zur interaktiven Erstellung von Beweisen
- Jape erlaubt
 - selber Logiken zu erfinden
 - Beweisregeln einzuführen
 - interaktiv Beweise zu führen
- Beweisregeln können durch
 - Mouseclicks
 - Gestures (nur unter Apple)
 - ausgeführt werden
- Beweise können durch Unifikation erleichtert werden



Jape Interaktion

- In einer „Conjecture-Datei“ werden zu beweisende Sätze aufgeschrieben
- In einem „Conjecture-Panel“ wählt man die zu beweisende Formel
- Die Anwendung der Beweisregeln wählt man
 - aus einem Menü, oder
 - durch Anklicken des zu bearbeitenden logischen Operators



Beweis durch point and click

Ein Doppelklick auf die Formel wendet die Regel des äußeren Operators an

\forall -R

\exists -R

m1 steht für einen noch unbekannten Term

1. $\exists x. \forall y. P(x,y) \vdash \forall y. \exists x. P(x,y)$

2. $\frac{\exists x. \forall y. P(x,y) \vdash \exists x. P(x,m)}{\exists x. \forall y. P(x,y) \vdash \forall y. \exists x. P(x,y)}$

3. $\frac{\forall y. P(m1,y) \vdash \exists x. P(x,m)}{\exists x. \forall y. P(x,y) \vdash \exists x. P(x,m)}$

$\frac{\exists x. \forall y. P(x,y) \vdash \exists x. P(x,m)}{\exists x. \forall y. P(x,y) \vdash \forall y. \exists x. P(x,y)}$

Beweis

- **m1** steht für eine Skolemkonstante
- **_B, _B1** stehen für Unifikationsvariable

Proof #1

File Edit Rules Window Help

$\forall y.P(m1,y) \vdash \exists x.P(x,m)$

$\exists x.\forall y.P(x,y) \vdash \exists x.P(x,m)$

$\exists x.\forall y.P(x,y) \vdash \forall y.\exists x.P(x,y)$

Proof #1

File Edit Rules Window Help

$P(m1, _B) \vdash \exists x.P(x,m)$

$\forall y.P(m1,y) \vdash \exists x.P(x,m)$

$\exists x.\forall y.P(x,y) \vdash \exists x.P(x,m)$

$\exists x.\forall y.P(x,y) \vdash \forall y.\exists x.P(x,y)$

Proof #1

File Edit Rules Window Help

$P(m1, _B) \vdash P(_B1,m)$

$P(m1, _B) \vdash \exists x.P(x,m)$

$\forall y.P(m1,y) \vdash \exists x.P(x,m)$

$\exists x.\forall y.P(x,y) \vdash \exists x.P(x,m)$

$\exists x.\forall y.P(x,y) \vdash \forall y.\exists x.P(x,y)$

1.

2.

3.

Unifikation

- 4 Eine Anwendung des Axioms

$$\Gamma, p \vdash \Delta, p$$

besteht in der Unifikation von $P(m1, _B)$ mit $P(_B1, m)$. Das ist möglich mit $\sigma = \{ B = m, _B1 = m1 \}$

- 4 Das beendet den Beweis.

The image shows three overlapping screenshots of a proof editor window titled "Proof #1". The window has a menu bar with "File", "Edit", "Rules", "Window", and "Help".

- The top-most screenshot shows the "Rules" menu open, with "axiom" selected. A blue arrow points to the "axiom" option.
- The middle screenshot shows the proof text with the goal $P(m1, _B) \vdash P(_B1, m)$ highlighted in red boxes. Below it, the proof steps are:
$$\frac{P(m1, _B) \vdash P(_B1, m)}{\vdash \exists}$$
$$P(m1, _B) \vdash \exists x.P(x, m)$$
$$\frac{\forall y.P(m1, y) \vdash \exists x.P(x, m)}{\vdash \forall}$$
$$\exists x.\forall y.P(x, y) \vdash \exists x.P(x, m)$$
$$\frac{\exists x.\forall y.P(x, y) \vdash \exists x.P(x, m)}{\vdash \forall}$$
$$\exists x.\forall y.P(x, y) \vdash \forall y.\exists x.P(x, y)$$
- The bottom-most screenshot shows the proof text after applying the axiom. The goal is now $P(m1, m) \vdash P(m1, m)$. The proof steps are:
$$\frac{}{\text{axiom}}$$
$$P(m1, m) \vdash P(m1, m)$$
$$\frac{P(m1, m) \vdash P(m1, m)}{\vdash \exists}$$
$$P(m1, m) \vdash \exists x.P(x, m)$$
$$\frac{\forall y.P(m1, y) \vdash \exists x.P(x, m)}{\vdash \forall}$$
$$\exists x.\forall y.P(x, y) \vdash \exists x.P(x, m)$$
$$\frac{\exists x.\forall y.P(x, y) \vdash \exists x.P(x, m)}{\vdash \forall}$$
$$\exists x.\forall y.P(x, y) \vdash \forall y.\exists x.P(x, y)$$

Beweisdarstellung

- 4 Jape kann Beweise in
- Box-Darstellung oder
 - Baumdarstellung anzeigen



Proof #1

File Edit Tracing Rules Auto Window Help

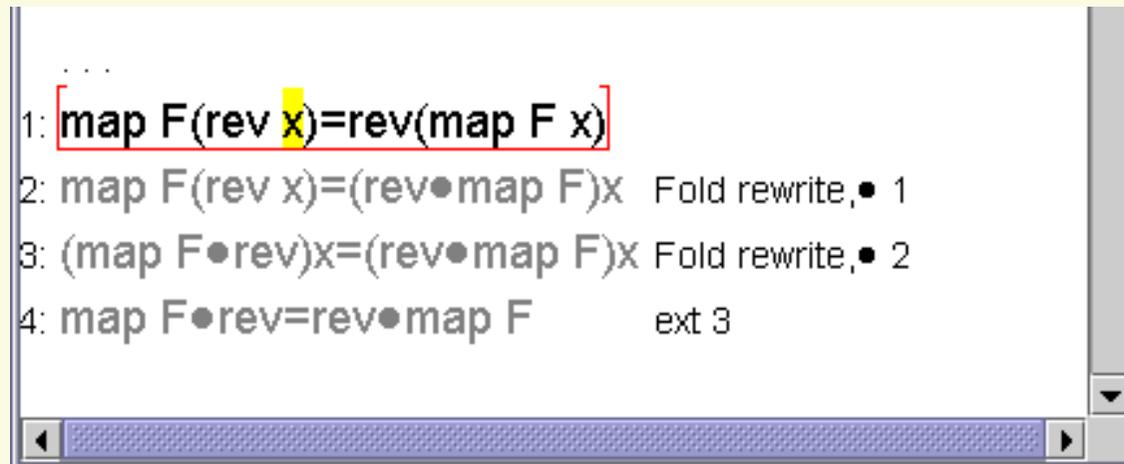
1:	$\exists x.P(x) \wedge \neg Q(x), \forall x.P(x) \rightarrow R(x)$	assumptions
2:	$P(m) \wedge \neg Q(m)$	assumption
3:	$P(m) \rightarrow R(m)$	assumption
4:	$P(m), \neg Q(m)$	assumptions
5:	$R(m)$	assumption
6:	$R(m) \wedge \neg Q(m)$	$\wedge \vdash$ 5,4.2
7:	$\exists x.R(x) \wedge \neg Q(x)$	$\exists \vdash$ 6
8:	$\exists x.R(x) \wedge \neg Q(x)$	$\rightarrow \vdash$ 3,4,1,5-7
9:	$\exists x.R(x) \wedge \neg Q(x)$	$\wedge \vdash$ 2,4-8
10:	$\exists x.R(x) \wedge \neg Q(x)$	$\forall \vdash$ 1,2,3-9
11:	$\exists x.R(x) \wedge \neg Q(x)$	$\exists \vdash$ 1.1,2-10

Tracing Rules Auto Window Help

$$\begin{array}{c}
 \frac{}{\text{hyp}} \quad \frac{}{\text{hyp}} \\
 \frac{P(m), \neg Q(m), R(m) \vdash R(m) \quad P(m), \neg Q(m), R(m) \vdash \neg Q(m)}{\wedge \vdash} \\
 \frac{}{\text{hyp}} \quad \frac{P(m), \neg Q(m), R(m) \vdash R(m) \wedge \neg Q(m)}{\exists \vdash} \\
 \frac{P(m), \neg Q(m) \vdash P(m) \quad P(m), \neg Q(m), R(m) \vdash \exists x.R(x) \wedge \neg Q(x)}{\rightarrow \vdash} \\
 \frac{P(m) \rightarrow R(m), P(m), \neg Q(m) \vdash \exists x.R(x) \wedge \neg Q(x)}{\wedge \vdash} \\
 \frac{P(m) \wedge \neg Q(m), P(m) \rightarrow R(m) \vdash \exists x.R(x) \wedge \neg Q(x)}{\forall \vdash} \\
 \frac{\forall x.P(x) \rightarrow R(x), P(m) \wedge \neg Q(m) \vdash \exists x.R(x) \wedge \neg Q(x)}{\exists \vdash} \\
 \exists x.P(x) \wedge \neg Q(x), \forall x.P(x) \rightarrow R(x) \vdash \exists x.R(x) \wedge \neg Q(x)
 \end{array}$$

Theorie funktionaler Programme

- 4 Beginn des Beweises von
 $\text{map } F \circ \text{rev} = \text{rev} \circ \text{map } F$
- 4 Teilterme können mit
Alt-Linke Maustaste
markiert werden



```
...
1: map F(rev x)=rev(map F x)
2: map F(rev x)=(rev•map F)x  Fold rewrite, • 1
3: (map F•rev)x=(rev•map F)x  Fold rewrite, • 2
4: map F•rev=rev•map F      ext 3
```

Eigene Logiken in Jape

- In Jape können beliebige Logiken selber erstellt werden
 - Syntax der Formeln
 - Regeln
 - Menüs für Regelauswahl
 - Mausinteraktionen
- Vorhanden sind u.a.
 - Sequenzenkalkül (MCSC)
 - Single-Conclusion Sequenzenkalkül (SCSC)
 - Natürliches Schließen
 - BAN-Kalkül (für Verifikation von Sicherheitsprotokollen)
 - Funktionales Programmieren
 - etc. ...

Beispiel für eine Jape-Definition:

- Regeln für Natürliche Herleitung

```
RULE "→-E"(A) IS FROM A AND A→B INFER B
RULE "∧-E(L)"(B) IS FROM A ∧ B INFER A
RULE "∧-E(R)"(A) IS FROM A ∧ B INFER B
RULE "∨-E"(A,B) IS FROM A ∨ B AND A ⊢ C AND B ⊢ C INFER C
RULE "¬-E" IS FROM ¬¬A INFER A
RULE "∀-E"(B) IS FROM ∀x. A(x) INFER A(B)
RULE "∃-E"(OBJECT c) WHERE FRESH c AND c NOT IN ∃x.A IS FROM ∃x.A(x) AND A(c) ⊢ C INFER C

RULE "→-I" IS FROM A ⊢ B INFER A→B
RULE "∧-I" IS FROM A AND B INFER A ∧ B
RULE "∨-I(L)"(B) IS FROM A INFER A ∨ B
RULE "∨-I(R)"(A) IS FROM B INFER A ∨ B
RULE "¬-I"(B) IS FROM A ⊢ B ∧ ¬B INFER ¬A
RULE "∀-I"(OBJECT c) WHERE FRESH c IS FROM A(c) INFER ∀x. A(x)
RULE "∃-I"(B) IS FROM A(B) INFER ∃x.A(x)
```

Anwendung von Regeln durch Mausclick

```
HYPHIT  A→B ⊢ IS "→⊢"
HYPHIT  A∨B ⊢ IS "∨⊢"
HYPHIT  A∧B ⊢ IS "∧⊢"
HYPHIT  ¬A ⊢ IS "¬⊢"
HYPHIT  ∀x.A ⊢ IS "∀⊢"
HYPHIT  ∃x.A ⊢ IS "∃⊢"
```

... im Antezedenz

```
CONCHIT  B∧C IS "⊢∧"
CONCHIT  B∨C IS "⊢∨"
CONCHIT  B→C IS "⊢→"
CONCHIT  ¬B IS "⊢¬"
CONCHIT  ∀x.B IS "⊢∀"
CONCHIT  ∃x.B IS "⊢∃"
```

... im Succedenz

Die definierte Jape-Logik in Aktion

The screenshot shows a Jape proof editor window titled "Proof #1". The menu bar includes "File", "Edit", "Rules", "Window", and "Help". A "Rules" panel on the left lists various logical rules, including "axiom", "∧⊢", "∨⊢", "→⊢", "¬⊢", "≡⊢", "∀⊢", "∃⊢", "⊢∧", "⊢∨", "⊢→", "⊢¬", "⊢≡", "⊢∀", "⊢∃", "cut", "weaken⊢", "⊢weaken", "contract⊢", and "⊢contract".

The main area of the window displays a complex logical derivation for the theorem $R \rightarrow S \vdash (P \rightarrow R) \rightarrow (P \rightarrow S)$. The derivation is structured as follows:

$$\begin{array}{c}
 \frac{}{P \vdash P, R, S} \text{ axiom} \quad \frac{}{P, R \vdash R, S} \text{ axiom} \\
 \frac{}{P \rightarrow R, P \vdash R, S} \rightarrow\vdash \quad \frac{}{P \rightarrow R, P, S \vdash S} \text{ axiom} \\
 \frac{}{R \rightarrow S, P \rightarrow R, P \vdash S} \rightarrow\vdash \\
 \frac{}{R \rightarrow S, P \rightarrow R \vdash P \rightarrow S} \vdash\rightarrow \\
 R \rightarrow S \vdash (P \rightarrow R) \rightarrow (P \rightarrow S)
 \end{array}$$

Die Menüdefinition ...

```
MENU Rules IS
ENTRY axiom
SEPARATOR
```

...

```
ENTRY "⊢∀"
ENTRY "⊢∃"
SEPARATOR
ENTRY cut
ENTRY "weaken⊢"
ENTRY "⊢weaken"
ENTRY "contract⊢"
ENTRY "⊢contract"
```

END