To be or not to be (LPF)

John Fitzgerald

Cliff Jones

The Logic of Partial Functions

Undefinedness is commonplace

```
hd []
if s <> [] then hd s else nil
d in set dom m and m(d) = 3

subp(i,j) == if i=j then 0 else subp(i,j+1)+1
```

Basic LPF

- A generalisation of classical logic
- Admits undefinedness, e.g.

  $x = 0 \vee x/x = 1$

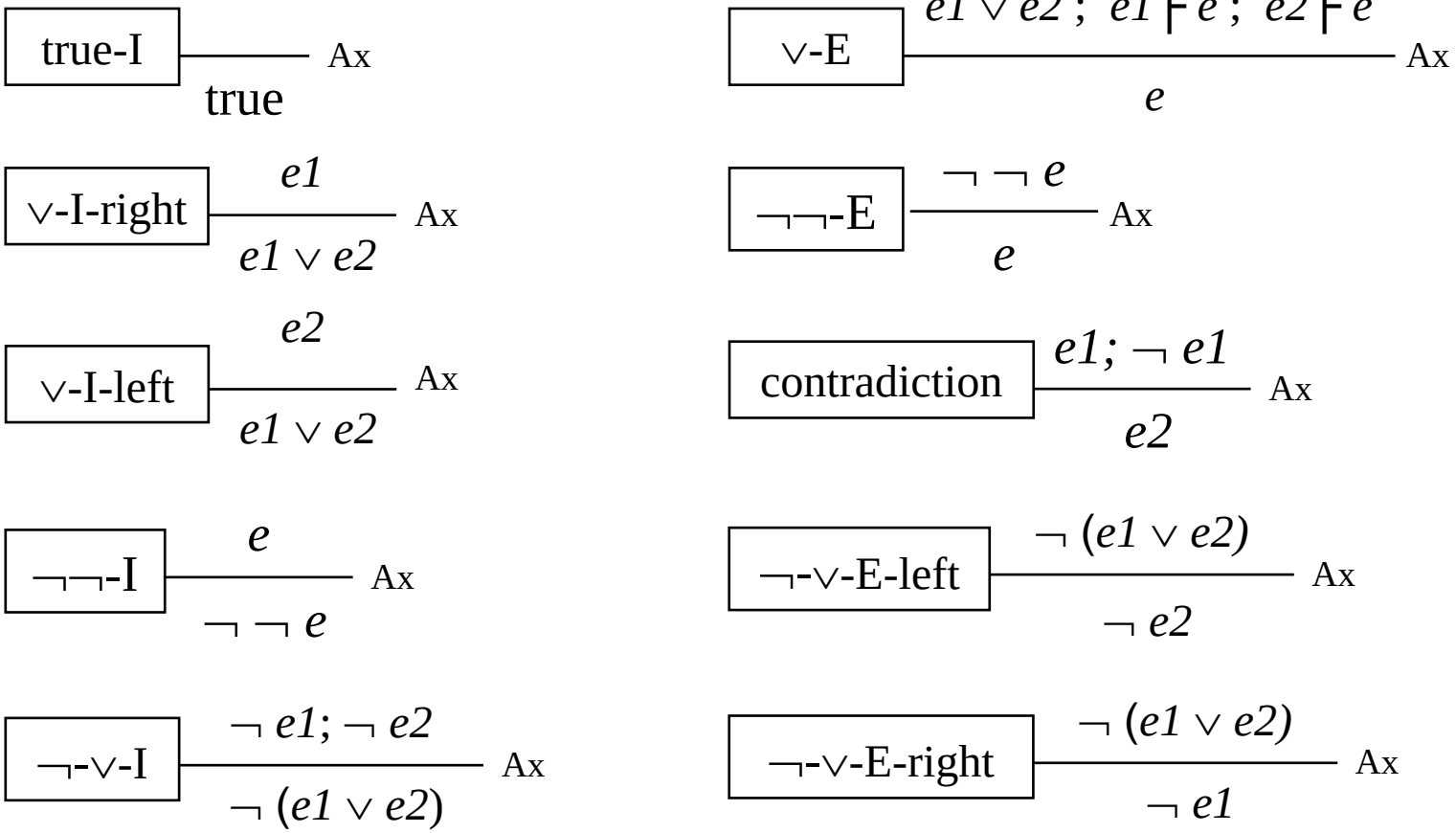
  application of partial functions outside their domains
- The model theory adds "⊥"

$\vee$	T	F	⊥
T	T	T	T
F	T	F	⊥
⊥	T	⊥	⊥

$\neg$	
T	F
F	T
⊥	⊥

- The proof theory builds on true, $\vee$, $\neg$

Basic LPF


true-I
Ax
true
∨-E
e1 ∨ e2 ; e1 ⊢ e ; e2 ⊢ e
Ax
e
∨-I-right
e1
Ax
e1 ∨ e2
¬¬-E
¬ ¬ e
Ax
e
∨-I-left
e2
Ax
e1 ∨ e2
contradiction
e1; ¬ e1
Ax
e2
¬¬-I
e
Ax
¬ ¬ e
¬-∨-E-left
¬ (e1 ∨ e2)
Ax
¬ e2
¬-∨-I
¬ e1; ¬ e2
Ax
¬ (e1 ∨ e2)
¬-∨-E-right
¬ (e1 ∨ e2)
Ax
¬ e1

Basic LPF

Definitions

$$\text{false} \quad \underline{\Delta} \quad \neg\, \text{true}$$

$$e1 \wedge e2 \quad \underline{\Delta} \quad \neg\, (\neg\, e1 \vee \neg\, e2\,)$$

$$e1 \Rightarrow e2 \; \underline{\Delta} \quad \neg\, e1 \vee \; e2$$

$$e1 \Leftrightarrow e2 \; \underline{\Delta} \quad e1 \Rightarrow e2 \wedge e2 \Rightarrow e1$$

Missing …

The 'excluded middle' $\dfrac{}{e \Rightarrow e}$ $\qquad$ $\dfrac{}{e \vee \neg\, e}$

The 'deduction theorem' $\dfrac{e1 \vdash e2}{e1 \Rightarrow e2}$

Basic LPF

We define

$$\delta e \;\; \underline{\Delta} \;\; e \vee \neg\, e$$

and there are derived rules for introduction and elimination of δ

$$\delta\text{-I}\;\frac{e}{\delta e} \qquad \delta\text{-I-}\neg\;\frac{\neg\, e}{\delta e} \qquad \delta\text{-E}\;\frac{\delta e1;\;\; e1 \vdash e\;;\;\; \neg e1 \vdash e}{e}$$

The qualified version of the excluded middle:

$$\Rightarrow\text{-I}\;\frac{\delta e1;\, e1 \vdash e2}{e1 \Rightarrow e2}$$

Typed LPF with Equality

- Undefinedness “rises” to the logic level via Boolean ops like =, < etc.
- So the definition of these ops, and the handling of definedness via typing is important.
- So … what equality?

=	0	1	2	…	$\perp_N$
0	T	F	F		$\perp$
1	F	T	F		$\perp$
2	F	F	T		$\perp$
…					
$\perp_N$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$

Weak Equality allows $\perp$ up into the logic.

$=\exists=$	0	1	2	…	$\perp_N$
0	T	F	F		F
1	F	T	F		F
2	F	F	T		F
…					
$\perp_N$	F	F	F		F

Existential Equality lets predicates denote even where operands fail to denote.

Typed LPF with Equality

Definedness interacts with the quantifiers:

$$\delta\exists\text{-inherit}\ \frac{x{:}A \vdash_x \delta P(x)}{\delta(\ \exists x{:}A \cdot P(x)\ )}\ \text{Ax} \qquad \delta\forall\text{-inherit}\ \frac{x{:}A \vdash_x \delta P(x)}{\delta(\ \forall x{:}A \cdot P(x)\ )}$$

Equality is “weak” (i.e. strict) in LPF:

$$=\text{-self-I}\ \frac{a{:}A}{a=a}\ \text{Ax} \qquad \delta\text{-=-I}\ \frac{a{:}A;\ b{:}A}{\delta(\ a=b\ )}\ \text{Ax}$$

In reasoning about VDM models, this leads to an abundance of typing hypotheses in rules relating to equality: easy but tedious to discharge (suggests automated support).

What Equality?

Consider

```
a in set dom m and m(a) =3
```

With the first conjunct false

- In FOPC with =, this is $\perp$
- In FOPC with $=\exists=$, this is false
- In LPF with =, this is false

“Goldsmith’s Conjecture”

$\vdash_3$ means provable in LPF+=

$\vdash$ means provable in FOPC+ $=\exists=$

$\vdash_3$ exp iff $\vdash$ exp

$\vdash_3$ exp $\rightarrow$ $\vdash$ exp

$\vdash_3$ e1=e2 $\rightarrow$ $\vdash$ e1 $=\exists=$ e2

$\vdash_3$ e1=e2 or p $\rightarrow$ $\vdash$ e1 $=\exists=$ e2 or p

$\vdash_3 \neg$exp $\rightarrow$ $\vdash \neg$exp

“Goldsmith’s Conjecture”

$\vdash_3$- means provable in LPF+=

$\vdash$ means provable in FOPC+ $=\exists=$

$\vdash_3$- exp iff $\vdash$ exp

$\vdash$ exp $\rightarrow$ $\vdash_3$- exp

$\vdash$ e1 $=\exists=$ e2 $\rightarrow$ $\vdash_3$- e1=e2

$\vdash$ e1 $=\exists=$ e2 or p $\rightarrow$ $\vdash_3$- e1=e2 or p

$\vdash \neg (\bot_N =\exists= 1)$ X$\rightarrow$ $\vdash_3$- $\neg (\bot_N = 1)$

So exclude negative occurrences of $=\exists=$

Some open questions

- In the Goldsmith conjecture … can we characterise the negative occurrence exclusion precisely? Role of delta, strong equality etc.
- Where is LPF in the spectrum (lattice?) of logics?
- LPF has properties that are suited to proof but reduce support for test-based analysis … what is the trade-off?