Clickable Proofs

Vincent van Oostrom
Tim Selier

Universiteit Utrecht

TF lunch, Utrecht, March 5, 2013

Proofs
Proofterms
Proofgraphs
Conclusion

Proofs

Proofterms

Proofgraphs

Conclusion

Natural Deduction

$$\alpha \qquad \frac{\bot}{\alpha}\ \bot\mathrm{E} \qquad \frac{\begin{array}{c}[\neg\alpha]\\ \triangledown\\ \bot\end{array}}{\alpha}\ \mathrm{RAA} \qquad \frac{\begin{array}{c}[\alpha]\\ \triangledown\\ \bot\end{array}}{\neg\alpha}\ \neg\mathrm{I} \qquad \frac{\alpha \quad \neg\alpha}{\bot}\ \neg\mathrm{E}$$

$$\frac{\alpha \quad \beta}{\alpha\wedge\beta}\ \wedge\mathrm{I} \qquad \frac{\alpha\wedge\beta}{\alpha}\ \wedge\mathrm{EL} \qquad \frac{\alpha\wedge\beta}{\beta}\ \wedge\mathrm{ER}$$

$$\frac{\alpha}{\alpha\vee\beta}\ \vee\mathrm{IL} \qquad \frac{\beta}{\alpha\vee\beta}\ \vee\mathrm{IR} \qquad \frac{\alpha\vee\beta \quad \begin{array}{c}[\alpha]\\ \triangledown\\ \gamma\end{array} \quad \begin{array}{c}[\beta]\\ \triangledown\\ \gamma\end{array}}{\gamma}\ \vee\mathrm{E}$$

$$\frac{\begin{array}{c}[\alpha]\\ \triangledown\\ \beta\end{array}}{\alpha\to\beta}\ \to\mathrm{I} \qquad \frac{\alpha \quad \alpha\to\beta}{\beta}\ \to\mathrm{E}$$

$$\frac{\begin{array}{c}[\alpha]\\ \triangledown\\ \beta\end{array} \quad \begin{array}{c}[\beta]\\ \triangledown\\ \alpha\end{array}}{\alpha\leftrightarrow\beta}\ \leftrightarrow\mathrm{I} \qquad \frac{\alpha \quad \alpha\leftrightarrow\beta}{\beta}\ \leftrightarrow\mathrm{EL} \qquad \frac{\alpha\leftrightarrow\beta \quad \beta}{\alpha}\ \leftrightarrow\mathrm{ER}$$

set of named (open) assumptions $\vdash$ conclusion

Proofs
Proofterms
Proofgraphs
Conclusion

Excluded middle proof

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[C]^y}{C \vee \neg C}\,\vee\mathrm{IL} \qquad [\neg(C\vee\neg C)]^x}{\bot}\,\neg\mathrm{E}}{\neg C}\,\neg\mathrm{I}^y}{C\vee\neg C}\,\vee\mathrm{IR} \qquad [\neg(C\vee\neg C)]^x}{\bot}\,\neg\mathrm{E}}{C\vee\neg C}\,\mathrm{RAA}^x$$

proof for $\varnothing \vdash C \vee \neg C$, for all formulas substituted for C.

Proofs as terms

(Standard) Ideas

- formalisation of informal devices (triangles,withdrawing)
- propositional formulas as base types
- proof rules as simply typed symbols over base types
- proofs as terms over the symbols

Proofs
Proofterms
Proofgraphs
Conclusion

Proofs as terms

(Standard) Ideas

- formalisation of informal devices (triangles,withdrawing)
- propositional formulas as base types
- proof rules as simply typed symbols over base types
- proofs as terms over the symbols

Change in perspective:
formulas and how proved ⇒ proofs and what they prove

Proofs
Proofterms
Proofgraphs
Conclusion

Proofs as terms

(Standard) Ideas

- formalisation of informal devices (triangles,withdrawing)
- propositional formulas as base types
- proof rules as simply typed symbols over base types
- proofs as terms over the symbols

Change in perspective:
formulas and how proved $\Rightarrow$ proofs and what they prove

Notations to suggest correspondence rules and symbols:

- product types $(A \times B)$ as juxtaposition $(A \quad B)$;
- function types $(A \rightarrow B)$ as fractions $\frac{A}{B}$;

Proofs
Proofterms
Proofgraphs
Conclusion

Natural deduction proofsignature

$$x : \alpha \qquad \bot\mathsf{E} : \frac{\bot}{\alpha} \qquad \mathsf{RAA} : \frac{\left(\frac{\neg\alpha}{\bot}\right)}{\alpha} \qquad \neg\mathsf{I} : \frac{\left(\frac{\alpha}{\bot}\right)}{\neg\alpha} \qquad \neg\mathsf{E} : \frac{\alpha \quad \neg\alpha}{\bot}$$

$$\wedge\mathsf{I} : \frac{\alpha \quad \beta}{\alpha \wedge \beta} \qquad \wedge\mathsf{EL} : \frac{\alpha \wedge \beta}{\alpha} \qquad \wedge\mathsf{ER} : \frac{\alpha \wedge \beta}{\beta}$$

$$\vee\mathsf{IL} : \frac{\alpha}{\alpha \vee \beta} \qquad \vee\mathsf{IR} : \frac{\beta}{\alpha \vee \beta} \qquad \vee\mathsf{E} : \frac{\alpha \vee \beta \quad \left(\frac{\alpha}{\gamma}\right) \quad \left(\frac{\beta}{\gamma}\right)}{\gamma}$$

$$\rightarrow\mathsf{I} : \frac{\left(\frac{\alpha}{\beta}\right)}{\alpha \rightarrow \beta} \qquad \rightarrow\mathsf{E} : \frac{\alpha \quad \alpha \rightarrow \beta}{\beta}$$

$$\leftrightarrow\mathsf{I} : \frac{\left(\frac{\alpha}{\beta}\right) \quad \left(\frac{\beta}{\alpha}\right)}{\alpha \leftrightarrow \beta} \qquad \leftrightarrow\mathsf{EL} : \frac{\alpha \quad \alpha \leftrightarrow \beta}{\beta} \qquad \leftrightarrow\mathsf{ER} : \frac{\alpha \leftrightarrow \beta \quad \beta}{\alpha}$$

set of typed (free) variables $\vdash$ type of proofterm

Excluded middle proofterm

$$\mathsf{RAA}(x.\neg\mathsf{E}(\vee\mathsf{IR}(\neg\mathsf{I}(y.\neg\mathsf{E}(\vee\mathsf{IL}(y),x))),x))$$

proofterm for $\varnothing \vdash C \vee \neg C$, for all formulas substituted for C

Excluded middle proofterm

$$\mathsf{RAA}(x.\neg\mathsf{E}(\vee\mathsf{IR}(\neg\mathsf{I}(y.\neg\mathsf{E}(\vee\mathsf{IL}(y),x))),x))$$

proofterm for $\varnothing \vdash C \vee \neg C$, for all formulas substituted for C

Lemma

There is a bijection between proofs and proofterms.

Proofs
Proofterms
Proofgraphs
Conclusion

Proofs as graphs

Ideas

- liberation from the inductive bottom–up straitjacket
- proof rules as nodes with ports labelled by formulas (input: premiss, output: conclusion, bound: assumption)
- proofs as graphs over the nodes
- partial correctness via conditions on proofgraph

Proofs
Proofterms
Proofgraphs
Conclusion

Proofs as graphs

Ideas

- liberation from the inductive bottom–up straitjacket
- proof rules as nodes with ports labelled by formulas (input: premiss, output: conclusion, bound: assumption)
- proofs as graphs over the nodes
- partial correctness via conditions on proofgraph

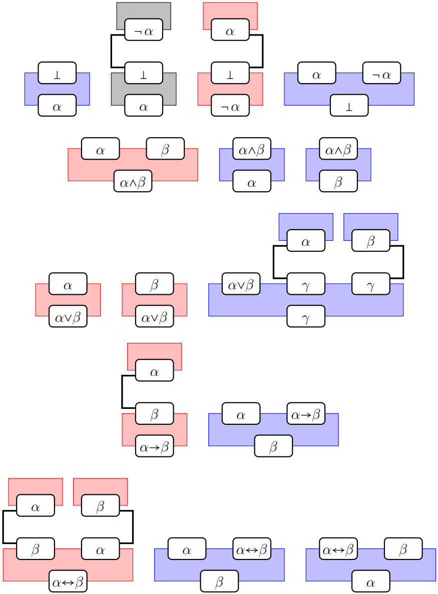
Proof construction by iteration

- introduce a fresh copy of a proofnode
- click two proofpieces together on their ports (formulas should unify; lego)

and undoing these actions

Proofs
Proofterms
Proofgraphs
Conclusion

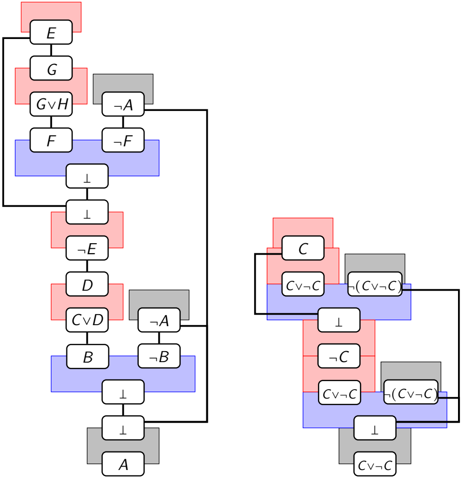
Natural deduction proofnodes



Universiteit Utrecht

set of labelled (free) ports ⊢ label of conclusion port

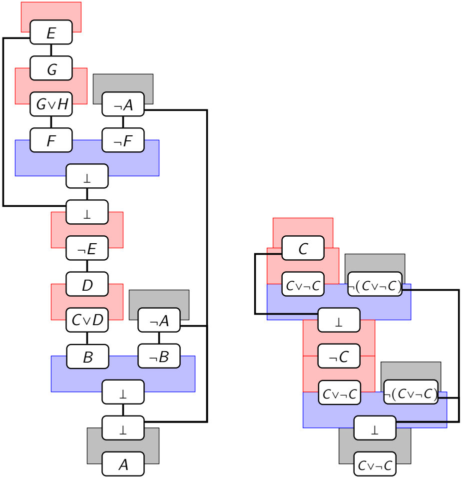
Excluded middle proofgraph



proofgraph for $\varnothing \vdash C \vee \neg C$, for all formulas substituted for C

Proofs
Proofterms
Proofgraphs
Conclusion

Excluded middle proofgraph



proofgraph for $\varnothing \vdash C \vee \neg C$, for all formulas substituted for C

Lemma

There is a bijection between proofs and correct *proofgraphs.*

Correctness

Proofs
Proofterms
Proofgraphs
Conclusion

Idea:

Correctness

The proof-like graph should be completable by further constructions, but without destruction, into a proofgraph (graph corresponding to a proofterm)

Correctness 1: unification

Definition

The *unification problem* of a proof-like graph is the set of equations arising from identifying the formulae of the ports connected by click-edges.

Example

Unification problem for excluded middle proof

$$\begin{array}{rcl@{\qquad}rcl@{\qquad}rcl} \bot & = & \bot & B & = & C \vee D & \neg B & = & \neg A \\ D & = & \neg E & \bot & = & \bot & F & = & G \vee H \\ \neg F & = & \neg A & G & = & E & & & \end{array}$$

Most general solution

$$A = B = F = C \vee \neg C \qquad E = G = C \qquad D = H = \neg C$$

Proofs
Proofterms
Proofgraphs
Conclusion

Correctness 1: unification

Definition

The *unification problem* of a proof-like graph is the set of equations arising from identifying the formulae of the ports connected by click-edges.

Example

Unification problem for excluded middle proof

$$\begin{array}{rcl@{\qquad}rcl@{\qquad}rcl} \bot & = & \bot & B & = & C \vee D & \neg B & = & \neg A \\ D & = & \neg E & \bot & = & \bot & F & = & G \vee H \\ \neg F & = & \neg A & G & = & E & & & \end{array}$$

Most general solution

$$A = B = F = C \vee \neg C \qquad E = G = C \qquad D = H = \neg C$$

Correctness

For a proof-like graph to be a proofgraph it is necessary that its unification problem be solvable.

Proofs
Proofterms
Proofgraphs
Conclusion

Correctness 2: click-forest

Correctness

For a proof-like graph to be a proofgraph it is necessary that its click-edges constitute a forest, all click-edges connect input to output ports, and no port is connected to two click-edges.

Correctness 2: click-forest

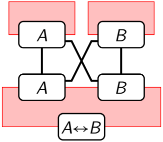
Correctness

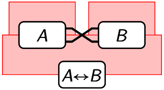
For a proof-like graph to be a proofgraph it is necessary that its click-edges constitute a forest, all click-edges connect input to output ports, and no port is connected to two click-edges.

enforced automatically by interface of app
(e.g. cannot drag one port of a proofpiece onto another)

Correctness 3: bind-forest

Binding problems (cyclic and dag)

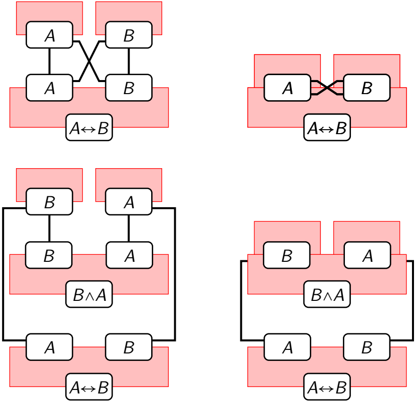




Proofs
Proofterms
Proofgraphs
Conclusion

Correctness 3: bind-forest

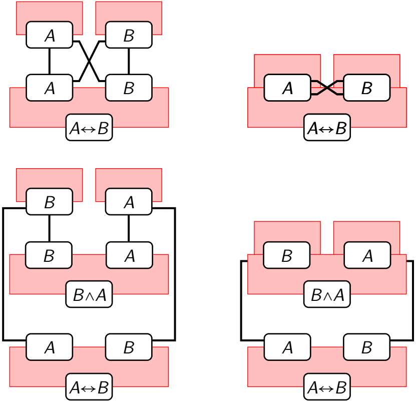
Binding problems (cyclic and dag)



Proofs
Proofterms
Proofgraphs
Conclusion

Correctness 3: bind-forest

Binding problems (cyclic and dag)



Correctness

For a proof-like graph to be a proofgraph it is necessary that click-edges can be adjoined to yield a forest such that all bind-edges are click-paths.

Graph problem

Proofs
Proofterms
Proofgraphs
Conclusion

Problem

Given a set of vertices and two sets E,P of ordered pairs of vertices, is there a (rooted, directed) forest on the vertices such that for each pair of vertices in E (P), there is an edge (a path) from the first to the second in the forest?

Graph problem

Problem

Given a set of vertices and two sets E,P of ordered pairs of vertices, is there a (rooted, directed) forest on the vertices such that for each pair of vertices in E (P), there is an edge (a path) from the first to the second in the forest?

cycle-checking easy; dag-checking seems hard

Proofs
Proofterms
Proofgraphs
Conclusion

Conclusions and questions

- Second-order signature adequate for natural deduction

Conclusions and questions

- Second-order signature adequate for natural deduction
- Complexity of graph problem?