Reproducibility, trust, and proof checking

From Universality of Facts to Universality of Proofs

Dale Miller

Inria Saclay & LIX, École Polytechnique
Palaiseau, France

18 October 2016

Reference: "Communicating and trusting proofs: The case for foundational proof certificates." Proc. of the 14th Congress of Logic, Methodology and Philosophy of Science, 2011.

	Universality of Facts	**Universality of Proofs**
Documents	Files, various formats	
Standards	SGML, HTML, etc	
Naming	URI, DOI	
Transport	HTTP, FTP, torrents	
Trust	certificate authorities, encryption, etc	

Access	the web, browsers	

Curation	Wikipedia, etc	

	Universality of Facts	**Universality of Proofs**
Documents	Files, various formats	Proofs, various formats
Standards	SGML, HTML, etc	
Naming	URI, DOI	
Transport	HTTP, FTP, torrents	
Trust	certificate authorities, encryption, etc	

Access	the web, browsers	

Curation	Wikipedia, etc	

	Universality of Facts	**Universality of Proofs**
Documents	Files, various formats	Proofs, various formats
Standards	SGML, HTML, etc	FPC, Dedukti, CPF, RUP, etc
Naming	URI, DOI	
Transport	HTTP, FTP, torrents	
Trust	certificate authorities, encryption, etc	

Access	the web, browsers	

Curation	Wikipedia, etc	

	Universality of Facts	**Universality of Proofs**
Documents	Files, various formats	Proofs, various formats
Standards	SGML, HTML, etc	FPC, Dedukti, CPF, RUP, etc
Naming	URI, DOI	e.g., hash of document
Transport	HTTP, FTP, torrents	
Trust	certificate authorities, encryption, etc	

Access	the web, browsers	

Curation	Wikipedia, etc	

	Universality of Facts	**Universality of Proofs**
Documents	Files, various formats	Proofs, various formats
Standards	SGML, HTML, etc	FPC, Dedukti, CPF, RUP, etc
Naming	URI, DOI	e.g., hash of document
Transport	HTTP, FTP, torrents	Same
Trust	certificate authorities, encryption, etc	

Access	the web, browsers	

Curation	Wikipedia, etc	

	Universality of Facts	**Universality of Proofs**
Documents	Files, various formats	Proofs, various formats
Standards	SGML, HTML, etc	FPC, Dedukti, CPF, RUP, etc
Naming	URI, DOI	e.g., hash of document
Transport	HTTP, FTP, torrents	Same
Trust	certificate authorities, encryption, etc	Reputation: signed by Coq 8.1, etc
		Reproducibility: recheck using trusted kernels

Access	the web, browsers	

Curation	Wikipedia, etc	

	Universality of Facts	**Universality of Proofs**
Documents	Files, various formats	Proofs, various formats
Standards	SGML, HTML, etc	FPC, Dedukti, CPF, RUP, etc
Naming	URI, DOI	e.g., hash of document
Transport	HTTP, FTP, torrents	Same
Trust	certificate authorities, encryption, etc	Reputation: signed by Coq 8.1, etc
		Reproducibility: recheck using trusted kernels

Access	the web, browsers	*proof browsers, readers*

Curation	Wikipedia, etc	

	Universality of Facts	**Universality of Proofs**
Documents	Files, various formats	Proofs, various formats
Standards	SGML, HTML, etc	FPC, Dedukti, CPF, RUP, etc
Naming	URI, DOI	e.g., hash of document
Transport	HTTP, FTP, torrents	Same
Trust	certificate authorities, encryption, etc	Reputation: signed by Coq 8.1, etc
		Reproducibility: recheck using trusted kernels
Access	the web, browsers	*proof browsers, readers*
Curation	Wikipedia, etc	*proof libraries, textbooks*

	Universality of Facts	**Universality of Proofs**
Documents	Files, various formats	Proofs, various formats
Standards	SGML, HTML, etc	FPC, Dedukti, CPF, RUP, etc
Naming	URI, DOI	e.g., hash of document
Transport	HTTP, FTP, torrents	Same
Trust	certificate authorities, encryption, etc	Reputation: signed by Coq 8.1, etc
		Reproducibility: recheck using trusted kernels

Access	the web, browsers	*proof browsers, readers*

Curation	Wikipedia, etc	*proof libraries, textbooks*

No centralized authority.

Sequent calculus and FPCs

Sequent calculi are not "just some choice of proof," as opposed to natural deduction, resolution refutations, etc.

Rather, we use them as a "machine language" of proof.

We position them at the back-end of "proof language compilers".

Sequent calculus and FPCs

Sequent calculi are not "just some choice of proof," as opposed to natural deduction, resolution refutations, etc.

Rather, we use them as a "machine language" of proof.

We position them at the back-end of "proof language compilers".

Focused sequent calculi organizes the tiny sequent rules by placing don't care and don't know non-determinism into different phases.

They also support sharing and parallel proof structures.

Sequent calculus and FPCs

Sequent calculi are not "just some choice of proof," as opposed to natural deduction, resolution refutations, etc.

Rather, we use them as a "machine language" of proof.

We position them at the back-end of "proof language compilers".

Focused sequent calculi organizes the tiny sequent rules by placing don't care and don't know non-determinism into different phases.

They also support sharing and parallel proof structures.

Foundational Proof Certificates (FPC)

Define client proof systems as synthetic inference rules from sequent calculus rules using the discipline of focused proof calculi.

A range of (textbook) proof systems have been defined in this way.