Evidence Algorithm

http://nevidal.org.ua

Mathematical texts in SAD

Anatoly Anisimov, Alexander Lyaletski,
Andrei Paskevich, and Konstantin Verchinine

Kiev National University — Université Paris 12

Kiev 29.05.2008

Plan of the talk

- Introduction
- Formal Theory Language (ForTheL)
- Calculus of Text Correctness
- System for Automated Deduction (SAD)
- Conclusion

Introduction

Evidence Algorithm

V.M. Glushkov – 1966 – Institute of Cybernetics – Kiev, Ukraine

Task: assistance to a working mathematician

Form: mathematical text processing, proof verification

Research:

- formal languages for mathematical text's presentation
- deductive routines which determine what is «evident»
- information environment, a library of mathematical knowledge
- interactive proof search

Principles:

- closeness to a natural language
- closeness to a natural reasoning

Developed:

- languages of formal theories
- goal-driven sequent calculi
- ...

Result: System for Automated Deduction (SAD) — 1978, 2003

Formalisation style

- Type theory (higher order logic) vs. Set theory (first order logic)
- Imperative proofs (series of tactics) vs. Declarative proofs («textbook» style)
- Large proof steps (strong prover) vs. Elementary proof steps (proof checker)

Formalisation style

- Type theory (higher order logic) vs. Set theory (first order logic)
- Imperative proofs (series of tactics) vs. Declarative proofs («textbook» style)
- Large proof steps (strong prover) vs. Elementary proof steps (proof checker)

System components

- Formal language for mathematical text presentation — ForTheL

must be close to the natural language of mathematical publications

Formalisation style

- Type theory (higher order logic) vs. Set theory (first order logic)
- Imperative proofs (series of tactics) vs. Declarative proofs («textbook» style)
- Large proof steps (strong prover) vs. Elementary proof steps (proof checker)

System components

- Formal language for mathematical text presentation — ForTheL

must be close to the natural language of mathematical publications

- Combinatorial inference search procedure — Otter, SPASS, E, *Moses*

completes proof steps in the text; is independent from the rest of the system, but can benefit from «naturally mathematical» specifics of submitted tasks: weak typing (sorts), definition handling, symbol orderings

Formalisation style

- Type theory (higher order logic) vs. Set theory (first order logic)
- Imperative proofs (series of tactics) vs. Declarative proofs («textbook» style)
- Large proof steps (strong prover) vs. Elementary proof steps (proof checker)

System components

- Formal language for mathematical text presentation — ForTheL

must be close to the natural language of mathematical publications

- Combinatorial inference search procedure — Otter, SPASS, E, *Moses*

completes proof steps in the text; is independent from the rest of the system, but can benefit from «naturally mathematical» specifics of submitted tasks: weak typing (sorts), definition handling, symbol orderings

- Reinforcing deductive techniques in human style — «reasoner»

split, filter, simplify, unfold definitions, apply lemmas, try different ways: faciliate the prover's duty as much as possible

Formal Theory Language

Formal Mathematical Text (Tarski-Knaster Theorem)

```
Definition DefCLat. A complete lattice is a set S such that
every subset of S has an infimum in S and a supremum in S.

Definition DefIso.  f is monotone iff for all x,y << Dom f
  x <= y  =>  f(x) <= f(y).

Theorem Tarski.
  Let U be a complete lattice and f be an monotone function on U.
  The set of fixed points of f is a complete lattice.
Proof.
  Let S be the set of fixed points of f and T be a subset of S.

  Let us show that T has a supremum in S.
    Take P = { x << U | f(x) <= x and x is an upper bound of T in U }.
    Take an infimum p of P in U.
    f(p) is a lower bound of P in U and an upper bound of T in U.
    Hence p is a fixed point of f and a supremum of T in S.
  end.

  Let us show that T has an infimum in S.
    Take Q = { x << U | f(x) >= x and x is a lower bound of T in U }.
    Take a supremum q of Q in U.
    f(q) is an upper bound of Q in U and a lower bound of T in U.
    Hence q is a fixed point of f and an infimum of T in S.
  end.
qed.
```

Tarski-Knaster Theorem (Mizar proof)

```
theorem
    FixPoints f is complete
proof
   set F = FixPoints f;
   set cF = the carrier of F;
   set cL = the carrier of L;
A1: cF = {x where x is Element of L:
            x is_a_fixpoint_of f} by Th39;
  let X be set;
  set Y = X /\ cF;
A2: Y c= X & Y c= cF by XBOOLE_1:17;
  set s = "\/"(Y, L);
     Y is_less_than f.s proof
    let q be Element of cL; assume
   A3: q in Y;
       then q [= s by LATTICE3:38;
   then A4: f.q [= f.s by QUANTAL1:def 12;
       reconsider q' = q as Element of L;
         q' is_a_fixpoint_of f by A2,A3,Th41;
    hence q [= f.s by A4,Def1;
   end;
then A5: s [= f.s by LATTICE3:def 21;
   then consider O such that
A6: Card O <=` Card cL & (f, O)+.s
                    is_a_fixpoint_of f by Th33;
  reconsider p' = (f, O)+.s as Element of L;
  reconsider p = p' as Element of cF by A6,Th41;
  reconsider p'' = p as Element of F;
  take p;
  thus X is_less_than p proof
   let q be Element of cF; assume
  A7: q in X;
      reconsider q' = q as Element of F;
        q in cF & cF c= cL by Th40;
      then reconsider qL' = q as Element of L;
        q in Y by A7,XBOOLE_0:def 3;
    then A8: qL' [= s by LATTICE3:38;
        s [= p' by A5,Th25;
      then qL' [= p' by A8,LATTICES:25;
      then q' [= p'' by Th42;
     hence q [= p;
    end;
    let r be Element of cF such that
  A9: X is_less_than r;
       r in the carrier of F;
     then consider r' being Element of L such that
  A10: r' = r & r' is_a_fixpoint_of f by A1;
     reconsider r'' = r as Element of F;
       Y is_less_than r' proof
      let q be Element of cL; assume
     A11: q in Y;
        then reconsider q'' = q as Element of F by A2;
        reconsider q' = q as Element of L;
        q'' [= r'' by A2,A9,A11,LATTICE3:def 17;
        then q' [= r' by A10,Th42;
      hence q [= r';
     end;
   then s [= r' by LATTICE3:def 21;
     then p' [= r' by A5,A10,Th37;
     then p'' [= r'' by A10,Th42;
    hence p [= r;
  end;
```

Tarski-Knaster Theorem (simplified, Isar proof)

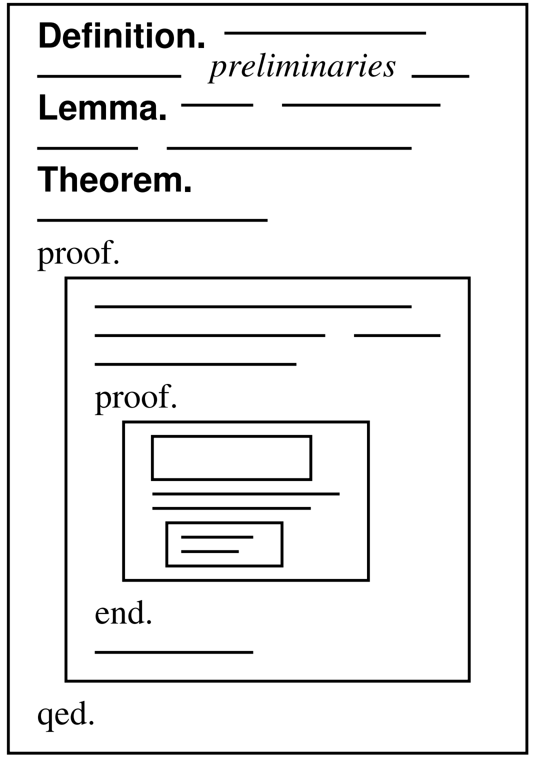
```
theorem KnasterTarski: "mono f ==> EX a::'a set. f a = a"
proof
  let ?H = "{u. f u <= u}"
  let ?a = "Inter ?H"
  assume mono: "mono f"
  show "f ?a = ?a"
  proof -
    {
      fix x
      assume H: "x : ?H"
      hence "?a <= x" by (rule Inter_lower)
      with mono have "f ?a <= f x" ..
      also from H have "... <= x" ..
      finally have "f ?a <= x" .
    }
    hence ge: "f ?a <= ?a" by (rule Inter_greatest)
    {
      also presume "... <= f ?a"
      finally (order_antisym) show ?thesis .
    }
    from mono ge have "f (f ?a) <= f ?a" ..
    hence "f ?a : ?H" ..
    thus "?a <= f ?a" by (rule Inter_lower)
  qed
qed
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction. Obvious.

Lemma Newman.
  Any locally confluent terminating rewriting system is confluent.
Proof.
  Let R be locally confluent and terminating.
  Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d. Indeed take x such that b,d -R*> x.
      c -R*> d. Indeed take y such that c,d -R*> y.
  end.
qed.
```

Formal Mathematical Text

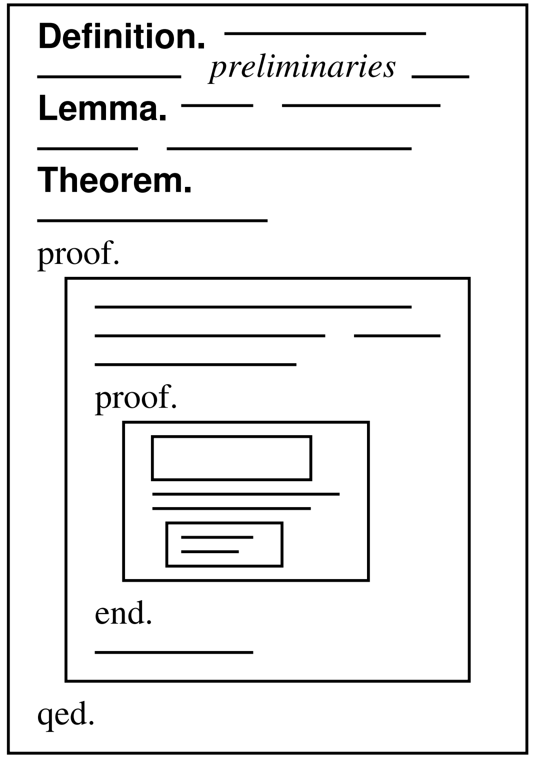
What is it: structured collection of propositions: assumptions, conjectures, definitions, proof cases...



Formal Mathematical Text

What is it: structured collection of propositions: assumptions, conjectures, definitions, proof cases...

Semantics: translation into first-order language



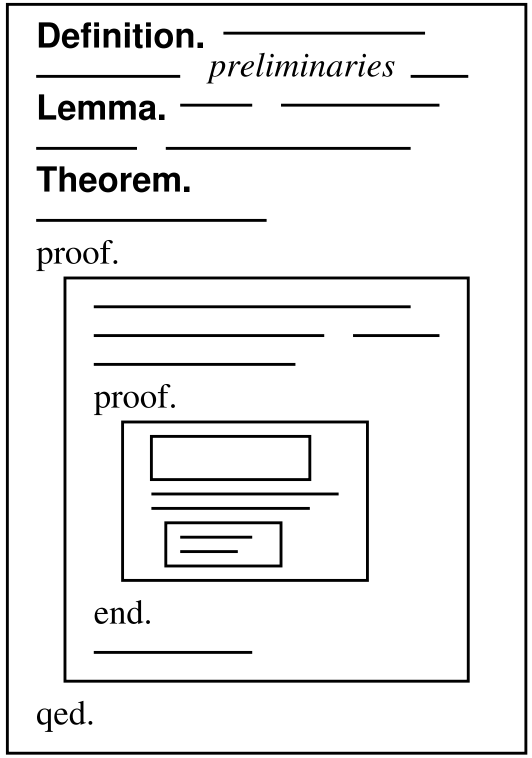
Formal Mathematical Text

What is it: structured collection of propositions: assumptions, conjectures, definitions, proof cases...

Semantics: translation into first-order language

Logical correctness:

– every assertion follows from its predecessors



Formal Mathematical Text

What is it: structured collection of propositions: assumptions, conjectures, definitions, proof cases...

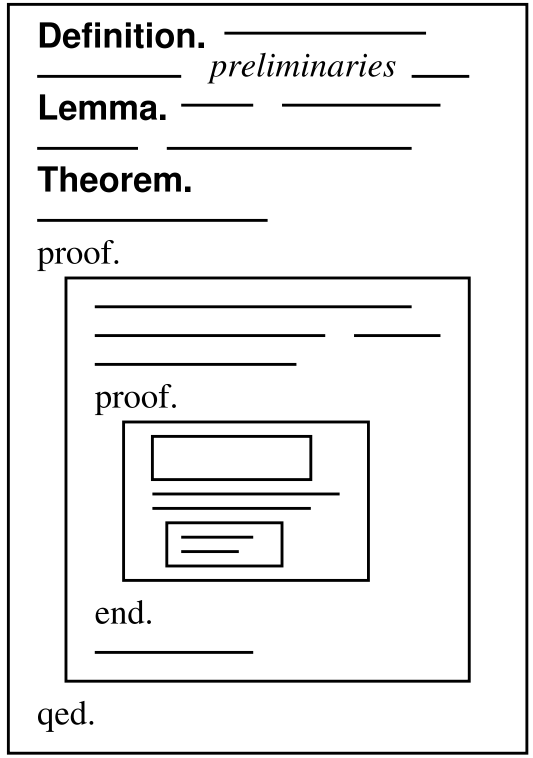
Semantics: translation into first-order language

Logical correctness:

– every assertion follows from its predecessors

Ontological correctness:

– every signature symbol is given a *domain*



Formal Mathematical Text

What is it: structured collection of propositions: assumptions, conjectures, definitions, proof cases...

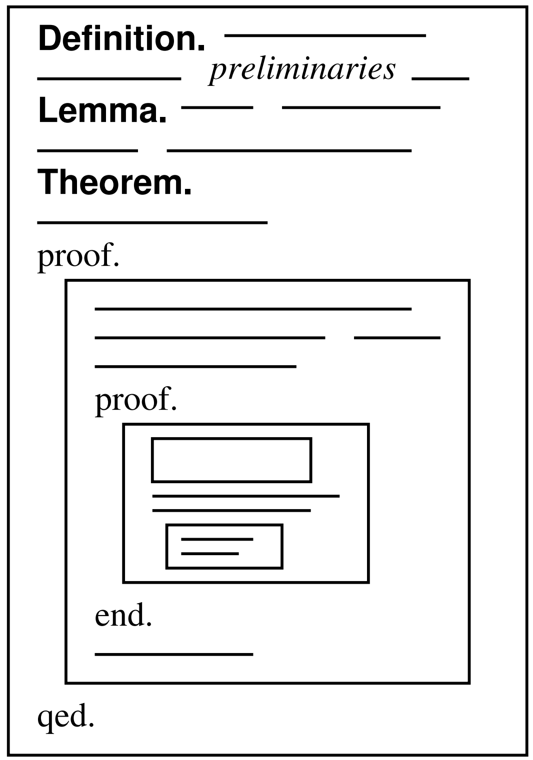
Semantics: translation into first-order language

Logical correctness:

– every assertion follows from its predecessors

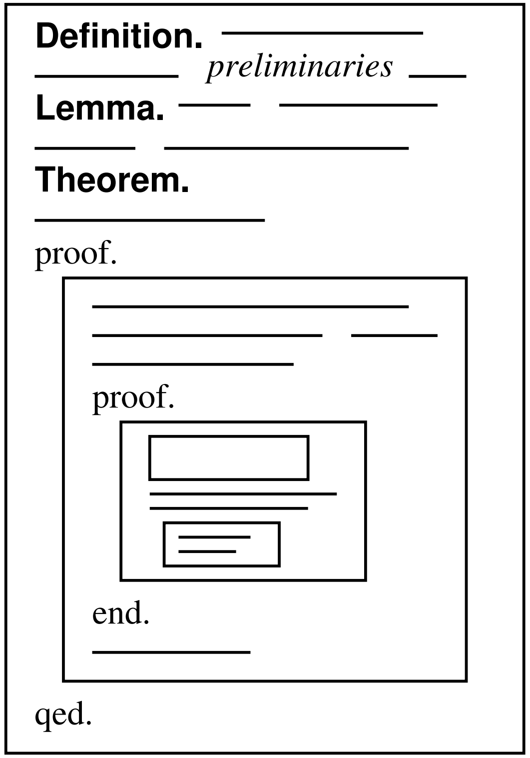
Ontological correctness:

– every signature symbol is given a *domain*
– every occurrence of a symbol is well-defined



Formal Mathematical Text

What is it: structured collection of propositions: assumptions, conjectures, definitions, proof cases...



Semantics: translation into first-order language

Logical correctness:

- every assertion follows from its predecessors

Ontological correctness:

- every signature symbol is given a *domain*
- every occurrence of a symbol is well-defined

Translation:

`every term x has a normal form in R`

$\longrightarrow \; \forall x\,(x\,\varepsilon\,\mathrm{Term} \supset \exists\, z(z\,\varepsilon\,\mathrm{NormalFormOfIn}(x, R)))$

`any locally confluent terminating rewriting system is confluent`

$\longrightarrow \; \forall R\,((R\,\varepsilon\,\mathrm{RewrSystem} \wedge \mathrm{isTerminating}(R) \wedge \mathrm{isLocallyConfluent}(R)) \supset \mathrm{isConfluent}(R))$

`some subgroup of every group is abelian`

$\longrightarrow \; \forall G\,(G\,\varepsilon\,\mathrm{Group} \supset \exists H\,(H\,\varepsilon\,\mathrm{SubgroupOf}(G) \supset \mathrm{isAbelian}(H)))$

Text Correctness

Formal Mathematical Text

What is it: structured collection of propositions: assumptions, conjectures, definitions, proof cases...

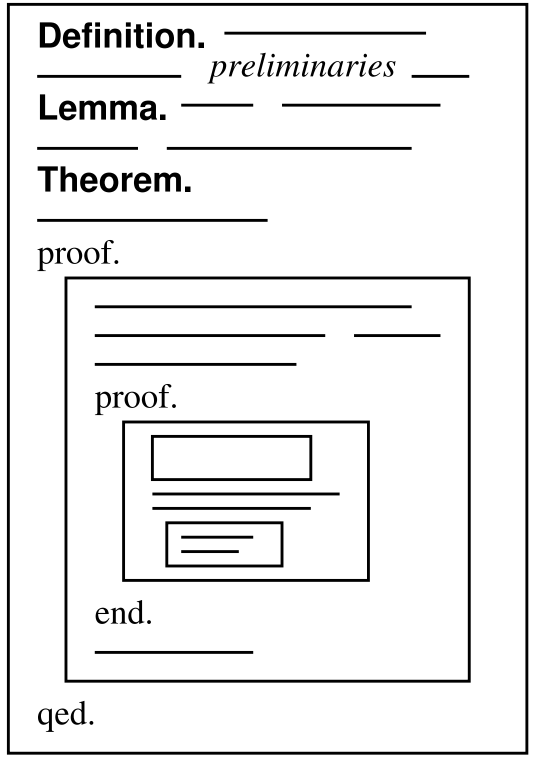
Semantics: translation into first-order language

Logical correctness:

- every assertion follows from its predecessors

Ontological correctness:

- every signature symbol is given a *domain*
- every occurrence of a symbol is well-defined



Calculus of Text Correctness

$$\frac{\Gamma \vdash G}{\Gamma \;\; \triangleright_G} \qquad\qquad \frac{(\Gamma \blacktriangleright F)^* \qquad \Gamma,\, (\texttt{posit}\ F)\ \triangleright_\top \Delta}{\Gamma \;\; \triangleright_\top \;\; (\texttt{posit}\ F),\, \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \vec{x} = \mathcal{DV}_\Gamma(F) \qquad \Gamma \vdash \forall \vec{x}\,(F \supset G') \supset G \qquad \Gamma,\, (\texttt{assume}\ F) \triangleright_{G'} \Delta}{\Gamma \;\; \triangleright_G \;\; (\texttt{assume}\ \Theta_G(F)),\, \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \mathcal{DV}_\Gamma(F) = \varnothing \qquad \Gamma \triangleright_F \Lambda \qquad \Gamma \vdash (F \wedge G') \supset G \qquad \Gamma,\, (\texttt{affirm}\ F\ [\Lambda]) \triangleright_{G'} \Delta}{\Gamma \;\; \triangleright_G \;\; (\texttt{affirm}\ \Theta_G(F)\ [\Lambda]),\, \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \vec{x} = \mathcal{DV}_\Gamma(F) \qquad \Gamma \triangleright_{\exists \vec{x}\, F} \Lambda \qquad \Gamma \vdash \exists \vec{x}\,(F \wedge G') \supset G \qquad \Gamma, (\texttt{select}\ F\ [\Lambda]) \triangleright_{G'} \Delta}{\Gamma \;\; \triangleright_G \;\; (\texttt{select}\ \Theta_G(F)\ [\Lambda]),\, \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \mathcal{DV}_\Gamma(F) = \varnothing \qquad \Gamma, (\texttt{assume}\ F) \triangleright_G \Lambda \qquad \Gamma,\, (\texttt{case}\ (F \supset G)\ [\Lambda]) \triangleright_{G \vee F} \Delta}{\Gamma \;\; \triangleright_G \;\; (\texttt{case}\ (F \supset \mathfrak{T})\ [\Lambda]),\, \Delta}$$

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\; \triangleright_G \;\; \Delta} \qquad\qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\, (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\, \Delta}{\Gamma \;\; \triangleright_G \;\; \Lambda, \Delta}$$

$$\frac{\Gamma \triangleright_\top \Lambda \qquad \Gamma, (\texttt{theorem}\ |\Lambda|\ [\Lambda]) \triangleright_\top \Delta}{\Gamma \;\; \triangleright_\top \;\; (\texttt{theorem}\ |\Lambda|\ [\Lambda]),\, \Delta} \qquad\qquad \frac{\Gamma \triangleright_\top \Lambda \qquad \Gamma, (\texttt{axiom}\ |\Lambda|\ [\Lambda]) \triangleright_\top \Delta}{\Gamma \;\; \triangleright_\top \;\; (\texttt{axiom}\ |\Lambda|\ [\Lambda]),\, \Delta}$$

$$\frac{\Gamma \triangleright_\top \Lambda \qquad \Gamma, (\texttt{defn}\ |\Lambda|\ [\Lambda]) \triangleright_\top \Delta}{\Gamma \;\; \triangleright_\top \;\; (\texttt{defn}\ |\Lambda|\ [\Lambda]),\, \Delta} \qquad\qquad \frac{\Gamma \triangleright_\top \Lambda \qquad \Gamma, (\texttt{sign}\ |\Lambda|\ [\Lambda]) \triangleright_\top \Delta}{\Gamma \;\; \triangleright_\top \;\; (\texttt{sign}\ |\Lambda|\ [\Lambda]),\, \Delta}$$

Calculus of Text Correctness

Section: (T F [Λ]) — (kind, formula image, body/proof)

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.
   Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.
   Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

— *affirmation*

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
```

$\forall R\,((R \,\varepsilon\, \mathrm{RewrSystem} \wedge \mathrm{isTerminating}(R) \wedge \mathrm{isLocallyConfluent}(R)) \supset \mathrm{isConfluent}(R))$ — *affirmation*

```
Proof.
   Let R be locally confluent and terminating.
   Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
```

$\forall R\,((R\,\varepsilon\,\text{RewrSystem} \wedge \text{isTerminating}(R) \wedge \text{isLocallyConfluent}(R)) \supset \text{isConfluent}(R))$ — *affirmation*

```
Proof.
```

proof

```
Let R be locally confluent and terminating.
Let us demonstrate by induction that for all a,b,c
 such that a -R*> b,c there exists d such that b,c -R*> d.
  Assume that a -R+> b,c.
  Take u such that a -R> u -R*> b.
  Take v such that a -R> v -R*> c.
  Take w such that u,v -R*> w.
  Take a normal form d of w in R.
  b -R*> d.  Indeed take x such that b,d -R*> x.
  c -R*> d.  Indeed take y such that c,d -R*> y.
end.
qed.
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
```

$\forall R\,((R\,\varepsilon\,\text{RewrSystem} \wedge \text{isTerminating}(R) \wedge \text{isLocallyConfluent}(R)) \supset \text{isConfluent}(R))$ — *affirmation*

```
Proof.
```

Let R be locally confluent and terminating. *proof*
Let us demonstrate by induction that for all a,b,c
such that a -R*> b,c there exists d such that b,c -R*> d.
Assume that a -R+> b,c.
Take u such that a -R> u -R*> b.
Take v such that a -R> v -R*> c.
Take w such that u,v -R*> w.
Take a normal form d of w in R.
$b \twoheadrightarrow_R d$. Indeed [take x such that b,d -R*> x.] — *affirmation*
c -R*> d. Indeed take y such that c,d -R*> y.
end.

```
qed.
```

Calculus of Text Correctness

Section: $(\mathrm{T}\ \ F\ \ [\Lambda])$ — (kind, formula image, body/proof)

Sequent: $\Gamma \triangleright_G \Delta$ — verify *text* Δ and prove *thesis* G in view of Γ

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.
⟶  Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y                Γ
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.               Γ
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.                         Γ
-->Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.
   Let us demonstrate by induction that for all a,b,c                      Δ
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
⟶     Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.      ⟶      G = isConfluent(R)
   Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

Calculus of Text Correctness

Section: $(\mathrm{T}\ \ F\ \ [\Lambda])$ — (kind, formula image, body/proof)

Sequent: $\Gamma\ \triangleright_G\ \Delta$ — verify *text* Δ and prove *thesis* G in view of Γ

Axiom: $\dfrac{\Gamma \vdash G}{\Gamma\ \triangleright_G}$ — when no proof is given, deduce the current thesis

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.
```

$\longrightarrow \quad G = \text{isConfluent}(R)$

```
qed.
```

Calculus of Text Correctness

Section: $(\mathrm{T}\ \ F\ \ [\Lambda])$ — (kind, formula image, body/proof)

Sequent: $\Gamma\ \triangleright_G\ \Delta$ — verify *text* Δ and prove *thesis* G in view of Γ

Axiom: $\dfrac{\Gamma \vdash G}{\Gamma\ \triangleright_G}$ — when no proof is given, deduce the current thesis

Rules for assumptions and affirmations:

$$\frac{\Gamma \blacktriangleright F \qquad \vec{x} = \mathcal{DV}_\Gamma(F) \qquad \Gamma \vdash \forall \vec{x}\,(F \supset G') \supset G \qquad \Gamma,\ (\texttt{assume}\ \ F) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{assume}\ \ \Theta_G(F)),\ \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \mathcal{DV}_\Gamma(F) = \varnothing \qquad \Gamma \triangleright_F \Lambda \qquad \Gamma \vdash (F \wedge G') \supset G \qquad \Gamma,\ (\texttt{affirm}\ \ F\ \ [\Lambda]) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{affirm}\ \ \Theta_G(F)\ \ [\Lambda]),\ \Delta}$$

Calculus of Text Correctness

Section: $(\mathrm{T}\ \ F\ \ [\Lambda])$ — (kind, formula image, body/proof)

Sequent: $\Gamma\ \triangleright_G\ \Delta$ — verify *text* Δ and prove *thesis* G in view of Γ

Axiom: $\dfrac{\Gamma \vdash G}{\Gamma\ \triangleright_G}$ — when no proof is given, deduce the current thesis

Rules for assumptions and affirmations:

$$\frac{\Gamma \blacktriangleright F \qquad \vec{x} = \mathcal{DV}_\Gamma(F) \qquad \Gamma \vdash \forall \vec{x}\,(F \supset G') \supset G \qquad \Gamma,\ (\texttt{assume}\ \ F) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{assume}\ \ \Theta_G(F)),\ \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \mathcal{DV}_\Gamma(F) = \varnothing \qquad \Gamma \triangleright_F \Lambda \qquad \Gamma \vdash (F \wedge G') \supset G \qquad \Gamma,\ (\texttt{affirm}\ \ F\ \ [\Lambda]) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{affirm}\ \ \Theta_G(F)\ \ [\Lambda]),\ \Delta}$$

– $\Gamma \blacktriangleright F$ — F is ontologically correct in view of Γ

Calculus of Text Correctness

Section: $(\mathrm{T}\ \ F\ \ [\Lambda])$ — (kind, formula image, body/proof)

Sequent: $\Gamma\ \triangleright_G\ \Delta$ — verify *text* Δ and prove *thesis* G in view of Γ

Axiom: $\dfrac{\Gamma \vdash G}{\Gamma\ \triangleright_G}$ — when no proof is given, deduce the current thesis

Rules for assumptions and affirmations:

$$\frac{\Gamma \blacktriangleright F \qquad \vec{x} = \mathcal{DV}_\Gamma(F) \qquad \Gamma \vdash \forall \vec{x}\,(F \supset G') \supset G \qquad \Gamma,\ (\texttt{assume}\ \ F) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{assume}\ \Theta_G(F)),\ \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \mathcal{DV}_\Gamma(F) = \varnothing \qquad \Gamma \triangleright_F \Lambda \qquad \Gamma \vdash (F \wedge G') \supset G \qquad \Gamma,\ (\texttt{affirm}\ \ F\ \ [\Lambda]) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{affirm}\ \Theta_G(F)\ \ [\Lambda]),\ \Delta}$$

- $\Gamma \blacktriangleright F$ — F is ontologically correct in view of Γ
- $\mathcal{DV}_\Gamma(F)$ — variables declared by the considered sentence

Formal Mathematical Text (Newman's Lemma)

Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef. A normal form of x in R is a term y
such that x -R*> y and y has no reducts in R.

Lemma TermNF. Let R be a terminating rewriting system. $\longleftarrow \quad \mathcal{DV} = \{R\}$
Every term x has a normal form in R.
Proof by induction. Obvious.

Lemma Newman.
Any locally confluent terminating rewriting system is confluent.
Proof.
Let R be locally confluent and terminating. $\longleftarrow \quad \mathcal{DV} = \{R\}$
Let us demonstrate by induction that for all a,b,c
such that a -R*> b,c there exists d such that b,c -R*> d.
Assume that a -R+> b,c. $\longleftarrow \quad \mathcal{DV} = \{a, b, c\}$
Take u such that a -R> u -R*> b. $\longleftarrow \quad \mathcal{DV} = \{u\}$
Take v such that a -R> v -R*> c. $\longleftarrow \quad \mathcal{DV} = \{v\}$
Take w such that u,v -R*> w. $\longleftarrow \quad \mathcal{DV} = \{w\}$
Take a normal form d of w in R. $\longleftarrow \quad \mathcal{DV} = \{d\}$
b -R*> d. Indeed take x such that b,d -R*> x. $\longleftarrow \quad \mathcal{DV} = \{x\}$
c -R*> d. Indeed take y such that c,d -R*> y. $\longleftarrow \quad \mathcal{DV} = \{y\}$
end.
qed.

Formal Mathematical Text (Newman's Lemma)

Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef. A normal form of x in R is a term y
such that x -R*> y and y has no reducts in R.

Lemma TermNF. Let R be a terminating rewriting system. $\longleftarrow$ $\mathcal{DV} = \{R\}$
Every term x has a normal form in R.
Proof by induction. Obvious.

Lemma Newman.
Any locally confluent terminating rewriting system is confluent.
Proof.
Let R be locally confluent and terminating. $\longleftarrow$ $\mathcal{DV} = \{R\}$
Let us demonstrate by induction that for all a,b,c
such that a -R*> b,c there exists d such that b,c -R*> d.
Assume that a -R+> b,c. $\longleftarrow$ $\mathcal{DV} = \{a, b, c\}$
Take u such that a -R> u -R*> b. $\longleftarrow$ $\mathcal{DV} = \{u\}$
Take v such that a -R> v -R*> c. $\longleftarrow$ $\mathcal{DV} = \{v\}$
Take w such that u,v -R*> w. $\longleftarrow$ $\mathcal{DV} = \{w\}$
Take a normal form d of w in R. $\longleftarrow$ $\mathcal{DV} = \{d\}$
b -R*> d. Indeed take x such that b,d -R*> x. $\longleftarrow$ $\mathcal{DV} = \{x\}$
c -R*> d. Indeed take y such that c,d -R*> y. $\longleftarrow$ $\mathcal{DV} = \{y\}$
end.
qed.

Calculus of Text Correctness

Section: $(\mathrm{T}\ \ F\ \ [\Lambda])$ — (kind, formula image, body/proof)

Sequent: $\Gamma\ \triangleright_G\ \Delta$ — verify *text* Δ and prove *thesis* G in view of Γ

Axiom: $\dfrac{\Gamma \vdash G}{\Gamma\ \triangleright_G}$ — when no proof is given, deduce the current thesis

Rules for assumptions and affirmations:

$$\frac{\Gamma \blacktriangleright F \qquad \vec{x} = \mathcal{DV}_\Gamma(F) \qquad \Gamma \vdash \forall \vec{x}\,(F \supset G') \supset G \qquad \Gamma,\ (\texttt{assume}\ \ F) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{assume}\ \Theta_G(F)),\ \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \mathcal{DV}_\Gamma(F) = \varnothing \qquad \Gamma \triangleright_F \Lambda \qquad \Gamma \vdash (F \wedge G') \supset G \qquad \Gamma,\ (\texttt{affirm}\ \ F\ \ [\Lambda]) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{affirm}\ \Theta_G(F)\ \ [\Lambda]),\ \Delta}$$

- $\Gamma \blacktriangleright F$ — F is ontologically correct in view of Γ
- $\mathcal{DV}_\Gamma(F)$ — variables declared by the considered sentence
- $\Gamma \triangleright_F \Lambda$ — verify the proof Λ and prove the statement F

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.
   Let us demonstrate by induction that for all a,b,c          affirmation
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.
   Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.                                         Λ
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

Calculus of Text Correctness

Section: $(\mathrm{T}\ \ F\ \ [\Lambda])$ — (kind, formula image, body/proof)

Sequent: $\Gamma\ \triangleright_G\ \Delta$ — verify *text* Δ and prove *thesis* G in view of Γ

Axiom: $\dfrac{\Gamma \vdash G}{\Gamma\ \triangleright_G}$ — when no proof is given, deduce the current thesis

Rules for assumptions and affirmations:

$$\frac{\Gamma \blacktriangleright F \qquad \vec{x} = \mathcal{DV}_\Gamma(F) \qquad \Gamma \vdash \forall \vec{x}\,(F \supset G') \supset G \qquad \Gamma,\ (\texttt{assume}\ \ F) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{assume}\ \ \Theta_G(F)),\ \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \mathcal{DV}_\Gamma(F) = \varnothing \qquad \Gamma \triangleright_F \Lambda \qquad \Gamma \vdash (F \wedge G') \supset G \qquad \Gamma,\ (\texttt{affirm}\ \ F\ \ [\Lambda]) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{affirm}\ \ \Theta_G(F)\ \ [\Lambda]),\ \Delta}$$

- $\Gamma \blacktriangleright F$ — F is ontologically correct in view of Γ
- $\mathcal{DV}_\Gamma(F)$ — variables declared by the considered sentence
- $\Gamma \triangleright_F \Lambda$ — verify the proof Λ and prove the statement F
- $\forall \vec{x}\,(F \supset G') \supset G,\quad (F \wedge G') \supset G$ — thesis reduction

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
```

```
qed.
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
```

Proof. $\longrightarrow$ $G = \forall R\,((R\,\varepsilon\,\mathrm{RewrSystem} \wedge \mathrm{isTerminating}(R) \wedge \mathrm{isLocallyConfluent}(R)) \supset \mathrm{isConfluent}(R))$

qed.

Formal Mathematical Text (Newman's Lemma)

Let a,b,c,d,u,v,w,x,y,z denote terms.

Let R,S,T denote rewriting systems.

Definition NFRDef. A normal form of x in R is a term y
such that x -R*> y and y has no reducts in R.

Lemma TermNF. Let R be a terminating rewriting system.
Every term x has a normal form in R.

Proof by induction. Obvious.

Lemma Newman.
Any locally confluent terminating rewriting system is confluent.

Proof. $\longrightarrow$ $G = \forall R\,((R \,\varepsilon\, \mathrm{RewrSystem} \wedge \mathrm{isTerminating}(R) \wedge \mathrm{isLocallyConfluent}(R)) \supset \mathrm{isConfluent}(R))$

Let R be locally confluent and terminating.

qed.

Formal Mathematical Text (Newman's Lemma)

Let a,b,c,d,u,v,w,x,y,z denote terms.

Let R,S,T denote rewriting systems.

Definition NFRDef. A normal form of x in R is a term y
such that x -R*> y and y has no reducts in R.

Lemma TermNF. Let R be a terminating rewriting system.
Every term x has a normal form in R.

Proof by induction. Obvious.

Lemma Newman.
Any locally confluent terminating rewriting system is confluent.

Proof. $\longrightarrow \quad G = \forall R\,((R \,\varepsilon\, \mathrm{RewrSystem} \wedge \mathrm{isTerminating}(R) \wedge \mathrm{isLocallyConfluent}(R)) \supset \mathrm{isConfluent}(R))$

Let R be locally confluent and terminating. $\longrightarrow \quad G' = \mathrm{isConfluent}(R)$

qed.

Calculus of Text Correctness

Section: $(\mathrm{T}\ \ F\ \ [\Lambda])$ — (kind, formula image, body/proof)

Sequent: $\Gamma \ \triangleright_G\ \Delta$ — verify *text* Δ and prove *thesis* G in view of Γ

Axiom: $\dfrac{\Gamma \vdash G}{\Gamma\ \triangleright_G}$ — when no proof is given, deduce the current thesis

Rules for assumptions and affirmations:

$$\frac{\Gamma \blacktriangleright F \qquad \vec{x} = \mathcal{DV}_\Gamma(F) \qquad \Gamma \vdash \forall \vec{x}\,(F \supset G') \supset G \qquad \Gamma,\ (\texttt{assume}\ \ F) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{assume}\ \ \Theta_G(F)),\ \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \mathcal{DV}_\Gamma(F) = \varnothing \qquad \Gamma \triangleright_F \Lambda \qquad \Gamma \vdash (F \wedge G') \supset G \qquad \Gamma,\ (\texttt{affirm}\ \ F\ \ [\Lambda]) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{affirm}\ \ \Theta_G(F)\ \ [\Lambda]),\ \Delta}$$

- $\Gamma \blacktriangleright F$ — F is ontologically correct in view of Γ
- $\mathcal{DV}_\Gamma(F)$ — variables declared by the considered sentence
- $\Gamma \triangleright_F \Lambda$ — verify the proof Λ and prove the statement F
- $\forall \vec{x}\,(F \supset G') \supset G,\quad (F \wedge G') \supset G$ — thesis reduction
- $\Gamma, \mathbb{A} \triangleright_{G'} \Delta$ — new thesis is G', verify the rest of the proof

Calculus of Text Correctness

Section: $(\mathrm{T}\ \ F\ \ [\Lambda])$ — (kind, formula image, body/proof)

Sequent: $\Gamma\ \triangleright_G\ \Delta$ — verify *text* Δ and prove *thesis* G in view of Γ

Axiom: $\dfrac{\Gamma \vdash G}{\Gamma\ \triangleright_G}$ — when no proof is given, deduce the current thesis

Rules for assumptions and affirmations:

$$\frac{\Gamma \blacktriangleright F \qquad \vec{x} = \mathcal{DV}_\Gamma(F) \qquad \Gamma \vdash \forall \vec{x}\,(F \supset G') \supset G \qquad \Gamma,\ (\texttt{assume}\ \ F) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{assume}\ \Theta_G(F)),\ \Delta}$$

$$\frac{\Gamma \blacktriangleright F \qquad \mathcal{DV}_\Gamma(F) = \varnothing \qquad \Gamma \triangleright_F \Lambda \qquad \Gamma \vdash (F \wedge G') \supset G \qquad \Gamma,\ (\texttt{affirm}\ \ F\ \ [\Lambda]) \triangleright_{G'} \Delta}{\Gamma\ \ \triangleright_G\ \ (\texttt{affirm}\ \Theta_G(F)\ \ [\Lambda]),\ \Delta}$$

- $\Gamma \blacktriangleright F$ — F is ontologically correct in view of Γ
- $\mathcal{DV}_\Gamma(F)$ — variables declared by the considered sentence
- $\Gamma \triangleright_F \Lambda$ — verify the proof Λ and prove the statement F
- $\forall \vec{x}\,(F \supset G') \supset G,\quad (F \wedge G') \supset G$ — thesis reduction
- $\Gamma, \mathbb{A} \triangleright_{G'} \Delta$ — new thesis is G', verify the rest of the proof
- $\Theta_G(F)$ — replace occurrences of G in F with `thesis`

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\; \triangleright_G \;\; \Delta} \qquad\qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\; \triangleright_G \;\; \Lambda, \Delta}$$

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\; \triangleright_G \;\; \Delta} \qquad\qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\; \triangleright_G \;\; \Lambda, \Delta}$$

- original thesis: $G = \forall \vec{x}\, (H \supset F)$
- induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\, (H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$
- induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\, (H' \supset ((t' \prec t) \supset F'))$

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\; \triangleright_G \;\; \Delta} \qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\; \triangleright_G \;\; \Lambda, \Delta}$$

– original thesis: $G = \forall \vec{x}\,(H \supset F)$

– induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\,(H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$

– induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\,(H' \supset ((t' \prec t) \supset F'))$

Example:

original thesis G :

```
For all natural numbers n,m,p
if p is prime and p | n * m then p | n or p | m.
```

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\triangleright_G\; \Delta} \qquad\qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\triangleright_G\; \Lambda, \Delta}$$

– original thesis: $G = \forall \vec{x}\,(H \supset F)$

– induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\,(H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$

– induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\,(H' \supset ((t' \prec t) \supset F'))$

Example:

original thesis G :

```
for all natural numbers n,m,p

if p is prime and p | n * m then p | n or p | m
```

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\; \triangleright_G \;\; \Delta} \qquad\qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\; \triangleright_G \;\; \Lambda, \Delta}$$

- original thesis: $G = \forall \vec{x}\, (H \supset F)$
- induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\, (H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$
- induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\, (H' \supset ((t' \prec t) \supset F'))$

Example:

original thesis G :

```
for all natural numbers n1,m1,p1

if p1 is prime and p1 | n1 * m1 then p1 | n1 or p1 | m1
```

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \rhd_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\; \rhd_G \;\; \Delta} \qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \rhd_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\; \rhd_G \;\; \Lambda, \Delta}$$

- original thesis: $G = \forall \vec{x}\,(H \supset F)$
- induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\,(H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$
- induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\,(H' \supset ((t' \prec t) \supset F'))$

Example:

induction hypothesis $\mathrm{IH}_{n+m+p}^{\prec}(G)$:

```
for all natural numbers n1,m1,p1
    if ((n1 + m1) + p1) -<- ((n + m) + p) then
if p1 is prime and p1 | n1 * m1 then p1 | n1 or p1 | m1
```

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\; \triangleright_G \;\; \Delta} \qquad\qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\; \triangleright_G \;\; \Lambda, \Delta}$$

- original thesis: $G = \forall \vec{x}\, (H \supset F)$
- induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\, (H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$
- induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\, (H' \supset ((t' \prec t) \supset F'))$

Example:

induction thesis $\mathrm{IT}_{n+m+p}^{\prec}(G)$:

```
For all natural numbers n,m,p if
    for all natural numbers n1,m1,p1
        if ((n1 + m1) + p1) -<- ((n + m) + p) then
    if p1 is prime and p1 | n1 * m1 then p1 | n1 or p1 | m1
then if p is prime and p | n * m then p | n or p | m.
```

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\; \triangleright_G \;\; \Delta} \qquad\qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\; \triangleright_G \;\; \Lambda, \Delta}$$

- original thesis: $G = \forall \vec{x}\,(H \supset F)$
- induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\,(H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$
- induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\,(H' \supset ((t' \prec t) \supset F'))$

Thesis reduction:

Let us show that L (a lattice) is complete. $\longrightarrow$ *L is complete*

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \rhd_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \rhd_G \Delta} \qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \rhd_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \rhd_G \Lambda, \Delta}$$

– original thesis: $G = \forall \vec{x}\,(H \supset F)$

– induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\,(H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$

– induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\,(H' \supset ((t' \prec t) \supset F'))$

Thesis reduction:

Let us show that L (a lattice) is complete. $\longrightarrow$ *L is complete*

Let S be a subset of L. $\longrightarrow$ *S has a supremum and an infimum in L*

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \triangleright_G \Delta} \qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \triangleright_G \Lambda, \Delta}$$

- original thesis: $G = \forall \vec{x}\,(H \supset F)$
- induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\,(H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$
- induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\,(H' \supset ((t' \prec t) \supset F'))$

Thesis reduction:

Let us show that L (a lattice) is complete.	$\longrightarrow$	*L is complete*
Let S be a subset of L.	$\longrightarrow$	*S has a supremum and an infimum in L*
S has a supremum in L.	$\longrightarrow$	*S has an infimum in L*

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \rhd_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\; \rhd_G \;\; \Delta} \qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \rhd_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\; \rhd_G \;\; \Lambda, \Delta}$$

- original thesis: $G = \forall \vec{x}\,(H \supset F)$
- induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\,(H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$
- induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\,(H' \supset ((t' \prec t) \supset F'))$

Thesis reduction:

Let us show that L (a lattice) is complete.	$\longrightarrow$	*L is complete*
Let S be a subset of L.	$\longrightarrow$	*S has a supremum and an infimum in L*
S has a supremum in L.	$\longrightarrow$	*S has an infimum in L*
S has an infimum in L.	$\longrightarrow$	$\top$

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \rhd_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \ \rhd_G \ \Delta} \qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \rhd_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \ \rhd_G \ \Lambda, \Delta}$$

- original thesis: $G = \forall \vec{x}\,(H \supset F)$
- induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\,(H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$
- induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\,(H' \supset ((t' \prec t) \supset F'))$

Thesis reduction:

Let us show that L (a lattice) is complete.	$\longrightarrow$	*L is complete*
Let S be a subset of L.	$\longrightarrow$	*S has a supremum and an infimum in L*
S has a supremum in L.	$\longrightarrow$	*S has an infimum in L*
S has an infimum in L.	$\longrightarrow$	$\top$

Soundness: $\vdash_{\mathbf{CTC}} \Gamma \rhd_G \Delta \quad \Rightarrow \quad \forall(\mathrm{IT}_{\mathbf{t}}^{\prec}(\mathbf{G}) \supset \mathbf{G}),\ \Gamma \vdash G$

Calculus of Text Correctness

Induction handling rules:

$$\frac{\Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Delta}{\Gamma \;\triangleright_G\; \Delta} \qquad \frac{\mathcal{DV}_{\Gamma,\Lambda}(\mathrm{IH}_t^{\prec}(G)) = \varnothing \qquad \Gamma \triangleright_{\mathrm{IT}_t^{\prec}(G)} \Lambda,\ (\texttt{assume}\ \mathrm{IH}_t^{\prec}(G)),\ \Delta}{\Gamma \;\triangleright_G\; \Lambda, \Delta}$$

– original thesis: $G = \forall \vec{x}\,(H \supset F)$

– induction thesis: $\mathrm{IT}_t^{\prec}(G) = \forall \vec{x}\,(H \supset (\mathrm{IH}_t^{\prec}(G) \supset F))$

– induction hypothesis: $\mathrm{IH}_t^{\prec}(G) = \forall \vec{x}'\,(H' \supset ((t' \prec t) \supset F'))$

Thesis reduction:

Let us show that L (a lattice) is complete.	$\longrightarrow$	*L is complete*
Let S be a subset of L.	$\longrightarrow$	*S has a supremum and an infimum in L*
S has a supremum in L.	$\longrightarrow$	*S has an infimum in L*
S has an infimum in L.	$\longrightarrow$	$\top$

Soundness:

$$\boxed{\vdash_{\mathbf{CTC}} \Gamma \triangleright_G \Delta \quad \Rightarrow \quad \forall(\mathrm{IT}_{\mathbf{t}}^{\prec}(\mathbf{G}) \supset \mathbf{G}),\, \Gamma \vdash G}$$

Interpretation: proofs are redundant

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.
   Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
      Assume that a -R+> b,c.
      Take u such that a -R> u -R*> b.
      Take v such that a -R> v -R*> c.
      Take w such that u,v -R*> w.
      Take a normal form d of w in R.
      b -R*> d.  Indeed take x such that b,d -R*> x.
      c -R*> d.  Indeed take y such that c,d -R*> y.
   end.
qed.
```

Formal Mathematical Text (Newman's Lemma)

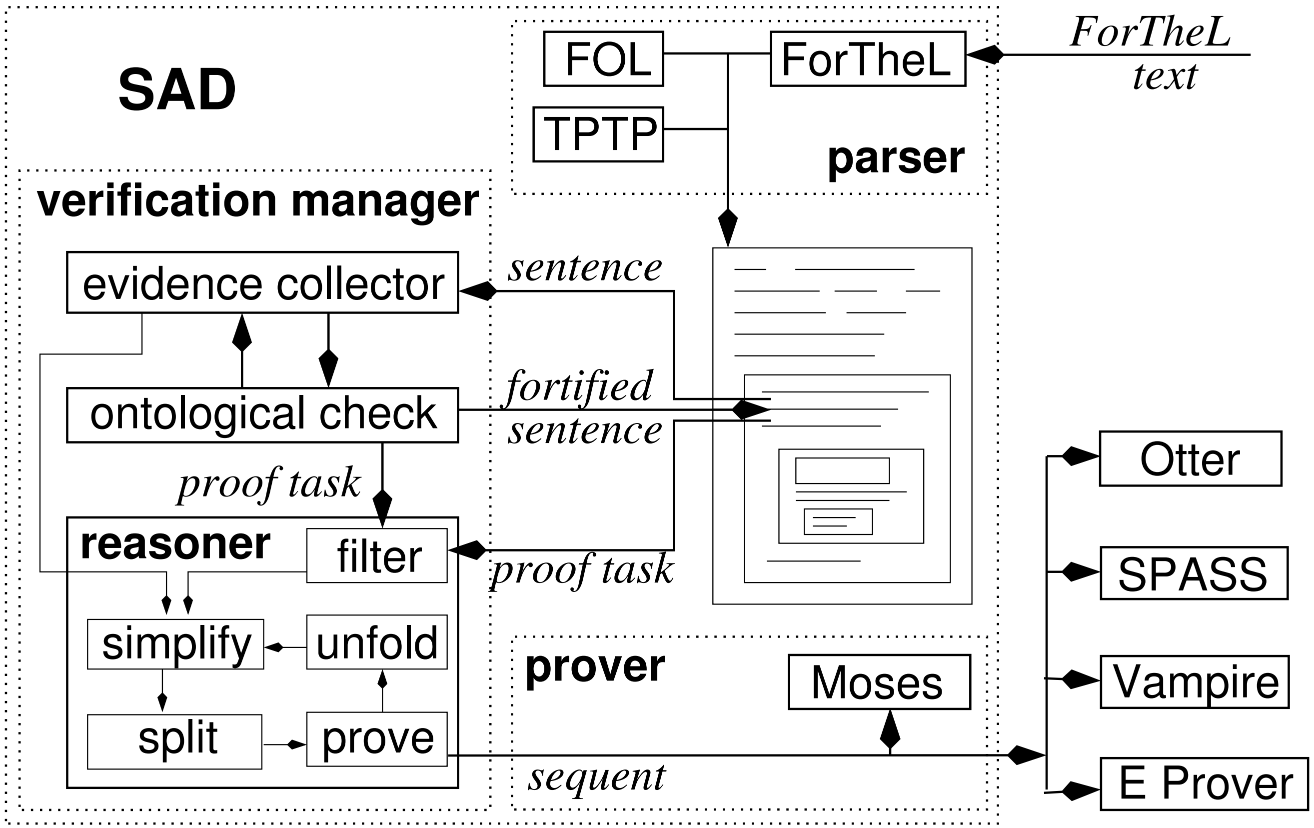
```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
Proof.
   Let R be locally confluent and terminating.
   Let us demonstrate by induction that for all a,b,c
    such that a -R*> b,c there exists d such that b,c -R*> d.
   Obvious.
qed.
```

Formal Mathematical Text (Newman's Lemma)

```
Let a,b,c,d,u,v,w,x,y,z denote terms.
Let R,S,T denote rewriting systems.

Definition NFRDef.  A normal form of x in R is a term y
                    such that x -R*> y and y has no reducts in R.

Lemma TermNF.   Let R be a terminating rewriting system.
                Every term x has a normal form in R.
Proof by induction.  Obvious.

Lemma Newman.
   Any locally confluent terminating rewriting system is confluent.
```

System for Automated Deduction

System for Automated Deduction



– **manager**: decompose input text into separate proof tasks

– **reasoner**: big steps of reasoning, heuristic proof methods

– **prover**: inference search in a sound and complete calculus

Reasoner capabilities

– Evidence generation (81% vs. 75% of succeeded goals):

evidence — a literal local property of a term occurrence

mostly useful for type information: $\exists x\,(x \in \mathbb{R}^* \wedge \ldots \boxed{\frac{\boxed{1}_{1\in\mathbb{R}}}{\boxed{x}_{x\in\mathbb{R}^*}}}_{\frac{1}{x}\in\mathbb{R}} \ldots)$

Reasoner capabilities

- Evidence generation (81% vs. 75% of succeeded goals):

  evidence — a literal local property of a term occurrence

  mostly useful for type information: $\exists x\,(x \in \mathbb{R}^* \wedge \ldots \boxed{\dfrac{\boxed{1}_{1\in\mathbb{R}}}{\boxed{x}_{x\in\mathbb{R}^*}}}_{\frac{1}{x}\in\mathbb{R}} \ldots)$

- Filtering: reduce unneeded premises (by default, definitions) to «simple rules»:

  definition of a subgroup $\longrightarrow$ a subgroup of a group is a group

  definition of a set union $\longrightarrow$ the union of two sets is a set

Reasoner capabilities

– Evidence generation (81% vs. 75% of succeeded goals):

evidence — a literal local property of a term occurrence

mostly useful for type information: $\exists x\, (x \in \mathbb{R}^* \land \ldots \boxed{\frac{\boxed{1}_{1\in\mathbb{R}}}{\boxed{x}_{x\in\mathbb{R}^*}}}_{\frac{1}{x}\in\mathbb{R}} \ldots)$

– Filtering: reduce unneeded premises (by default, definitions) to «simple rules»:

definition of a subgroup $\longrightarrow$ a subgroup of a group is a group

definition of a set union $\longrightarrow$ the union of two sets is a set

– Goal splitting: $\Gamma \vdash (F \supset (G \land H)) \quad \longrightarrow \quad \Gamma, F \vdash G$ and $\Gamma, F, G \vdash H$

Reasoner capabilities

- Evidence generation (81% vs. 75% of succeeded goals):

  evidence — a literal local property of a term occurrence

  mostly useful for type information: $\exists x \, (x \in \mathbb{R}^* \wedge \ldots \boxed{\dfrac{\boxed{1}_{1 \in \mathbb{R}}}{\boxed{x}_{x \in \mathbb{R}^*}}}_{\frac{1}{x} \in \mathbb{R}} \ldots)$

- Filtering: reduce unneeded premises (by default, definitions) to «simple rules»:

  definition of a subgroup $\longrightarrow$ a subgroup of a group is a group

  definition of a set union $\longrightarrow$ the union of two sets is a set

- Goal splitting: $\Gamma \vdash (F \supset (G \wedge H)) \quad \longrightarrow \quad \Gamma, F \vdash G$ and $\Gamma, F, G \vdash H$

- Simplification: replace redundant ($\equiv$ locally true) literals with $\top$

Reasoner capabilities

- Evidence generation (81% vs. 75% of succeeded goals):

  evidence — a literal local property of a term occurrence

  mostly useful for type information: $\exists x\,(x \in \mathbb{R}^* \wedge \ldots \boxed{\dfrac{\boxed{1}_{1\in\mathbb{R}}}{\boxed{x}_{x\in\mathbb{R}^*}}}_{\frac{1}{x}\in\mathbb{R}} \ldots)$

- Filtering: reduce unneeded premises (by default, definitions) to «simple rules»:

  definition of a subgroup $\longrightarrow$ a subgroup of a group is a group

  definition of a set union $\longrightarrow$ the union of two sets is a set

- Goal splitting: $\Gamma \vdash (F \supset (G \wedge H)) \quad \longrightarrow \quad \Gamma, F \vdash G$ and $\Gamma, F, G \vdash H$

- Simplification: replace redundant ($\equiv$ locally true) literals with $\top$

- Definition expansion (81% vs. 28% of succeeded goals):

Reasoner capabilities

– Evidence generation (81% vs. 75% of succeeded goals):

evidence — a literal local property of a term occurrence

mostly useful for type information: $\exists x\,(x \in \mathbb{R}^* \wedge \ldots \boxed{\dfrac{\boxed{1}_{1\in\mathbb{R}}}{\boxed{x}_{x\in\mathbb{R}^*}}}_{\frac{1}{x}\in\mathbb{R}} \ldots)$

– Filtering: reduce unneeded premises (by default, definitions) to «simple rules»:

definition of a subgroup $\longrightarrow$ a subgroup of a group is a group

definition of a set union $\longrightarrow$ the union of two sets is a set

– Goal splitting: $\Gamma \vdash (F \supset (G \wedge H)) \quad \longrightarrow \quad \Gamma, F \vdash G$ and $\Gamma, F, G \vdash H$

– Simplification: replace redundant ($\equiv$ locally true) literals with $\top$

– Definition expansion (81% vs. 28% of succeeded goals):

- *destructive* — expansion formula replaces the unfolded occurrence
- *conservative* — expansion formula is added alongside (more flexible)

Reasoner capabilities

- Evidence generation (81% vs. 75% of succeeded goals):

  evidence — a literal local property of a term occurrence

  mostly useful for type information: $\exists x\,(x \in \mathbb{R}^* \wedge \ldots \boxed{\dfrac{\boxed{1}_{1\in\mathbb{R}}}{\boxed{x}_{x\in\mathbb{R}^*}}}_{\frac{1}{x}\in\mathbb{R}} \ldots)$

- Filtering: reduce unneeded premises (by default, definitions) to «simple rules»:

  definition of a subgroup $\longrightarrow$ a subgroup of a group is a group

  definition of a set union $\longrightarrow$ the union of two sets is a set

- Goal splitting: $\Gamma \vdash (F \supset (G \wedge H)) \quad \longrightarrow \quad \Gamma, F \vdash G$ and $\Gamma, F, G \vdash H$

- Simplification: replace redundant ($\equiv$ locally true) literals with $\top$

- Definition expansion (81% vs. 28% of succeeded goals):

  - *destructive* — expansion formula replaces the unfolded occurrence
  - *conservative* — expansion formula is added alongside (more flexible)
  - expansion strategies: according to the definition hierarchy,

    by «weight» of an occurrence, $\boxed{\text{expand every occurrence in sight}}$

Conclusion

Conclusion

System for Automated Deduction:

• rich natural-like language		concise
• special reasoning methods	$\Rightarrow$	easy-to-read-and-produce
• powerful inference search engine		formalizations

Formalized and verified:

- Ramsey's Infinite and Finite theorems
- Properties of a refinement relation on program specifications
- Cauchy-Bouniakowsky-Schwarz inequality
- For any prime p, $\sqrt{p} \notin \mathbb{Q}$
- Chinese remainders theorem and Bezout's identity in rings
- Tarski-Knaster fixed point theorem
- Newman's lemma on rewriting systems confluence

Thanks!