A Proof-Theoretic Approach to Hierarchical Math Library Organization

Kamal Aboul-Hosn
Terese Damhøj Andersen

Cornell University

- Motivation
- Related Work
- Proof System
- Example
- Conclusions/Future Work

Basic Questions

- What is the difference between lemmas and theorems?
  - "Theorems are more important than lemmas."
  - "Theorems apply in more places than lemmas."
  - "Lemmas are only used in proofs of theorems."
- Do our choices in mathematical proofs create an inherent structure that can be captured formally?

Relationship Between Theorems & Lemmas

- Levels of importance and dependency
- Qualitative difference is in *scope*
- Scope for variables and assumptions already exists
- Theorems apply anywhere, lemmas are limited

A Motivating Example

Consider a Boolean algebra $(B, \vee, \wedge, \neg, 0, 1)$
with axioms of equality:

$$
\begin{array}{rcl}
\text{ref} & : & x = x \\
\text{sym} & : & x = y \rightarrow y = x \\
\text{trans} & : & x = y \rightarrow y = z \rightarrow x = z \\
\text{cong}_{\wedge} & : & x = y \rightarrow z \wedge x = z \wedge y \\
\text{cong}_{\vee} & : & x = y \rightarrow z \vee x = z \vee y \\
\text{cong}_{\neg} & : & x = y \rightarrow \neg x = \neg y
\end{array}
$$

Theorem 1:

$$\forall a, b, c, z. \quad a = b \rightarrow a = c \rightarrow z \vee (a \wedge b) = z \vee (a \wedge c)$$

A Motivating Example

Lemma 1:

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Proof of Theorem:

$$\begin{array}{lcll} z \vee (a \wedge a) & = & z \vee (a \wedge b) & (\text{Lemma 1}) \\ z \vee (a \wedge a) & = & z \vee (a \wedge c) & (\text{Lemma 1}) \\ z \vee (a \wedge b) & = & z \vee (a \wedge a) & (\text{sym}) \\ z \vee (a \wedge b) & = & z \vee (a \wedge c) & (\text{trans}) \end{array}$$

Theorem 1:

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Scope

- Limit scope of lemma to theorem
- Two possible quantifications of z
  - "Lemma 1: For all x, y, and z,..." vs.
  - "Let z be an arbitrary, but fixed Boolean value. Lemma 1: For all x and y,..."
- Subtle, stylistic differences that can be captured formally

- Motivation
- Related Work
- Proof System
- Example
- Conclusions/Future Work

Related Work

- Mostly in the context of automated theorem provers
- Coq, Isabelle, NuPRL make no distinction between theorems and lemmas
- Three primary areas
  - Variable and assumption scoping
  - Proof reuse
  - Library structuring

Variable Scoping

- Kammüller, Ballarin: Isabelle's *locales*

  + Limit use of set of local variables and assumptions to current theory

  + Nested locales allowed

  + Variables and assumptions can be moved outward in nesting

  - Theorems do not have scope

Proof Reuse

- Melis & Whittle, Owen, Munyer....: Proof by analogy
- Melis & Schairer: Reuse in formal software verification
- Kolbe & Walther: Proof generalization and reuse
- Mostly focus on tactics and proof step reuse

+ Allows proof steps to be performed automatically

- No organization of commonly used tactics into hierarchical structure

Library Structuring

- Lorigo et al.: WWW search techniques based on theorems in proofs

+ Find structure of mathematical topics and categories of theorems

- For use with already existing libraries

- No restructuring of libraries to match relationships

- Motivation
- Related Work
- Proof System
- Example
- Conclusions/Future Work

Proof Representation

- Based on publish/cite by Kozen & Ramanarayanan
- Universal Horn equational logic
  - Individual variables $X = \{x,y,...\}$
  - First-order signature $\Sigma = \{f,g,...\}$
  - Individual terms $s,t,...$
    - An individual variable
    - An expression $f\ t_1...t_n$, f is an n-ary function in Σ and $t_1...t_n$ are individual variables
  - Equations $d,e,...$ between two terms, $s = t$

Proof Representation

- Theorem: A universally quantified Horn formula

$$\forall x_1, \ldots, x_m.\quad \varphi_1 \quad \rightarrow \quad \varphi_2 \quad \rightarrow \quad \cdots \quad \rightarrow \quad \varphi_n \rightarrow \psi$$

- φ_i : Equations (premises)
- ψ : Equation (conclusion)
- $x_1, \ldots, x_m$: Free variables
- Arbitrary specialization through term substitution
  - $\forall x, y, z.\quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$

    with substitution [*x*/*a*,*y*/*b*,*z*/*z*]

    becomes $a = b \quad \rightarrow \quad z \vee (a \wedge a) = z \vee (a \wedge b)$

Proof Term

- A variable p
- A constant--name of a theorem
- An application $\pi\ \tau$, where π and τ are proof terms
- An application $\pi\ t$, where π is a proof term and t is an individual term
- An abstraction $\lambda p.\tau$, where p is a proof variable and τ is a proof term
- An abstraction $\lambda x.\tau$ where x is an individual variable and τ is a proof term

Proof Term

- Sequence: $\tau_1; \ldots; \tau_n$, where $\tau_1, \ldots, \tau_n$ are proof terms
- Scoping: let $L_1 = \tau_1 \ldots L_n = \tau_n$ in τ end
  - Define proofs $\tau_1, \ldots, \tau_n$
  - Assign to new names $L_1, \ldots, L_n$
  - L_i can appear in τ_k, where $i < k$, and in τ
  - Corresponds to variable scoping in SML lets

Typing Rules

$$\frac{}{\Gamma, p : e \vdash p : e} \qquad \frac{}{\Gamma, c : \varphi \vdash c : \varphi}$$

$$\frac{\Gamma \vdash \pi : e \to \varphi \quad \Gamma \vdash \tau : e}{\Gamma \vdash \pi\tau : \varphi} \qquad \frac{\Gamma \vdash \pi : \forall x.\varphi}{\Gamma \vdash \pi t : \varphi[x/t]}$$

$$\frac{\Gamma, p : e \vdash \tau : \varphi}{\Gamma \vdash \lambda p.\tau : e \to \varphi} \qquad \frac{\Gamma \vdash \tau : \varphi}{\Gamma \vdash \lambda x.\tau : \forall x.\varphi}$$

$$\frac{\Gamma \vdash \tau_1 : \varphi_1 \quad \ldots \quad \Gamma \vdash \tau_n : \varphi_n}{\Gamma \vdash \tau_1; \ldots; \tau_n : \varphi_1 \wedge \ldots \wedge \varphi_n}$$

$$\frac{\begin{array}{l}\Gamma \vdash \tau_1 : \varphi_1 \\ \Gamma, L_1 : \varphi_1 \vdash \tau_2 : \varphi_2 \\ \ldots \\ \Gamma, L_1 : \varphi_1, \ldots, L_{n-1} : \varphi_{n-1} \vdash \tau_n : \varphi_n \\ \Gamma, L_1 : \varphi_1, \ldots, L_n : \varphi_n \vdash \tau : \varphi\end{array}}{\Gamma \vdash \mathsf{let}\ L_1 = \tau_1 \ldots L_n = \tau_n\ \mathsf{in}\ \tau\ \mathsf{end} : \varphi_1 \to \ldots \to \varphi_n \to \varphi}$$

Motivating Example

thm =
  let lem = $\lambda x \lambda y \lambda z \lambda P.$(Proof of lemma)
  in
    $\lambda a \lambda b \lambda c \lambda z \lambda Q \lambda R.$trans (sym (lem Q)) (lem R)
  end

- P: $x = y$, Q: $a = b$, R: $a = c$
- According to Curry-Howard Isomorphism
  - Type of λ-term corresponds theorem
  - λ-term corresponds to proof of theorem

Motivating Example

- "Lemma 1: For all x, y, and z,..."

  thm =

  let lem = $\lambda x \lambda y \lambda z \lambda P.$(Proof of lemma)

  in

  $\lambda a \lambda b \lambda c \lambda z \lambda Q \lambda R.$trans (sym (lem Q)) (lem R)

  end

- "Let z be an arbitrary, but fixed Boolean value.
  Lemma 1: For all x and y,..."

  thm =

  $\lambda z.$let lem = $\lambda x \lambda y \lambda P.$(Proof of lemma)

  in

  $\lambda a \lambda b \lambda c \lambda Q \lambda R.$trans (sym (lem Q)) (lem R)

  end

Library Structure

- $\mathcal{L}; \mathcal{C}; \mathcal{T}$
- Library of theorems $\mathcal{L} : T_1 = \pi_1, \ldots, T_n = \pi_n$
- Lemmas in scope $\mathcal{C} : L_1 = \tau_1, \ldots, L_m = \tau_m$
- Annotated proof tasks $\mathcal{T} : A \vdash \pi : \varphi$

Library Typing Rules

- Assignments, tasks, and library all have types
- Similar to typing for **let** expression
- Enforces ordering on theorems and lemmas
- Prevents circularity in proofs

Library Proof Rules

(assume)
$$\frac{\mathcal{L}\ ;\ \mathcal{C}\ ;\ \mathcal{T},\quad A \vdash \tau : e}{\mathcal{L}\ ;\ \mathcal{C}\ ;\ \mathcal{T},\quad A, p : d \vdash \tau : e}$$

(ident)
$$\frac{\mathcal{L}\ ;\ \mathcal{C}\ ;\ \mathcal{T}}{\mathcal{L}\ ;\ \mathcal{C}\ ;\ \mathcal{T},\quad p : e \vdash p : e}$$

(mp)
$$\frac{\mathcal{L}\ ;\ \mathcal{C}\ ;\ \mathcal{T},\quad A \vdash \pi : e \to \varphi \quad A \vdash \tau : e}{\mathcal{L}\ ;\ \mathcal{C}\ ;\ \mathcal{T},\quad A \vdash \pi\ \tau : \varphi}$$

(discharge)
$$\frac{\mathcal{L}\ ;\ \mathcal{C}\ ;\ \mathcal{T},\quad A, p : e \vdash \tau : \varphi}{\mathcal{L}\ ;\ \mathcal{C}\ ;\ \mathcal{T},\quad A \vdash \lambda p.\tau : e \to \varphi}$$

(collect)
$$\frac{\mathcal{L}\ ;\ \overline{M} = \overline{\pi}\ ;\ \vdash \tau_1 : \varphi_1 \ldots \vdash \tau_n : \varphi_n}{\mathcal{L}\ ;\quad L = \begin{array}{l}\mathsf{let}\ \overline{M} = \overline{\pi} \\ \mathsf{in}\ \lambda\overline{x}_1.\tau_1; \ldots; \lambda\overline{x}_n.\tau_n\ \mathsf{end}\end{array}\ ;} \qquad \overline{x}_i = FV(\varphi_i)$$

(publish)
$$\frac{\mathcal{L}\ ;\ \overline{L} = \overline{\tau}\ ;}{\mathcal{L}, \overline{L} = \overline{\tau}\ ;\ ;}$$

Collect

$$\frac{\mathcal{L}\ ;\ \overline{M} = \overline{\pi}\ ;\ \ \vdash \tau_1 : \varphi_1 \ldots \vdash \tau_n : \varphi_n}{\mathcal{L}\ ;\ \begin{array}{rl} L = & \mathsf{let}\ \overline{M} = \overline{\pi} \\ & \mathsf{in}\ \lambda\overline{x}_1.\tau_1; \ldots; \lambda\overline{x}_n.\tau_n\ \mathsf{end} \end{array}\ ;} \qquad \overline{x}_i = FV(\varphi_i)$$

- Form universal closures of φ_is and corresponding λ-closures of τ_is
- Assign new name L
- Take lemmas $\overline{M}$ out of scope

Library Proof Rules

(tcite)
$$\frac{\mathcal{L}_1, T = \pi, \mathcal{L}_2 \;;\; \mathcal{C} \;;\; \mathcal{T}}{\mathcal{L}_1, T = \pi, \mathcal{L}_2 \;;\; \mathcal{C} \;;\; \mathcal{T}, \quad \vdash T[j]\ \overline{t} : \varphi[\overline{x}/\overline{t}]} \quad T[j] : \forall \overline{x}.\varphi$$

(lcite)
$$\frac{\mathcal{L} \;;\; \mathcal{C}_1, L = \pi, \mathcal{C}_2 \;;\; \mathcal{T}}{\mathcal{L} \;;\; \mathcal{C}_1, L = \pi, \mathcal{C}_2 \;;\; \mathcal{T}, \quad \vdash L[j]\ \overline{t} : \varphi[\overline{x}/\overline{t}]} \quad L[j] : \forall \overline{x}.\varphi$$

(tforget)
$$\frac{\mathcal{L}_1, T = \pi, \mathcal{L}_2 \;;\; \mathcal{C} \;;\; \mathcal{T}}{\mathcal{L}_1, \mathcal{L}_2[T/\pi] \;;\; \mathcal{C}[T/\pi] \;;\; \mathcal{T}[T/\pi]}$$

(lforget)
$$\frac{\mathcal{L} \;;\; \mathcal{C}_1, L = \pi, \mathcal{C}_2 \;;\; \mathcal{T}}{\mathcal{L} \;;\; \mathcal{C}_1, \mathcal{C}_2[L/\pi] \;;\; \mathcal{T}[L/\pi]}$$

(reorder)
$$\frac{\mathcal{L} \;;\; \mathcal{C}_1, L = \lambda\alpha_1 \ldots \lambda\alpha_i \lambda\alpha_j \ldots \lambda_n.\pi, \mathcal{C}_2 \;;}{\mathcal{L} \;;\; \mathcal{C}_1, L = \lambda\alpha_1 \ldots \lambda\alpha_j \lambda\alpha_i \ldots \lambda_n.\pi, \mathcal{C}_2[L(i,j)/L(j,i)] \;;} \quad (*)$$

(promote)
$$\frac{\mathcal{L} \;;\; \mathcal{L}_1, L = \mathsf{let}\ \overline{M} = \overline{\tau}\ \mathsf{in}\ \pi\ \mathsf{end}, \mathcal{L}_2 \;;}{\mathcal{L} \;;\; \mathcal{L}_1, \overline{M} = \overline{\tau}, L = \pi, \mathcal{L}_2 \;;}$$

Promote

$$\frac{\mathcal{L}\ ;\ \mathcal{L}_1, L = \mathsf{let}\ \overline{M} = \overline{\tau}\ \mathsf{in}\ \pi\ \mathsf{end}, \mathcal{L}_2\ ;}{\mathcal{L}\ ;\ \mathcal{L}_1, \overline{M} = \overline{\tau}, L = \pi, \mathcal{L}_2\ ;}$$

$$L = \mathsf{let}\ M = \tau\ \mathsf{in}\ \pi\ \mathsf{end} \quad \Rightarrow \quad M = \tau, L = \pi$$

- M may apply in more places than just π
- M may have same relative importance as L
- Apply other rules to stress different relations

Proof Term Proof Rules

(push) $$\frac{\lambda\alpha.(\pi_1;\ldots;\pi_n)}{\lambda\alpha.\pi_1;\ldots;\lambda\alpha.\pi_n}$$

(pull) $$\frac{\lambda\alpha.\pi_1;\ldots;\lambda\alpha.\pi_n}{\lambda\alpha.(\pi_1;\ldots;\pi_n)}$$

(generalize) $$\frac{\lambda\alpha.\mathsf{let}\ \overline{L} = \overline{\pi}\ \mathsf{in}\ \tau\ \mathsf{end}}{\mathsf{let}\ \overline{L} = \overline{\lambda\alpha.\pi[\overline{L}/\overline{L}\ \alpha]}\ \mathsf{in}\ \lambda\alpha.\tau[\overline{L}/\overline{L}\ \alpha]\ \mathsf{end}}$$

(specialize) $$\frac{\mathsf{let}\ \overline{L} = \lambda\alpha.\pi\ \mathsf{in}\ \lambda\alpha.\tau\ \mathsf{end}}{\lambda\alpha.\mathsf{let}\ \overline{L} = \overline{\pi[\overline{L}\ \alpha/\overline{L}]}\ \mathsf{in}\ \tau[\overline{L}\ \alpha/\overline{L}]\ \mathsf{end}}\quad (**)$$

(split) $$\frac{\mathsf{let}\ \overline{L} = \overline{\pi_L}, \overline{M} = \overline{\pi_M}\ \mathsf{in}\ \tau\ \mathsf{end}}{\mathsf{let}\ \overline{L} = \overline{\pi_L}\ \mathsf{in}\ \mathsf{let}\ \overline{M} = \overline{\pi_M}\ \mathsf{in}\ \tau\ \mathsf{end}\ \mathsf{end}}$$

(merge) $$\frac{\mathsf{let}\ \overline{L = \pi_L}\ \mathsf{in}\ \mathsf{let}\ \overline{M = \pi_M}\ \mathsf{in}\ \tau\ \mathsf{end}\ \mathsf{end}}{\mathsf{let}\ \overline{L} = \overline{\pi_L}, \overline{M} = \overline{\pi_M}\ \mathsf{in}\ \tau\ \mathsf{end}}$$

(rename) $$\frac{\lambda\alpha.\pi}{\lambda\beta.\pi[\alpha/\beta]}\quad (\#)$$

Generalize/Specialize

- $\lambda x.$let $L = \lambda P.\pi$ in $\lambda Q.(L\ Q)$ end
  - "Consider an arbitrary, but fixed value x.
    Lemma L: If x has property P, then ....
    Theorem: If x has property Q, then ....
    Proof: Apply L with the assumption Q"

- let $L = \lambda x.\lambda P.\pi$ in $\lambda x.\lambda Q.(L\ x\ Q)$ end
  - "Lemma L: For all x, if x has property P, then ....
    Theorem: For all x, if x has property Q, then ....
    Proof: Apply L to x with the assumption Q"

Soundness

- Proof rules transform proof terms
- Type can change during transformation
- Justified by axioms of first order logic

- Motivation
- Related Work
- Proof System
- Example
- Conclusions/Future Work

Motivating Example

- Axioms:

$$\begin{aligned}
\text{sym} &: \forall x, y.\ \ x = y \ \rightarrow\ y = x \\
\text{trans} &: \forall x, y, z.\ \ x = y \ \rightarrow\ y = z \ \rightarrow\ x = z \\
\text{cong}_{\wedge} &: \forall x, y, z.\ \ x = y \ \rightarrow\ (z \wedge x) = (z \wedge y) \\
\text{cong}_{\vee} &: \forall x, y, z.\ \ x = y \ \rightarrow\ (z \vee x) = (z \vee y)
\end{aligned}$$

- Theorem to prove:

$$\forall a, b, c, z.\ \ a = b \ \rightarrow\ a = c \ \rightarrow\ z \vee (a \wedge b) = z \vee (a \wedge c)$$

- Lemma to prove:

$$\forall x, y, z.\ \ x = y \ \rightarrow\ z \vee (x \wedge x) = z \vee (x \wedge y)$$

Lemma to prove

$$\forall x, y, z. \quad x = y$$
$$\rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b$$
$$\rightarrow \quad a = c$$
$$\rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule
Theorem
Substitution

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (ident)
Theorem
Substitution

$$P \ : \ x = y \quad \vdash \quad P \ : \ x = y$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule
(tcite), (assume)
Theorem
$\mathsf{cong}_{\wedge} : \forall x, y, z. x = y \rightarrow (z \wedge x) = (z \wedge y)$
Substitution
x/x
y/y
z/x

$$P \ : \ x = y \quad \vdash \quad P \ : \ x = y$$

$$P \ : \ x = y \quad \vdash \quad \mathsf{cong}_{\wedge} \ : \ x = y \ \rightarrow \ (x \wedge x) = (x \wedge y)$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (mp)
Theorem
Substitution

$P \ : \ x = y \quad \vdash \quad P \ : \ x = y$

$P \ : \ x = y \quad \vdash \quad \mathsf{cong}_{\wedge} \ : \ x = y \ \rightarrow \ (x \wedge x) = (x \wedge y)$

$P \ : \ x = y \quad \vdash \quad \mathsf{cong} \quad P \ : \ (x \wedge x) = (x \wedge y)$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule
(tcite), (assume)
Theorem
$\mathsf{cong}_{\vee} : \forall x, y, z. x = y \rightarrow (z \vee x) = (z \vee y)$
Substitution
$x / x \wedge x$
$y / x \wedge y$
z / z

$$P \ : \ x = y \quad \vdash \quad \mathsf{cong} \quad P \ : \ (x \wedge x) = (x \wedge y)$$

$$P \ : \ x = y \quad \vdash \quad \mathsf{cong}_{\vee} \ : \ (x \wedge x) = (x \wedge y) \ \rightarrow \ z \vee (x \wedge x) = z \vee (x \wedge y)$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (mp)
Theorem
Substitution

$P \ : \ x = y \quad \vdash \quad \mathsf{cong} \quad P \ : \ (x \wedge x) = (x \wedge y)$

$P \ : \ x = y \quad \vdash \quad \mathsf{cong}_{\vee} \ : \ (x \wedge x) = (x \wedge y) \ \rightarrow \ z \vee (x \wedge x) = z \vee (x \wedge y)$

$P \ : \ x = y \quad \vdash \quad \mathsf{cong}_{\vee} \ (\mathsf{cong}_{\wedge} \ P) \ : \ z \vee (x \wedge x) = z \vee (x \wedge y)$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (discharge)
Theorem
Substitution

$$P \ : \ x = y \quad \vdash \quad \mathsf{cong}_{\vee} \ (\mathsf{cong}_{\wedge} \ P) \ : \ z \vee (x \wedge x) = z \vee (x \wedge y)$$

$$\vdash \quad \lambda P.\mathsf{cong}_{\vee} \ (\mathsf{cong}_{\wedge} \ P) \ : \ x = y \ \rightarrow \ z \vee (x \wedge x) = z \vee (x \wedge y)$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (collect)
Theorem
Substitution

$$\vdash \quad \lambda P.\mathsf{cong}_{\vee}\ (\mathsf{cong}_{\wedge}\ P)\ :\ x = y\ \rightarrow\ z \vee (x \wedge x) = z \vee (x \wedge y)$$

$$\mathsf{lem} = \lambda x \lambda y \lambda z \lambda P.\mathsf{cong}_{\vee}\ (\mathsf{cong}_{\wedge}\ P)\ :\ \forall x, y, z.\ x = y\ \rightarrow\ z \vee (x \wedge x) = z \vee (x \wedge y)$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule

Theorem

Substitution

Lemma to prove

$$\forall x, y, z. \quad x = y$$
$$\rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b$$
$$\rightarrow \quad a = c$$
$$\rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (ident)
Theorem
Substitution

$$Q \ : \ a = b \quad \vdash \quad Q \ : \ a = b$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule
(lcite), (assume)
Theorem
lem : $\forall x, y, z. x = x = y \rightarrow z \vee (x \wedge x) = z \vee (x \wedge y)$
Substitution
x/a
y/b
z/z

$$Q \ : \ a = b \quad \vdash \quad Q \ : \ a = b$$

$$Q \ : \ a = b \quad \vdash \quad \mathsf{lem} \ : \ a = b \ \rightarrow \ z \vee (a \wedge a) = z \vee (a \wedge b)$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (mp)
Theorem
Substitution

$Q \ : \ a = b \quad \vdash \quad Q \ : \ a = b$

$Q \ : \ a = b \quad \vdash \quad \mathsf{lem} \ : \ a = b \rightarrow z \vee (a \wedge a) = z \vee (a \wedge b)$

$Q \ : \ a = b \quad \vdash \quad \mathsf{lem}\ Q \ : \ z \vee (a \wedge a) = z \vee (a \wedge b)$

Lemma to prove

$$\forall x, y, z.x = y \rightarrow z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \rightarrow a = c \rightarrow z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule **(tcite), (assume)**
Theorem sym : $\forall x, y.x = y \rightarrow y = x$
Substitution $x/z \vee (a \wedge a)$ $y/z \vee (a \wedge b)$

$$Q : a = b \vdash \text{lem } Q : z \vee (a \wedge a) = z \vee (a \wedge b)$$

$$Q : a = b \vdash \text{sym} : z \vee (a \wedge a) = z \vee (a \wedge b) \rightarrow z \vee (a \wedge b) = z \vee (a \wedge a)$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (mp)
Theorem
Substitution

$Q \ : \ a = b \quad \vdash \quad \mathsf{lem}\ Q \ : \ z \vee (a \wedge a) = z \vee (a \wedge b)$

$Q \ : \ a = b \quad \vdash \quad \mathsf{sym} \ : \ z \vee (a \wedge a) = z \vee (a \wedge b) \ \rightarrow \ z \vee (a \wedge b) = z \vee (a \wedge a)$

$Q \ : \ a = b \quad \vdash \quad \mathsf{sym}\ (\mathsf{lem}\ Q) \ : \ z \vee (a \wedge b) = z \vee (a \wedge a)$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (ident)
Theorem
Substitution

$$Q \ : \ a = b \quad \vdash \quad \mathsf{sym}\ (\mathsf{lem}\ Q) \ : \ z \vee (a \wedge b) = z \vee (a \wedge a)$$

$$R \ : \ a = c \quad \vdash \quad R \ : \ a = c$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule
(lcite), (assume)
Theorem
lem : $\forall x, y, z. x = x = y \rightarrow z \vee (x \wedge x) = z \vee (x \wedge y)$
Substitution
x/a
y/c
z/z

$$Q \ : \ a = b \quad \vdash \quad \mathsf{sym}\ (\mathsf{lem}\ Q) \ : \ z \vee (a \wedge b) = z \vee (a \wedge a)$$

$$R \ : \ a = c \quad \vdash \quad R \ : \ a = c$$

$$R \ : \ a = c \quad \vdash \quad \mathsf{lem} \ : \ a = c \ \rightarrow \ z \vee (a \wedge a) = z \vee (a \wedge c)$$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (mp)
Theorem
Substitution

$Q : a = b \quad \vdash \quad \mathsf{sym}\ (\mathsf{lem}\ Q) : z \vee (a \wedge b) = z \vee (a \wedge a)$

$R : a = c \quad \vdash \quad R : a = c$

$R : a = c \quad \vdash \quad \mathsf{lem} : a = c \rightarrow z \vee (a \wedge a) = z \vee (a \wedge c)$

$R : a = c \quad \vdash \quad \mathsf{lem}\ R : z \vee (a \wedge a) = z \vee (a \wedge c)$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (tcite)
Theorem
trans : $\forall x, y, z. x = y \rightarrow y = z \rightarrow x = z$
Substitution
$x/z \vee (a \wedge b)$
$y/z \vee (a \wedge a)$
$z/z \vee (a \wedge c)$

Q : $a = b$ $\vdash$ sym (lem Q) : $z \vee (a \wedge b) = z \vee (a \wedge a)$

R : $a = c$ $\vdash$ lem R : $z \vee (a \wedge a) = z \vee (a \wedge c)$

$\vdash$ trans : $z \vee (a \wedge b) = z \vee (a \wedge a) \rightarrow z \vee (a \wedge a) = z \vee (a \wedge c) \rightarrow z \vee (a \wedge b) = z \vee (a \wedge c)$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (assume)
Theorem
Substitution

$Q \ : \ a = b \quad \vdash \quad \mathsf{sym}\ (\mathsf{lem}\ Q) \ : \ z \vee (a \wedge b) = z \vee (a \wedge a)$

$R \ : \ a = c \quad \vdash \quad \mathsf{lem}\ R \ : \ z \vee (a \wedge a) = z \vee (a \wedge c)$

$\vdash \quad \mathsf{trans} \ : \ z \vee (a \wedge b) = z \vee (a \wedge a) \ \rightarrow \ z \vee (a \wedge a) = z \vee (a \wedge c) \ \rightarrow \ z \vee (a \wedge b) = z \vee (a \wedge c)$

$Q \ : \ a = b, R \ : \ a = c \quad \vdash \quad \mathsf{sym}\ (\mathsf{lem}\ Q) \ : \ z \vee (a \wedge b) = z \vee (a \wedge a)$

$Q \ : \ a = b, R \ : \ a = c \quad \vdash \quad \mathsf{lem}\ R \ : \ z \vee (a \wedge a) = z \vee (a \wedge c)$

$Q \ : \ a = b, R \ : \ a = c \quad \vdash \quad \mathsf{trans} \ : \ z \vee (a \wedge b) = z \vee (a \wedge a) \ \rightarrow \ \ldots$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (mp)
Theorem
Substitution

$Q : a = b, R : a = c \quad \vdash \quad \mathsf{sym}\ (\mathsf{lem}\ Q) : z \vee (a \wedge b) = z \vee (a \wedge a)$

$Q : a = b, R : a = c \quad \vdash \quad \mathsf{lem}\ R : z \vee (a \wedge a) = z \vee (a \wedge c)$

$Q : a = b, R : a = c \quad \vdash \quad \mathsf{trans} : z \vee (a \wedge b) = z \vee (a \wedge a) \rightarrow \ldots$

$Q : a = b, R : a = c \quad \vdash \quad \mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q)) : z \vee (a \wedge a) = z \vee (a \wedge c) \rightarrow z \vee (a \wedge b) = z \vee (a \wedge c)$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (mp)
Theorem
Substitution

$Q : a = b, R : a = c \quad \vdash \quad \mathsf{lem}\ R : z \vee (a \wedge a) = z \vee (a \wedge c)$

$Q : a = b, R : a = c \quad \vdash \quad \mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q)) : z \vee (a \wedge a) = z \vee (a \wedge c) \rightarrow z \vee (a \wedge b) = z \vee (a \wedge c)$

$Q : a = b, R : a = c \quad \vdash \quad \mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q))\ (\mathsf{lem}\ R) : z \vee (a \wedge b) = z \vee (a \wedge c)$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (discharge)
Theorem
Substitution

$Q : a = b, R : a = c \quad \vdash \quad \mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q))\ (\mathsf{lem}\ R) : z \vee (a \wedge b) = z \vee (a \wedge c)$

$\vdash \quad \lambda Q \lambda R.\mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q))\ (\mathsf{lem}\ R) : a = b \rightarrow a = c \rightarrow z \vee (a \wedge b) = z \vee (a \wedge c)$

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (collect)
Theorem
Substitution

$$\vdash \quad \lambda Q \lambda R.\mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q))\ (\mathsf{lem}\ R) \quad : \quad a = b \rightarrow a = c \rightarrow z \vee (a \wedge b) = z \vee (a \wedge c)$$

thm =

let lem $= \lambda x \lambda y \lambda z \lambda P.\mathsf{cong}_{\vee}\mathsf{cong}_{\wedge} P : \forall x, y, z.\ x = y \rightarrow z \vee (x \wedge x) = z \vee (x \wedge y)$

in

$\lambda a \lambda b \lambda c \lambda z \lambda Q \lambda R.\mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q))\ (\mathsf{lem}\ R) \quad : \quad \forall a, b, c, z.\ a = b \rightarrow a = c \rightarrow z \vee (a \wedge b) = z \vee (a \wedge c)$

end

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (reorder)
Theorem
Substitution

thm =
let lem = $\lambda x \lambda y \lambda z \lambda P.\mathsf{cong}_{\vee}\mathsf{cong}_{\wedge} P : \forall x, y, z.\ x = y \ \rightarrow\ z \vee (x \wedge x) = z \vee (x \wedge y)$
in
$\lambda a \lambda b \lambda c \lambda z \lambda Q \lambda R.\mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q))\ (\mathsf{lem}\ R) \quad : \quad \forall a, b, c, z.\ a = b \ \rightarrow\ a = c \ \rightarrow\ z \vee (a \wedge b) = z \vee (a \wedge c)$
end

thm =
let lem = $\lambda z \lambda x \lambda y \lambda P.\mathsf{cong}_{\vee}\mathsf{cong}_{\wedge} P : \forall z, x, y.\ x = y \ \rightarrow\ z \vee (x \wedge x) = z \vee (x \wedge y)$
in
$\lambda z \lambda a \lambda b \lambda c \lambda Q \lambda R.\mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q))\ (\mathsf{lem}\ R) \quad : \quad \forall z, a, b, c.\ a = b \ \rightarrow\ a = c \ \rightarrow\ z \vee (a \wedge b) = z \vee (a \wedge c)$
end

Lemma to prove

$$\forall x, y, z. \quad x = y \quad \rightarrow \quad z \vee (x \wedge x) = z \vee (x \wedge y)$$

Theorem to prove

$$\forall a, b, c, z. \quad a = b \quad \rightarrow \quad a = c \quad \rightarrow \quad z \vee (a \wedge b) = z \vee (a \wedge c)$$

Rule (specialize)
Theorem
Substitution

thm =
let lem = $\lambda z \lambda x \lambda y \lambda P.\mathsf{cong}_{\vee}\mathsf{cong}_{\wedge} P : \forall z, x, y. x = y \rightarrow z \vee (x \wedge x) = z \vee (x \wedge y)$
in
$\lambda z \lambda a \lambda b \lambda c \lambda Q. \lambda R.\mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q))\ (\mathsf{lem}\ R) \quad : \quad \forall z, a, b, c. a = b \rightarrow a = c \rightarrow z \vee (a \wedge b) = z \vee (a \wedge c)$
end

thm =
$\lambda z.$let lem = $\lambda x \lambda y \lambda P.\mathsf{cong}_{\vee}\mathsf{cong}_{\wedge} P : \forall x, y.\ x = y \ \rightarrow\ z \vee (x \wedge x) = z \vee (x \wedge y)$
in
$\lambda a \lambda b \lambda c \lambda Q \lambda R.\mathsf{trans}\ (\mathsf{sym}\ (\mathsf{lem}\ Q))\ (\mathsf{lem}\ R) \quad : \quad \forall z, a, b, c.\ a = b \ \rightarrow\ a = c \ \rightarrow\ z \vee (a \wedge b) = z \vee (a \wedge c)$
end

- Motivation
- Related Work
- Proof System
- Example
- Conclusions/Future Work

Library Structuring

- Structure reflects similarity of theorems
- Group based on shared variables, assumptions, and lemmas
- Ease in maintaining modularity
- Break down larger libraries naturally

Heuristics

- Makes proof similarities more apparent
- Prefer lemmas to theorems when possible
- *Proof Refactorization*: Detect similar subproofs and make them lemmas (common subexpression elimination)

Implementation

- Java implementation for Kleene algebra with tests
- Uses tree structure with natural correspondence to let expressions
- Graphical representation of library
- Ability to manipulate structure in GUI to see different relations
- Manipulations guided by strong underlying formalism