Reliable Analysis of Conditional Term Rewrite Systems[1]

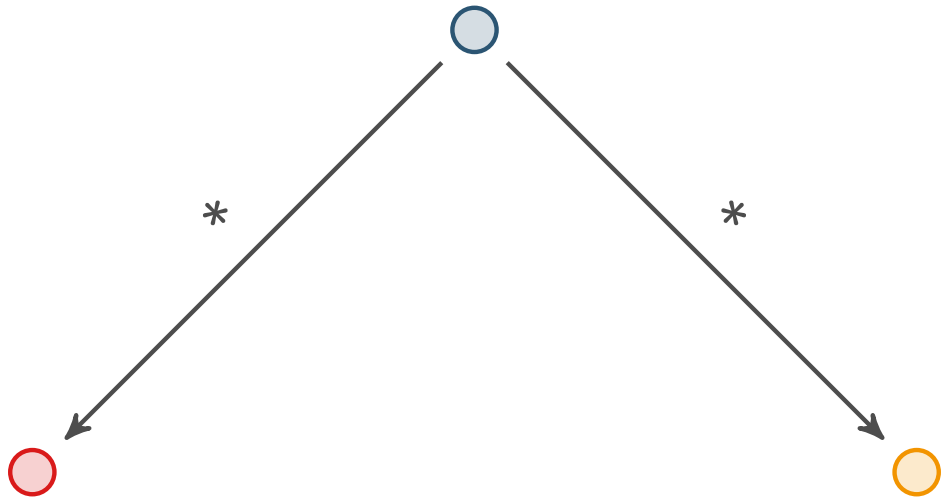
Christian Sternagel and Thomas Sternagel

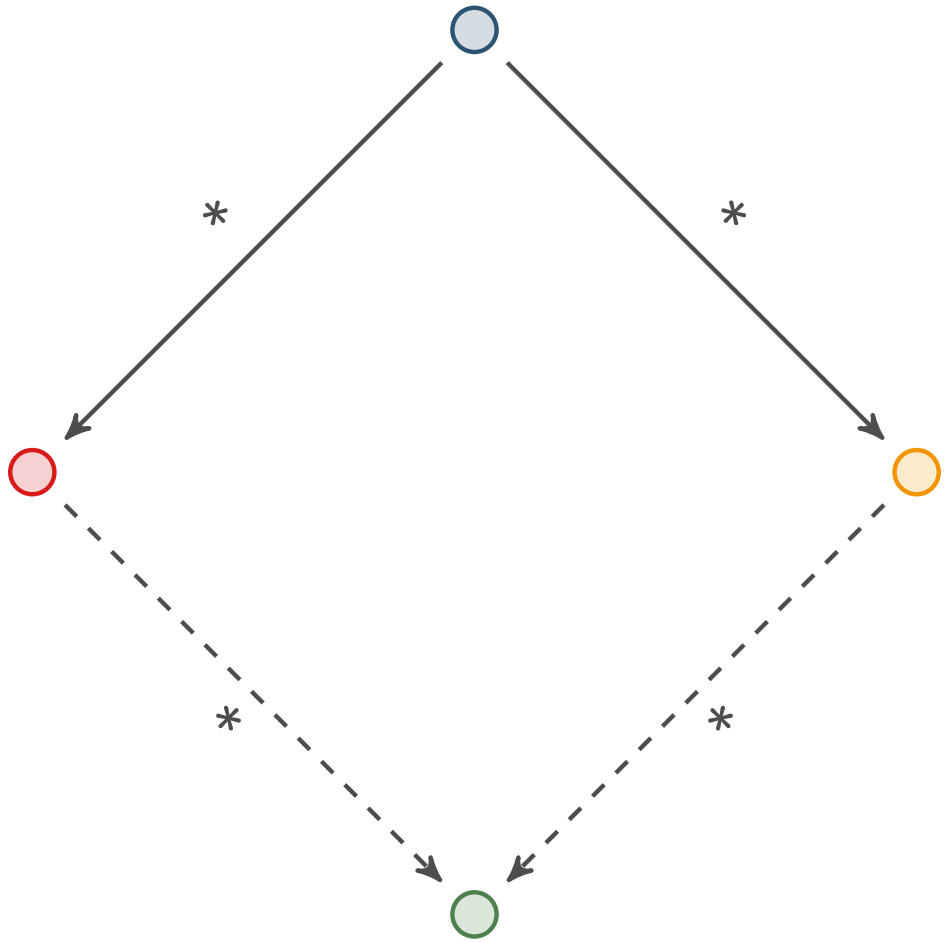
Computational Logic Group, University of Innsbruck

Valencia March 8, 2017

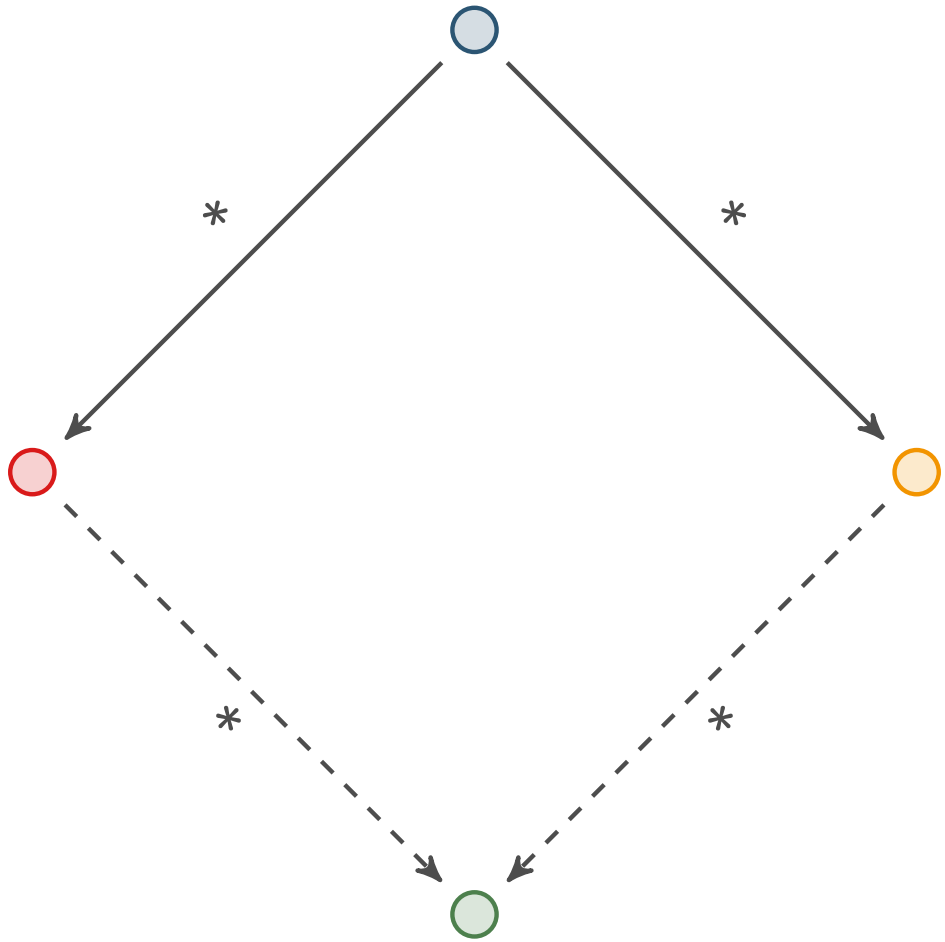
[1]Supported by the Austrian Science Fund (FWF): P27502

Termination





Confluence



Termination

result in finite time

Confluence

same result for same input

Undecidable Decision Problems

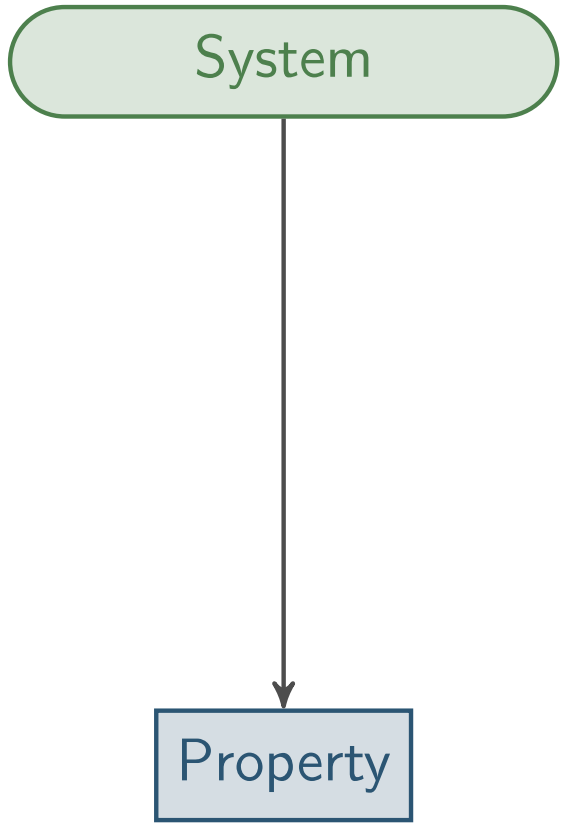
Termination

result in finite time

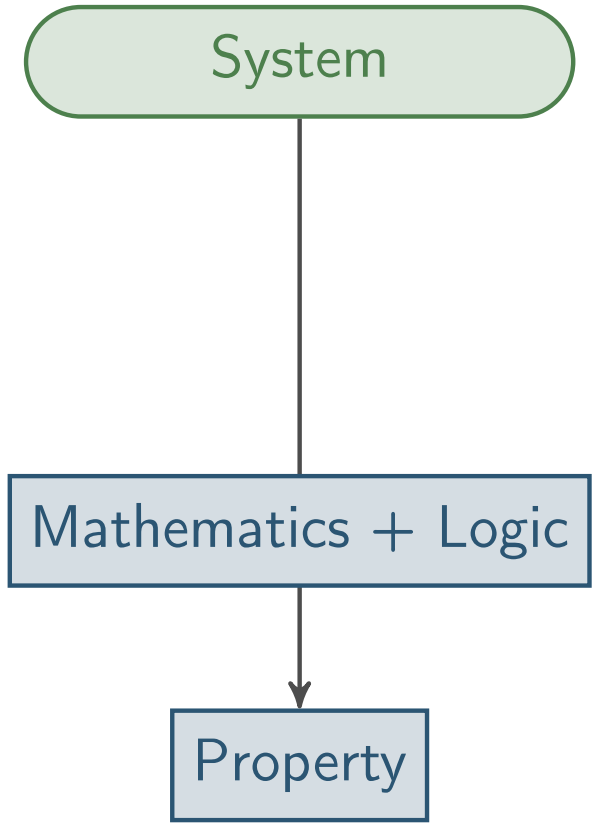
Confluence

same result for same input

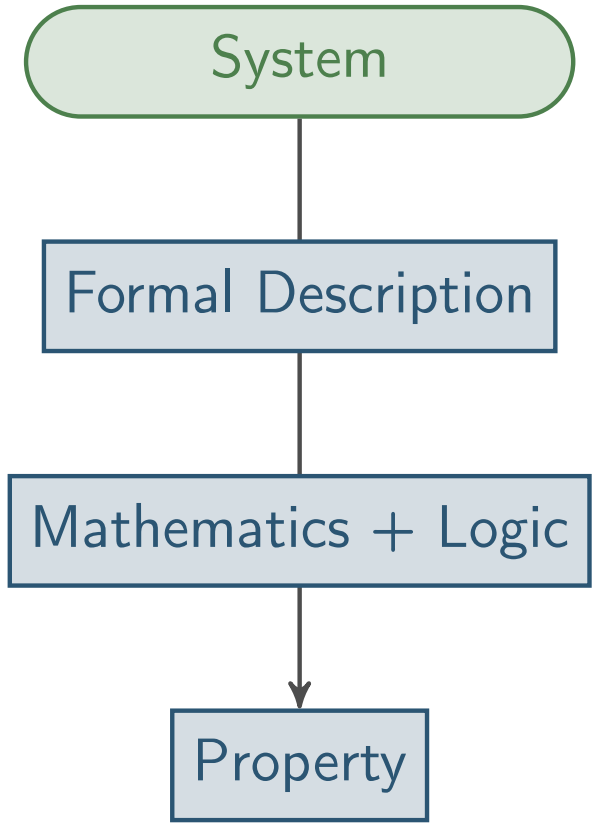
Formal Verification



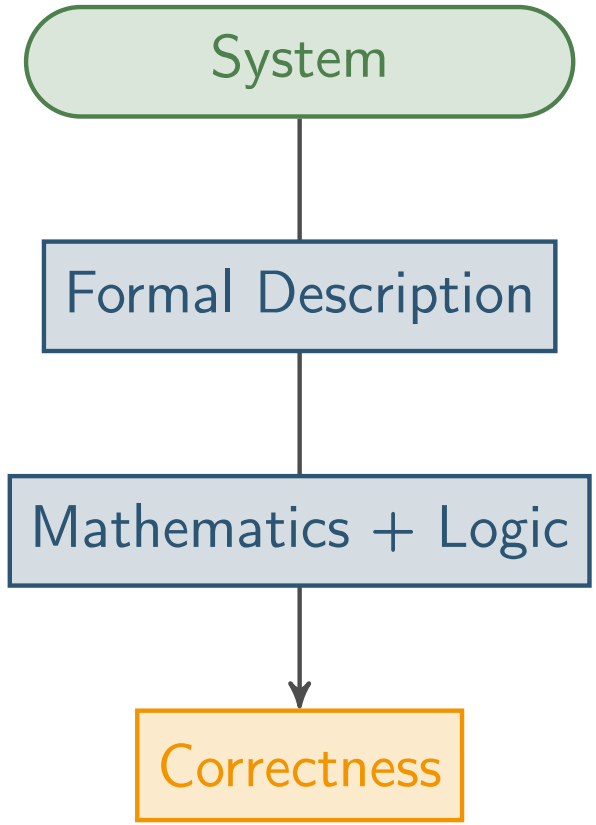
Formal Verification



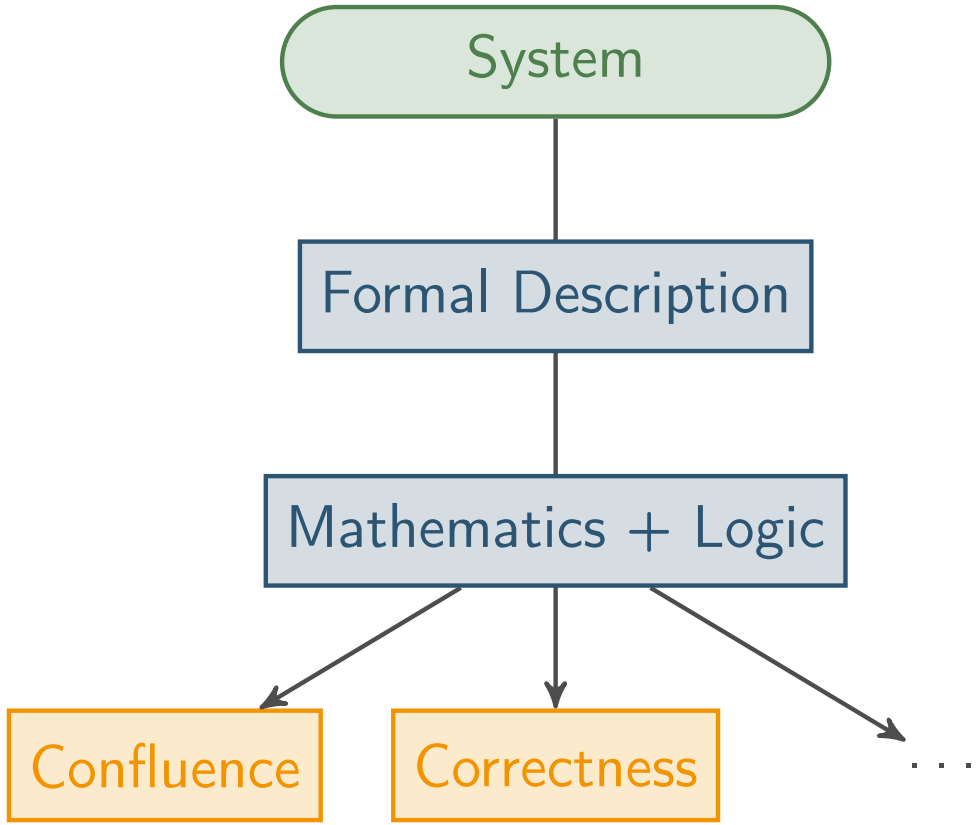
Formal Verification



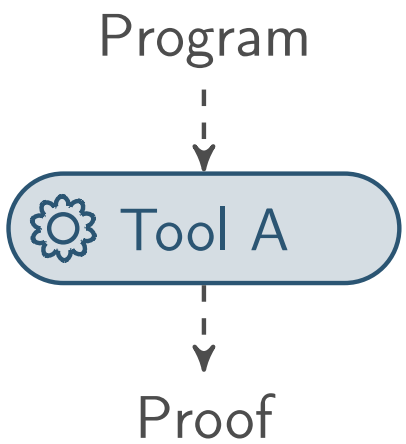
Formal Verification



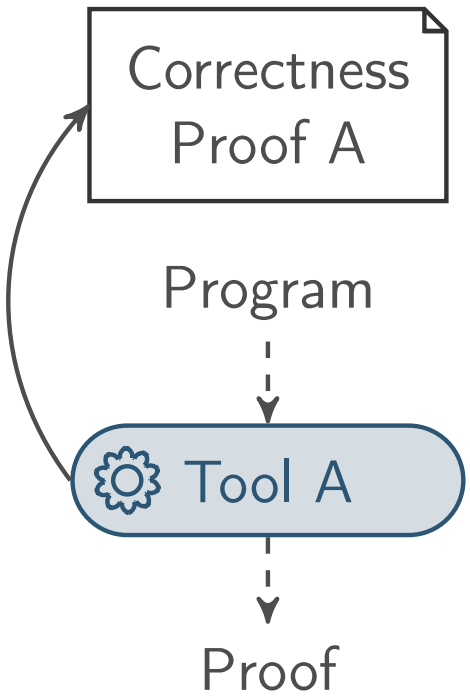
Formal Verification



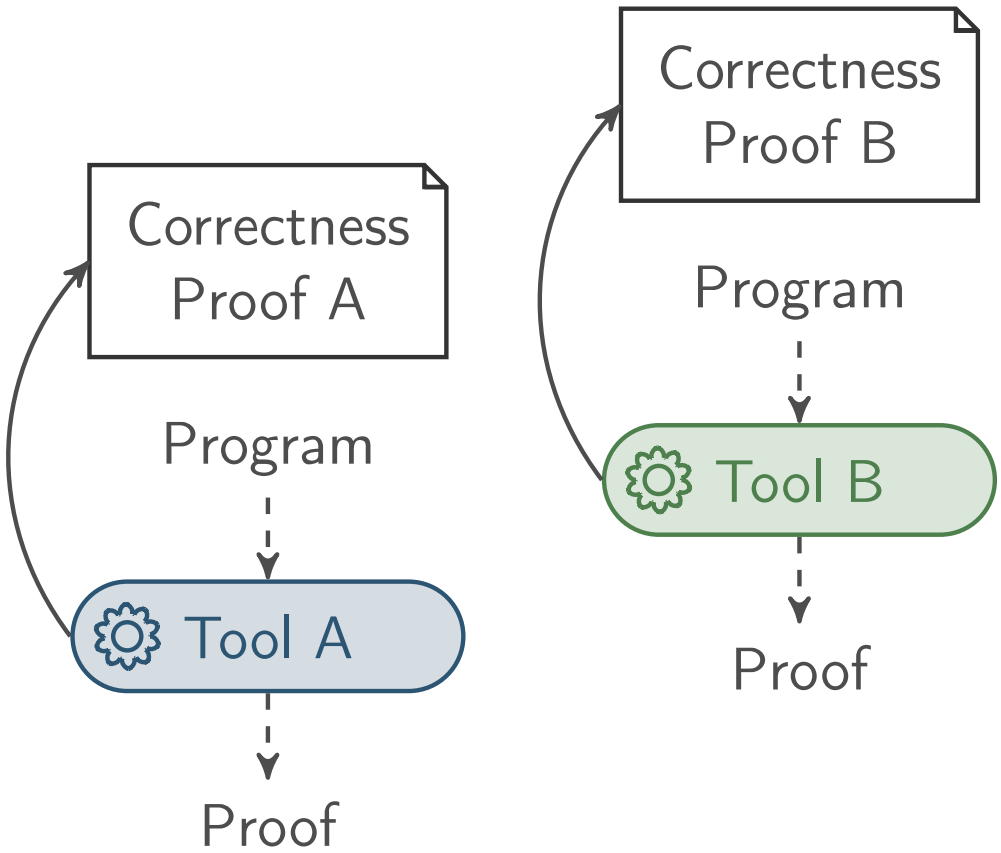
Automation



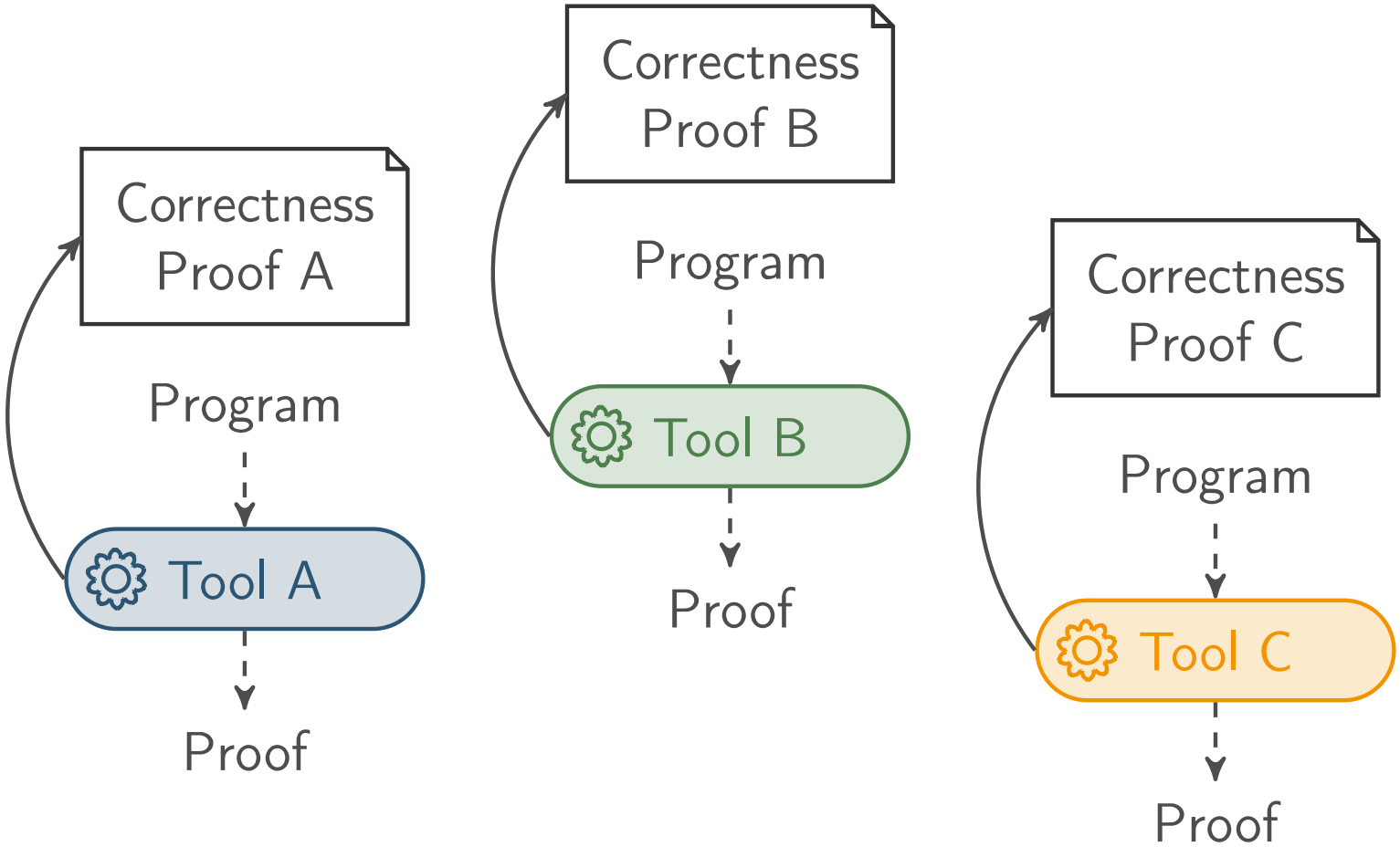
Automation



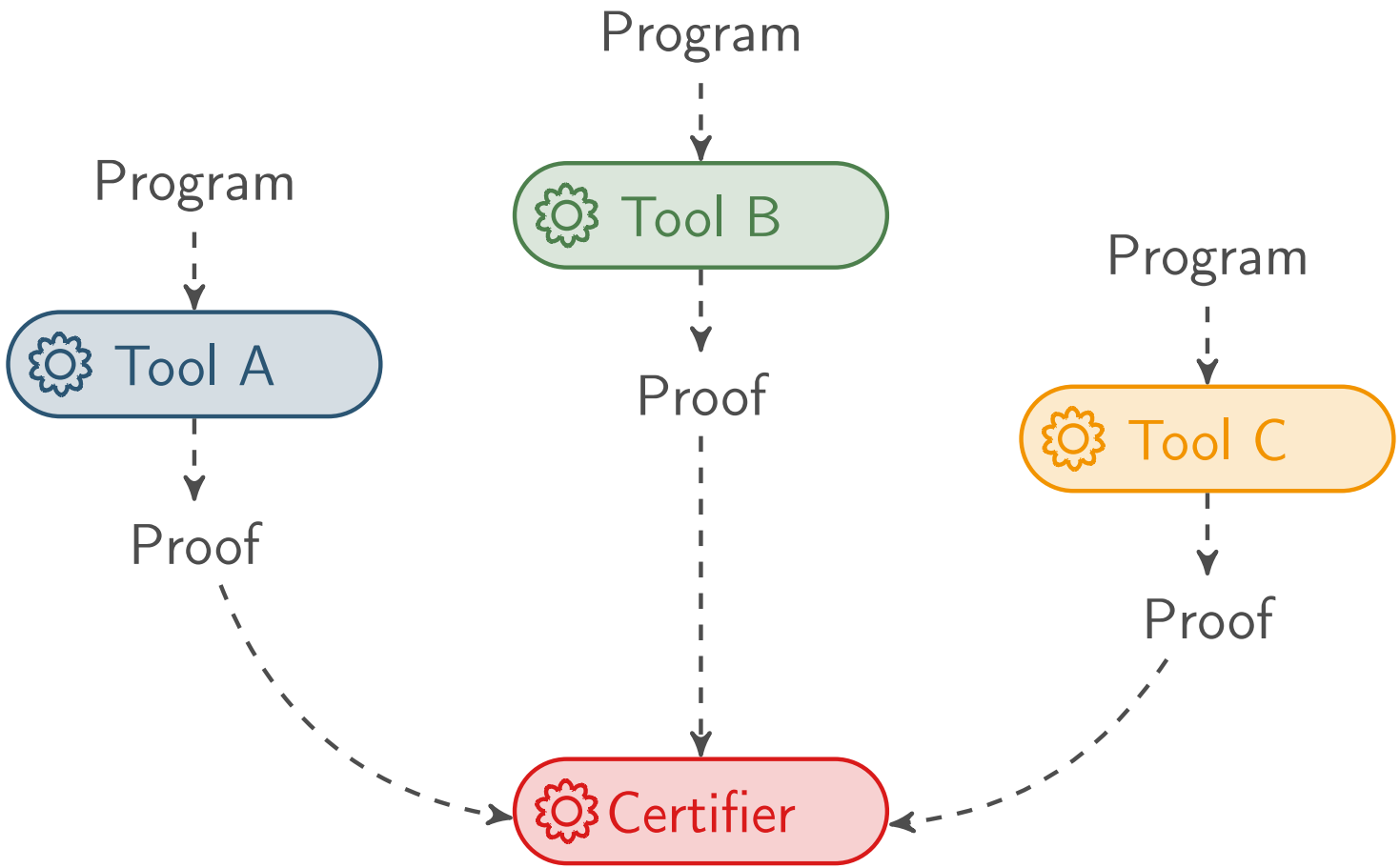
Automation


Correctness
Proof A
Program
Tool A
Proof
Correctness
Proof B
Program
Tool B
Proof

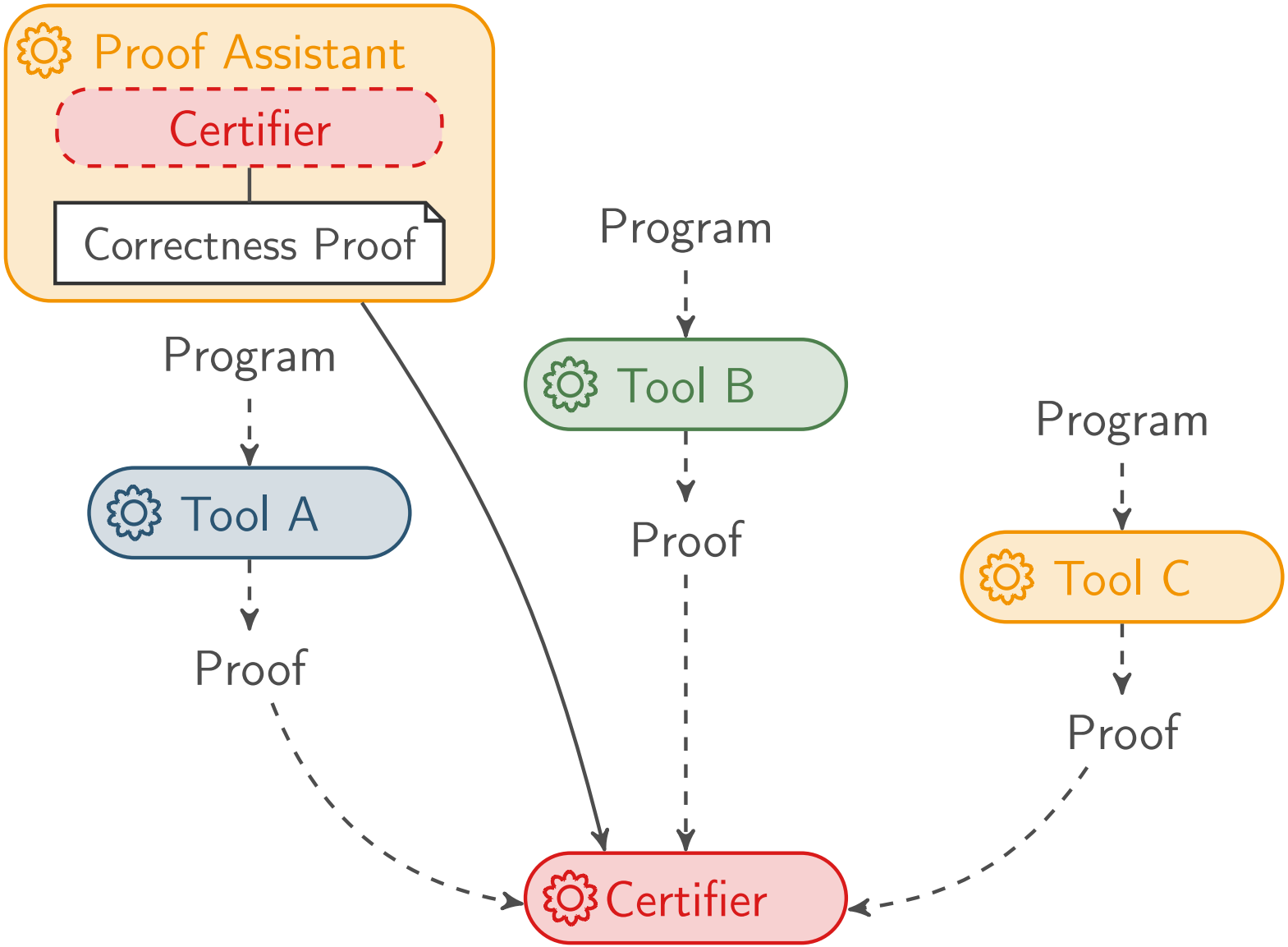
Automation


Correctness
Proof A
Program
Tool A
Proof
Correctness
Proof B
Program
Tool B
Proof
Correctness
Proof C
Program
Tool C
Proof

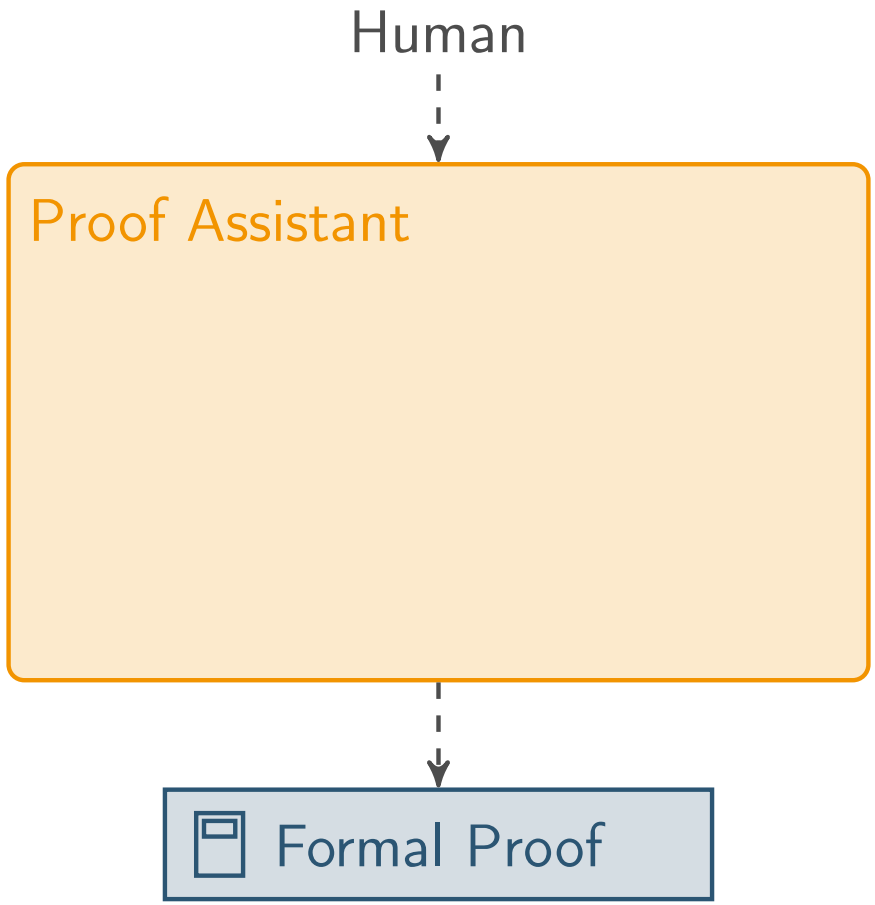
Automation


Program
Tool A
Proof
Program
Tool B
Proof
Program
Tool C
Proof
Certifier

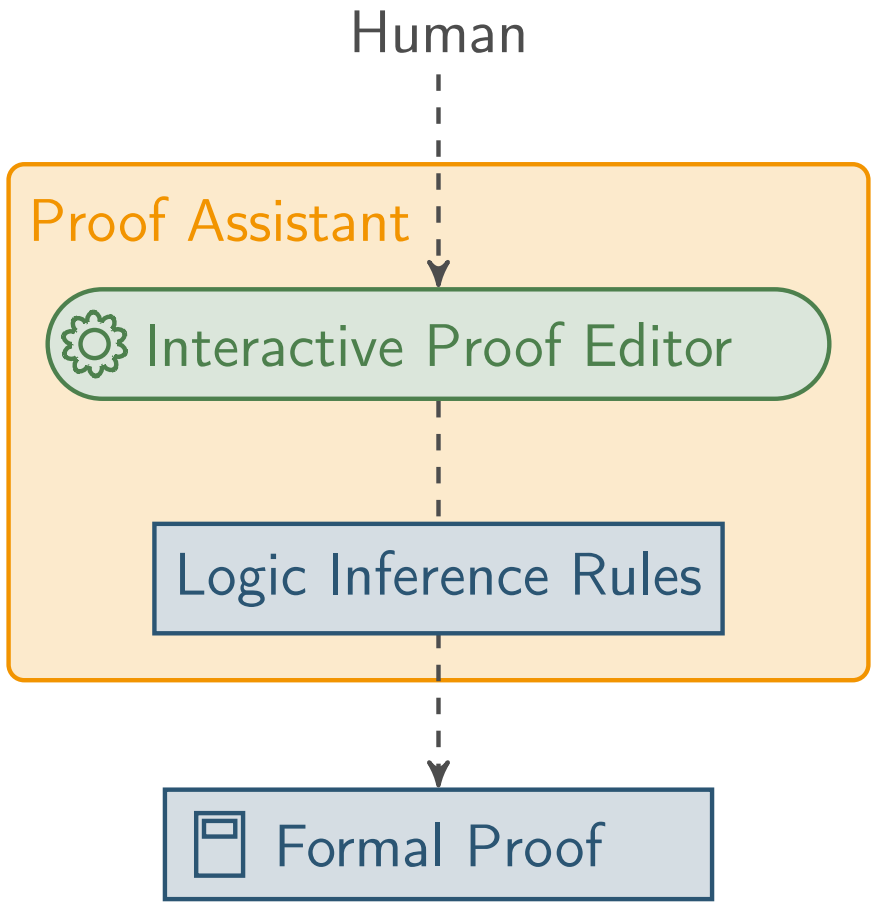
Automation


Proof Assistant
Certifier
Correctness Proof
Program
Tool A
Proof
Program
Tool B
Proof
Program
Tool C
Proof
Certifier

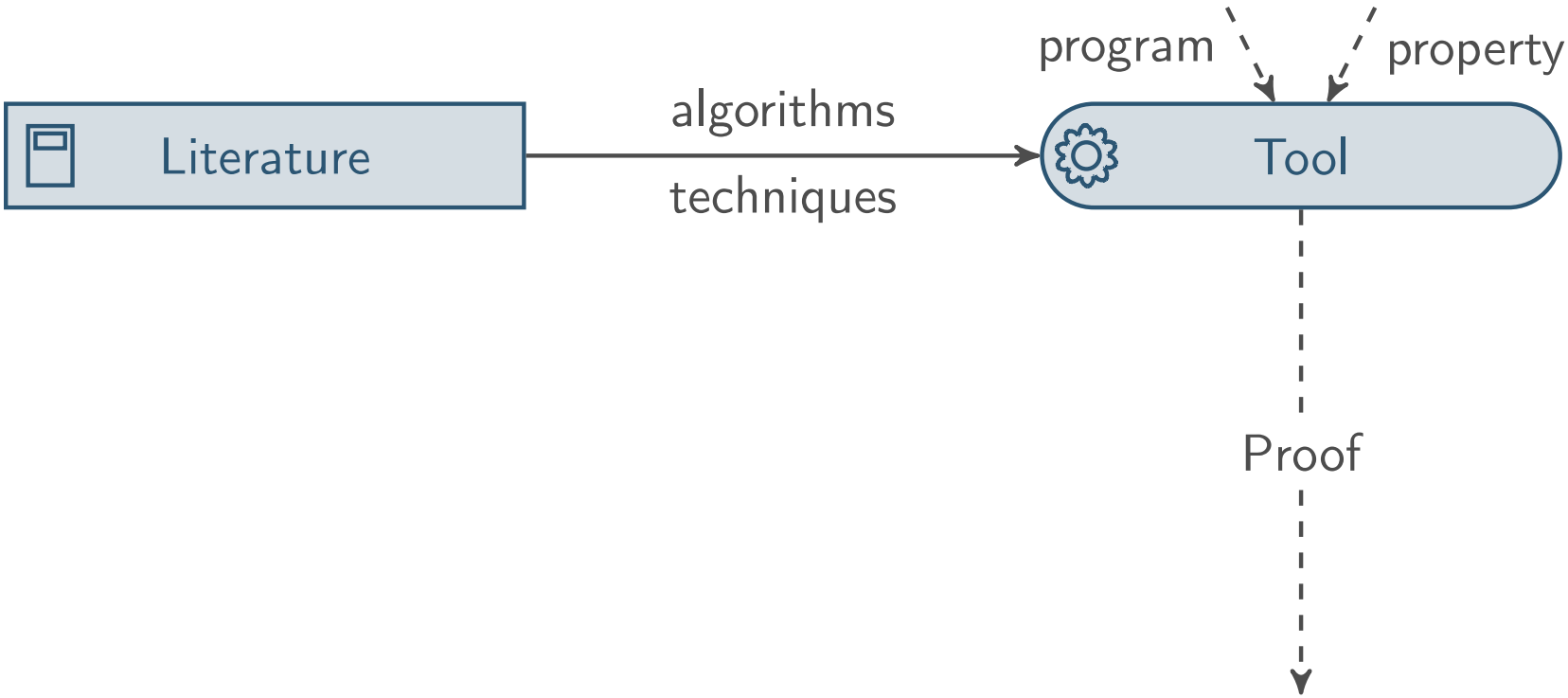
Proof Assistant



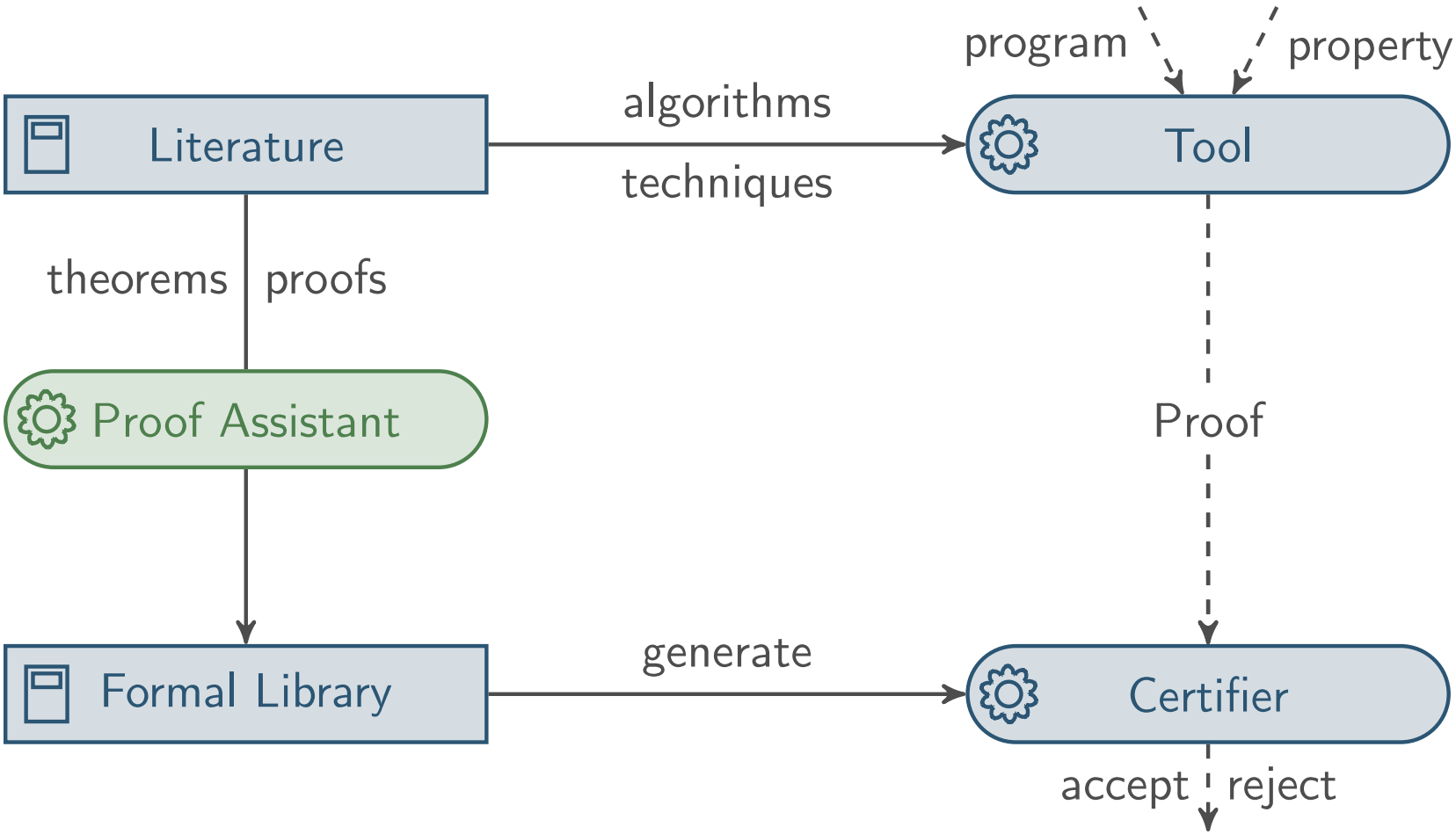
Proof Assistant



Putting it all together



Putting it all together



Conditional Term Rewriting

```
split x [] = ([], [])
split x (y : ys)
  | x ⩽ y = (xs, y : zs)
  | otherwise = (y : xs, zs)
  where (xs, zs) = split x ys

qsort [] = []
qsort (x : xs) = qsort ys ++ (x : qsort zs)
  where (ys, zs) = split x xs
```

Conditional Term Rewriting

$$
\begin{aligned}
&\mathbf{split}(\mathbf{x},\ [])\ &&\to ([],\ [])\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{xs},\ \mathbf{y} : \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{true},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{y} : \mathbf{xs},\ \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{false},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
\\
&\mathbf{qsort}([])\ &&\to []\\
&\mathbf{qsort}(\mathbf{x} : \mathbf{xs})\ &&\to \mathbf{qsort}(\mathbf{ys}) +\!\!+ (\mathbf{x} : \mathbf{qsort}(\mathbf{zs}))\\
&&&\Leftarrow \mathbf{split}(\mathbf{x},\ \mathbf{xs}) \to (\mathbf{ys},\ \mathbf{zs})
\end{aligned}
$$

Conditional Term Rewriting

$$
\begin{array}{lll}
\mathbf{split}(\mathbf{x},\ [\,]) & \to ([\,],\ [\,]) & \\
\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys}) & \to (\mathbf{xs},\ \mathbf{y} : \mathbf{zs}) & \\
 & \Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{true},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs}) & \\
\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys}) & \to (\mathbf{y} : \mathbf{xs},\ \mathbf{zs}) & \\
 & \Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{false},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs}) & \\
 & & \\
\mathbf{qsort}([\,]) & \to [\,] & \\
\mathbf{qsort}(\mathbf{x} : \mathbf{xs}) & \to \mathbf{qsort}(\mathbf{ys}) +\!\!+ (\mathbf{x} : \mathbf{qsort}(\mathbf{zs})) & \\
 & \Leftarrow \mathbf{split}(\mathbf{x},\ \mathbf{xs}) \to (\mathbf{ys},\ \mathbf{zs}) &
\end{array}
$$

$$\mathbf{qsort}\,(2{:}1{:}[\,]) \ \to$$

Conditional Term Rewriting

$$
\begin{aligned}
&\mathbf{split}(\mathbf{x},\ [])\ &&\to ([],\ [])\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{xs},\ \mathbf{y} : \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{true},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{y} : \mathbf{xs},\ \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{false},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
\\
&\mathbf{qsort}([])\ &&\to []\\
&\mathbf{qsort}(\mathbf{x} : \mathbf{xs})\ &&\to \mathbf{qsort}(\mathbf{ys}) +\!\!+ (\mathbf{x} : \mathbf{qsort}(\mathbf{zs}))\\
&&&\Leftarrow \mathbf{split}(\mathbf{x},\ \mathbf{xs}) \to (\mathbf{ys},\ \mathbf{zs})
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{qsort}\ (2{:}1{:}[])\ \to\\
&\qquad\qquad \mathbf{split}\ (2,\ \ 1{:}[])\ \to
\end{aligned}
$$

Conditional Term Rewriting

$$
\begin{aligned}
&\mathbf{split}(\mathbf{x},\ [])\ &&\to ([],\ [])\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{xs},\ \mathbf{y} : \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{true},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{y} : \mathbf{xs},\ \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{false},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{qsort}([])\ &&\to []\\
&\mathbf{qsort}(\mathbf{x} : \mathbf{xs})\ &&\to \mathbf{qsort}(\mathbf{ys}) +\!\!+ (\mathbf{x} : \mathbf{qsort}(\mathbf{zs}))\\
&&&\Leftarrow \mathbf{split}(\mathbf{x},\ \mathbf{xs}) \to (\mathbf{ys},\ \mathbf{zs})
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{qsort}\,(2{:}1{:}[])\ \to\\
&\qquad\mathbf{split}\,(2,\ \ 1{:}[])\ \to\\
&\qquad\qquad 2 \leqslant 1 \to \mathbf{false},\\
&\qquad\qquad \mathbf{split}\,(2,\ \ [])\ \to ([],\ [])
\end{aligned}
$$

Conditional Term Rewriting

$$
\begin{aligned}
&\mathbf{split}(\mathbf{x},\ [])\ &&\to ([],\ [])\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{xs},\ \mathbf{y} : \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{true},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{y} : \mathbf{xs},\ \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{false},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{qsort}([])\ &&\to []\\
&\mathbf{qsort}(\mathbf{x} : \mathbf{xs})\ &&\to \mathbf{qsort}(\mathbf{ys}) +\!\!+ (\mathbf{x} : \mathbf{qsort}(\mathbf{zs}))\\
&&&\Leftarrow \mathbf{split}(\mathbf{x},\ \mathbf{xs}) \to (\mathbf{ys},\ \mathbf{zs})
\end{aligned}
$$

$$
\begin{aligned}
&\mathbf{qsort}\,(2{:}1{:}[])\ \to\\
&\qquad\qquad \mathbf{split}\,(2,\ \ 1{:}[])\ \to (1{:}[],\ [])
\end{aligned}
$$

Conditional Term Rewriting

$$
\begin{aligned}
&\mathbf{split}(\mathbf{x},\ [])\ &&\to ([],\ [])\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{xs},\ \mathbf{y} : \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{true},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{y} : \mathbf{xs},\ \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{false},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
\\
&\mathbf{qsort}([])\ &&\to []\\
&\mathbf{qsort}(\mathbf{x} : \mathbf{xs})\ &&\to \mathbf{qsort}(\mathbf{ys}) +\!\!+ (\mathbf{x} : \mathbf{qsort}(\mathbf{zs}))\\
&&&\Leftarrow \mathbf{split}(\mathbf{x},\ \mathbf{xs}) \to (\mathbf{ys},\ \mathbf{zs})
\end{aligned}
$$

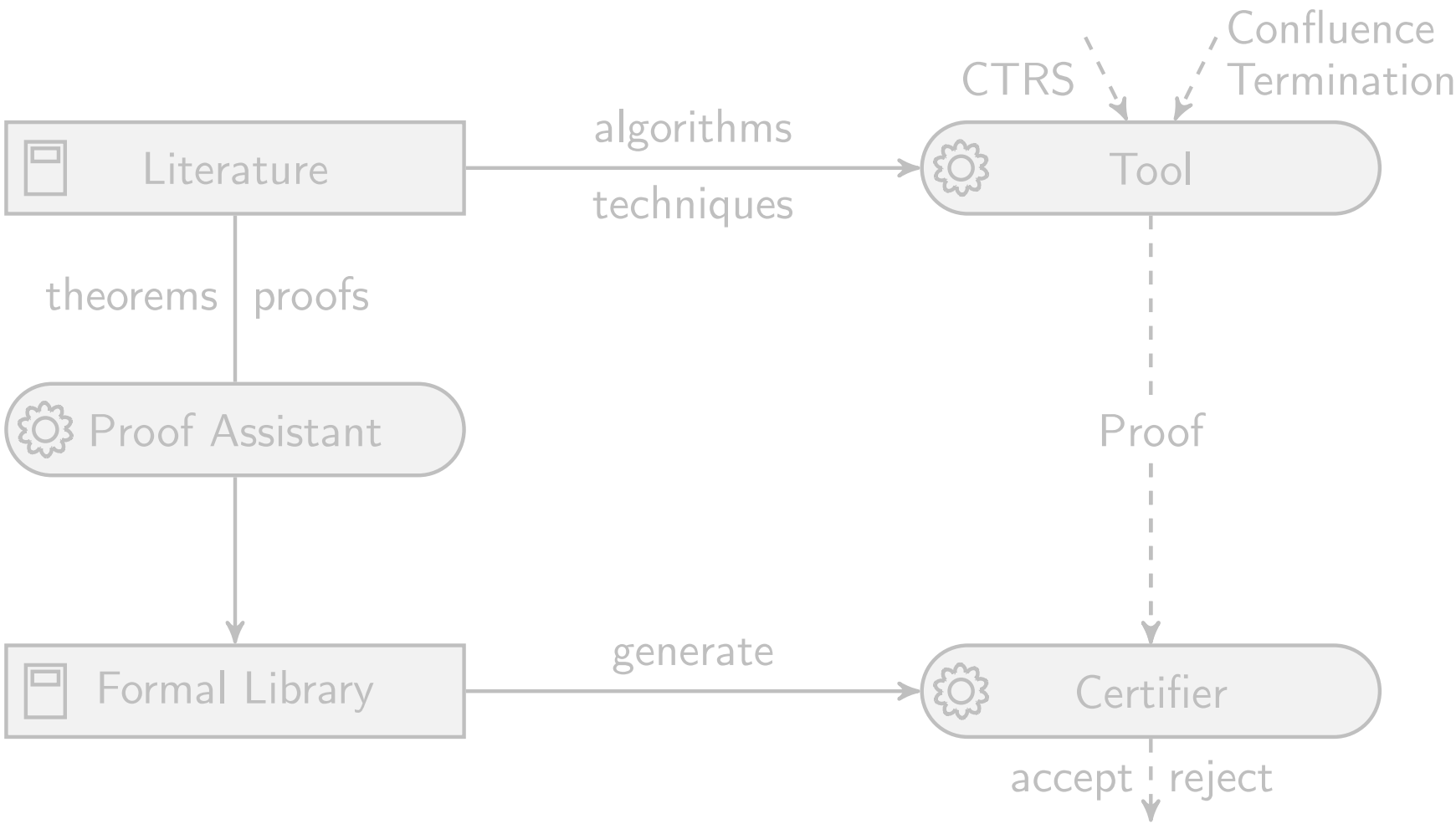
$$
\mathbf{qsort}\,(2{:}1{:}[])\ \to \mathbf{qsort}(1{:}[]) +\!\!+ (2{:}\mathbf{qsort}([]))
$$

Conditional Term Rewriting

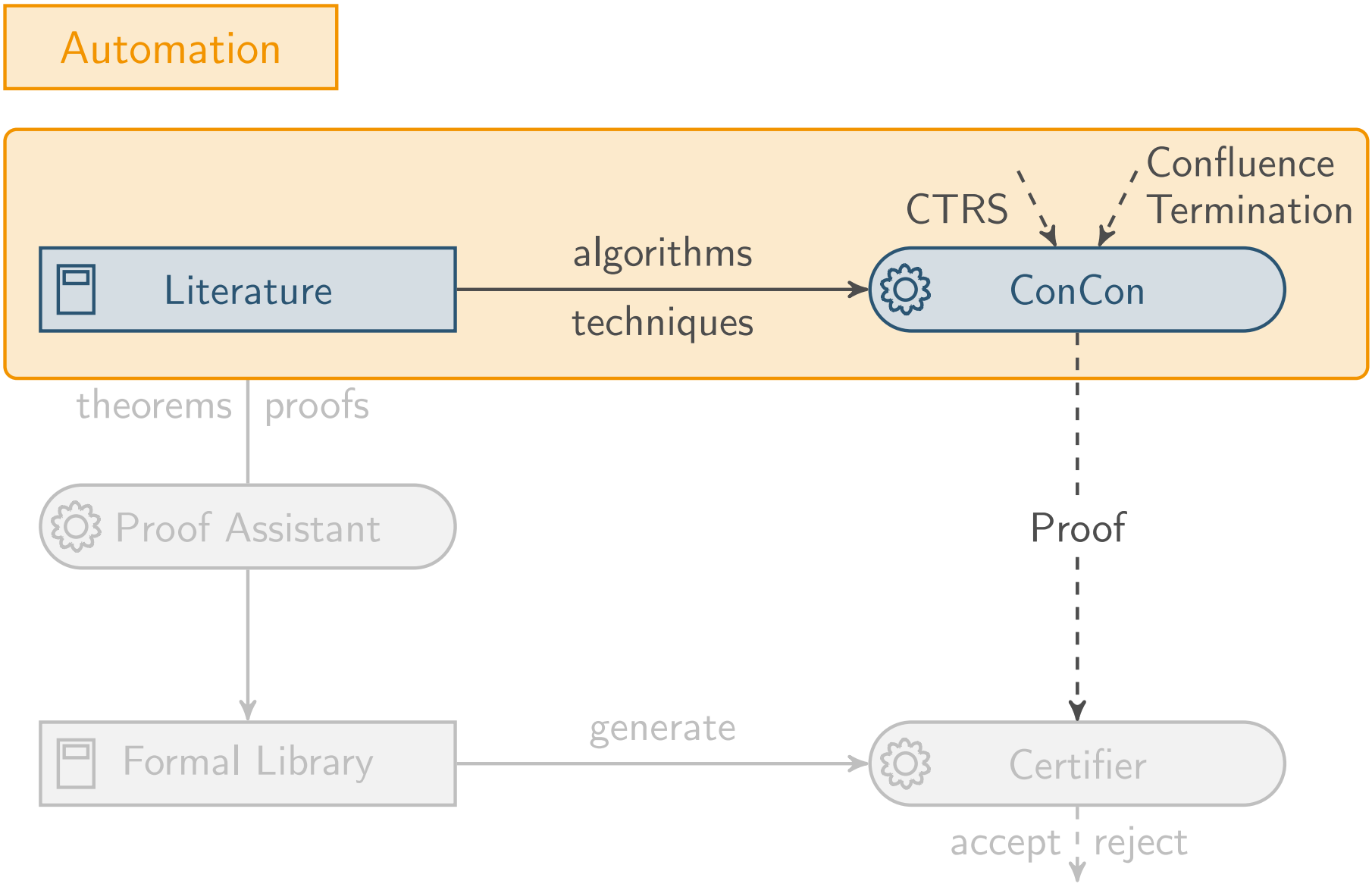
$$
\begin{aligned}
&\mathbf{split}(\mathbf{x},\ [])\ &&\to ([],\ [])\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{xs},\ \mathbf{y} : \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{true},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
&\mathbf{split}(\mathbf{x},\ \mathbf{y} : \mathbf{ys})\ &&\to (\mathbf{y} : \mathbf{xs},\ \mathbf{zs})\\
&&&\Leftarrow \mathbf{x} \leqslant \mathbf{y} \to \mathbf{false},\ \mathbf{split}(\mathbf{x},\ \mathbf{ys}) \to (\mathbf{xs},\ \mathbf{zs})\\
\\
&\mathbf{qsort}([])\ &&\to []\\
&\mathbf{qsort}(\mathbf{x} : \mathbf{xs})\ &&\to \mathbf{qsort}(\mathbf{ys}) +\!\!+ (\mathbf{x} : \mathbf{qsort}(\mathbf{zs}))\\
&&&\Leftarrow \mathbf{split}(\mathbf{x},\ \mathbf{xs}) \to (\mathbf{ys},\ \mathbf{zs})
\end{aligned}
$$

$$
\mathbf{qsort}\,(2{:}1{:}[]) \ \to \mathbf{qsort}(1{:}[]) +\!\!+ (2{:}\mathbf{qsort}([])) \to \cdots \to 1{:}2{:}[]
$$

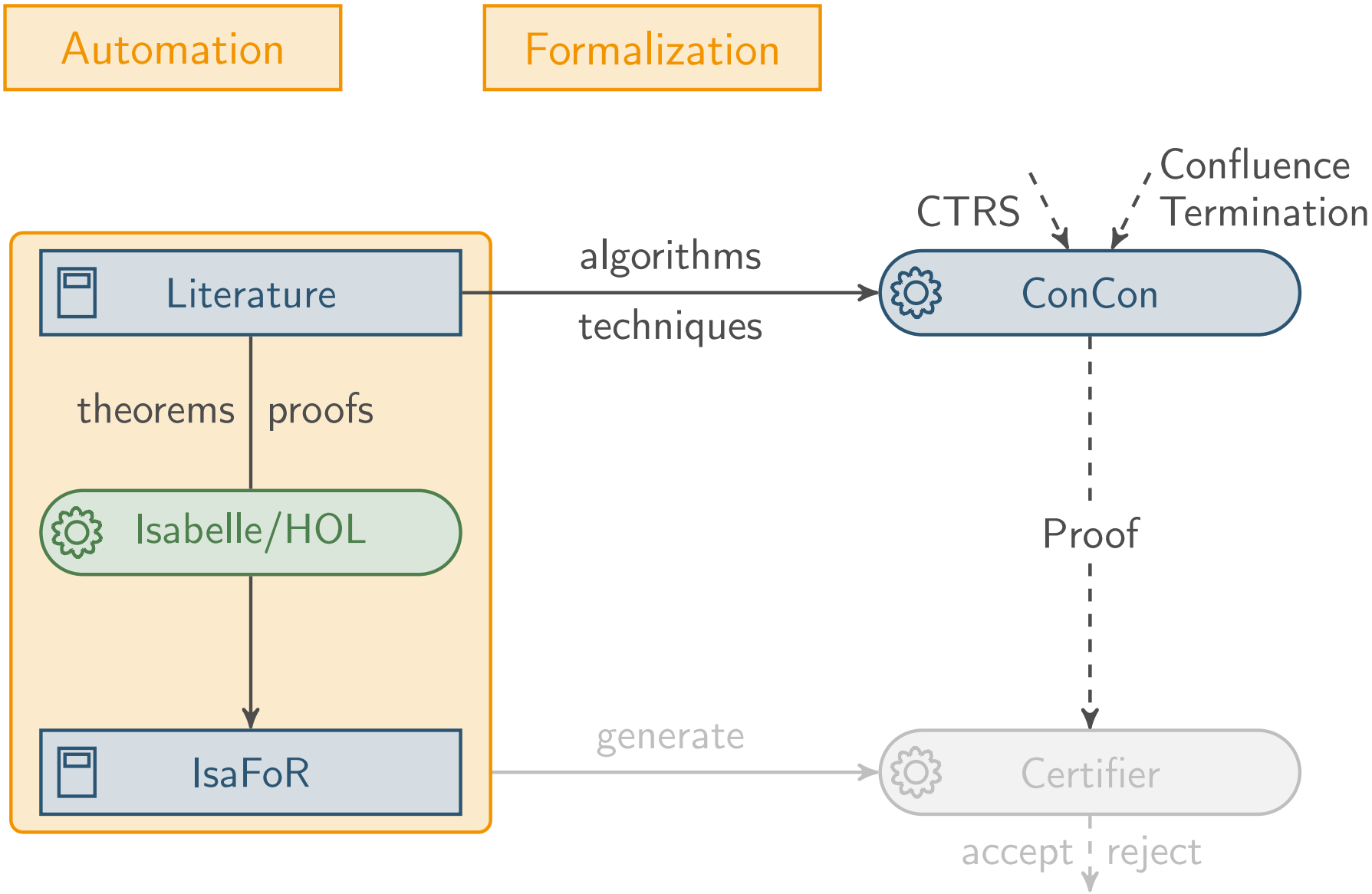
Our Contribution - Overview



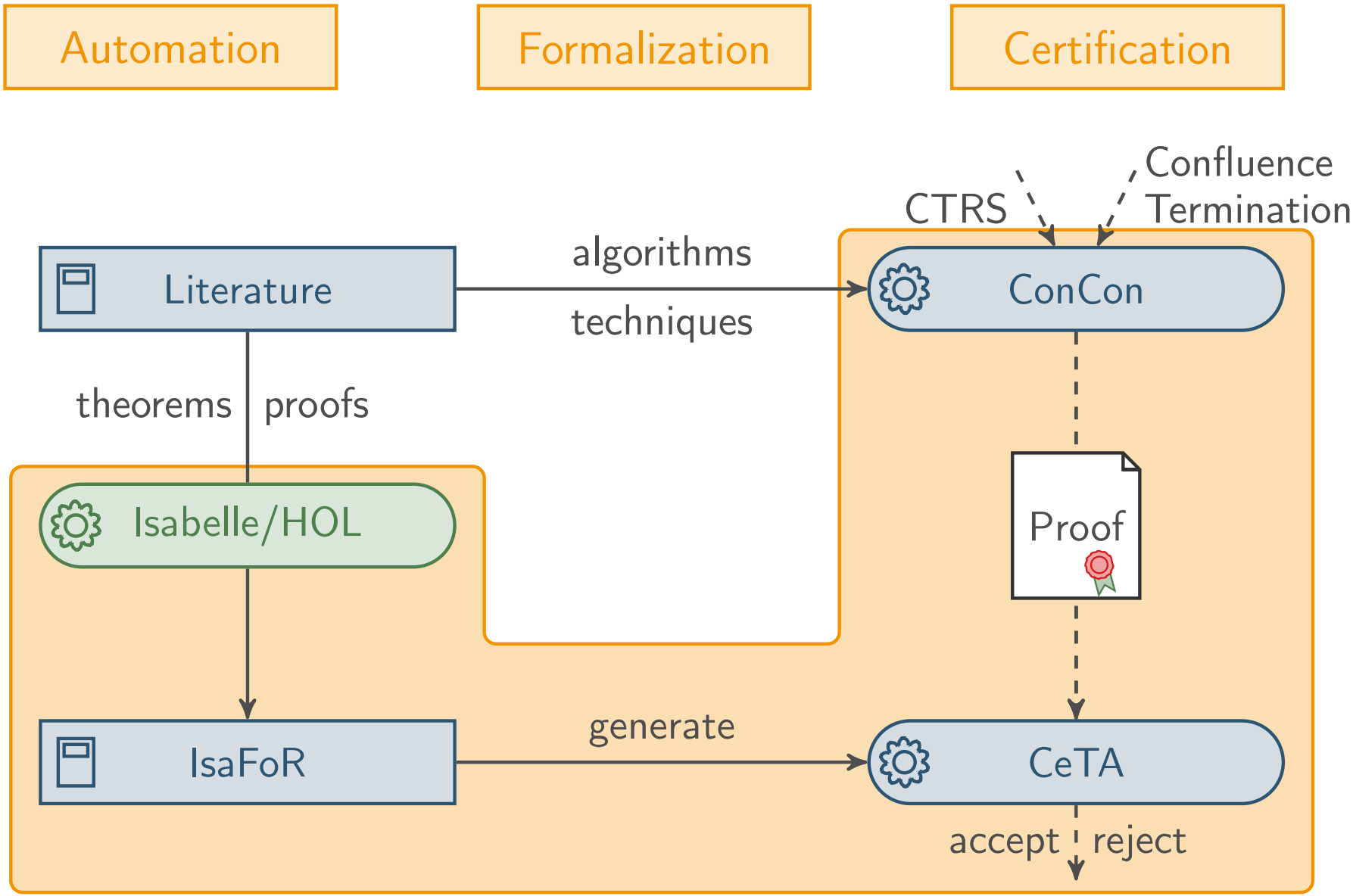
Our Contribution - Overview



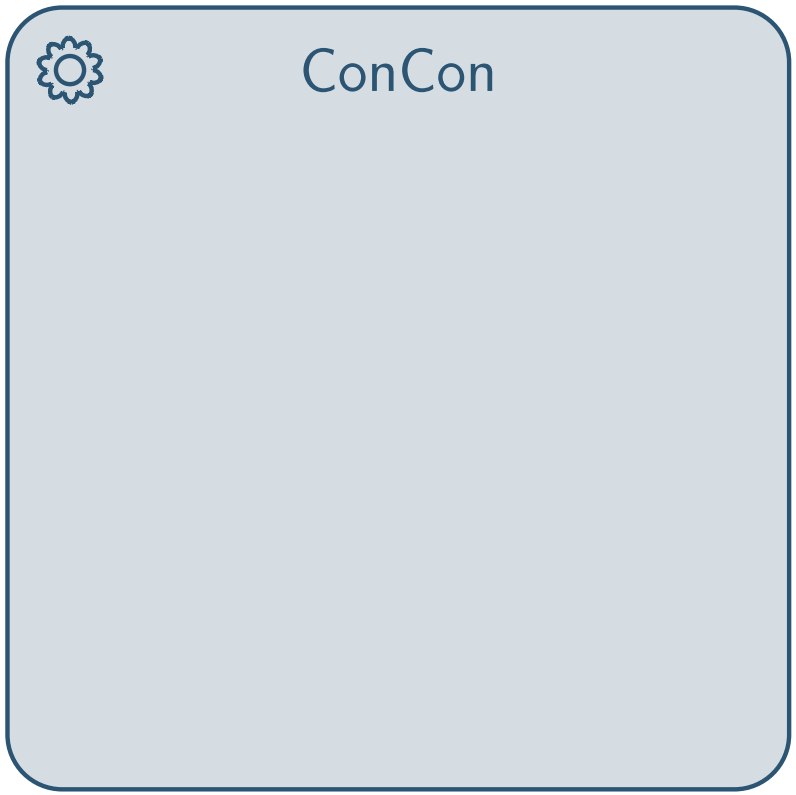
Our Contribution - Overview



Our Contribution - Overview

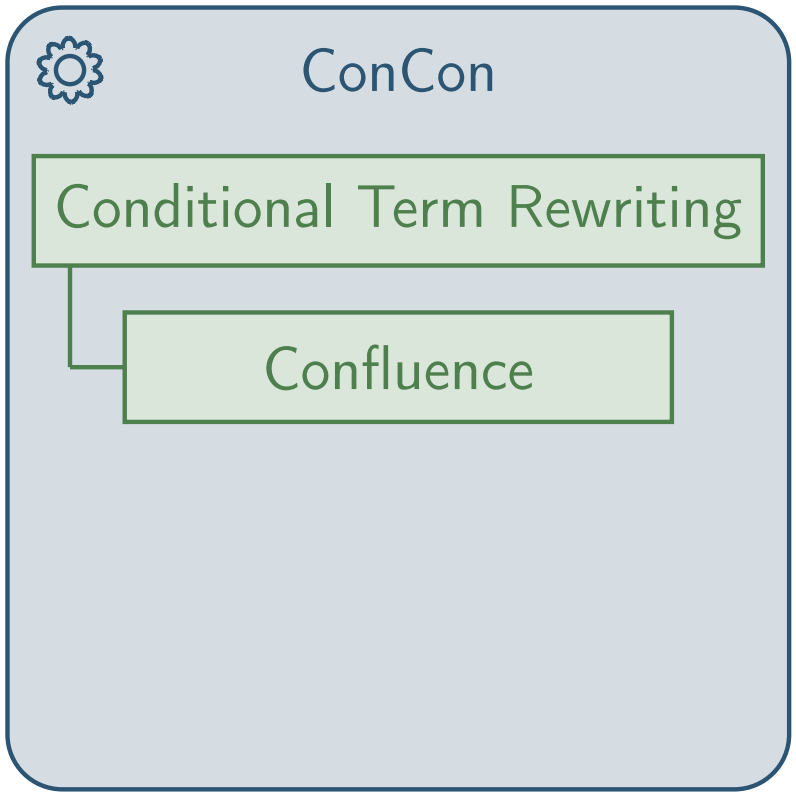


Our Contribution I - Automation

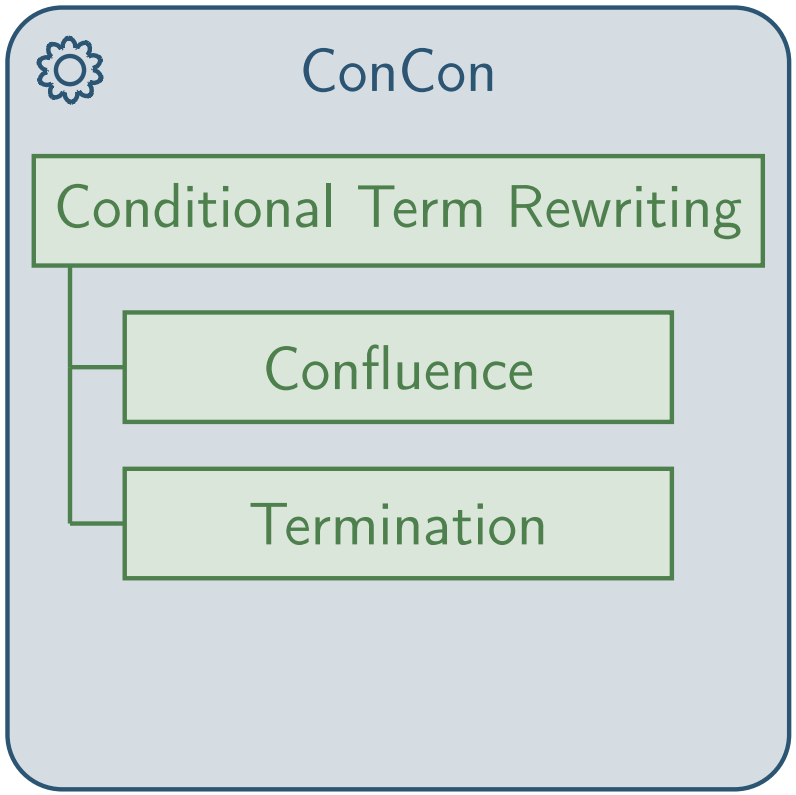


Our Contribution I - Automation

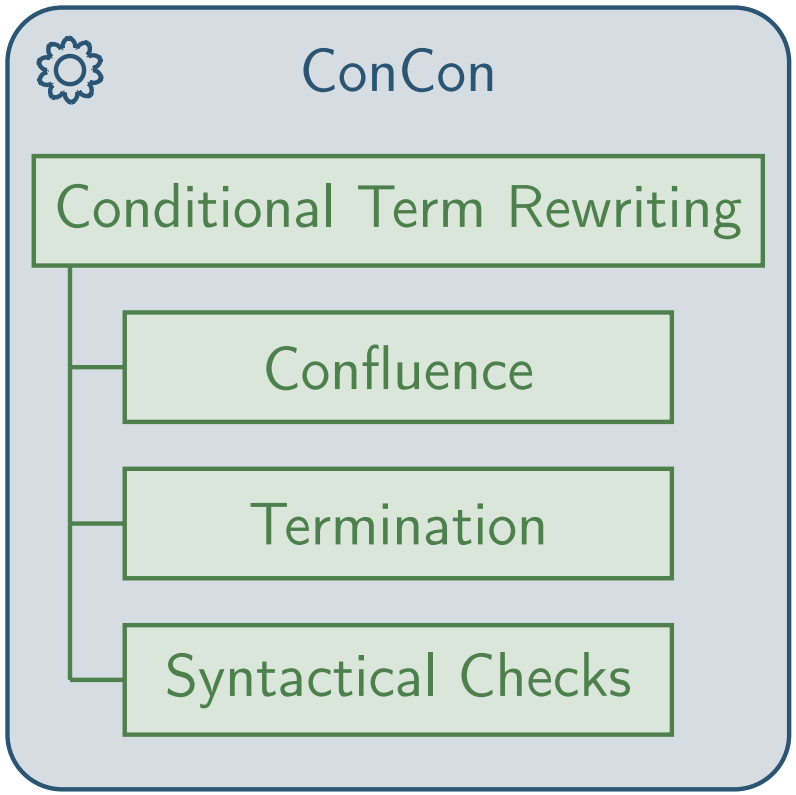
Our Contribution I - Automation



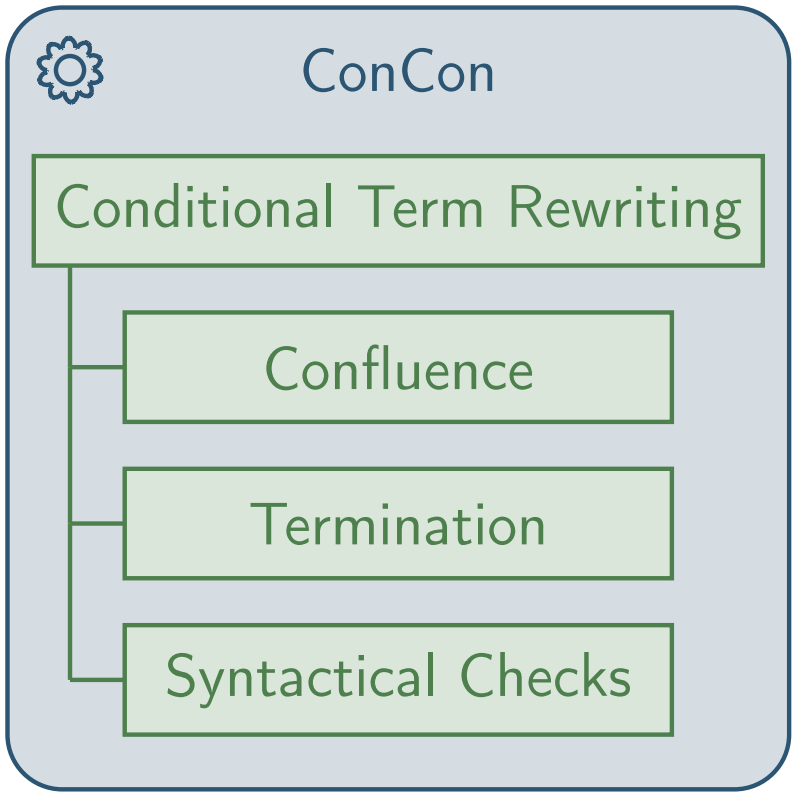
Our Contribution I - Automation



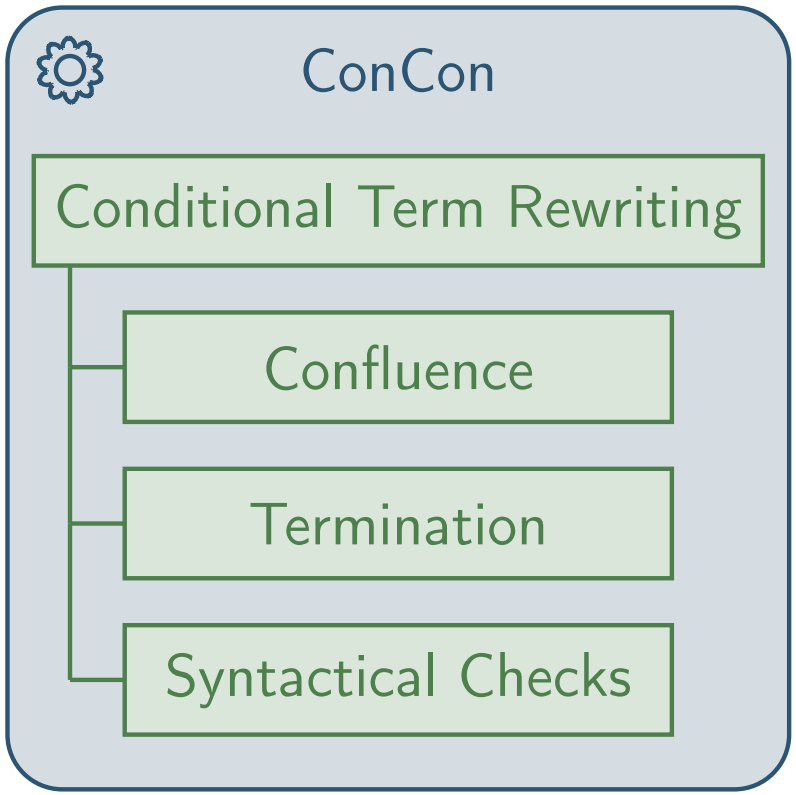
Our Contribution I - Automation



Our Contribution I - Automation



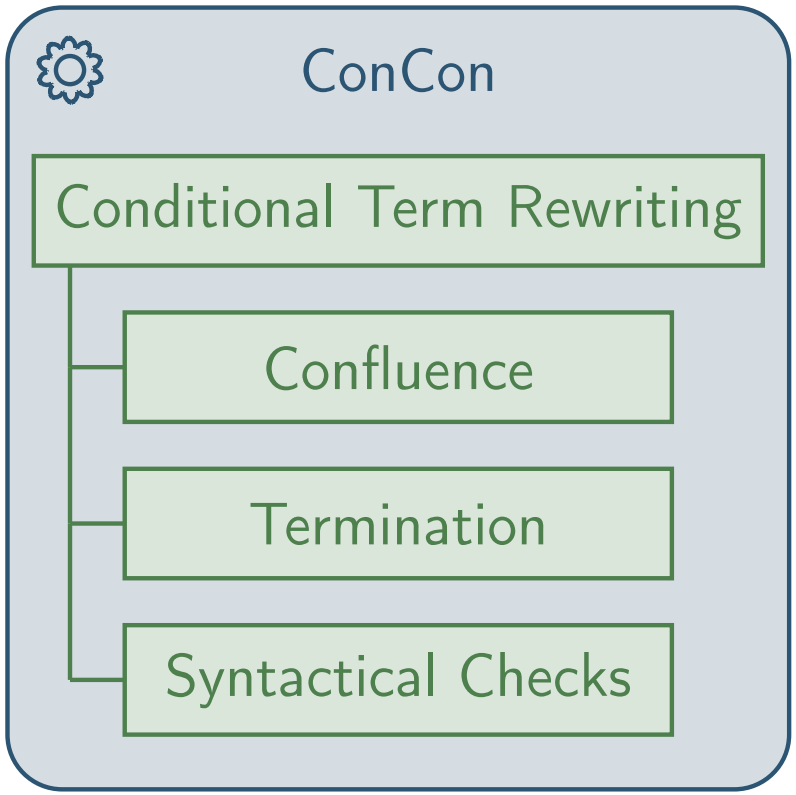
Our Contribution I - Automation



Scala

LGPL
Free Software
Free as in Freedom

Our Contribution I - Automation

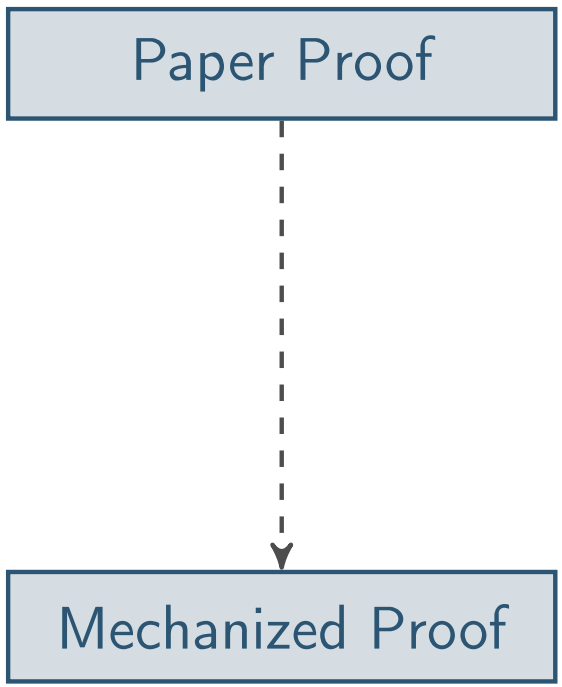


Our Contribution II - Formalization

Our Contribution II - Formalization

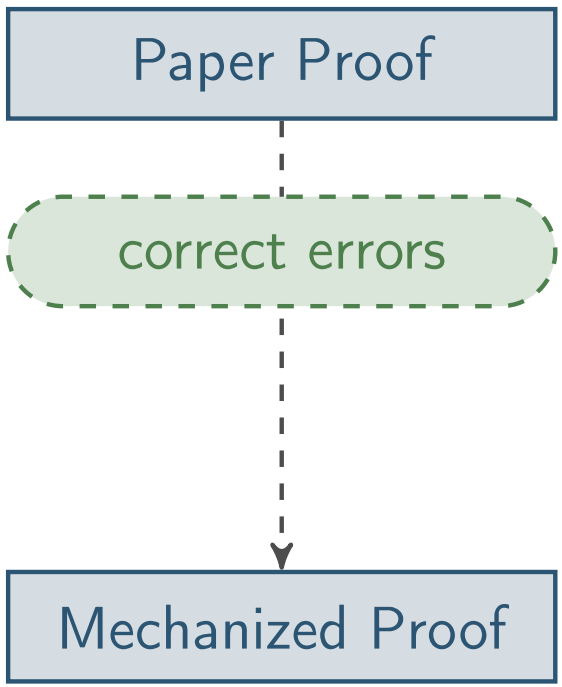
Our Contribution II - Formalization

Challenges



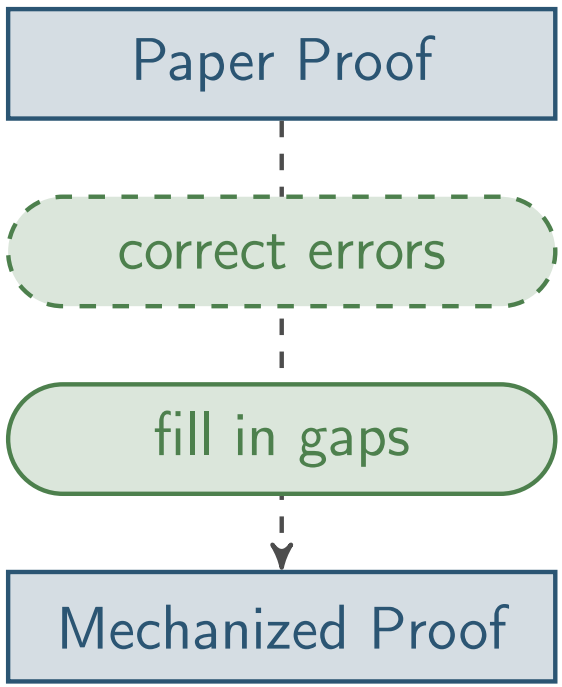
Our Contribution II - Formalization

Challenges



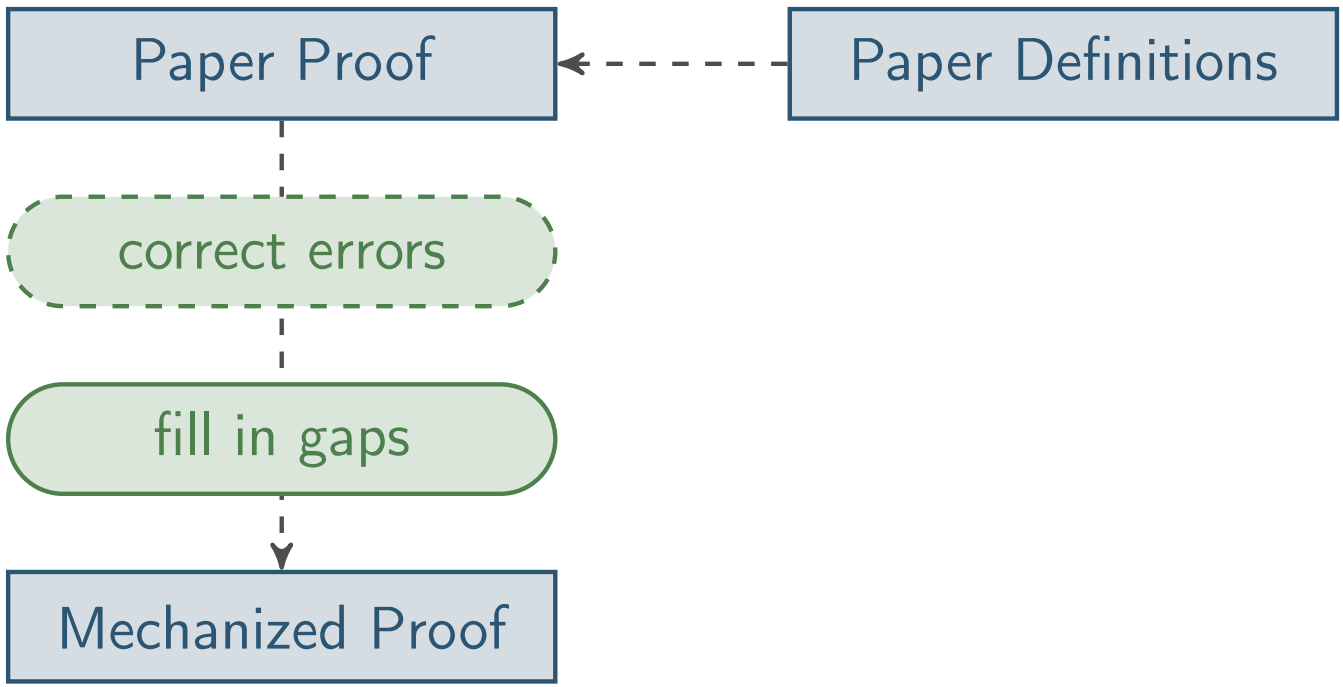
Our Contribution II - Formalization

Challenges



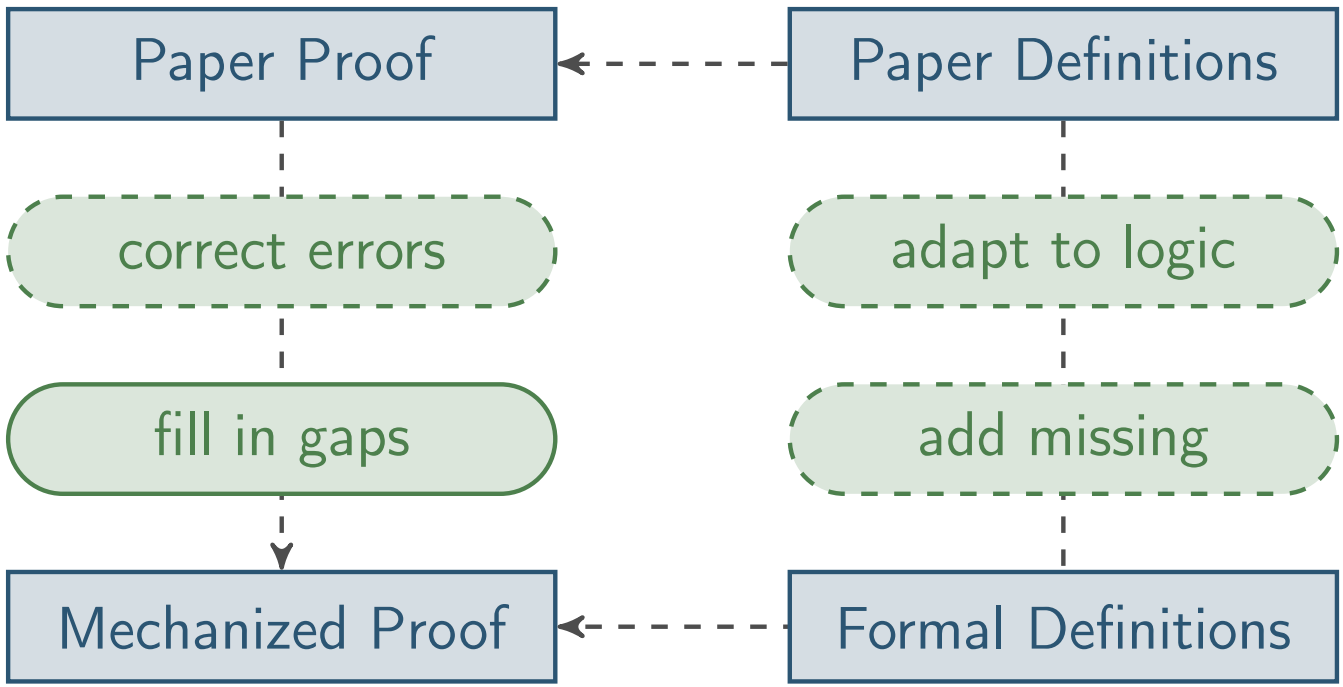
Our Contribution II - Formalization

Challenges



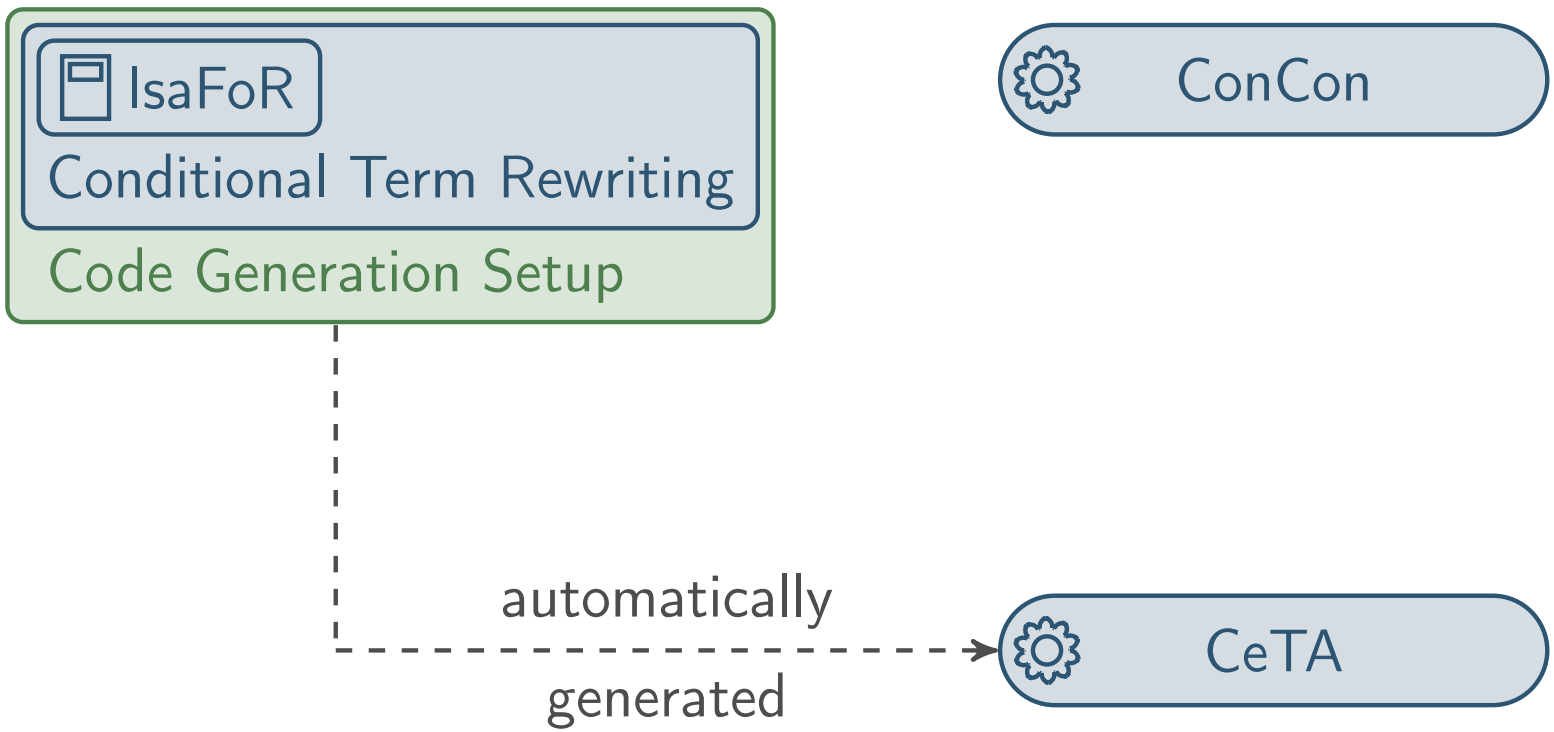
Our Contribution II - Formalization

Challenges

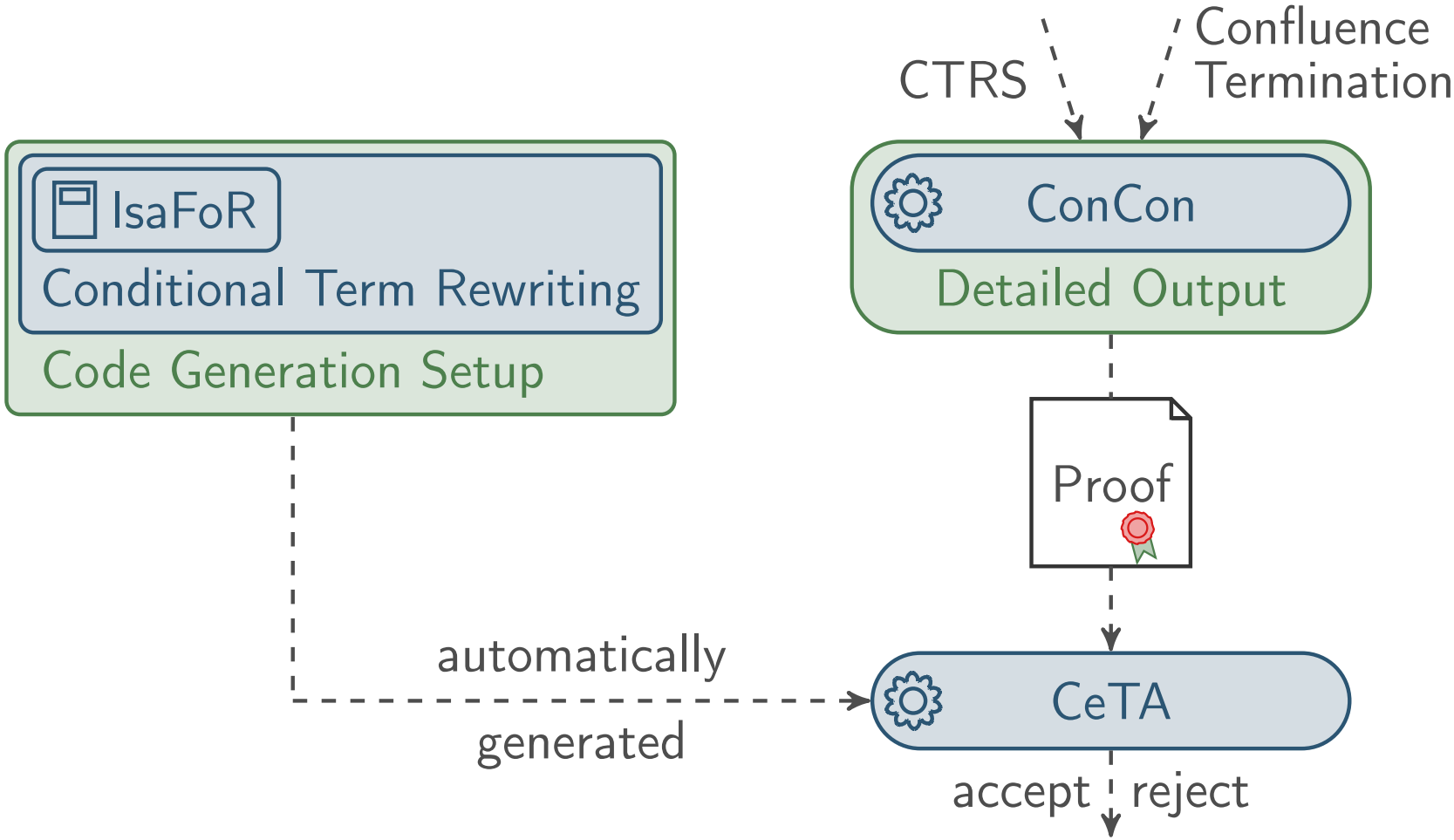


Our Contribution III - Certification

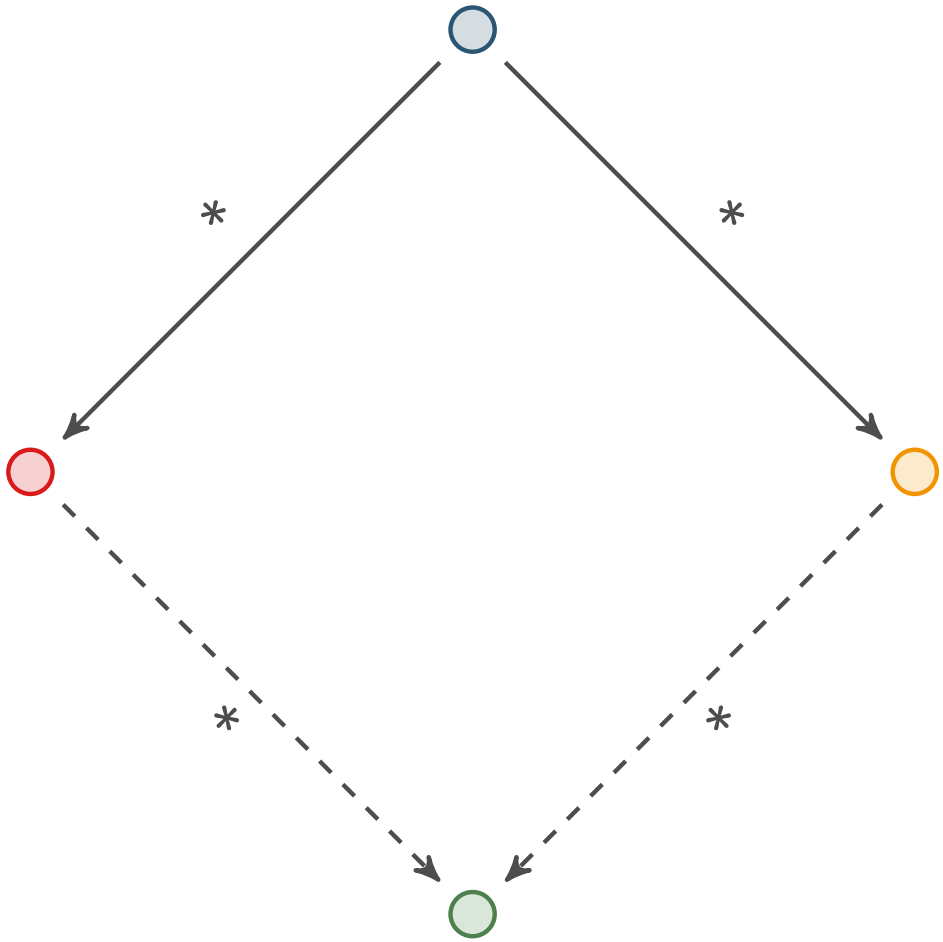
Our Contribution III - Certification



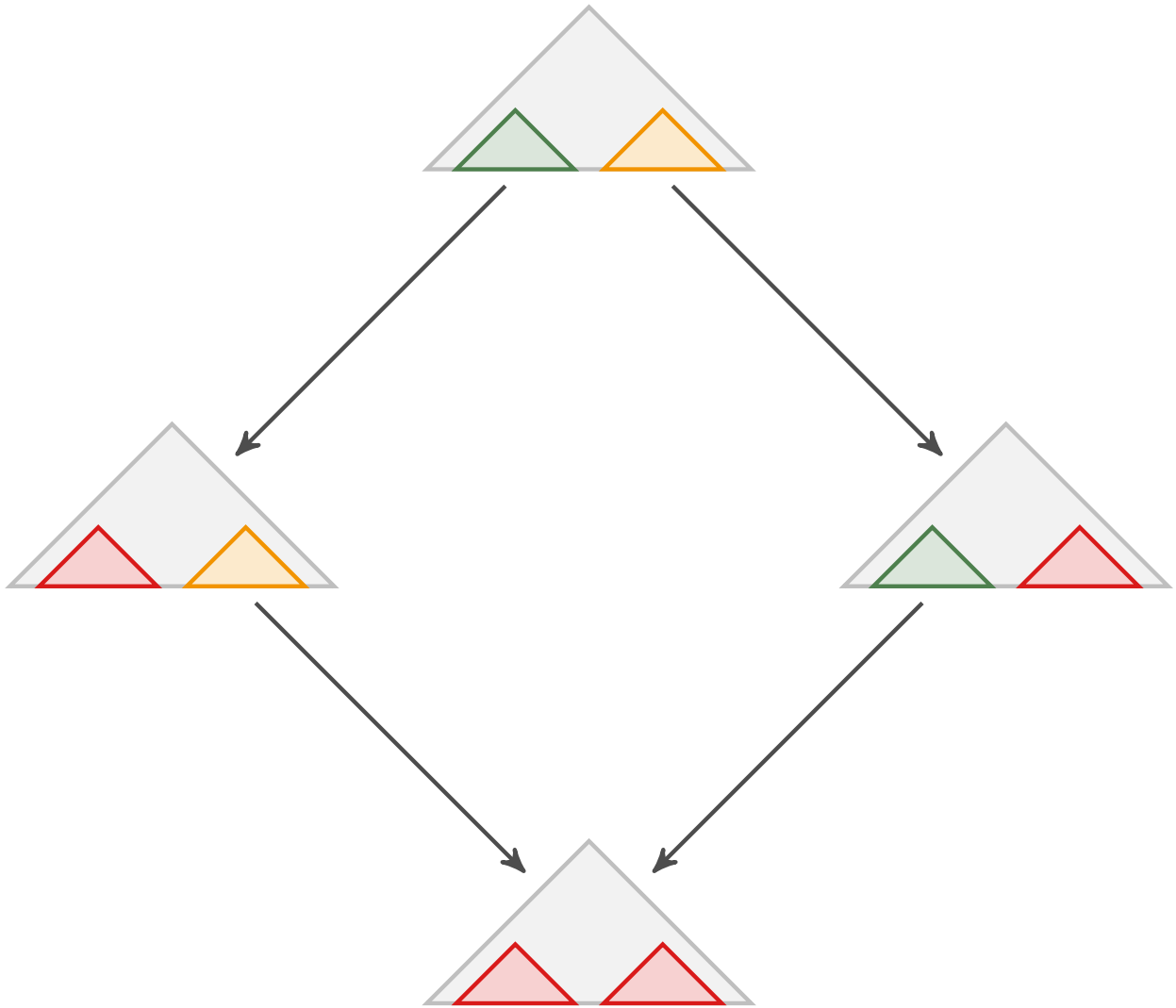
Our Contribution III - Certification



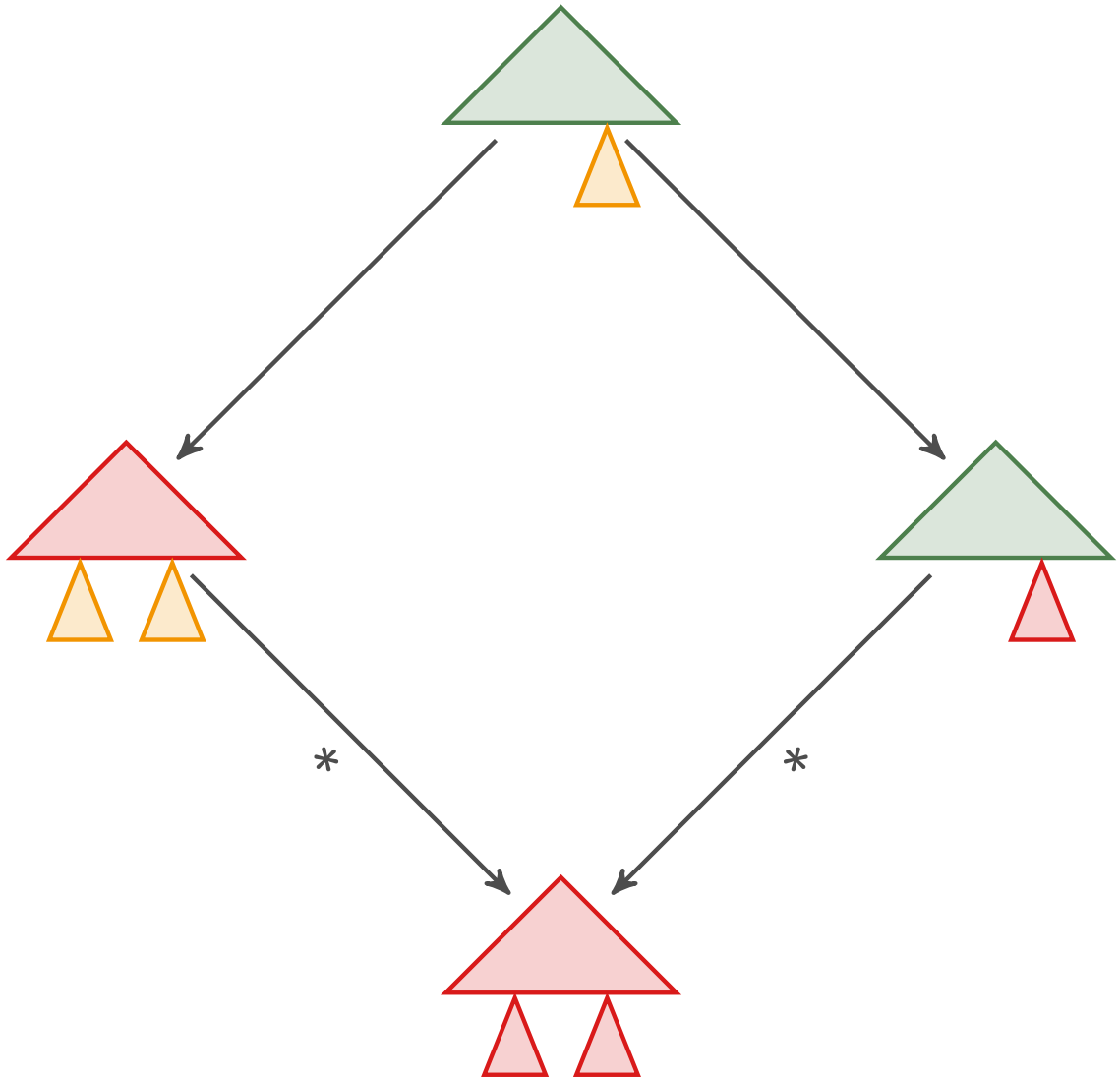
Analyzing (Non-)Confluence



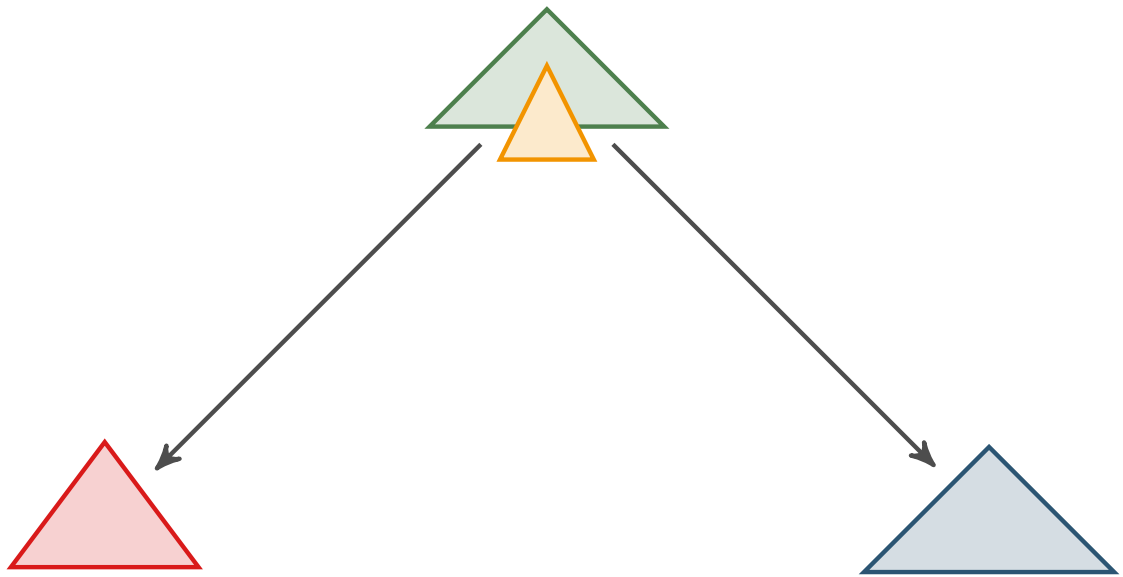
Analyzing (Non-)Confluence



Analyzing (Non-)Confluence



Analyzing (Non-)Confluence



Confluence Methods

Theorem I

A DTRS is confluent if its unraveling is left-linear and confluent.

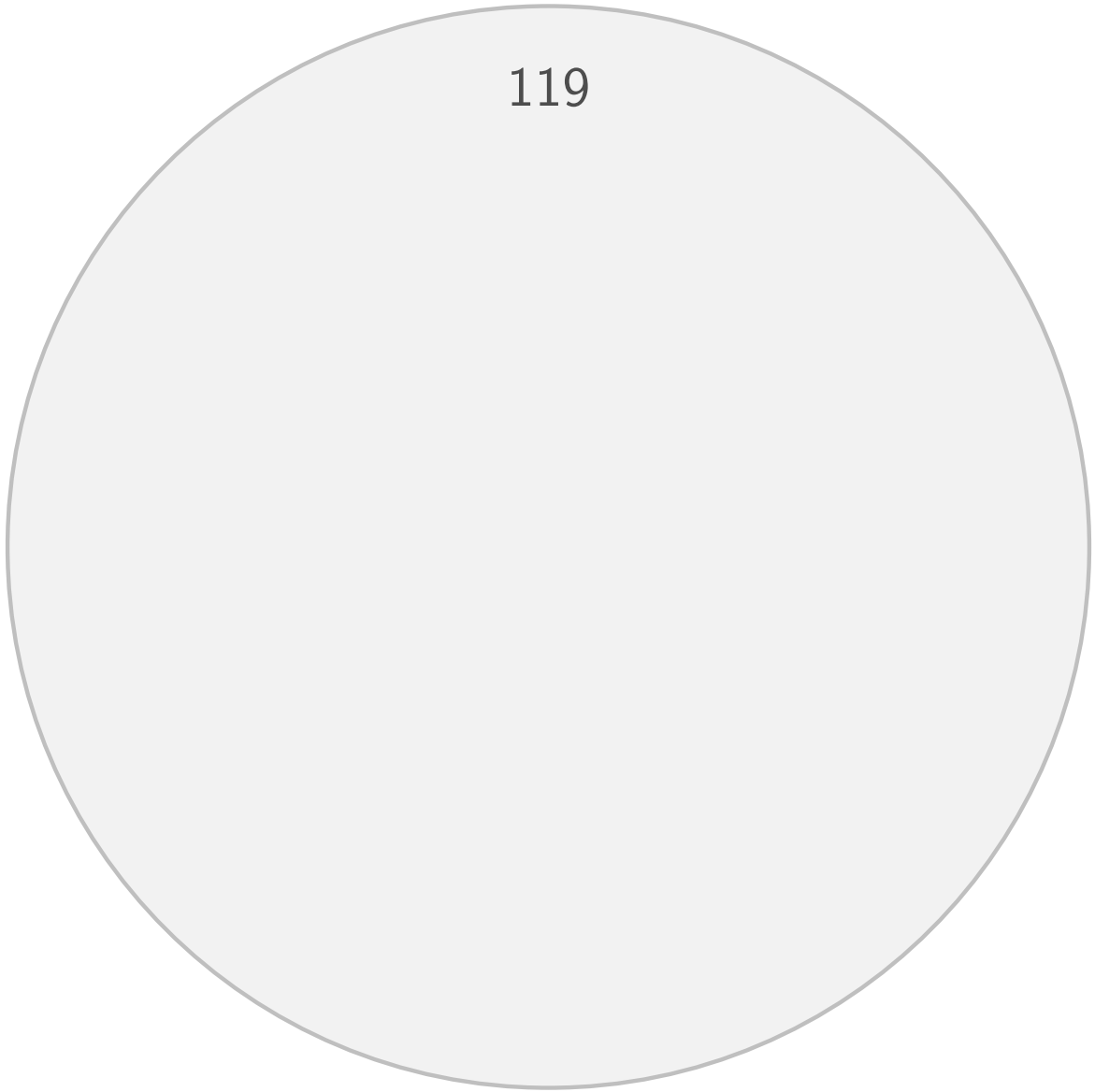
Theorem II

An orthogonal, properly oriented, right-stable CTRS is confluent.

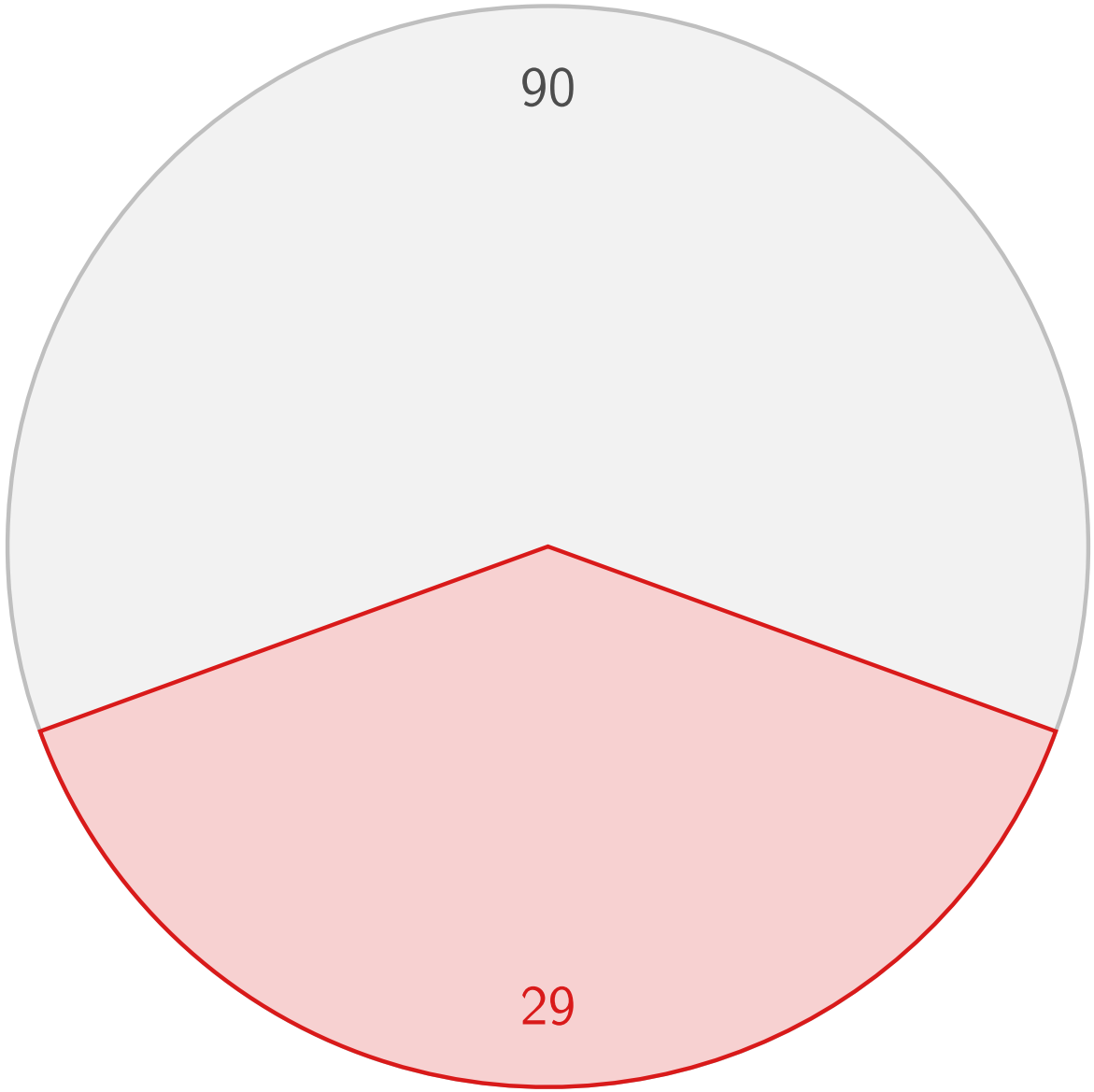
Theorem III

A quasi-decreasing SDTRS is confluent if all its CCPs are joinable.

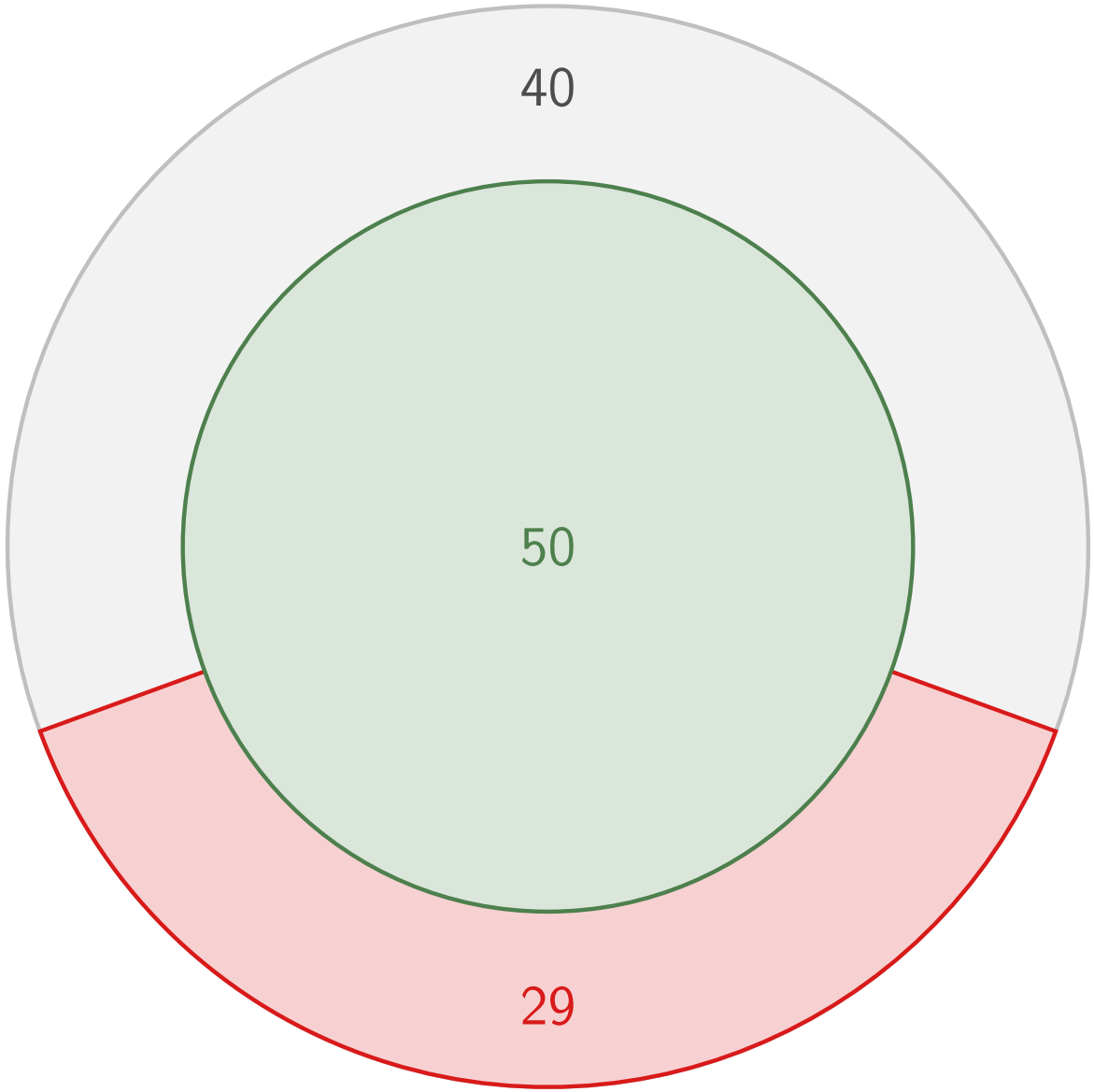
Experimental Results



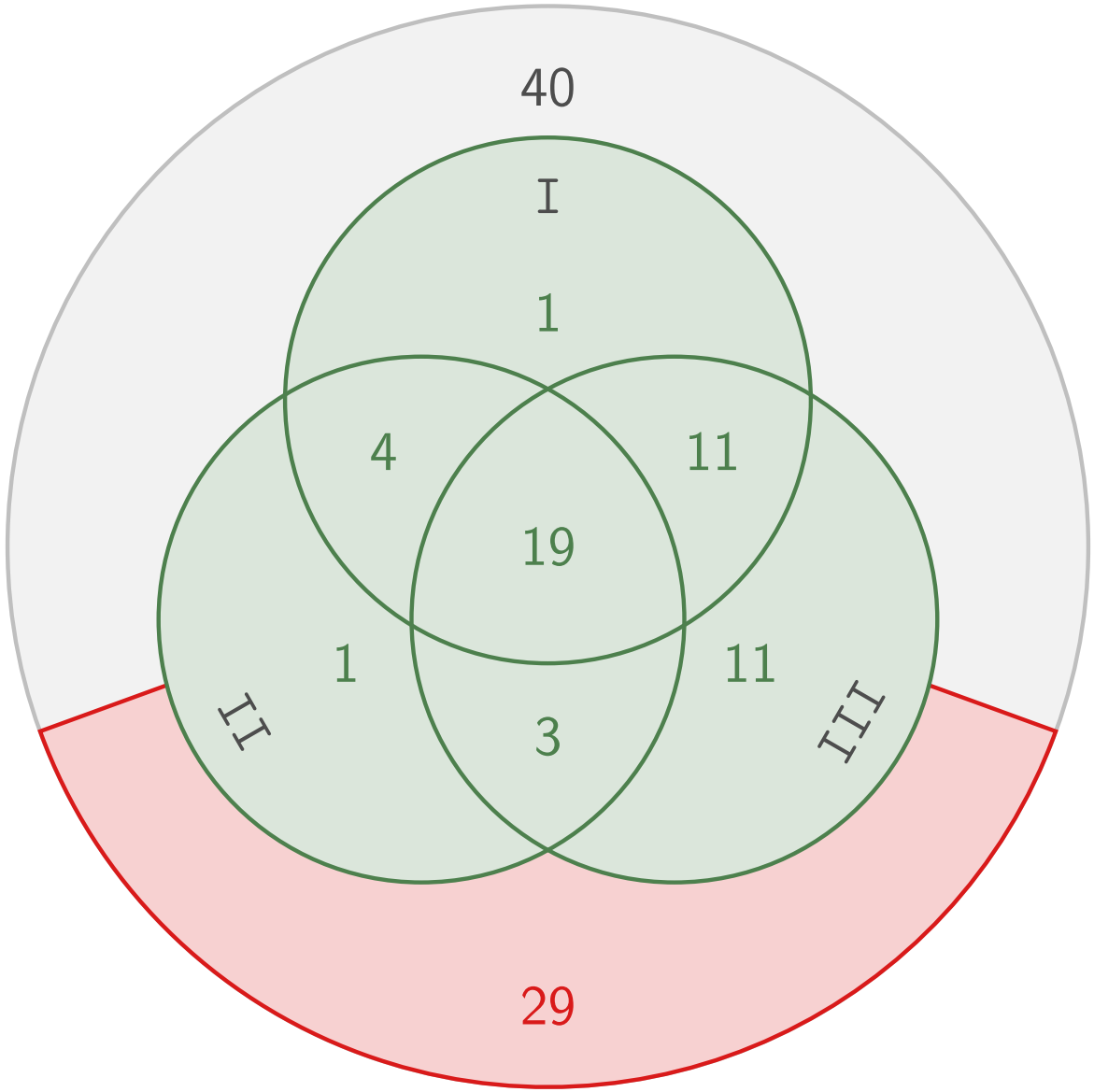
Experimental Results



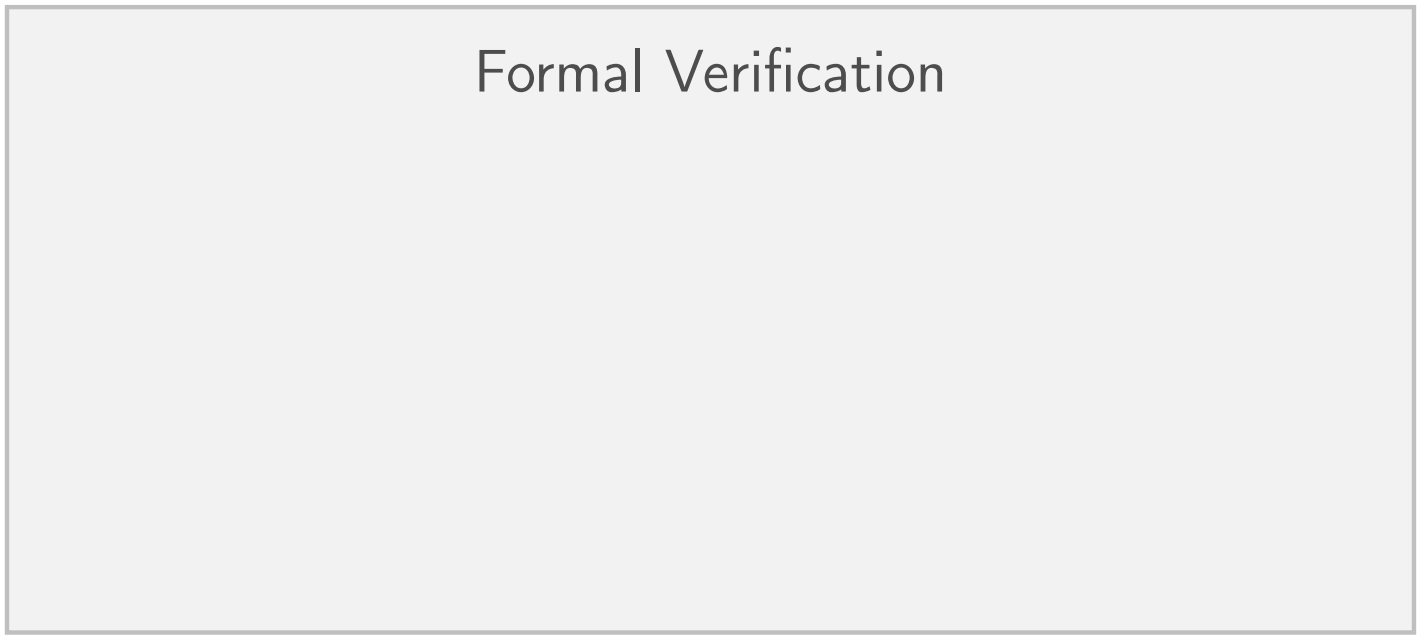
Experimental Results



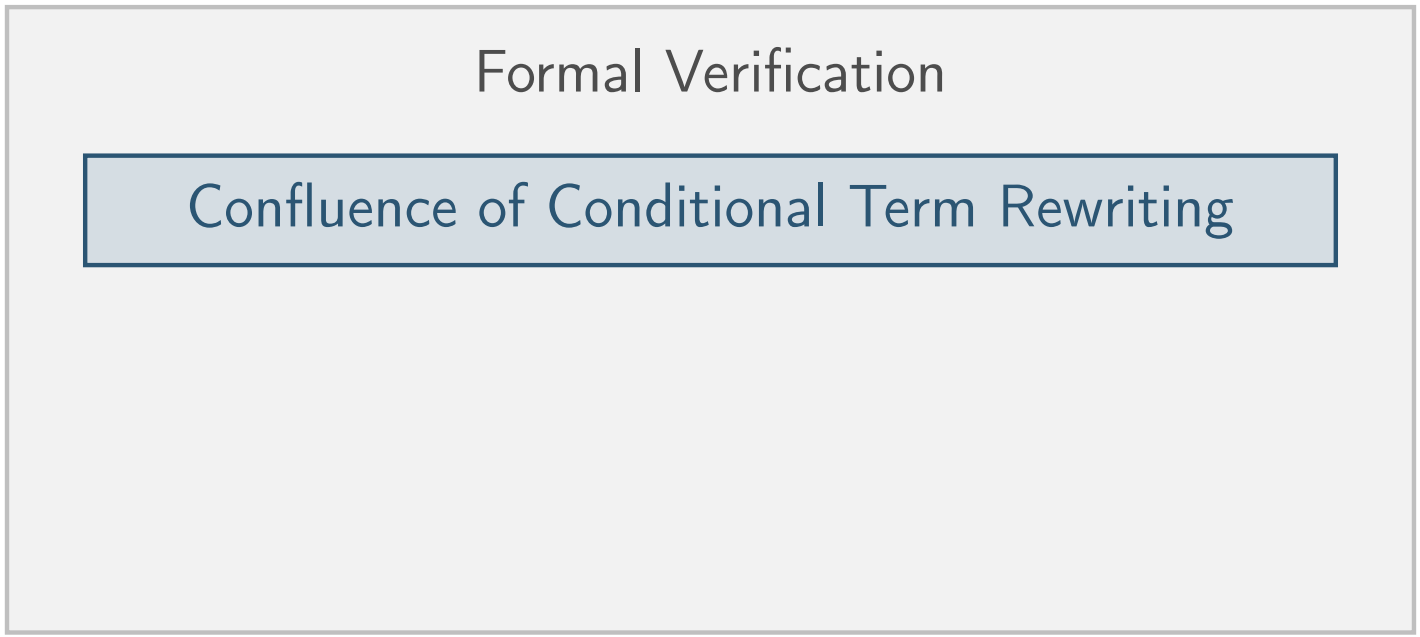
Experimental Results



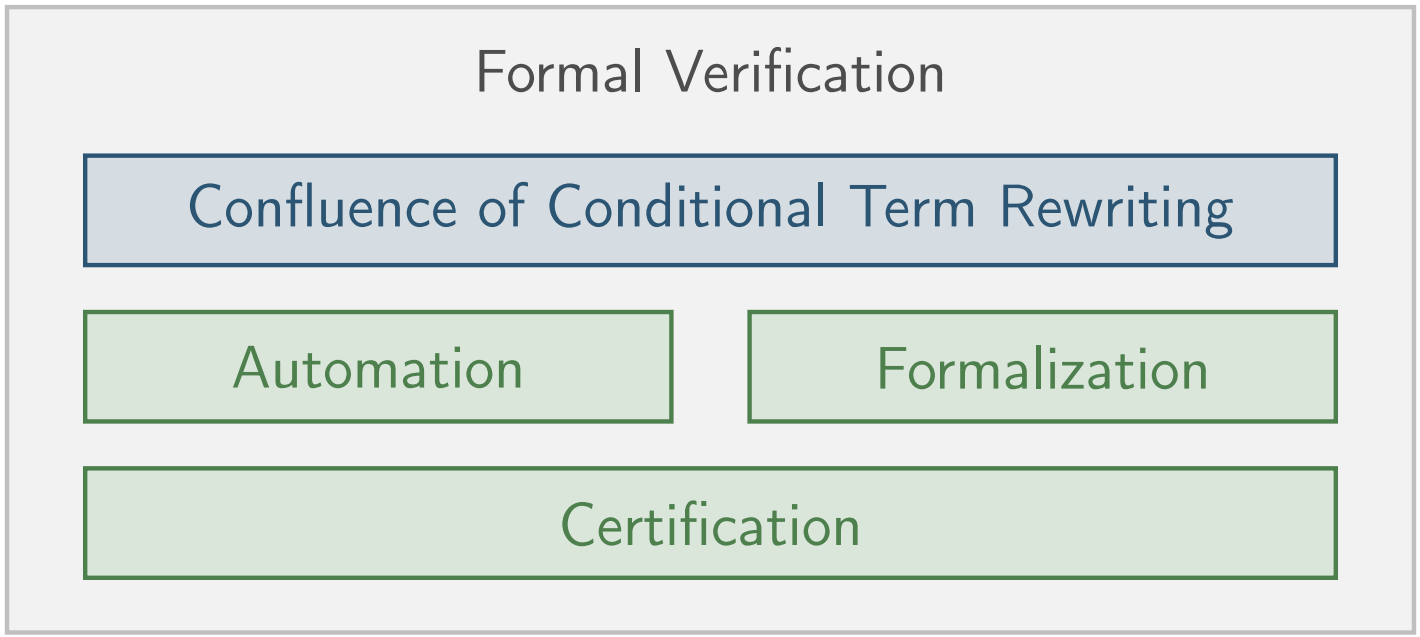
Conclusion



Conclusion


Formal Verification
Confluence of Conditional Term Rewriting

Conclusion


Formal Verification
Confluence of Conditional Term Rewriting
Automation
Formalization
Certification

Publications

C. Sternagel and T. Sternagel
Certifying Confluence of Almost Orthogonal CTRSs via Exact Tree Automata Completion
In *Proc. 1st FSCD*, *LIPIcs*, pages 29:1–29:16, 2016.

T. Sternagel and C. Sternagel
Formalized Confluence of Quasi-Decreasing, Strongly Deterministic Conditional TRSs
In *Proc. 5th IWC*, pages 60–64, 2016.

T. Sternagel and C. Sternagel
A Characterization of Quasi-Decreasingness
In *Proc. 15th WST*, pages 12:1–12:5, 2016.

C. Sternagel and T. Sternagel
Level-Confluence of 3-CTRSs in Isabelle/HOL
In *Proc. 4th IWC*, pages 28–32, 2015.

T. Sternagel and A. Middeldorp
Infeasible Conditional Critical Pairs
In *Proc. 4th IWC*, pages 13–17, 2015.

T. Sternagel and A. Middeldorp
Conditional Confluence (System Description)
In *Proc. Joint 25th RTA and 12th TLCA*, *LNCS*, pages 456–465, 2014.