Analysing installation scenarios of Debian packages

Nicolas Jeannerod
nicolas.jeannerod@irif.fr

joint work with Benedikt Becker, Claude Marché
Yann Régis-Gianas, Mihaela Sighireanu, Ralf Treinen

IRIF, Université de Paris

April 8, 2020

IRIF PhD Seminar

Debian GNU/Linux

- Linux distribution
  - Operating System
- Widely used
  - as OS for servers
  - as OS for desktop computers
  - as basis for derived distributions — eg. Ubuntu

Installation of a Package

```
root@debian:~# apt install firefox
```

Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
```

Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd
Fetched 51.3 MB in 5s (9,569 kB/s)
```

Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd
Fetched 51.3 MB in 5s (9,569 kB/s)
(Reading database ... 140834 files and directories currently insta
Preparing to unpack .../firefox_74.0.1-1_amd64.deb ...
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
```

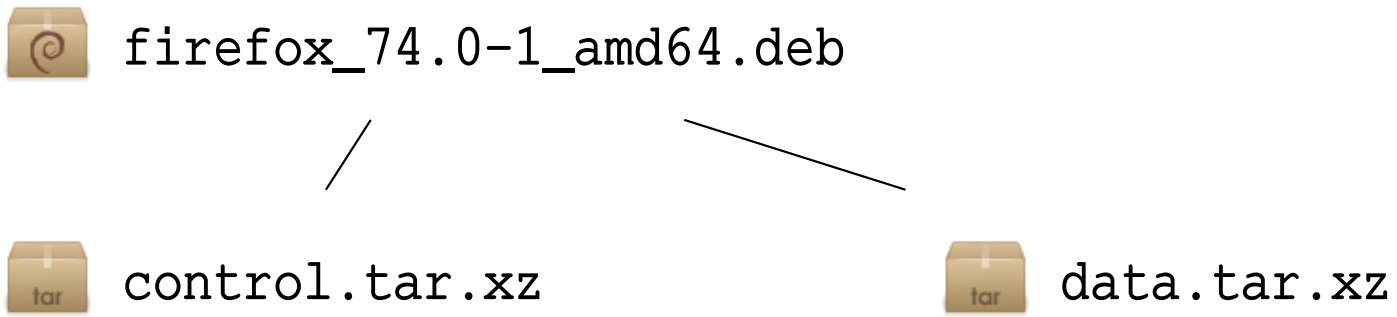
Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd
Fetched 51.3 MB in 5s (9,569 kB/s)
(Reading database ... 140834 files and directories currently insta
Preparing to unpack .../firefox_74.0.1-1_amd64.deb ...
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
root@debian:~#
```

Content of a Package

`firefox_74.0-1_amd64.deb`

Content of a Package



Content of a Package

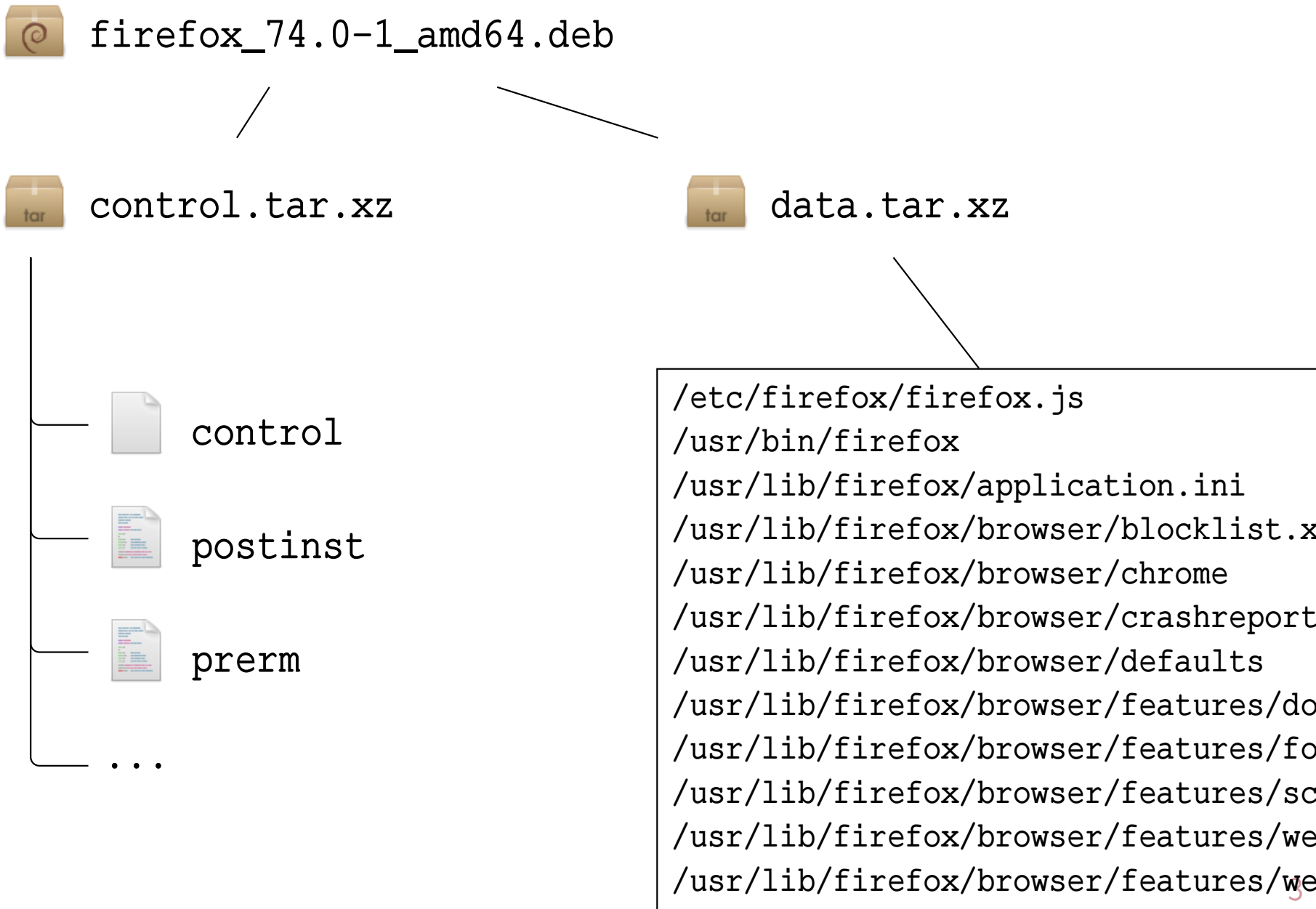
firefox_74.0-1_amd64.deb

control.tar.xz

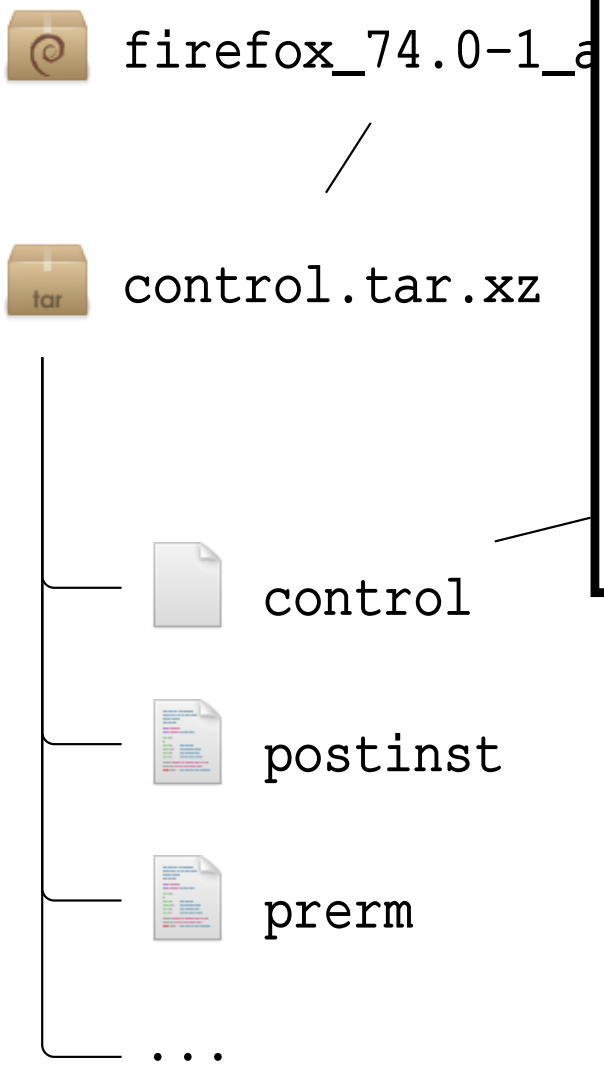
data.tar.xz

```
/etc/firefox/firefox.js
/usr/bin/firefox
/usr/lib/firefox/application.ini
/usr/lib/firefox/browser/blocklist.x
/usr/lib/firefox/browser/chrome
/usr/lib/firefox/browser/crashreport
/usr/lib/firefox/browser/defaults
/usr/lib/firefox/browser/features/do
/usr/lib/firefox/browser/features/fo
/usr/lib/firefox/browser/features/sc
/usr/lib/firefox/browser/features/we
/usr/lib/firefox/browser/features/we
```

Content of a Package



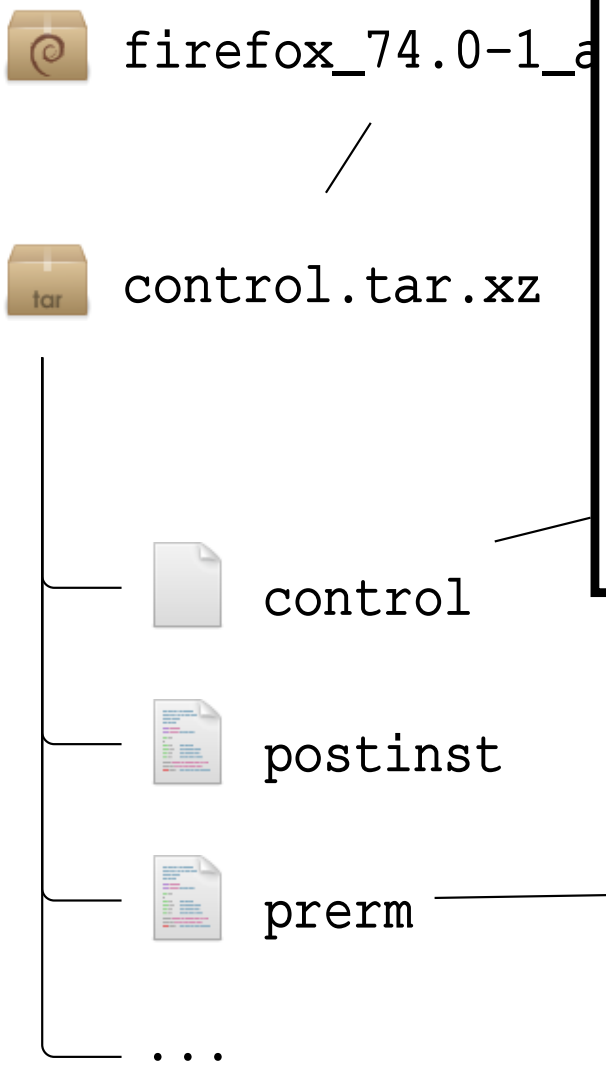
Content of a Package




```
Package: firefox
Version: 74.0-1
Architecture: amd64
...
Depends: libatk1.0-0 (>= 1.12.4), libc6 (>= 2.29)
1.10.0), libcairo2 (>= 1.10.0), ...
...
Description: Mozilla Firefox web browser
Firefox is a powerful, extensible web browser with
web application technologies.
```

```
/usr/bin/firefox
/usr/lib/firefox/application.ini
/usr/lib/firefox/browser/blocklist.x
/usr/lib/firefox/browser/chrome
/usr/lib/firefox/browser/crashreport
/usr/lib/firefox/browser/defaults
/usr/lib/firefox/browser/features/do
/usr/lib/firefox/browser/features/fo
/usr/lib/firefox/browser/features/sc
/usr/lib/firefox/browser/features/we
/usr/lib/firefox/browser/features/we
```

Content of a Package




```
Package: firefox
Version: 74.0-1
Architecture: amd64
...
Depends: libatk1.0-0 (>= 1.12.4), libc6 (>= 2.29)
1.10.0), libcairo2 (>= 1.10.0), ...
...
Description: Mozilla Firefox web browser
Firefox is a powerful, extensible web browser with
we
```

```
#!/bin/sh -e

if [ "$1" = "remove" ] || [ "$1" = "
    update-alternatives --remove x-w
    update-alternatives --remove gno
fi

if [ "$1" = "remove" ]; then
    rm -rf /usr/lib/firefox/updates
fi
```

Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 nc
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main an
Fetched 51.3 MB in 5s (9,569 kB/s)
Preparing to unpack .../firefox_74.0.1-1_amd64.deb
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1)
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
root@debian:~#
```

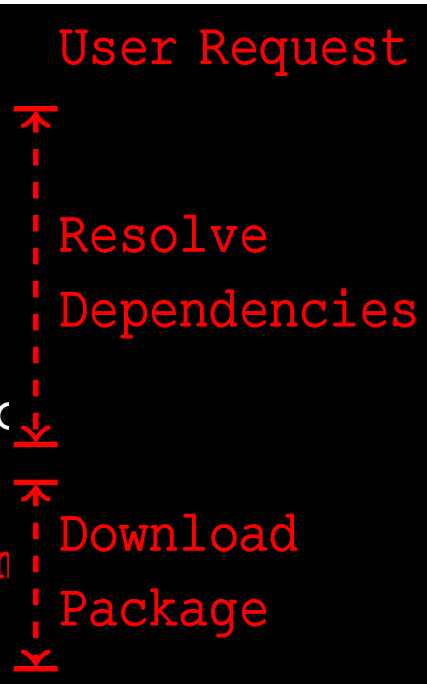
User Request

Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 nc
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main an
Fetched 51.3 MB in 5s (9,569 kB/s)
Preparing to unpack .../firefox_74.0.1-1_amd64.deb
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1)
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
root@debian:~#
```

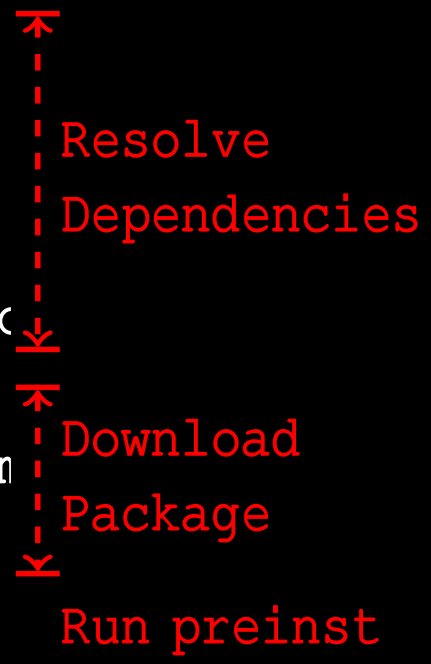
Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 nc
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main am
Fetched 51.3 MB in 5s (9,569 kB/s)
Preparing to unpack .../firefox_74.0.1-1_amd64.deb
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1)
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
root@debian:~#
```



Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 nc
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main an
Fetched 51.3 MB in 5s (9,569 kB/s)
Preparing to unpack .../firefox_74.0.1-1_amd64.deb
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1)
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
root@debian:~#
```



Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 nc
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main an
Fetched 51.3 MB in 5s (9,569 kB/s)
Preparing to unpack .../firefox_74.0.1-1_amd64.deb
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1)
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
root@debian:~#
```

User Request

Resolve Dependencies

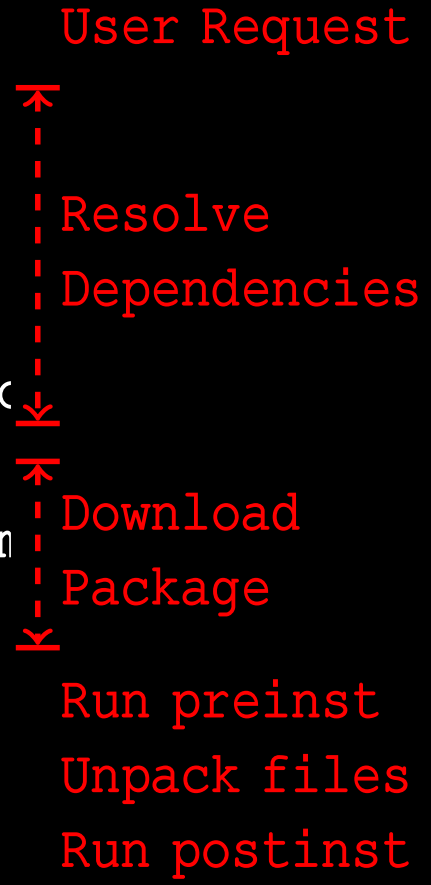
Download Package

Run preinst

Unpack files

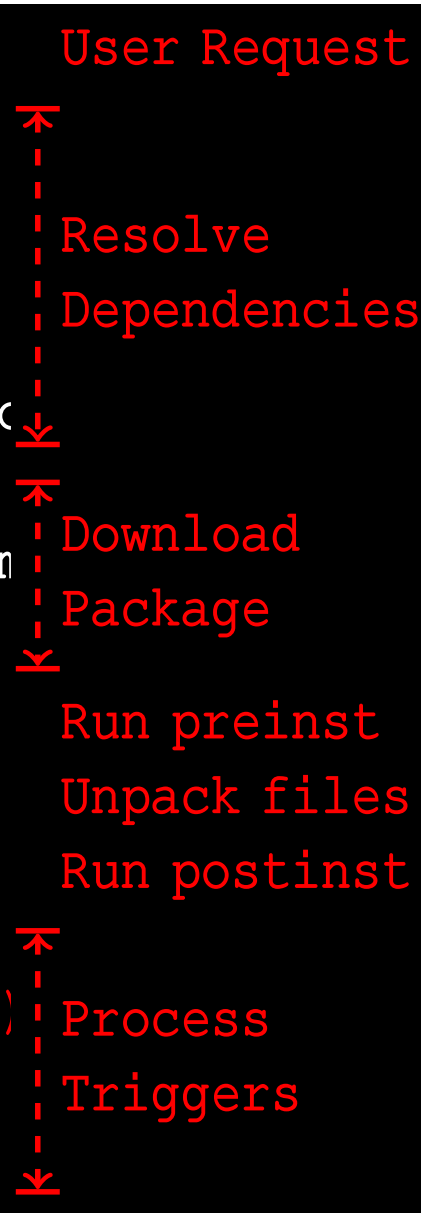
Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 nc
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main an
Fetched 51.3 MB in 5s (9,569 kB/s)
Preparing to unpack .../firefox_74.0.1-1_amd64.deb
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1)
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
root@debian:~#
```



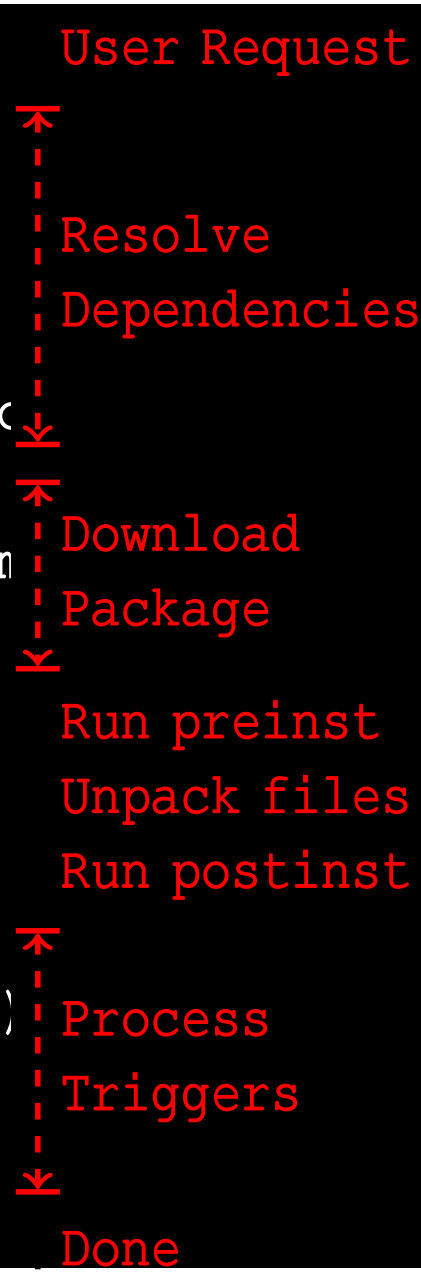
Installation of a Package

```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 nc
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main an
Fetched 51.3 MB in 5s (9,569 kB/s)
Preparing to unpack .../firefox_74.0.1-1_amd64.deb
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1)
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
root@debian:~#
```

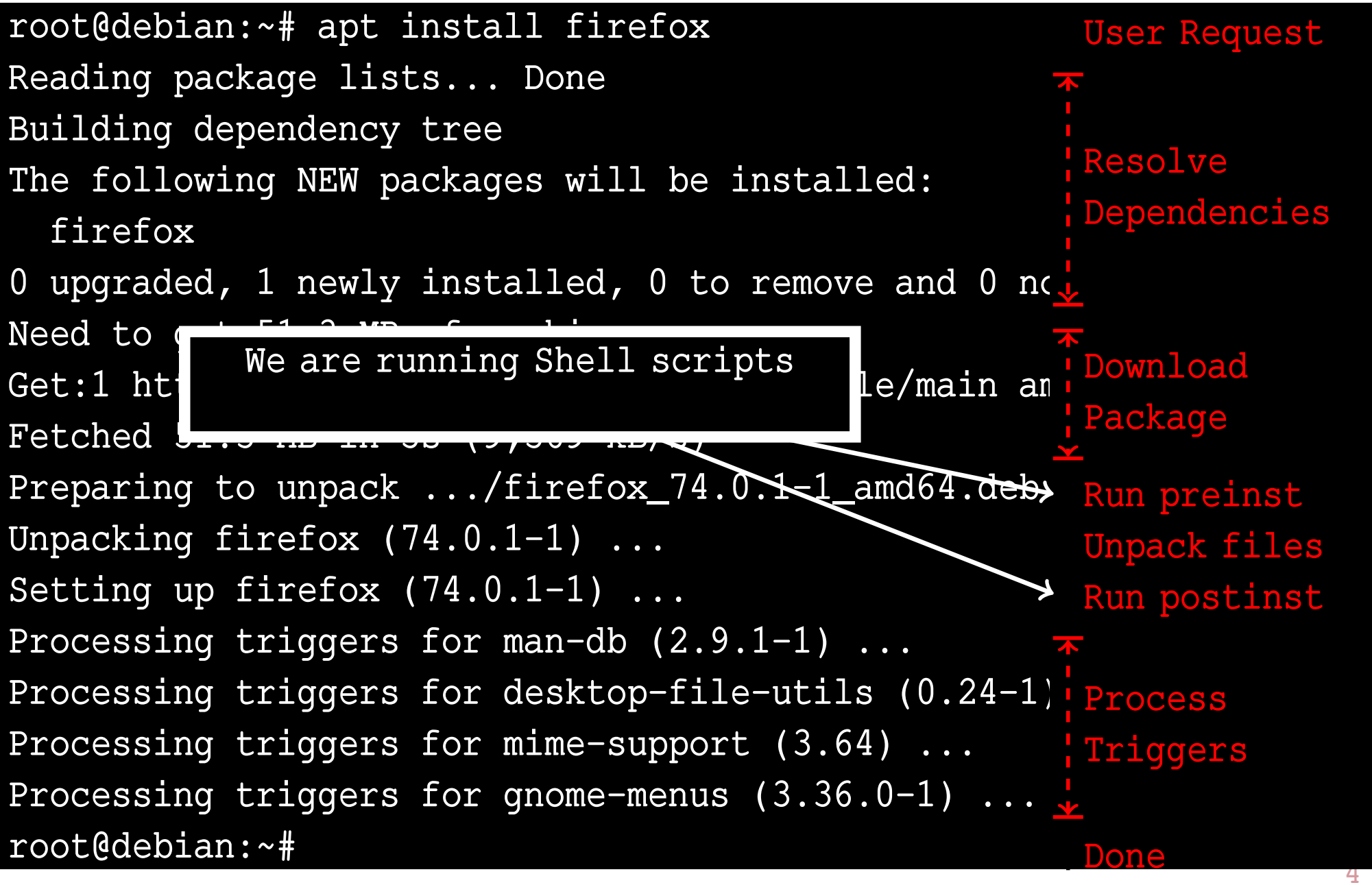


Installation of a Package

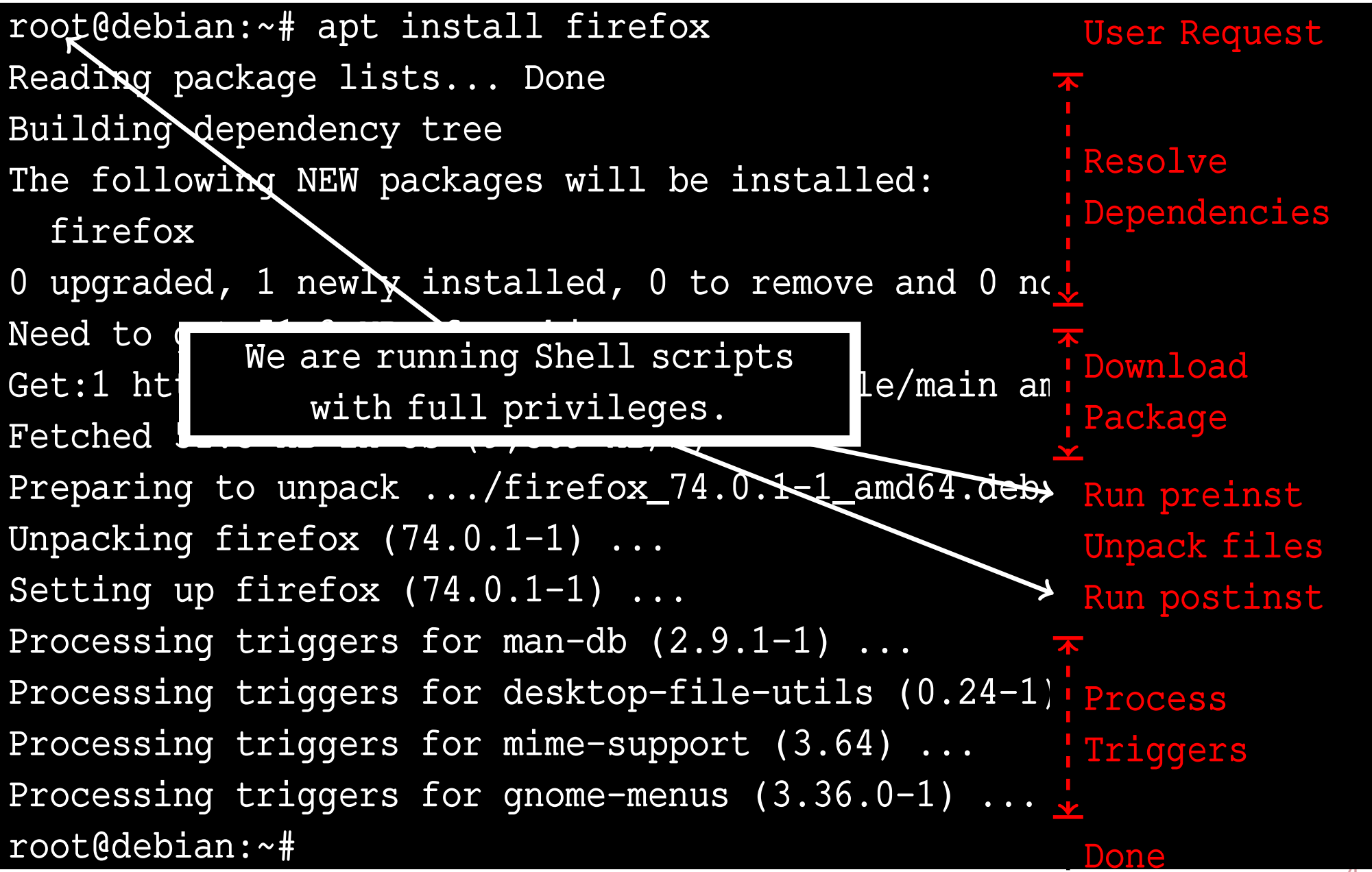
```
root@debian:~# apt install firefox
Reading package lists... Done
Building dependency tree
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 nc
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main an
Fetched 51.3 MB in 5s (9,569 kB/s)
Preparing to unpack .../firefox_74.0.1-1_amd64.deb
Unpacking firefox (74.0.1-1) ...
Setting up firefox (74.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1)
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
root@debian:~#
```



Installation of a Package



Installation of a Package



What Could Possibly Go Wrong?

From: "Aaron M. Ucko" <ucko@debian.org>
To: Debian Bug Tracking System <submit@bugs.debian.org>
Subject: cmigrep: broken emacsen-install script
Date: Fri, 29 Jun 2007 20:27:06 -0400

```
Package: cmigrep
Version: 1.3-1
Severity: critical
Justification: breaks unrelated software

cmigrep's emacsen-install script is overzealous; specifically, it
inappropriately attempts to compile all .el files in
/usr/share/emacs/site-lisp even if they don't work with the current
emacsen flavor (for instance, remembrance-agent's remem.el
vs. xemacs), and compounds the problem by removing
/usr/share/$FLAVOR/site-lisp/*.el, which may contain files belonging
to other packages (for instance, auctex's tex-site.el).

Could you please rein it int to compile only cmigrep.el, with none of
```

The CoLiS Project

> Correctness of Linux Scripts

The CoLiS Project

- Correctness of Linux Scripts
- ANR project from October 2015 to September 2020.

The CoLiS Project

- Correctness of Linux Scripts
- ANR project from October 2015 to September 2020.
- Goal: applying formal methods to the quality assessment of Debian Packages.

The CoLiS Project

- Correctness of Linux Scripts
- ANR project from October 2015 to September 2020.
- Goal: applying formal methods to the quality assessment of Debian Packages.
- Goal (reformulated): making sure that installing/updating/removing software does not:

The CoLiS Project

- Correctness of Linux Scripts
- ANR project from October 2015 to September 2020.
- Goal: applying formal methods to the quality assessment of Debian Packages.
- Goal (reformulated): making sure that installing/updating/removing software does not:
  - make other softwares unusable,

The CoLiS Project

- Correctness of Linux Scripts
- ANR project from October 2015 to September 2020.
- Goal: applying formal methods to the quality assessment of Debian Packages.
- Goal (reformulated): making sure that installing/updating/removing software does not:
  - make other softwares unusable,
  - make the whole computer unusable,

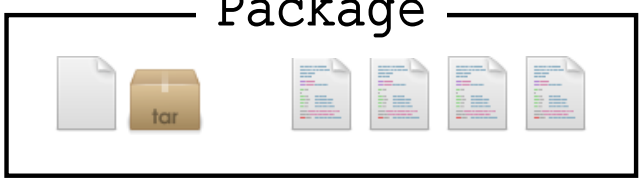
The CoLiS Project

- Correctness of Linux Scripts
- ANR project from October 2015 to September 2020.
- Goal: applying formal methods to the quality assessment of Debian Packages.
- Goal (reformulated): making sure that installing/updating/removing software does not:
  - make other softwares unusable,
  - make the whole computer unusable,
  - remove your personal files,

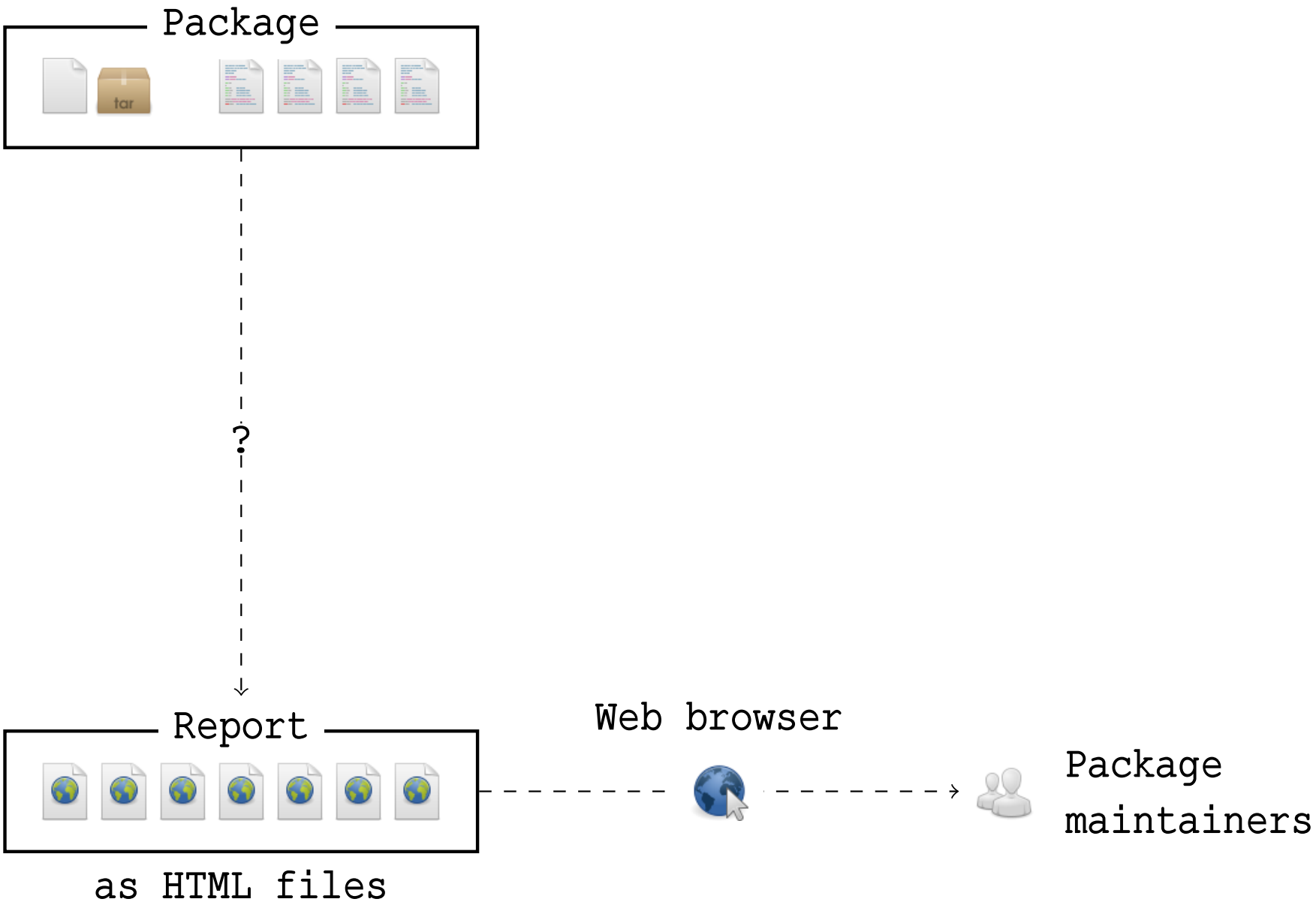
The CoLiS Project

- Correctness of Linux Scripts
- ANR project from October 2015 to September 2020.
- Goal: applying formal methods to the quality assessment of Debian Packages.
- Goal (reformulated): making sure that installing/updating/removing software does not:
  - make other softwares unusable,
  - make the whole computer unusable,
  - remove your personal files,
  - etc.

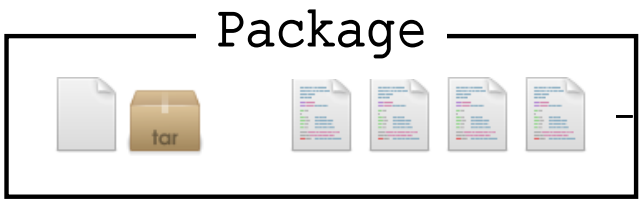
Battle Plan



Battle Plan

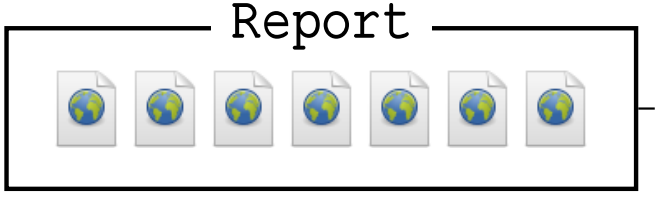

Package
tar
?
Report
as HTML files
Web browser
Package
maintainers

Battle Plan



Parsing and conversion

Scripts in “clean” intermediary language

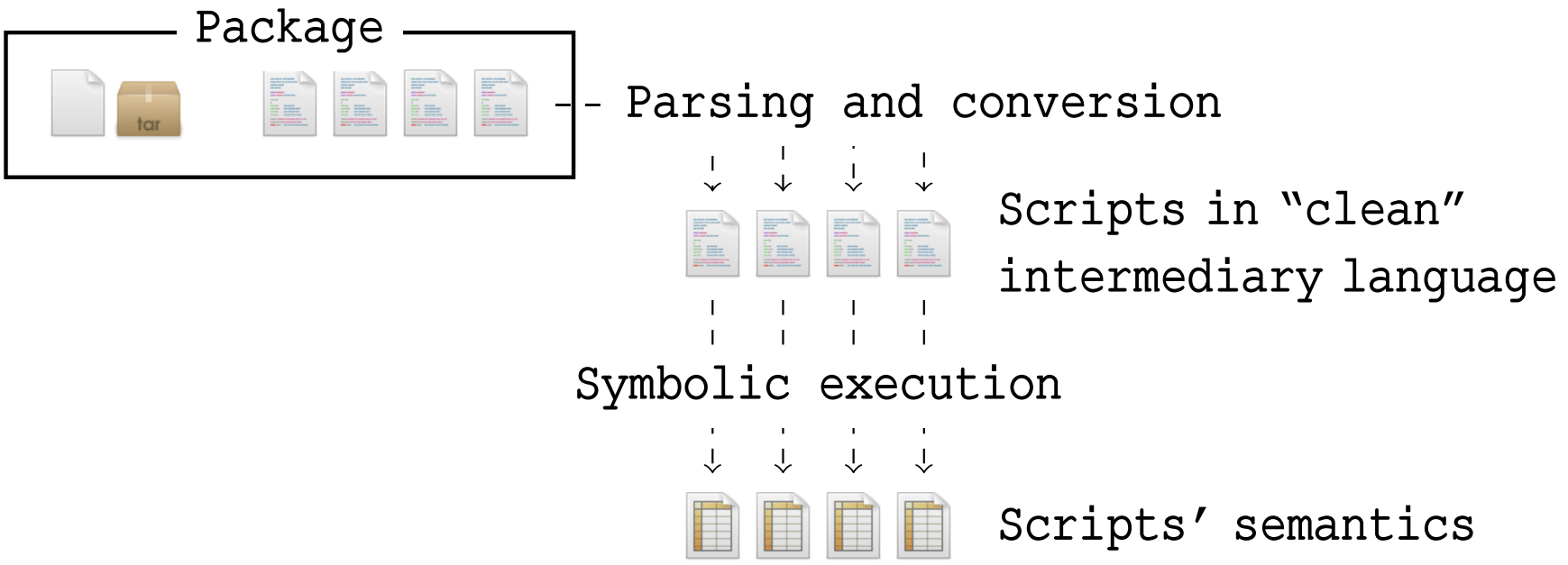


as HTML files

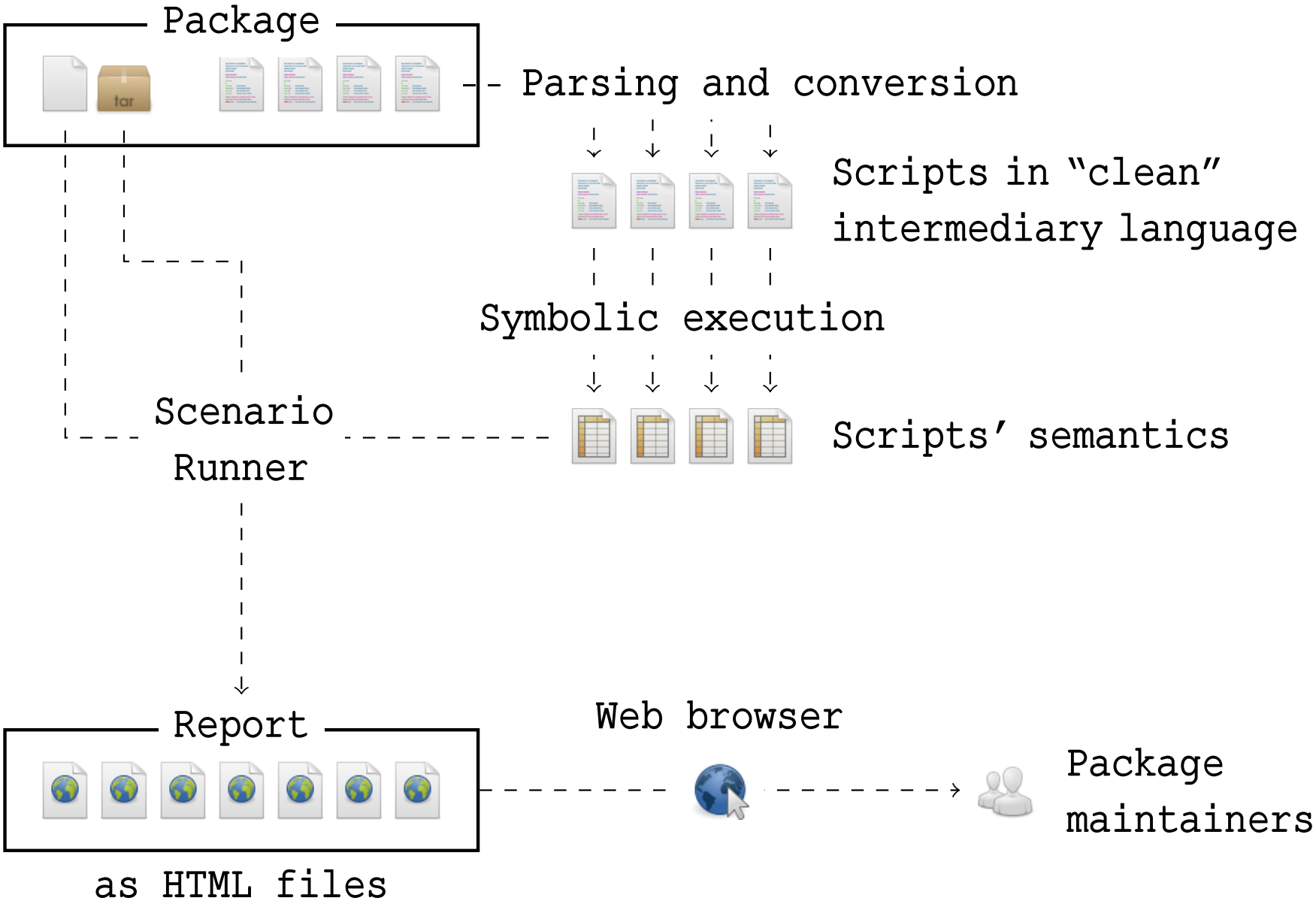
Web browser

Package maintainers

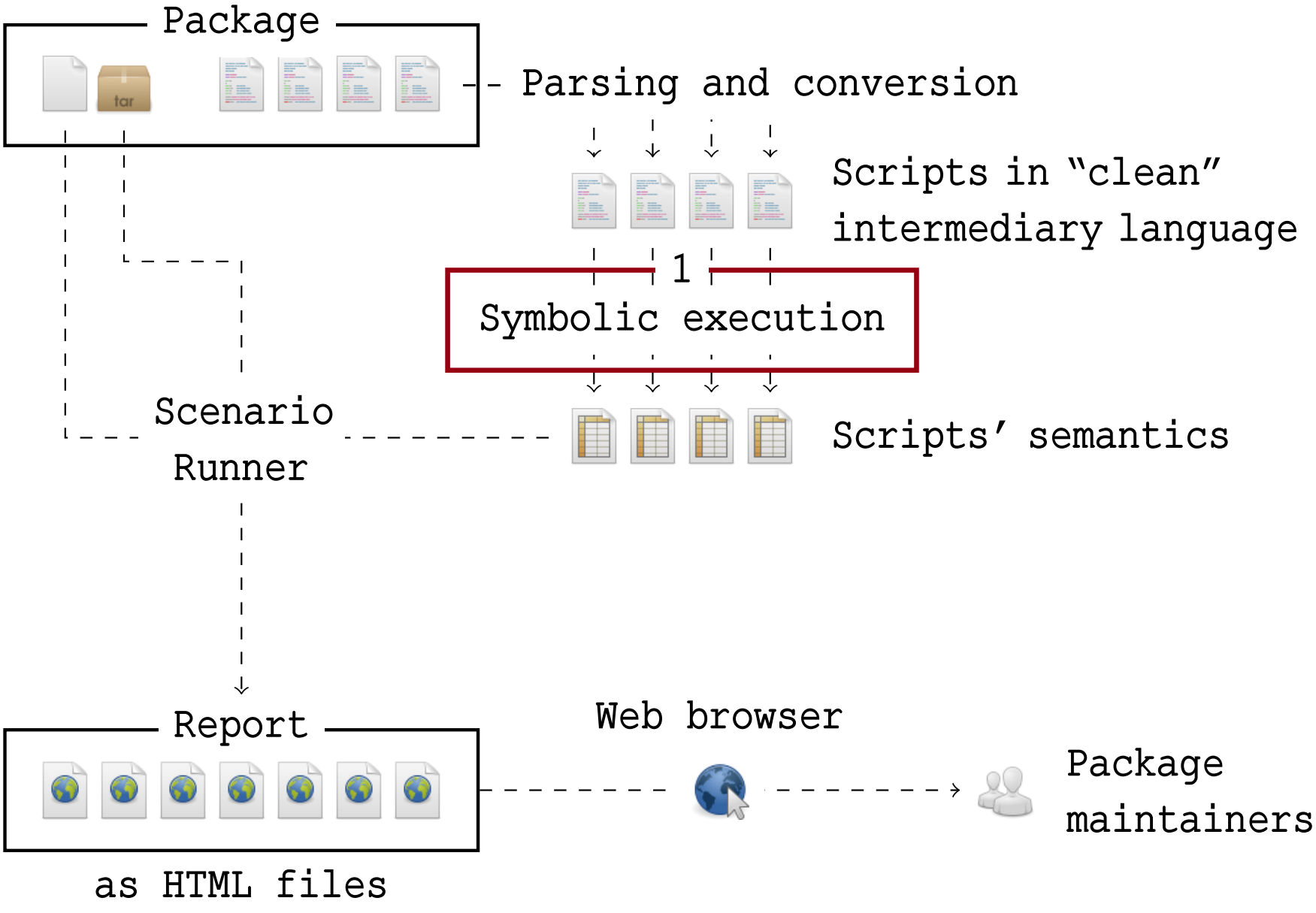
Battle Plan


Package
tar
Parsing and conversion
Scripts in "clean"
intermediary language
Symbolic execution
Scripts' semantics
Report
as HTML files
Web browser
Package
maintainers

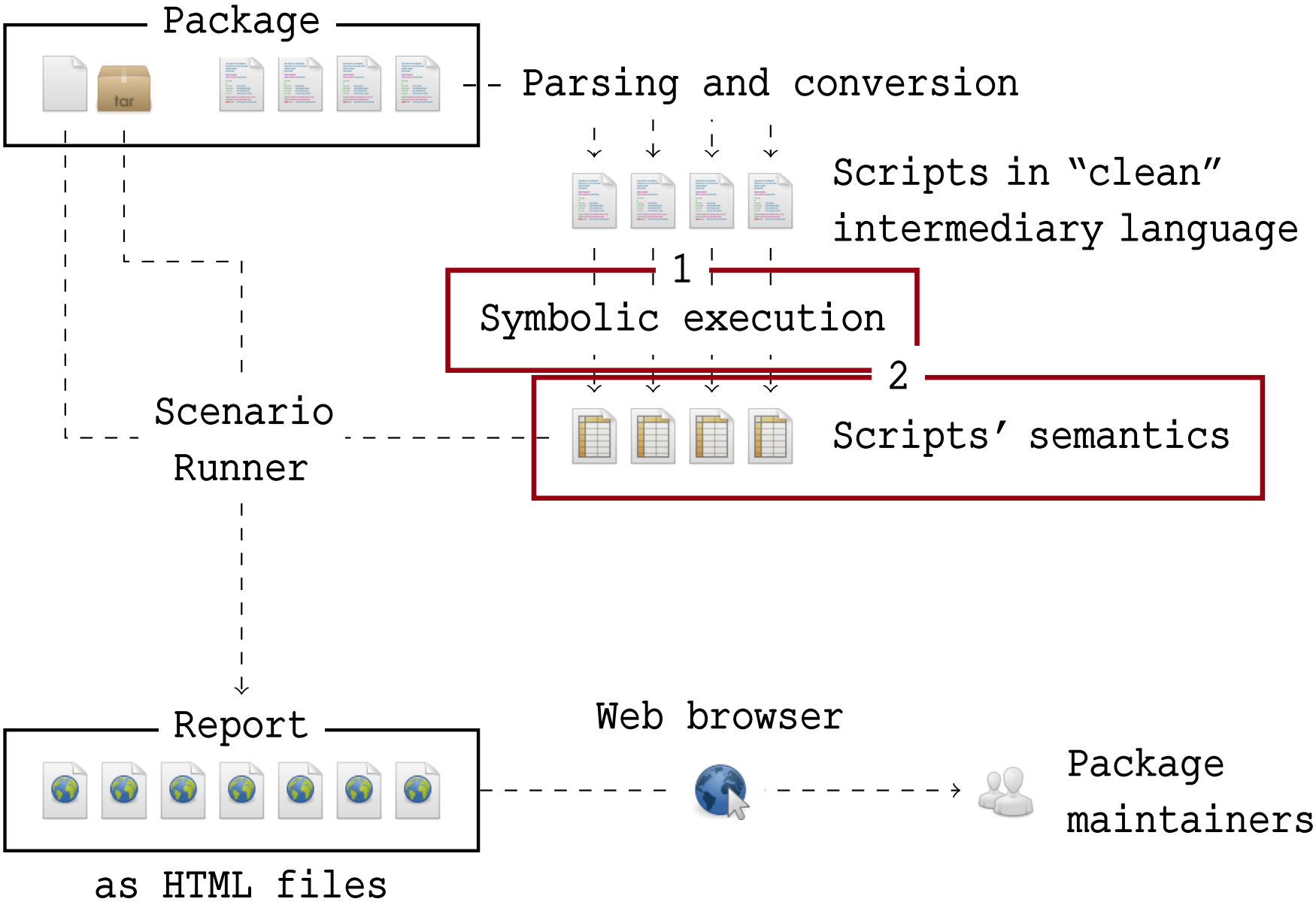
Battle Plan


Package
tar
Parsing and conversion
Scripts in "clean"
intermediary language
Symbolic execution
Scenario
Runner
Scripts' semantics
Report
Web browser
Package
maintainers
as HTML files

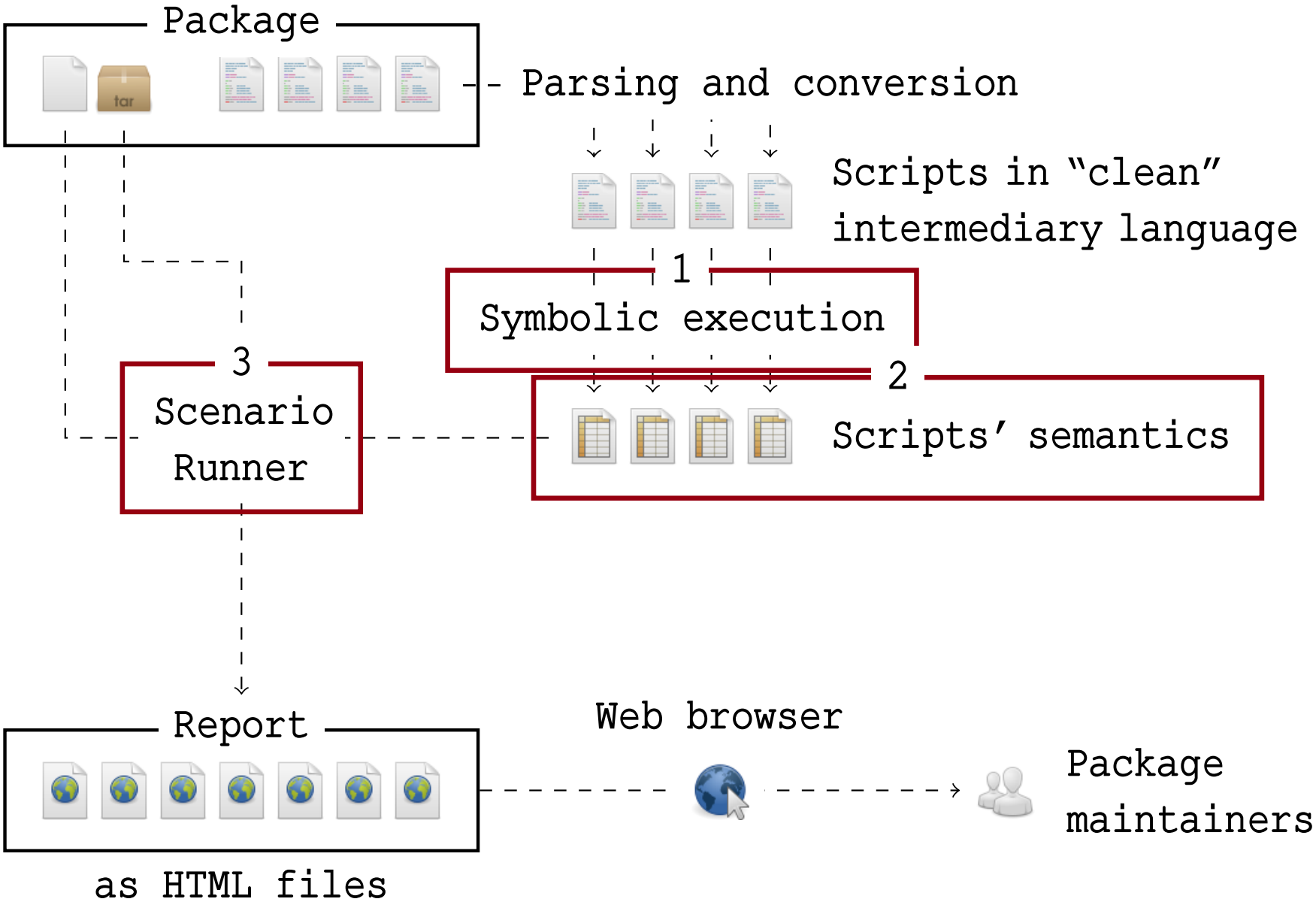
Battle Plan


Package
tar
Parsing and conversion
Scripts in "clean"
intermediary language
1
Symbolic execution
Scenario
Runner
Scripts' semantics
Report
Web browser
Package
maintainers
as HTML files

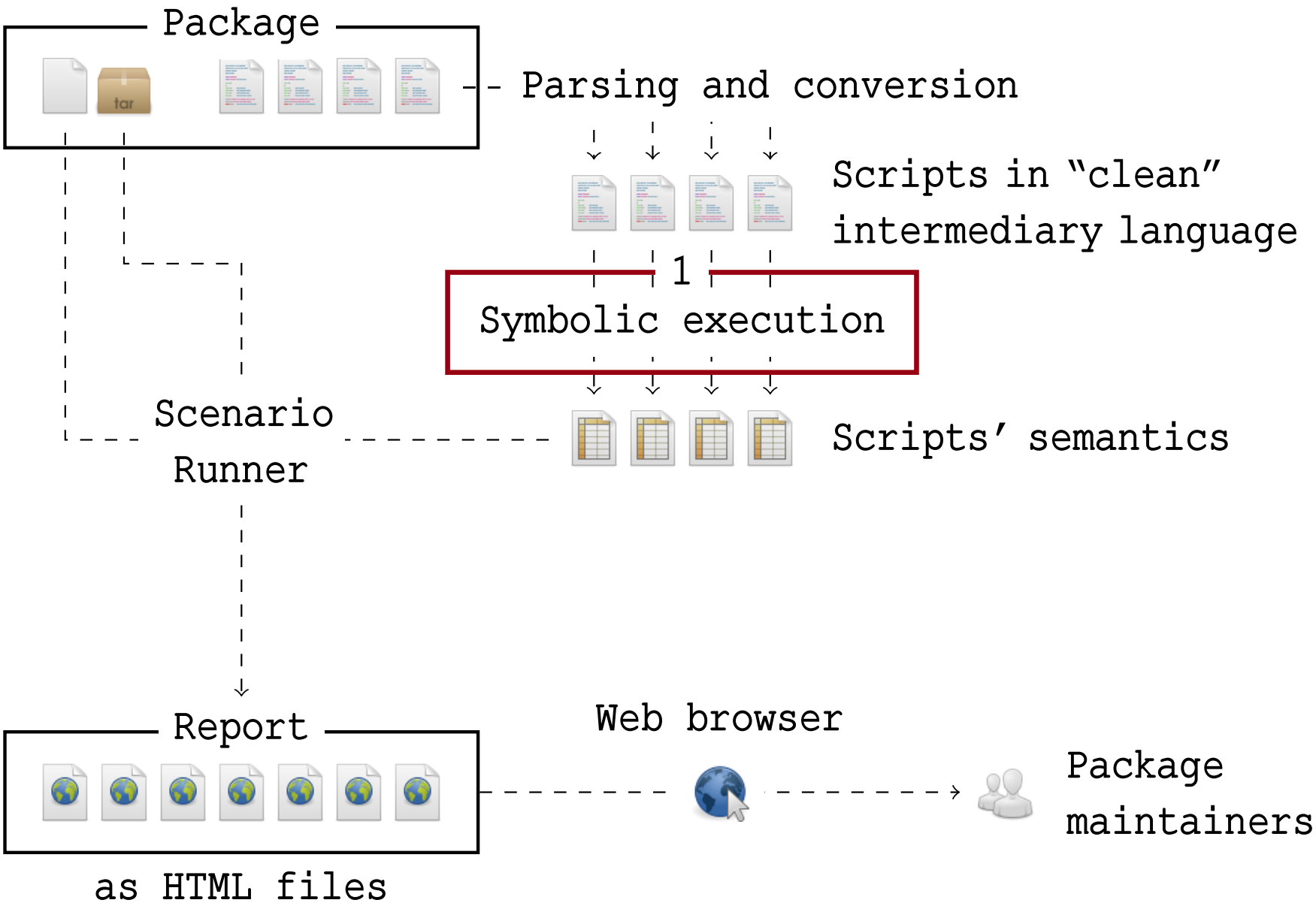
Battle Plan


Package
tar
Parsing and conversion
Scripts in "clean"
intermediary language
1
Symbolic execution
2
Scripts' semantics
Scenario
Runner
Report
Web browser
Package
maintainers
as HTML files

Battle Plan


Package
tar
Parsing and conversion
Scripts in "clean"
intermediary language
1
Symbolic execution
2
Scripts' semantics
3
Scenario
Runner
Report
as HTML files
Web browser
Package
maintainers

Battle Plan


Package
tar
Parsing and conversion
Scripts in "clean"
intermediary language
1
Symbolic execution
Scenario
Runner
Scripts' semantics
Report
Web browser
Package
maintainers
as HTML files

Symbolic Execution

```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```

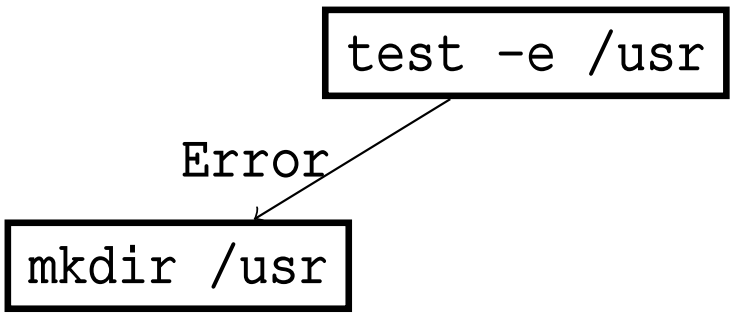
Symbolic Execution

```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```

`test -e /usr`

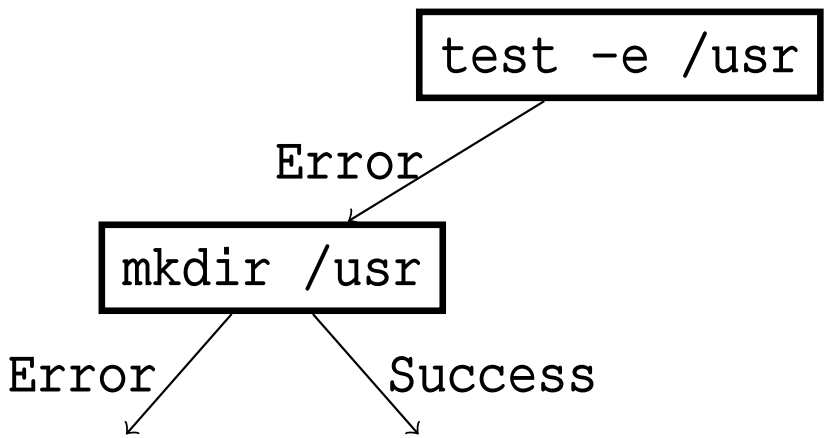
Symbolic Execution

```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```



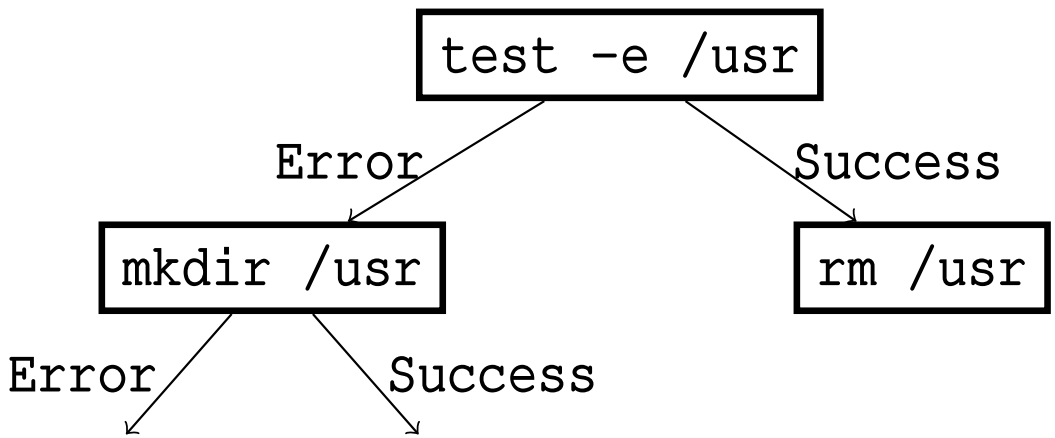
Symbolic Execution

```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```



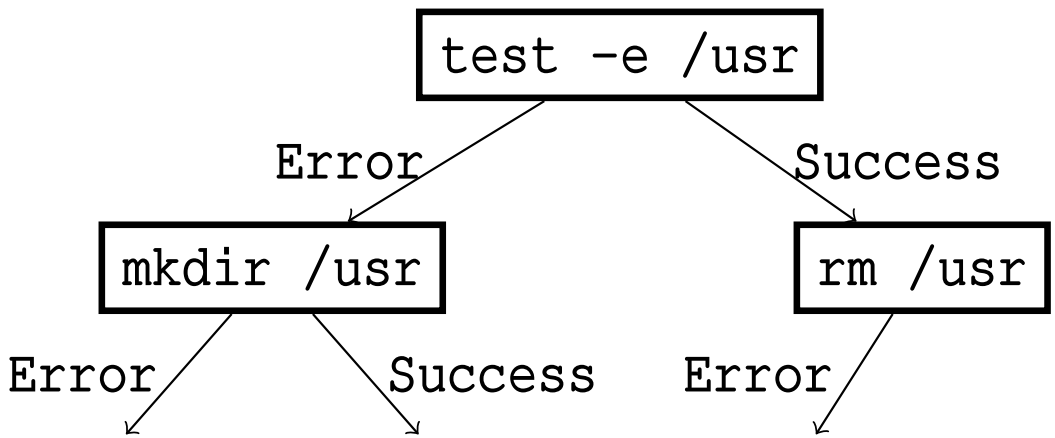
Symbolic Execution

```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```



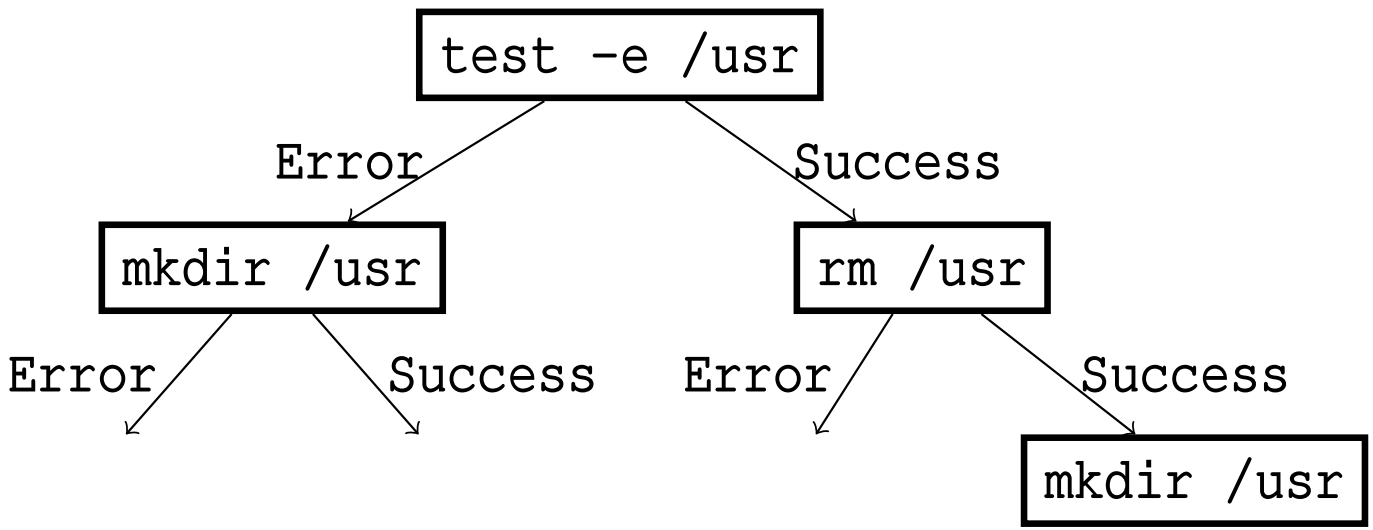
Symbolic Execution

```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```



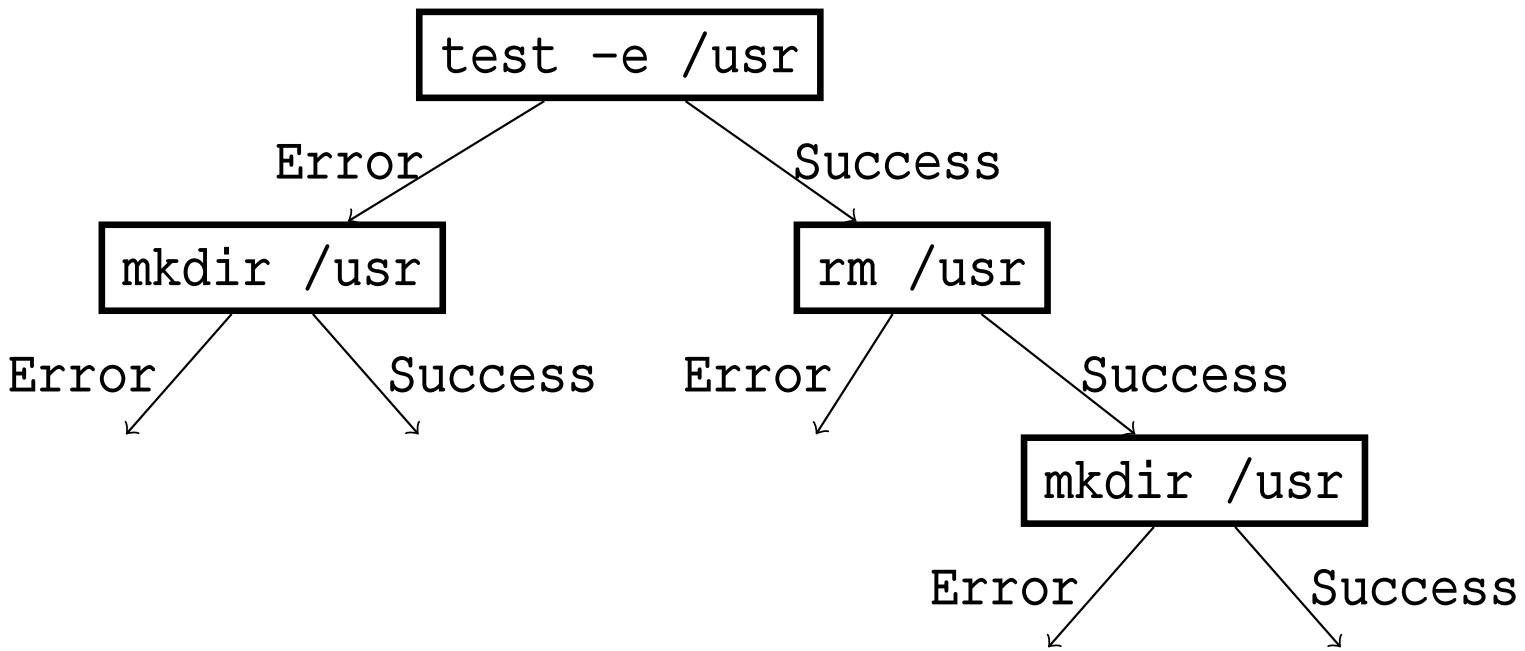
Symbolic Execution

```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```



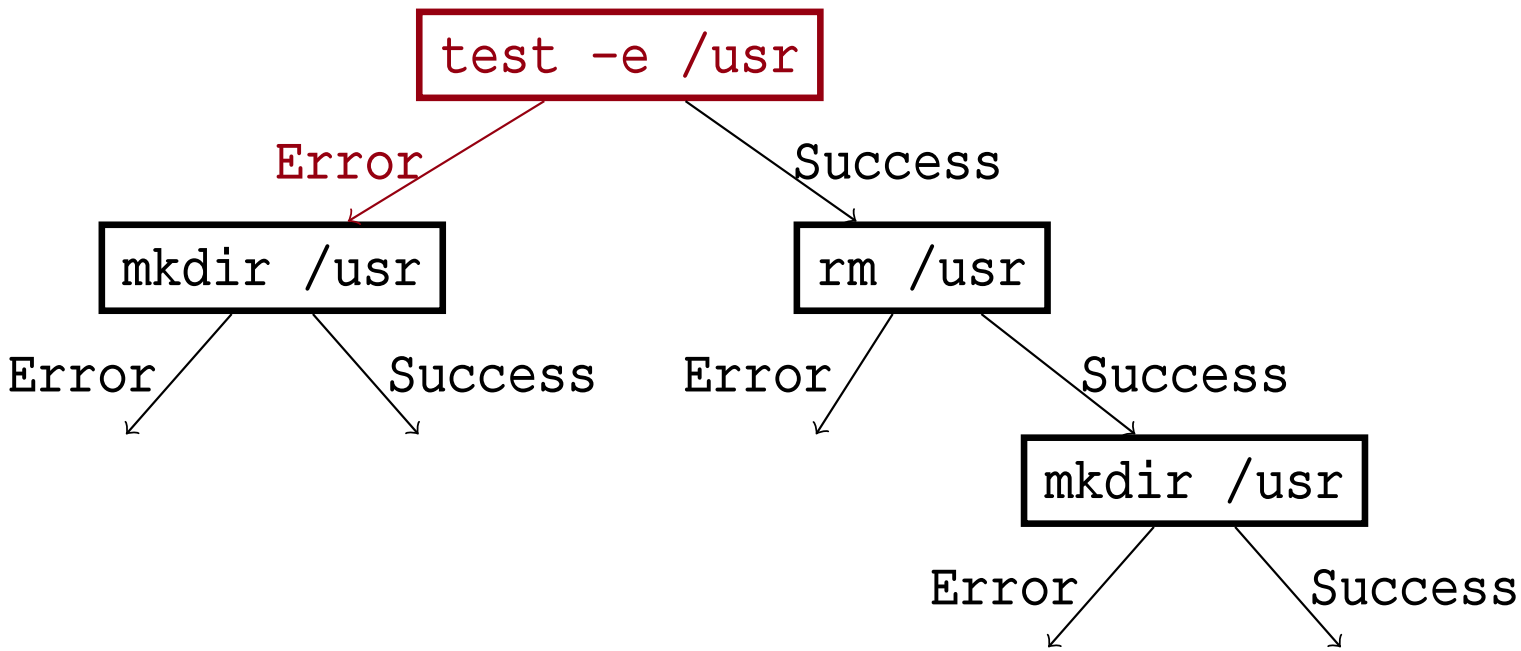
Symbolic Execution

```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```



Symbolic Execution

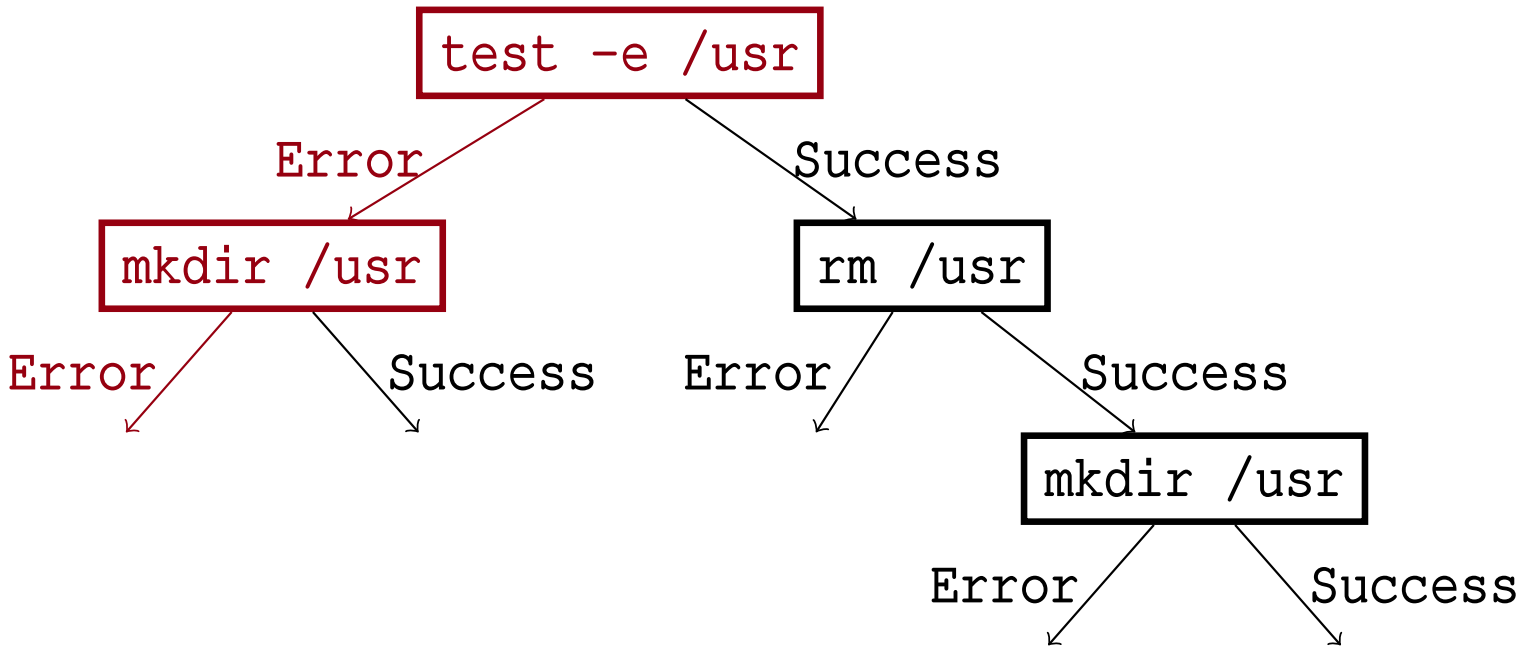
```
test -e /usr:
Success: /usr existed;
  nothing changed
Error: /usr did not exist;
  nothing changed
```



Symbolic Execution

```
test -e /usr:
Success: /usr existed;
  nothing changed
Error: /usr did not exist;
  nothing changed
```

```
mkdir /usr:
Success: /usr did not exist; it is now
  a directory
Error: /usr existed; nothing changed
```



Symbolic Execution

test -e /usr:

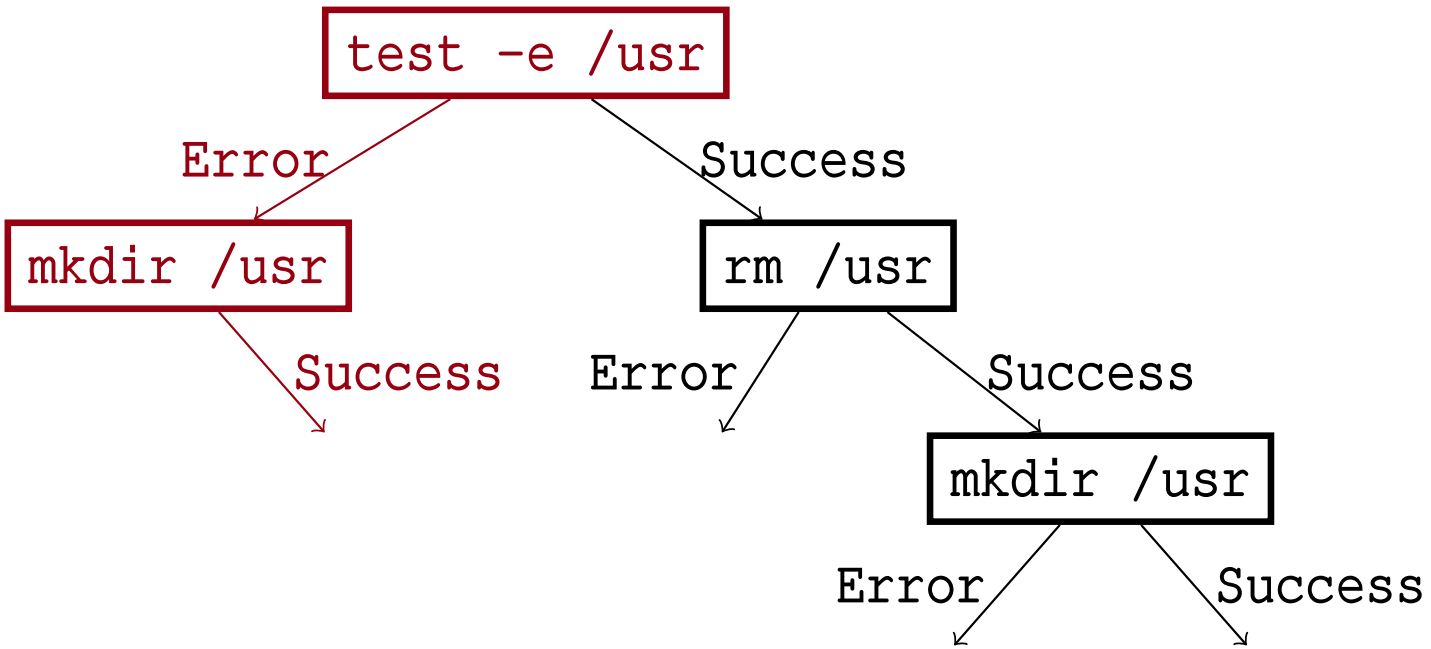
Success: /usr existed;
nothing changed

Error: /usr did not exist;
nothing changed

mkdir /usr:

Success: /usr did not exist; it is now
a directory

Error: /usr existed; nothing changed



Symbolic Execution

test -e /usr:

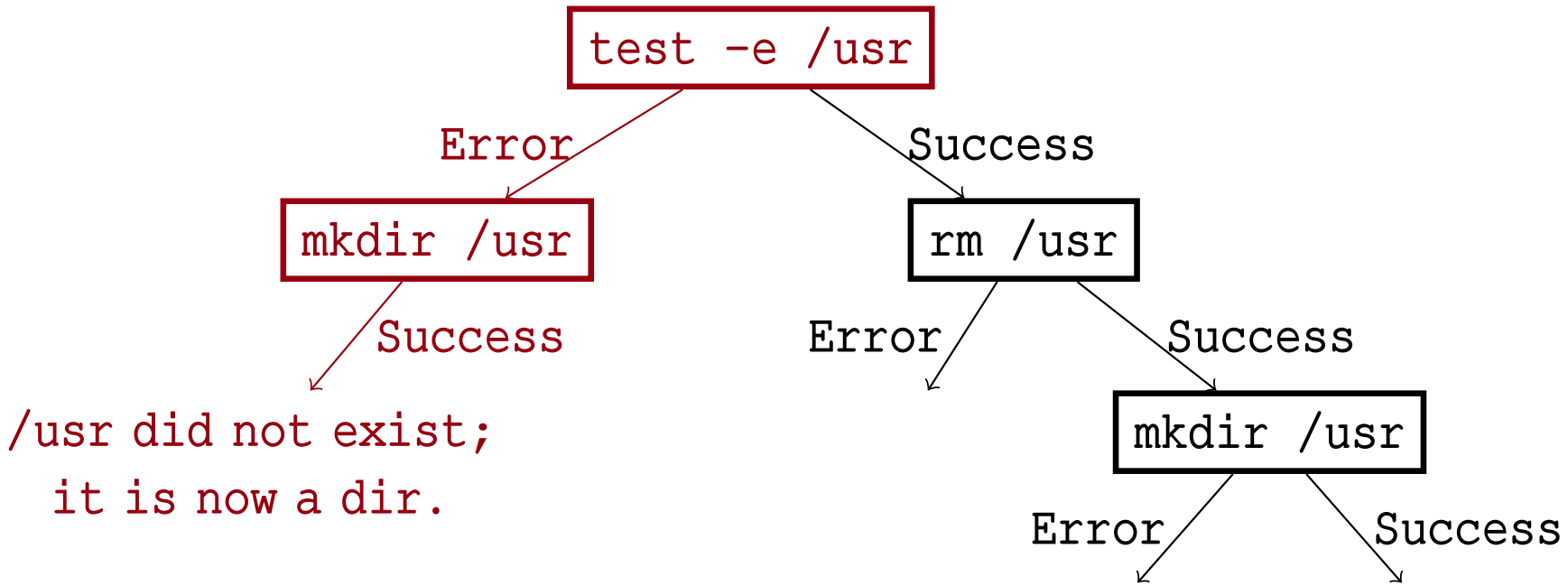
Success: /usr existed;
nothing changed

Error: /usr did not exist;
nothing changed

mkdir /usr:

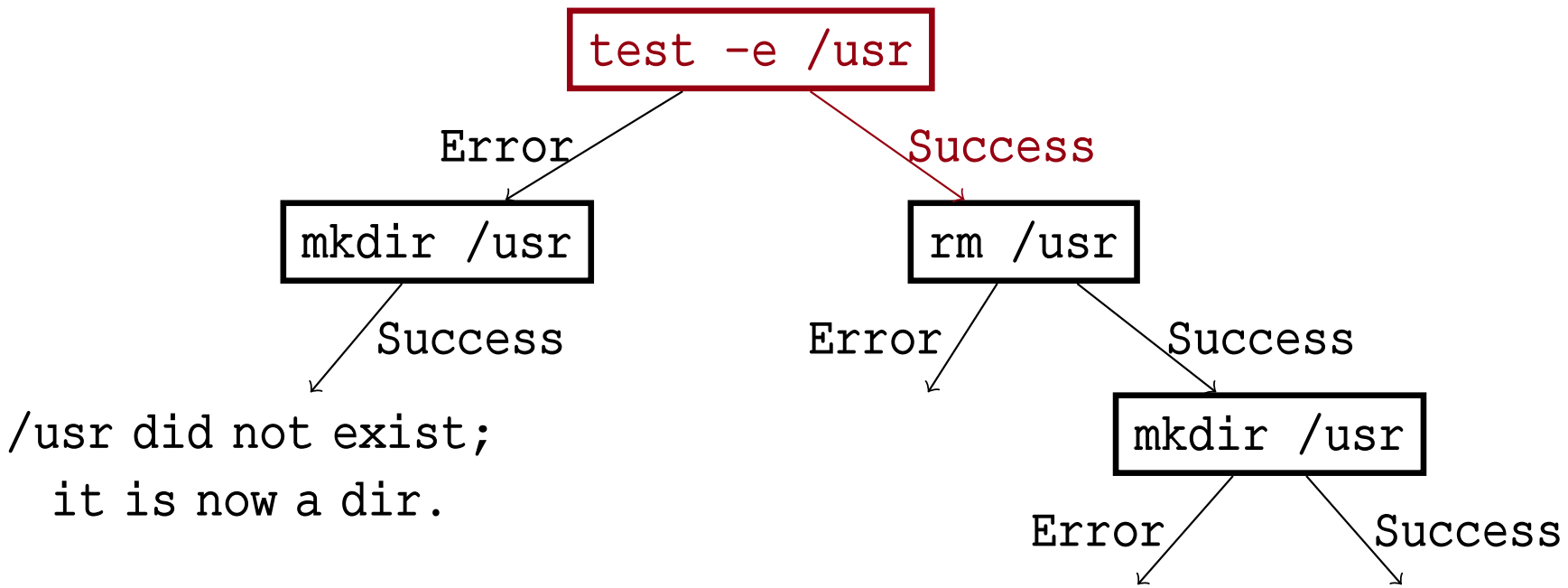
Success: /usr did not exist; it is now
a directory

Error: /usr existed; nothing changed



Symbolic Execution

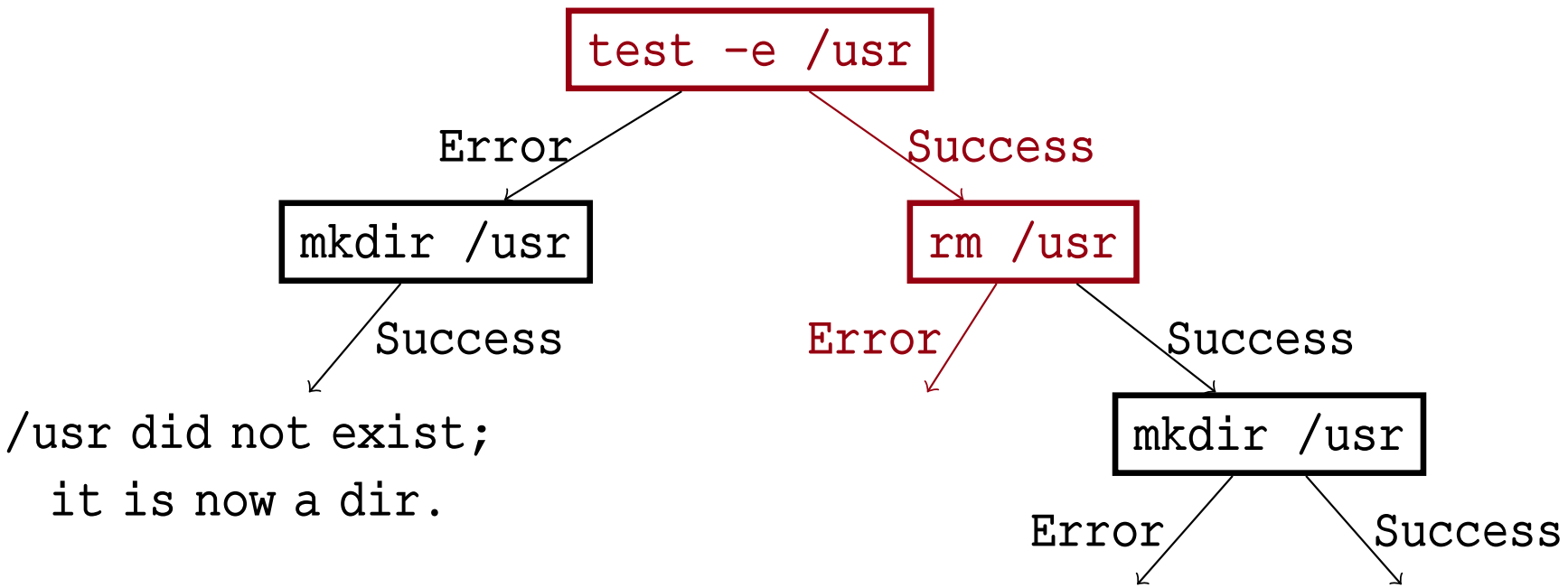
```
test -e /usr:
Success: /usr existed;
  nothing changed
Error: /usr did not exist;
  nothing changed
```



Symbolic Execution

```
test -e /usr:
Success: /usr existed;
  nothing changed
Error: /usr did not exist;
  nothing changed
```

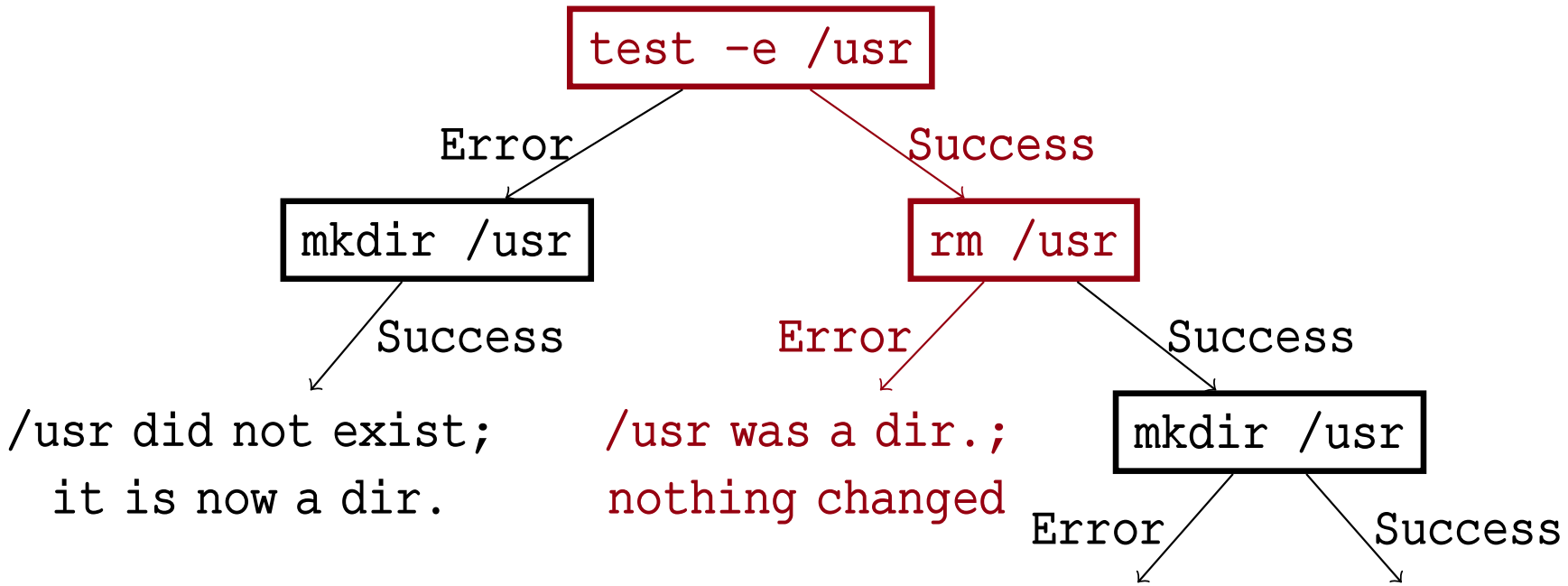
```
rm /usr:
Success: /usr existed and was not a
  directory; it does not exist anymore
Error: /usr did not exist or was a
  directory; nothing changed
```



Symbolic Execution

```
test -e /usr:
Success: /usr existed;
  nothing changed
Error: /usr did not exist;
  nothing changed
```

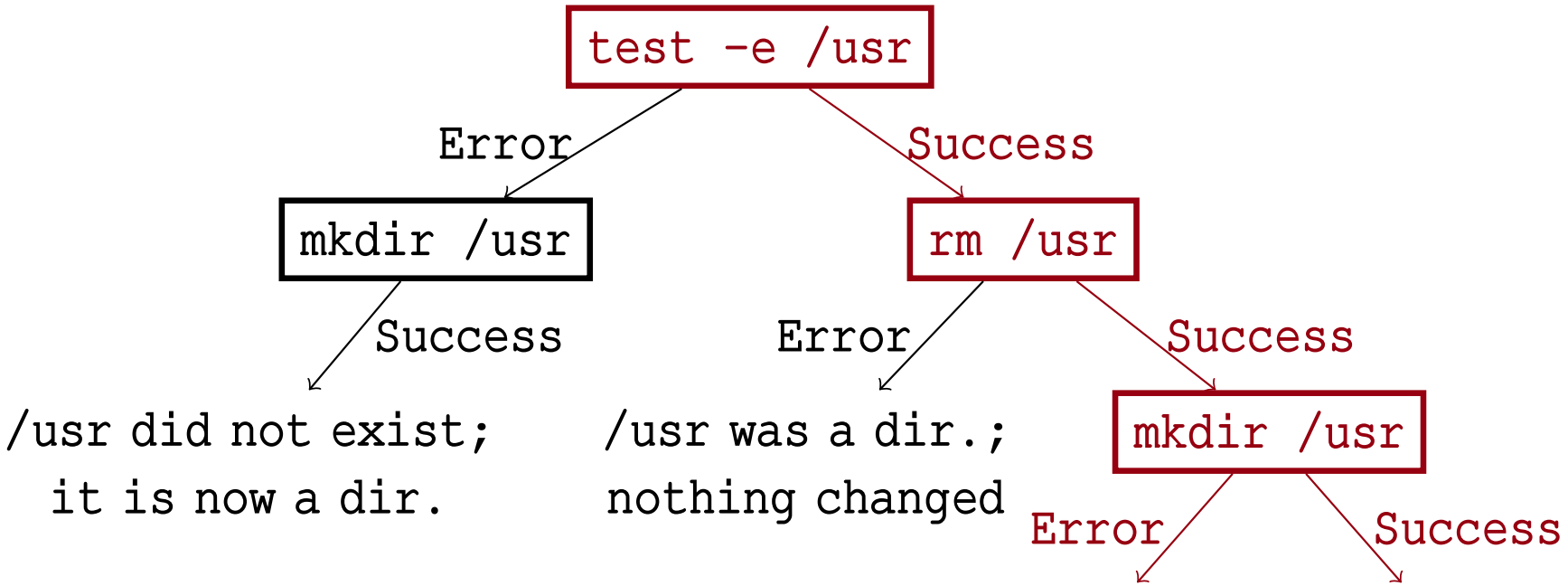
```
rm /usr:
Success: /usr existed and was not a
  directory; it does not exist anymore
Error: /usr did not exist or was a
  directory; nothing changed
```



Symbolic Execution

```
test -e /usr:
Success: /usr existed;
  nothing changed
Error: /usr did not exist;
  nothing changed
```

```
rm /usr:
Success: /usr existed and was not a
  directory; it does not exist anymore
Error: /usr did not exist or was a
  directory; nothing changed
```



Symbolic Execution

test -e /usr:

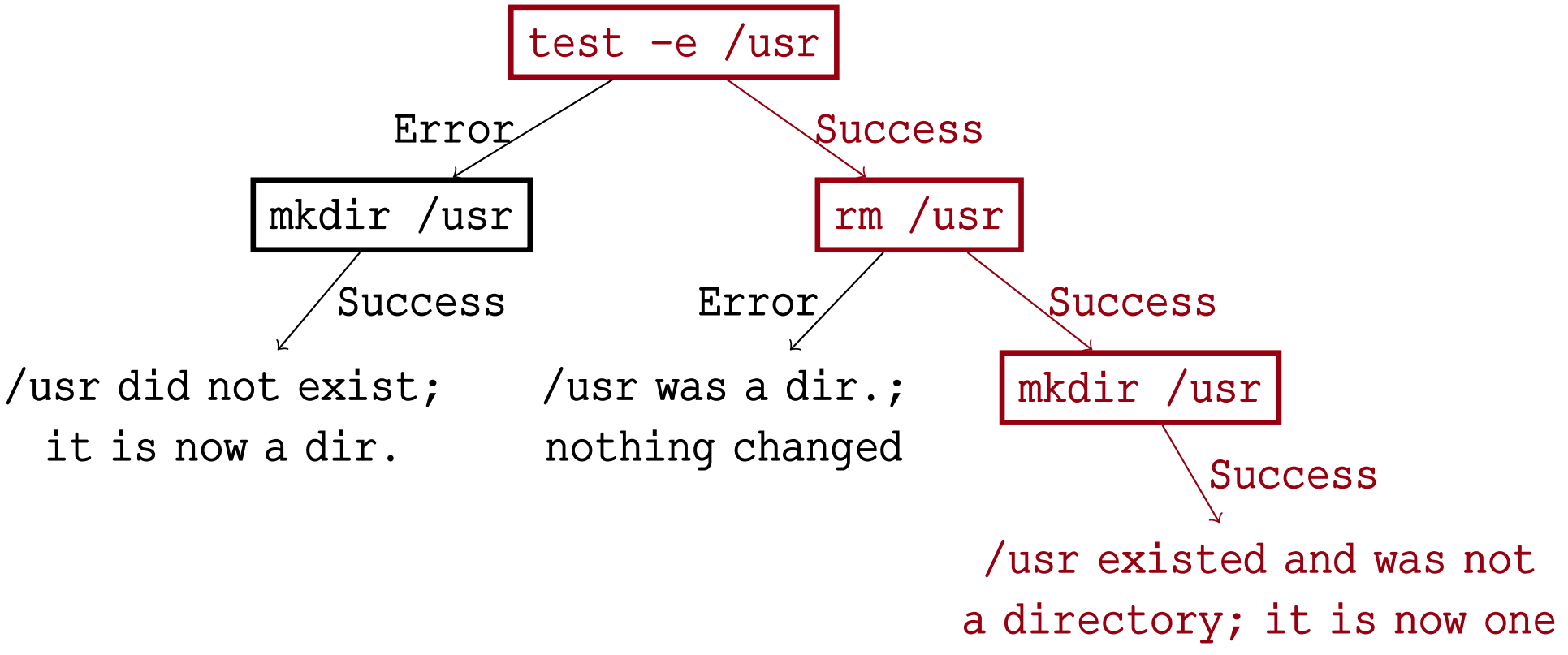
Success: /usr existed; nothing changed

Error: /usr did not exist; nothing changed

rm /usr:

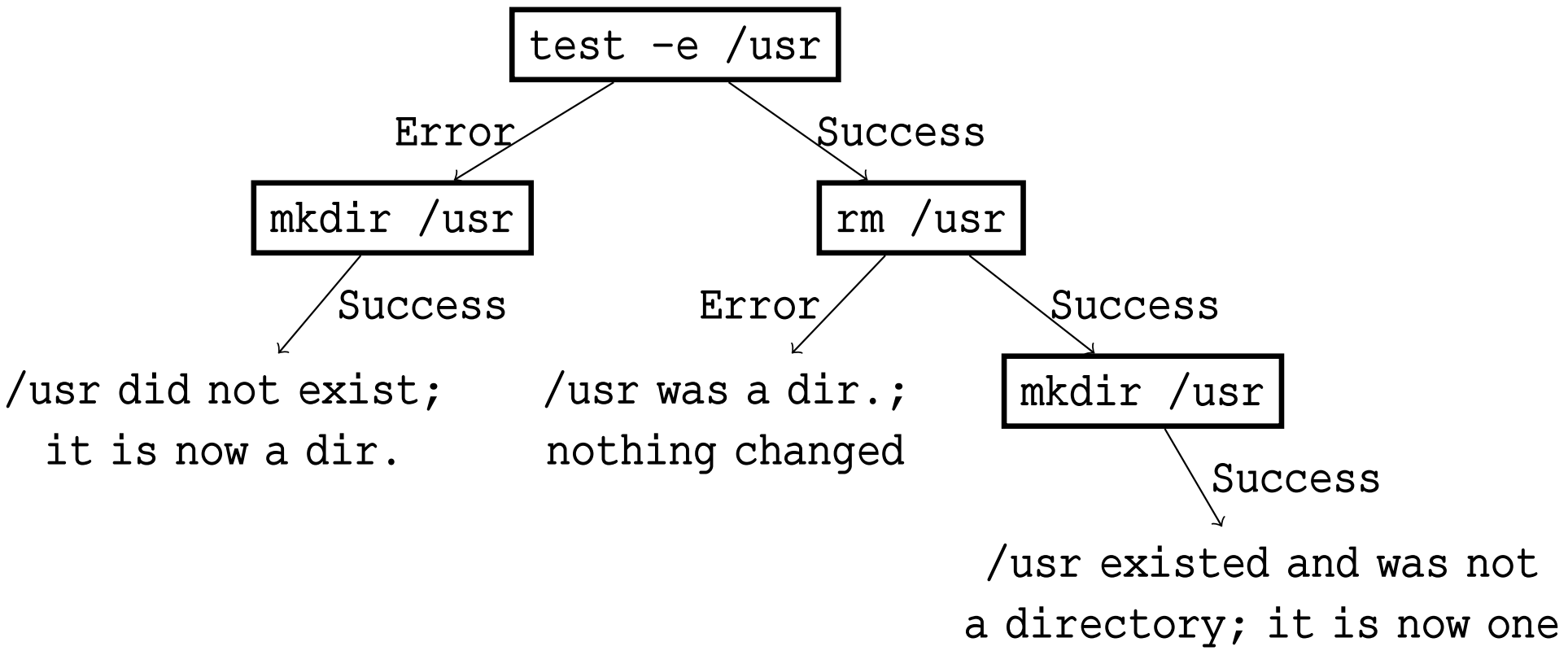
Success: /usr existed and was not a directory; it does not exist anymore

Error: /usr did not exist or was a directory; nothing changed



Symbolic Execution

```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```



Backend Requirements

Backend Requirements

Tree relations

Backend Requirements

Tree relations

Expressivity to specify POSIX utilities

Backend Requirements

Tree relations
Expressivity to specify POSIX utilities
Composition of relations

Backend Requirements

Tree relations
Expressivity to specify POSIX utilities
Composition of relations
Detection of impossible cases

Backend Requirements

Tree relations
Expressivity to specify POSIX utilities
Composition of relations
Detection of impossible cases
Transformation of a relation in a more understandable one

Backend Requirements

	Tree Transducers
Tree relations	
Expressivity to specify POSIX utilities	
Composition of relations	
Detection of impossible cases	
Transformation of a relation in a more understandable one	

Backend Requirements

	Tree Transducers	Feature Tree Logics
Tree relations		
Expressivity to specify POSIX utilities		
Composition of relations		
Detection of impossible cases		
Transformation of a relation in a more understandable one		

Backend Requirements

	Tree Transducers	Feature Tree Logics
Tree relations	by definition	
Expressivity to specify POSIX utilities		
Composition of relations		
Detection of impossible cases		
Transformation of a relation in a more understandable one		

Backend Requirements

	Tree Transducers	Feature Tree Logics
Tree relations	by definition	if two free variables
Expressivity to specify POSIX utilities		
Composition of relations		
Detection of impossible cases		
Transformation of a relation in a more understandable one		

Backend Requirements

	Tree Transducers	Feature Tree Logics
Tree relations	by definition	if two free variables
Expressivity to specify POSIX utilities	?	?
Composition of relations		
Detection of impossible cases		
Transformation of a relation in a more understandable one		

Backend Requirements

	Tree Transducers	Feature Tree Logics
Tree relations	by definition	if two free variables
Expressivity to specify POSIX utilities	?	?
Composition of relations	composition of transducers	
Detection of impossible cases		
Transformation of a relation in a more understandable one		

Backend Requirements

	Tree Transducers	Feature Tree Logics
Tree relations	by definition	if two free variables
Expressivity to specify POSIX utilities	?	?
Composition of relations	composition of transducers	$\exists \mathrm{r}' \cdot \phi_1(\mathrm{r}_1, \mathrm{r}') \wedge \phi_2(\mathrm{r}', \mathrm{r}_2)$
Detection of impossible cases		
Transformation of a relation in a more understandable one		

Backend Requirements

	Tree Transducers	Feature Tree Logics
Tree relations	by definition	if two free variables
Expressivity to specify POSIX utilities	?	?
Composition of relations	composition of transducers	$\exists \mathrm{r}' \cdot \phi_1(\mathrm{r}_1, \mathrm{r}') \wedge \phi_2(\mathrm{r}', \mathrm{r}_2)$
Detection of impossible cases	emptiness of the domain	
Transformation of a relation in a more understandable one		

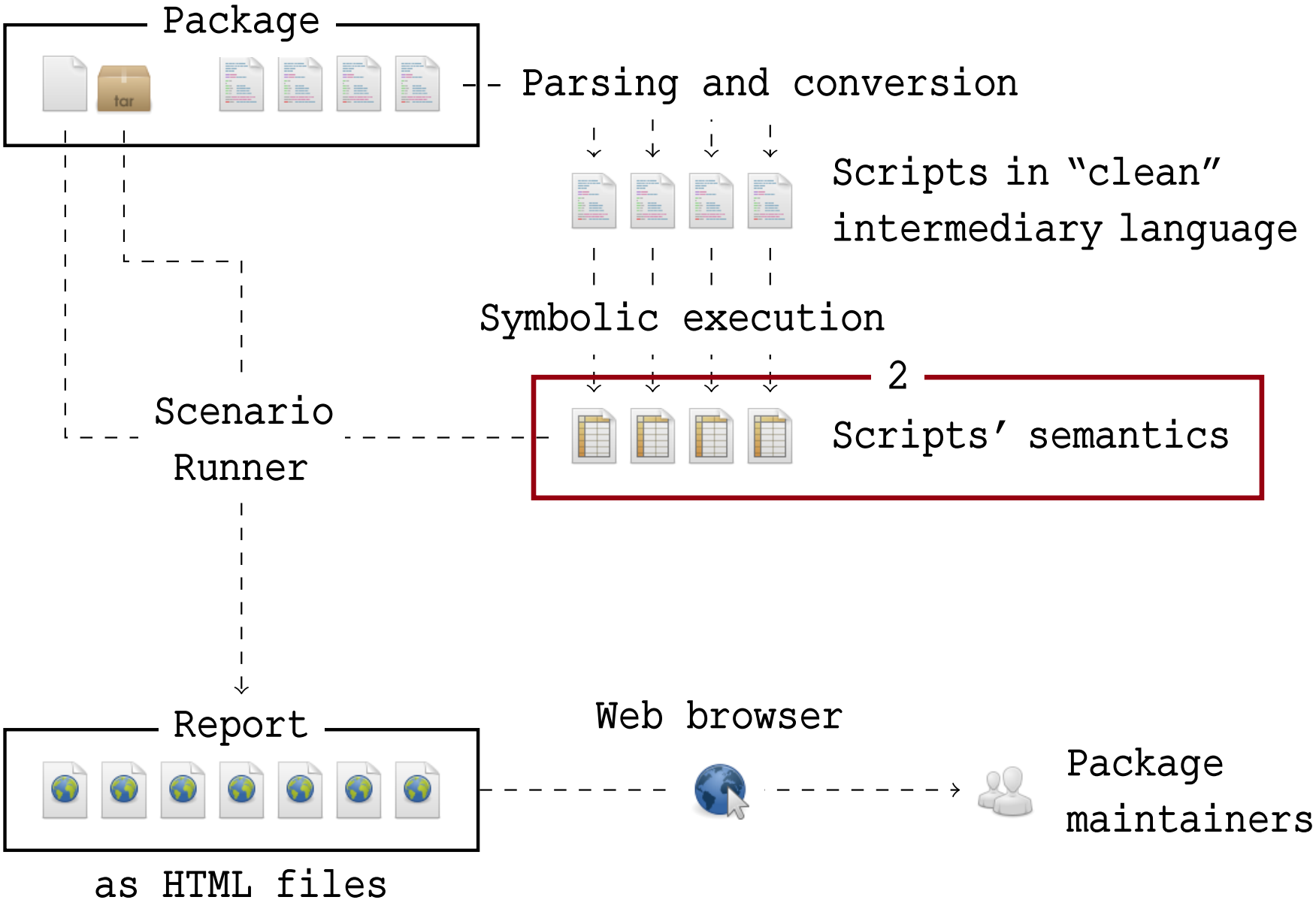
Backend Requirements

	Tree Transducers	Feature Tree Logics
Tree relations	by definition	if two free variables
Expressivity to specify POSIX utilities	?	?
Composition of relations	composition of transducers	$\exists \mathrm{r}' \cdot \phi_1(\mathrm{r}_1, \mathrm{r}') \wedge \phi_2(\mathrm{r}', \mathrm{r}_2)$
Detection of impossible cases	emptiness of the domain	unsatisfiability
Transformation of a relation in a more understandable one		

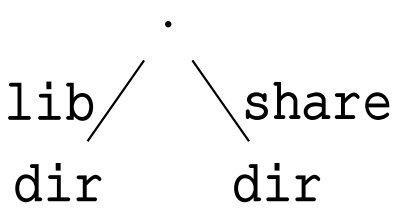
Backend Requirements

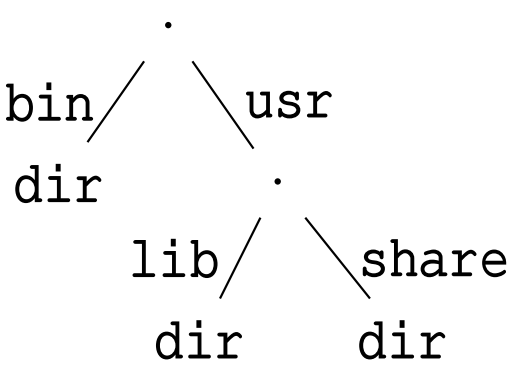
	Tree Transducers	Feature Tree Logics
Tree relations	by definition	if two free variables
Expressivity to specify POSIX utilities	?	?
Composition of relations	composition of transducers	$\exists \mathrm{r}' \cdot \phi_1(\mathrm{r}_1, \mathrm{r}') \wedge \phi_2(\mathrm{r}', \mathrm{r}_2)$
Detection of impossible cases	emptiness of the domain	unsatisfiability
Transformation of a relation in a more understandable one	?	?

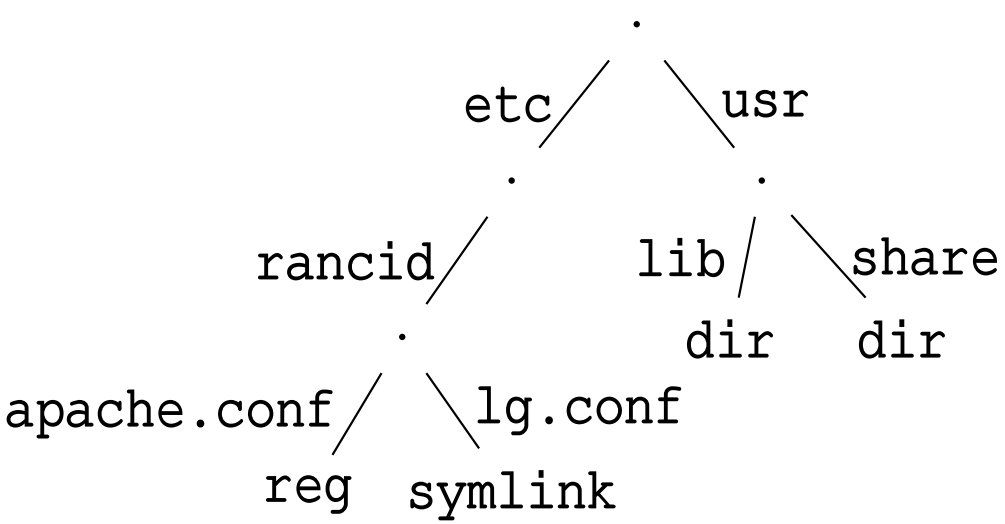
Battle Plan


Package
tar
Parsing and conversion
Scripts in "clean"
intermediary language
Symbolic execution
2
Scripts' semantics
Scenario
Runner
Report
Web browser
Package
maintainers
as HTML files

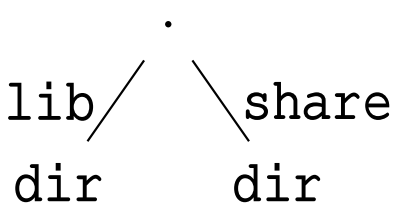
Feature Trees

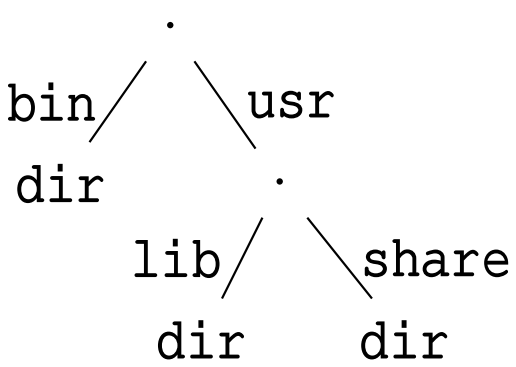


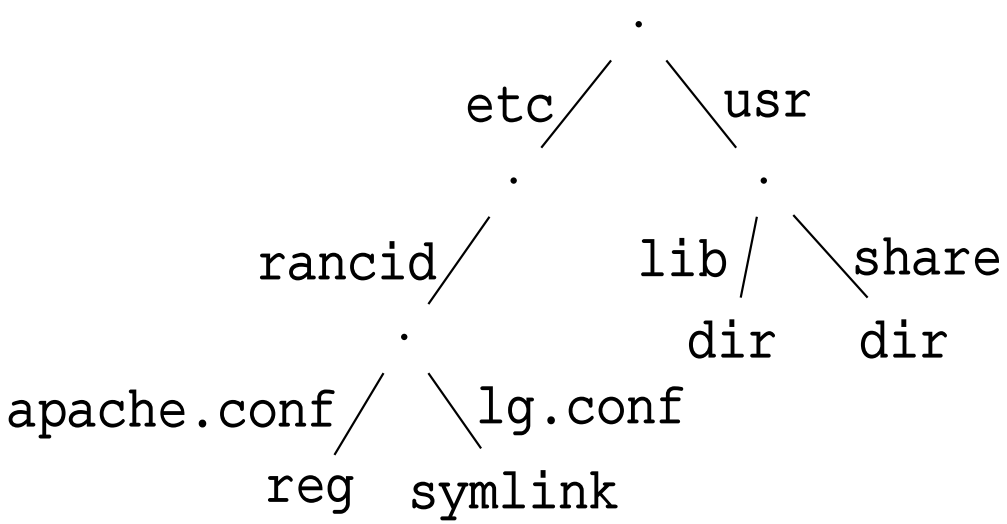




Feature Trees







$$\mathcal{FT} := \texttt{reg} \mid \texttt{symlink} \mid \cdots \mid \texttt{dir}(\mathcal{F} \rightsquigarrow \mathcal{FT})$$

Basic Constraints

Basic Constraints

Equality	$x = y$

Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$

Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	

Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x[f]y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$

Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$
Absence	$\mathtt{x}[\mathtt{f}]\uparrow$	

Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$
Absence	$\mathtt{x}[\mathtt{f}]\uparrow$	$\mathtt{f} \notin \mathtt{dom}(\rho(\mathtt{x}))$

Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$
Absence	$\mathtt{x}[\mathtt{f}]\uparrow$	$\mathtt{f} \notin \mathtt{dom}(\rho(\mathtt{x}))$
Fence	$\mathtt{x}[\mathtt{F}]$	

Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$
Absence	$\mathtt{x}[\mathtt{f}]\uparrow$	$\mathtt{f} \notin \mathtt{dom}(\rho(\mathtt{x}))$
Fence	$\mathtt{x}[\mathtt{F}]$	$\mathtt{dom}(\rho(\mathtt{x})) \subseteq \mathtt{F}$

Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$
Absence	$\mathtt{x}[\mathtt{f}]\uparrow$	$\mathtt{f} \notin \mathtt{dom}(\rho(\mathtt{x}))$
Fence	$\mathtt{x}[\mathtt{F}]$	$\mathtt{dom}(\rho(\mathtt{x})) \subseteq \mathtt{F}$
Similarity	$\mathtt{x} \sim_{\mathtt{F}} \mathtt{y}$	

Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$
Absence	$\mathtt{x}[\mathtt{f}]\uparrow$	$\mathtt{f} \notin \mathtt{dom}(\rho(\mathtt{x}))$
Fence	$\mathtt{x}[\mathtt{F}]$	$\mathtt{dom}(\rho(\mathtt{x})) \subseteq \mathtt{F}$
Similarity	$\mathtt{x} \sim_{\mathtt{F}} \mathtt{y}$	$\rho(\mathtt{x})_{\mid \mathtt{C}_\mathtt{F}} = \rho(\mathtt{y})_{\mid \mathtt{C}_\mathtt{F}}$

Basic Constraints

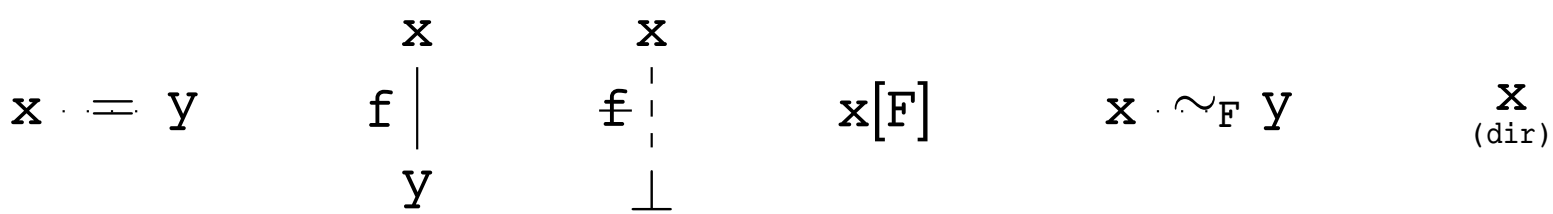
		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$
Absence	$\mathtt{x}[\mathtt{f}]\uparrow$	$\mathtt{f} \notin \mathtt{dom}(\rho(\mathtt{x}))$
Fence	$\mathtt{x}[\mathtt{F}]$	$\mathtt{dom}(\rho(\mathtt{x})) \subseteq \mathtt{F}$
Similarity	$\mathtt{x} \sim_{\mathtt{F}} \mathtt{y}$	$\rho(\mathtt{x})_{\mid \mathtt{C_F}} = \rho(\mathtt{y})_{\mid \mathtt{C_F}}$
Directory	$\mathtt{dir}(\mathtt{x})$	

Basic Constraints

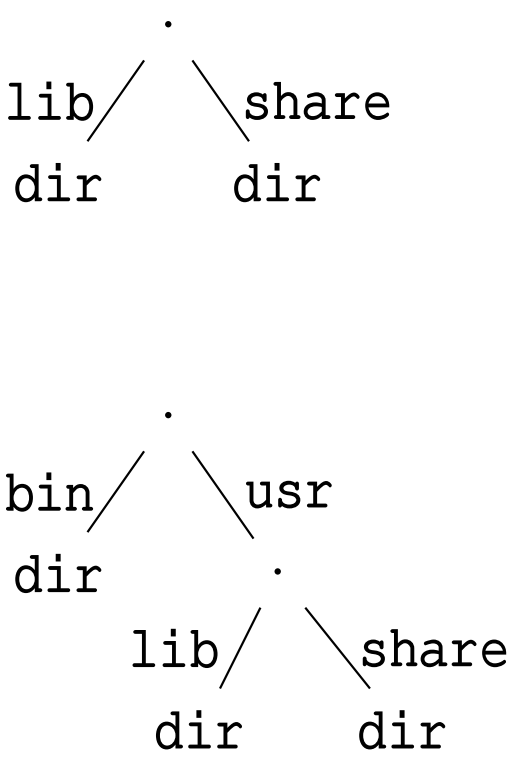
		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$
Absence	$\mathtt{x}[\mathtt{f}]\uparrow$	$\mathtt{f} \notin \mathtt{dom}(\rho(\mathtt{x}))$
Fence	$\mathtt{x}[\mathtt{F}]$	$\mathtt{dom}(\rho(\mathtt{x})) \subseteq \mathtt{F}$
Similarity	$\mathtt{x} \sim_{\mathtt{F}} \mathtt{y}$	$\rho(\mathtt{x})_{\mid \mathtt{C_F}} = \rho(\mathtt{y})_{\mid \mathtt{C_F}}$
Directory	$\mathtt{dir}(\mathtt{x})$	$\rho(\mathtt{x}) = \mathtt{dir}$

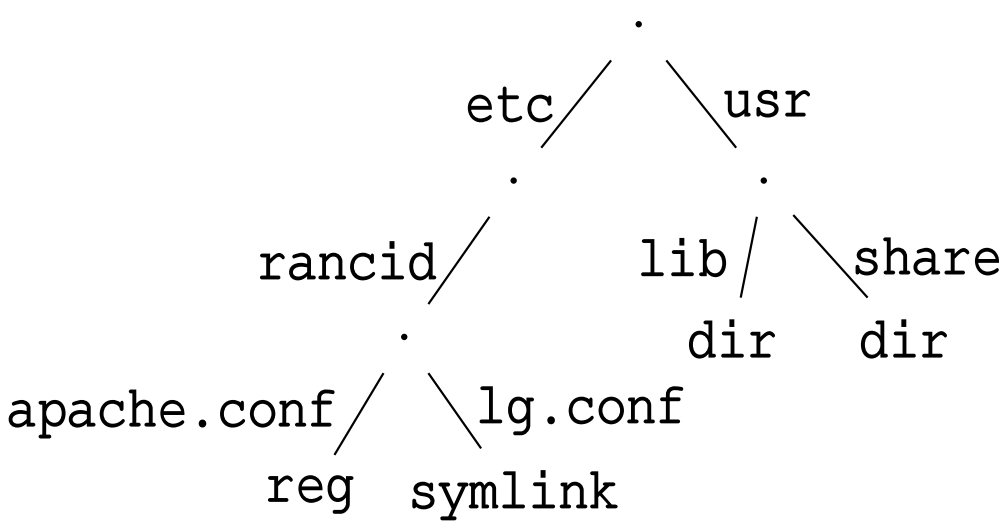
Basic Constraints

		ρ is a model if
Equality	$\mathtt{x} = \mathtt{y}$	$\rho(\mathtt{x}) = \rho(\mathtt{y})$
Feature	$\mathtt{x}[\mathtt{f}]\mathtt{y}$	$\rho(\mathtt{x})(\mathtt{f}) = \rho(\mathtt{y})$
Absence	$\mathtt{x}[\mathtt{f}]\uparrow$	$\mathtt{f} \notin \mathtt{dom}(\rho(\mathtt{x}))$
Fence	$\mathtt{x}[\mathtt{F}]$	$\mathtt{dom}(\rho(\mathtt{x})) \subseteq \mathtt{F}$
Similarity	$\mathtt{x} \sim_{\mathtt{F}} \mathtt{y}$	$\rho(\mathtt{x})_{\mid \mathtt{C_F}} = \rho(\mathtt{y})_{\mid \mathtt{C_F}}$
Directory	$\mathtt{dir}(\mathtt{x})$	$\rho(\mathtt{x}) = \mathtt{dir}$

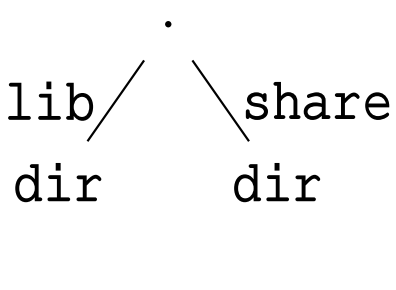


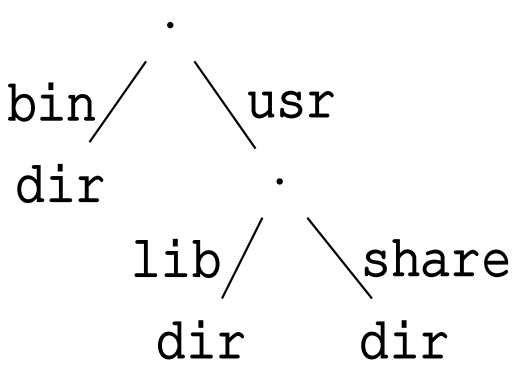
An Example

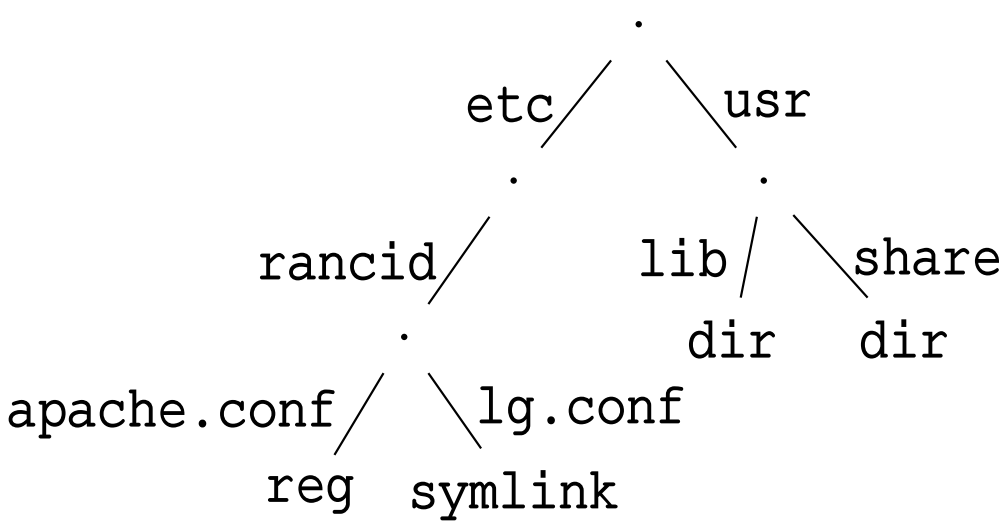

.
lib
share
dir
dir
.
bin
usr
dir
.
lib
share
dir
dir


.
etc
usr
.
.
rancid
lib
share
.
dir
dir
apache.conf
lg.conf
reg
symlink

An Example

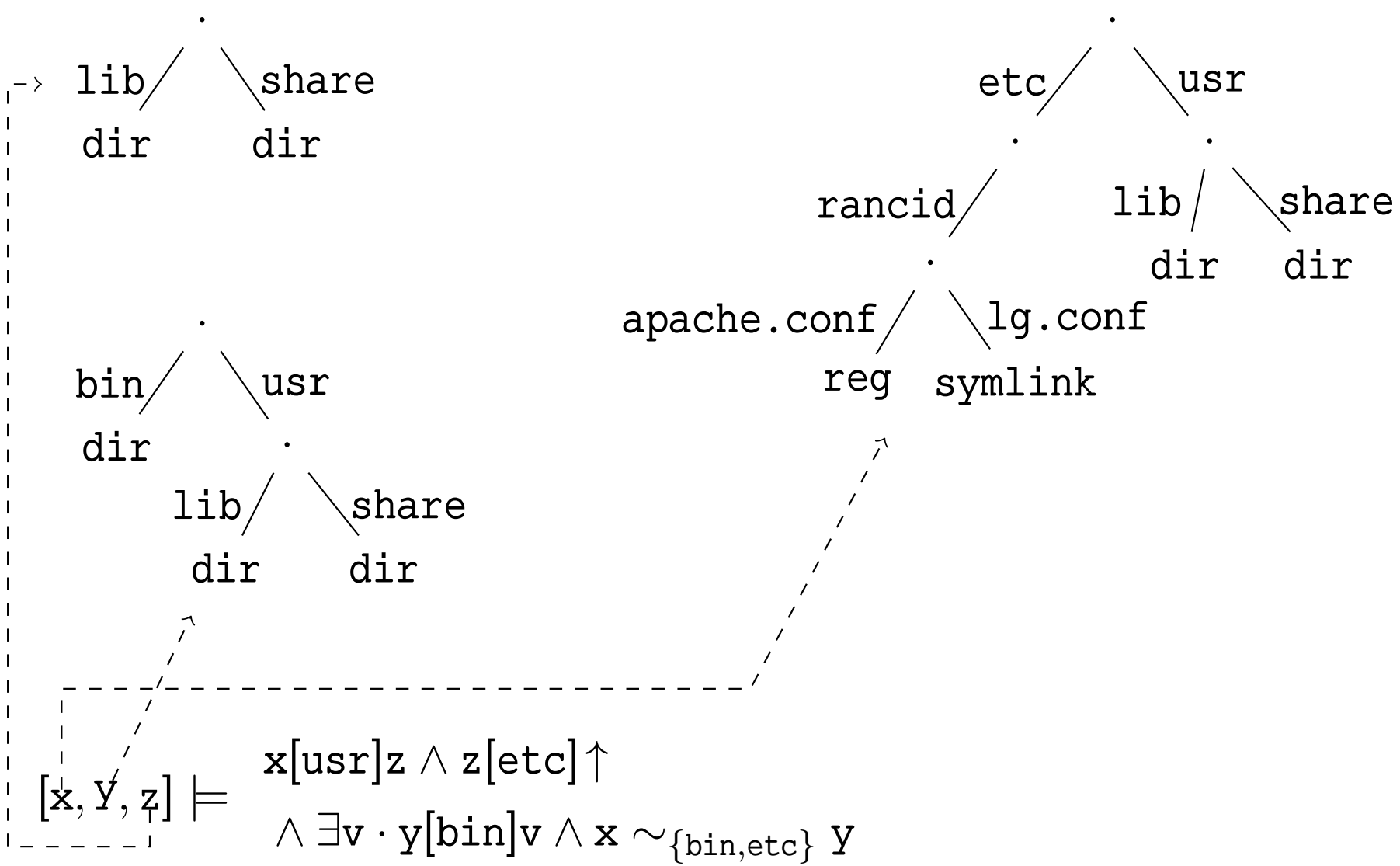




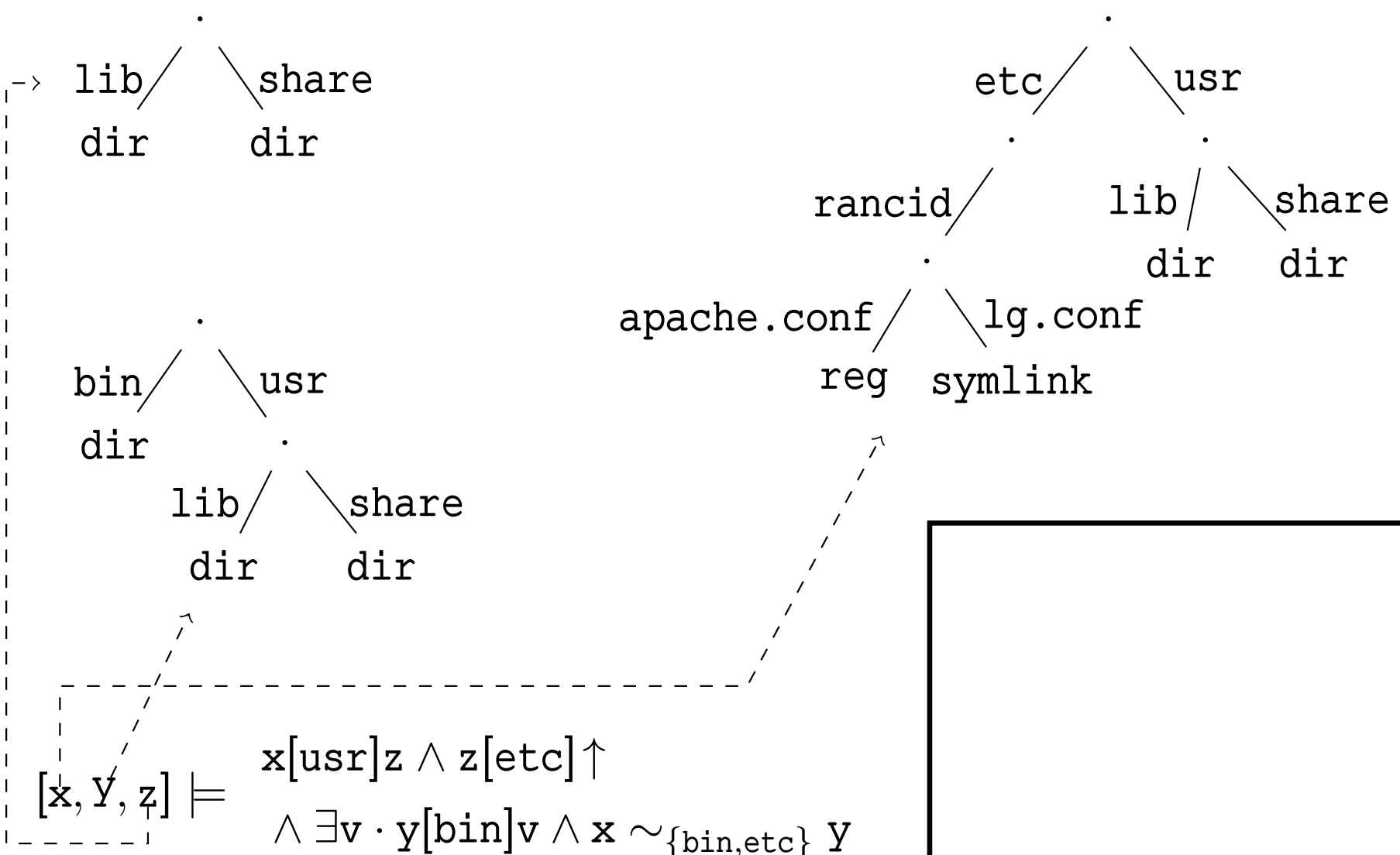


$$x[\mathtt{usr}]z \wedge z[\mathtt{etc}]{\uparrow}$$
$$\wedge\, \exists v \cdot y[\mathtt{bin}]v \wedge x \sim_{\{\mathtt{bin},\mathtt{etc}\}} y$$

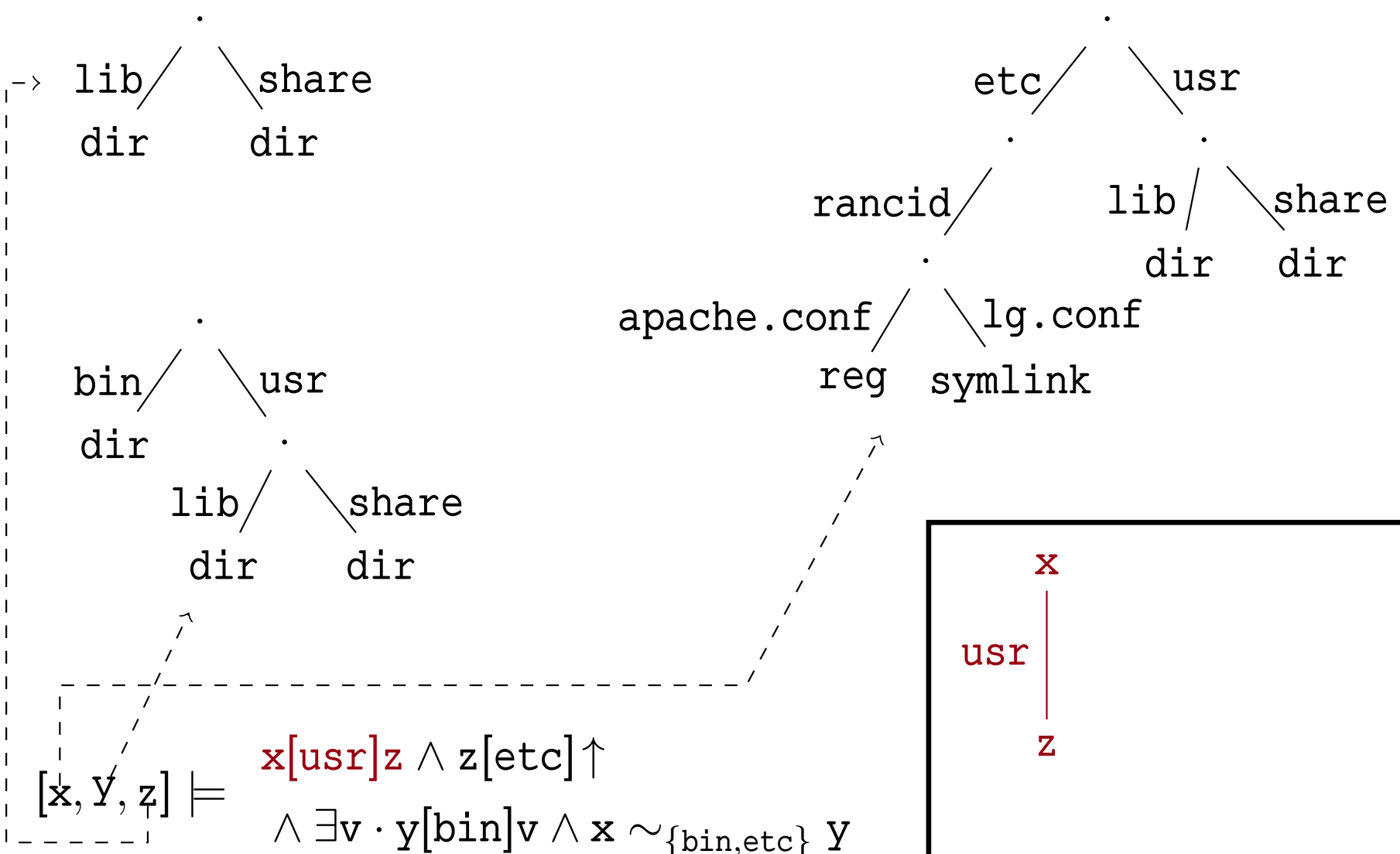
An Example

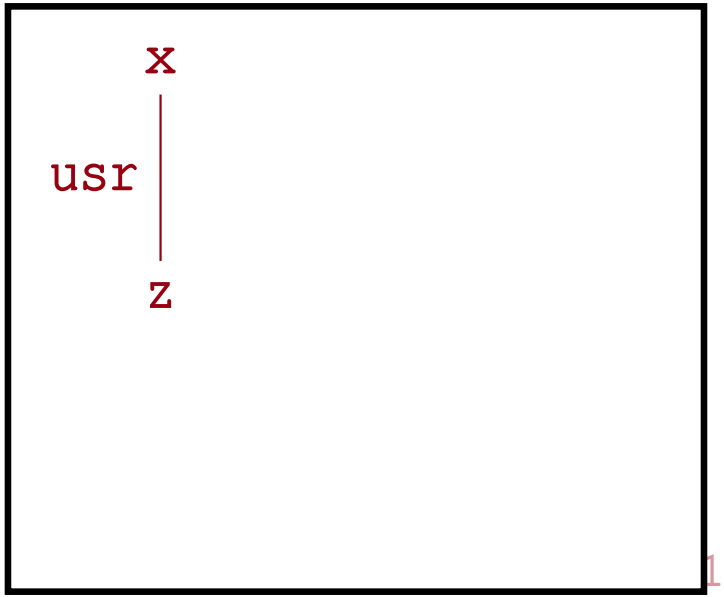

lib
share
dir
dir
etc
usr
rancid
lib
share
dir
dir
apache.conf
lg.conf
reg
symlink
bin
usr
dir
lib
share
dir
dir
[x, y, z] ⊨
x[usr]z ∧ z[etc]↑
∧ ∃v · y[bin]v ∧ x ∼{bin,etc} y

An Example

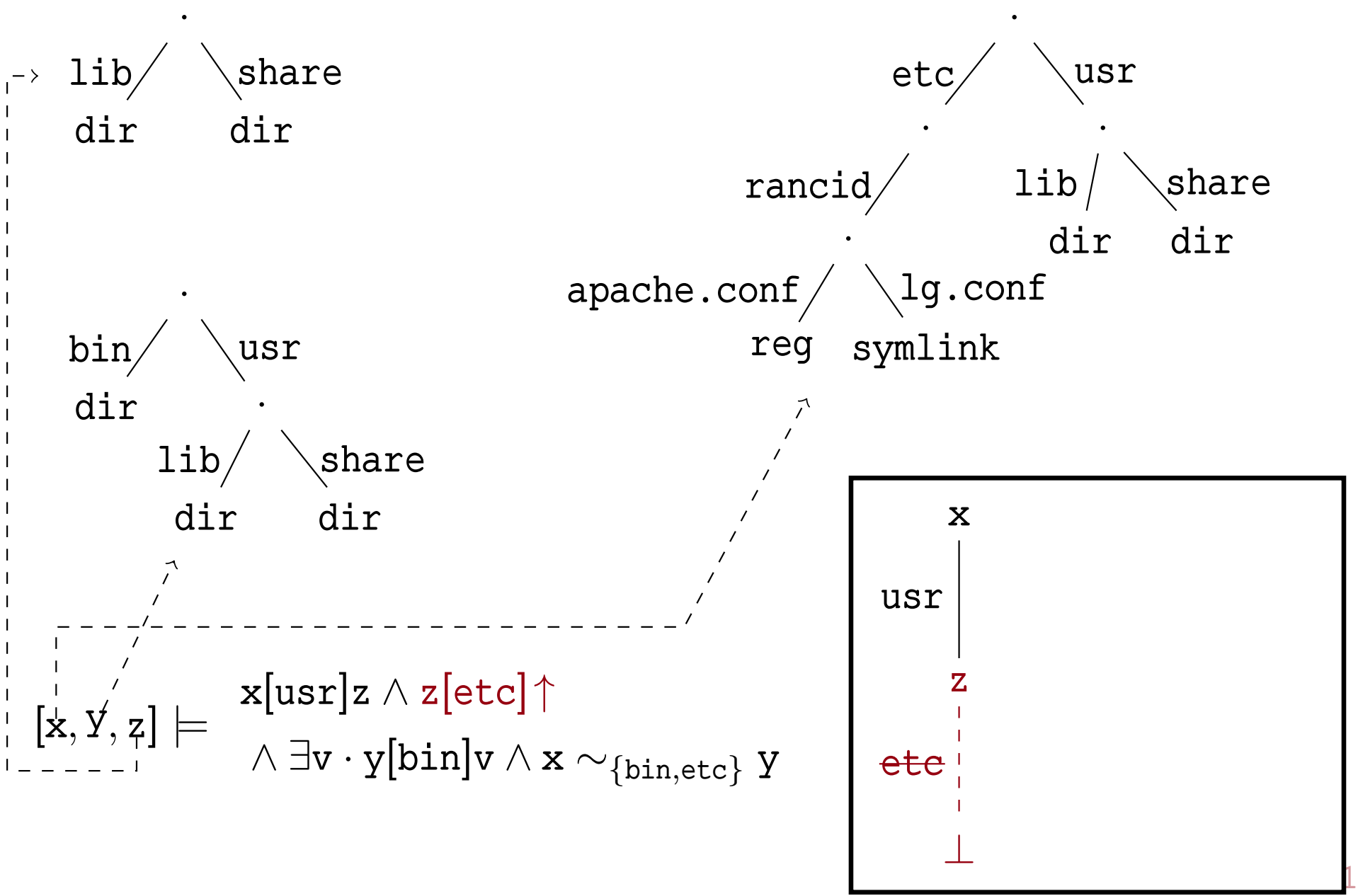

.
lib
share
dir
dir
.
bin
usr
dir
.
lib
share
dir
dir
.
etc
usr
.
.
rancid
lib
share
.
dir
dir
apache.conf
lg.conf
reg
symlink
[x, y, z] ⊨
x[usr]z ∧ z[etc]↑
∧ ∃v · y[bin]v ∧ x ∼{bin,etc} y

An Example

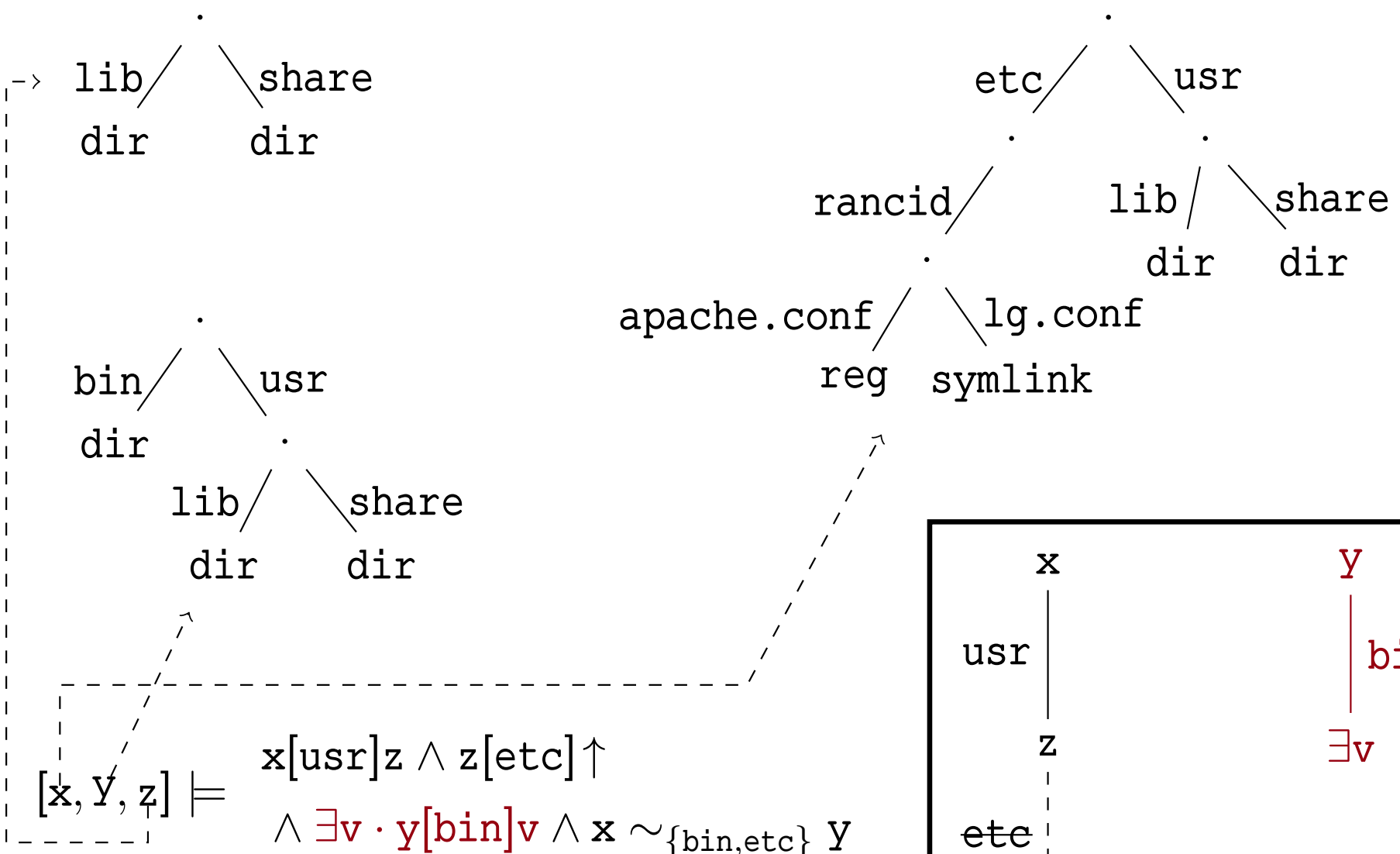

lib
share
dir
dir
etc
usr
rancid
lib
share
dir
dir
apache.conf
lg.conf
reg
symlink
bin
usr
dir
lib
share
dir
dir
[x, y, z] ⊨
x[usr]z ∧ z[etc]↑
∧ ∃v · y[bin]v ∧ x ∼{bin,etc} y

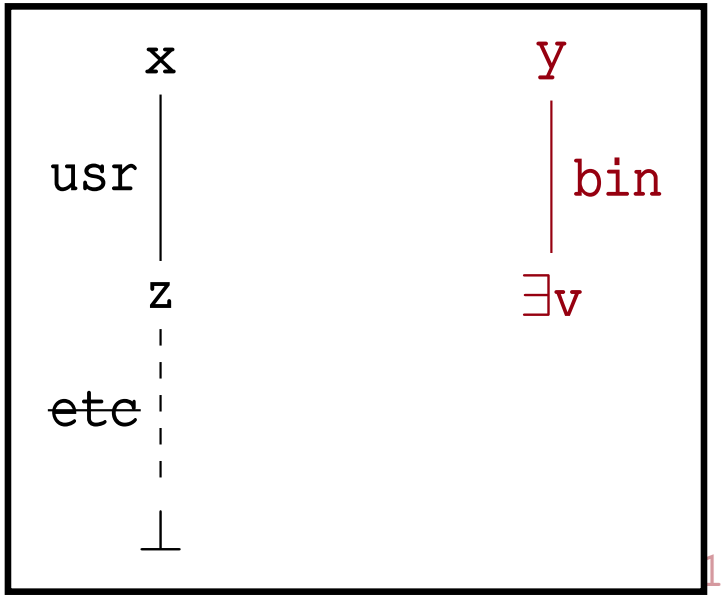

x
usr
z

An Example

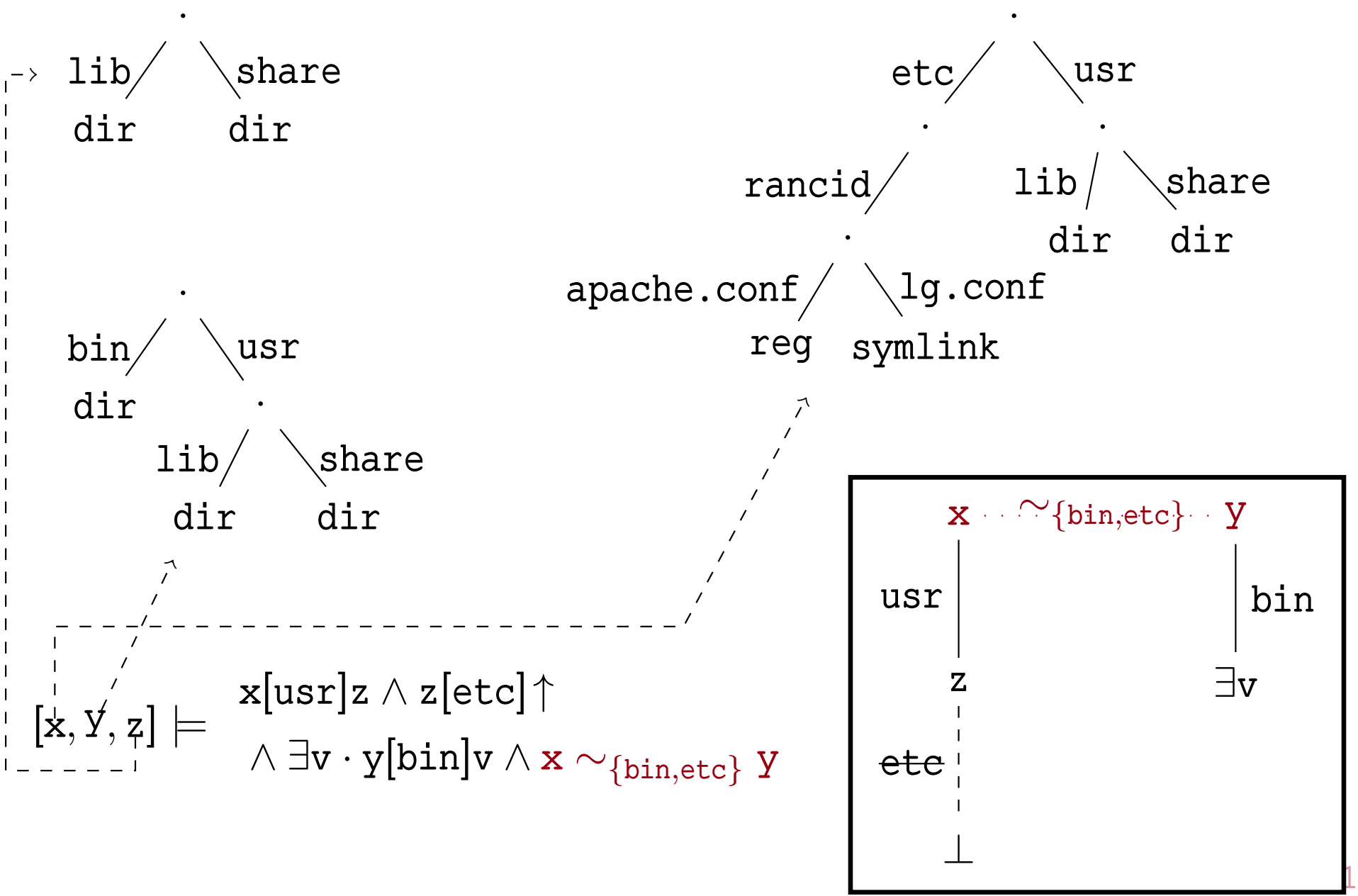

lib
share
dir
dir
etc
usr
rancid
lib
share
dir
dir
apache.conf
lg.conf
reg
symlink
bin
usr
dir
lib
share
dir
dir
[x, y, z] ⊨
x[usr]z ∧ z[etc]↑
∧ ∃v · y[bin]v ∧ x ∼{bin,etc} y
x
usr
z
etc
⊥

An Example

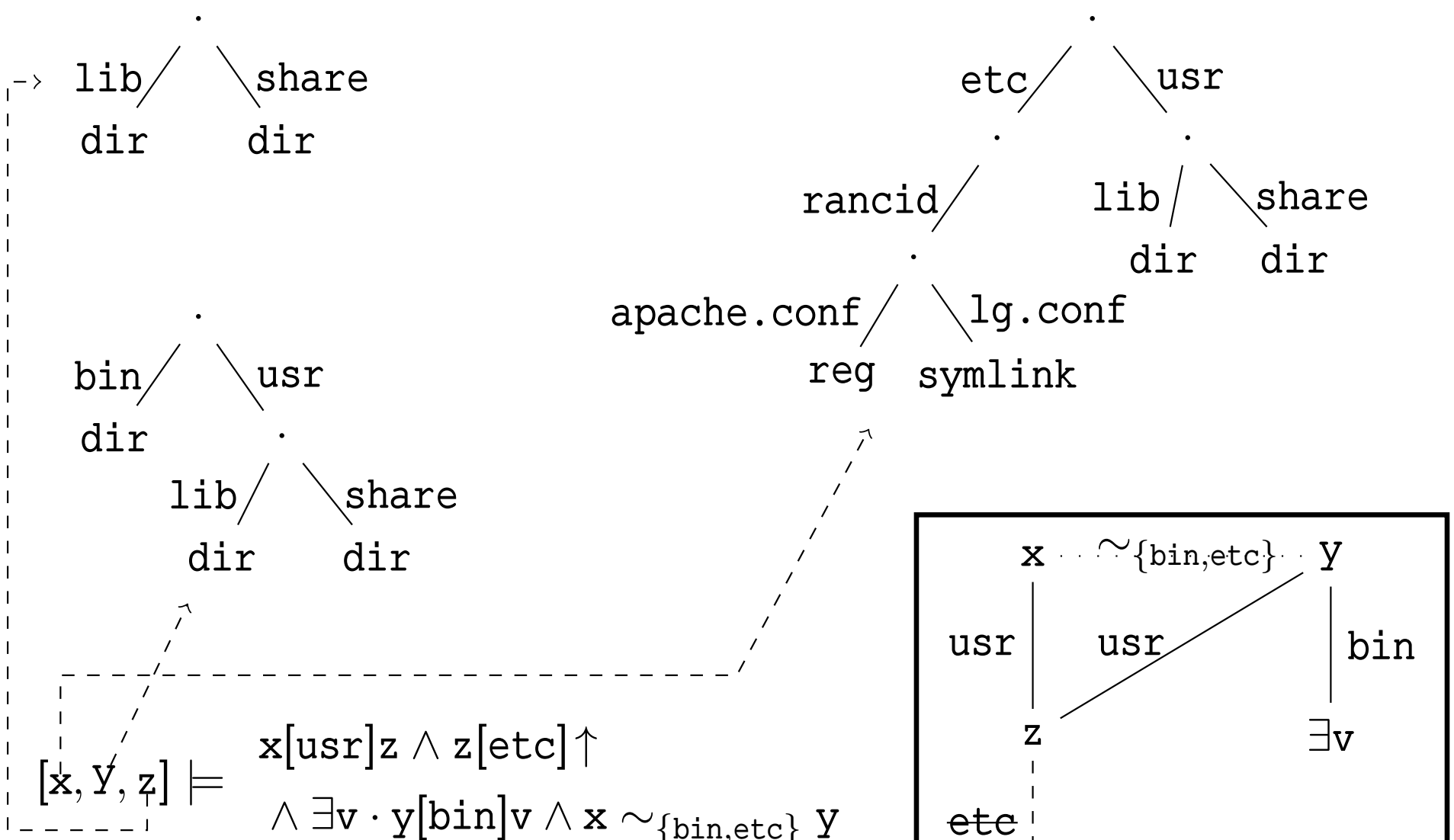

lib
share
dir
dir
etc
usr
rancid
lib
share
dir
dir
apache.conf
lg.conf
reg
symlink
bin
usr
dir
lib
share
dir
dir
[x, y, z] ⊨
x[usr]z ∧ z[etc]↑
∧ ∃v · y[bin]v ∧ x ∼{bin,etc} y


x
y
usr
bin
z
∃v
etc
⊥

An Example


lib
share
dir
dir
etc
usr
rancid
lib
share
dir
dir
apache.conf
lg.conf
reg
symlink
bin
usr
dir
lib
share
dir
dir
[x, y, z] ⊨
x[usr]z ∧ z[etc]↑
∧ ∃v · y[bin]v ∧ x ∼{bin,etc} y
x
∼{bin,etc}
y
usr
bin
z
∃v
etc
⊥

An Example


lib
share
dir
dir
etc
usr
rancid
lib
share
dir
dir
apache.conf
lg.conf
reg
symlink
bin
usr
dir
lib
share
dir
dir
[x, y, z] ⊨
x[usr]z ∧ z[etc]↑
∧ ∃v · y[bin]v ∧ x ∼{bin,etc} y
x
∼{bin,etc}
y
usr
usr
bin
z
∃v
etc
⊥

Example Specification: mkdir q/f

Success	$\exists \mathtt{x}, \mathtt{x}', \mathtt{y}' \cdot$ $\mathtt{resolve}(\mathtt{r}, \mathtt{cwd}, \mathtt{q}, \mathtt{x}) \wedge \mathtt{dir}(\mathtt{x}) \wedge \mathtt{x}[\mathtt{f}]\uparrow$ $\wedge\, \mathtt{similar}(\mathtt{r}, \mathtt{r}', \mathtt{cwd}, \mathtt{q}, \mathtt{x}, \mathtt{x}') \wedge \mathtt{x} \sim_{\{\mathtt{f}\}} \mathtt{x}'$ $\wedge\, \mathtt{dir}(\mathtt{x}') \wedge \mathtt{x}'[\mathtt{f}]\mathtt{y}' \wedge \mathtt{dir}(\mathtt{y}') \wedge \mathtt{y}'[\varnothing]$
Error: file exists	$\exists \mathtt{y} \cdot \mathtt{resolve}(\mathtt{r}, \mathtt{cwd}, \mathtt{q}/\mathtt{f}, \mathtt{y}) \wedge \mathtt{r} = \mathtt{r}'$
Error: no parent	$\mathtt{noresolve}(\mathtt{r}, \mathtt{cwd}, \mathtt{q}) \wedge \mathtt{r} = \mathtt{r}'$
Error: parent is not a directory	$\exists \mathtt{x} \cdot \mathtt{resolve}(\mathtt{r}, \mathtt{cwd}, \mathtt{q}, \mathtt{x}) \wedge \neg\mathtt{dir}(\mathtt{x}) \wedge \mathtt{r} = \mathtt{r}'$

Example Specification: mkdir q/f

Success	$\exists \mathtt{x}, \mathtt{x}', \mathtt{y}' \cdot$ $\mathtt{resolve}(\mathtt{r}, \mathtt{cwd}, \mathtt{q}, \mathtt{x}) \wedge \mathtt{dir}(\mathtt{x}) \wedge \mathtt{x}[\mathtt{f}]\uparrow$ $\wedge\, \mathtt{similar}(\mathtt{r}, \mathtt{r}', \mathtt{cwd}, \mathtt{q}, \mathtt{x}, \mathtt{x}') \wedge \mathtt{x} \sim_{\{\mathtt{f}\}} \mathtt{x}'$ $\wedge\, \mathtt{dir}(\mathtt{x}') \wedge \mathtt{x}'[\mathtt{f}]\mathtt{y}' \wedge \mathtt{dir}(\mathtt{y}') \wedge \mathtt{y}'[\varnothing]$
Error: file exists	$\exists \mathtt{y}$
Error: no parent	no
Error: parent is not a directory	$\exists \mathtt{x}$ $\wedge\, \mathtt{r} = \mathtt{r}'$

Example Specification: mkdir q/f

Success

$$\exists x, x', y' \cdot \mathtt{resolve}(r, \mathtt{cwd}, q, x) \wedge \mathtt{dir}(x) \wedge x[f]\uparrow \wedge \mathtt{similar}(r, r', \mathtt{cwd}, q, x, x') \wedge x \sim_{\{f\}} x' \wedge \mathtt{dir}(x') \wedge x'[f]y' \wedge \mathtt{dir}(y') \wedge y'[\varnothing]$$

Error: file exists

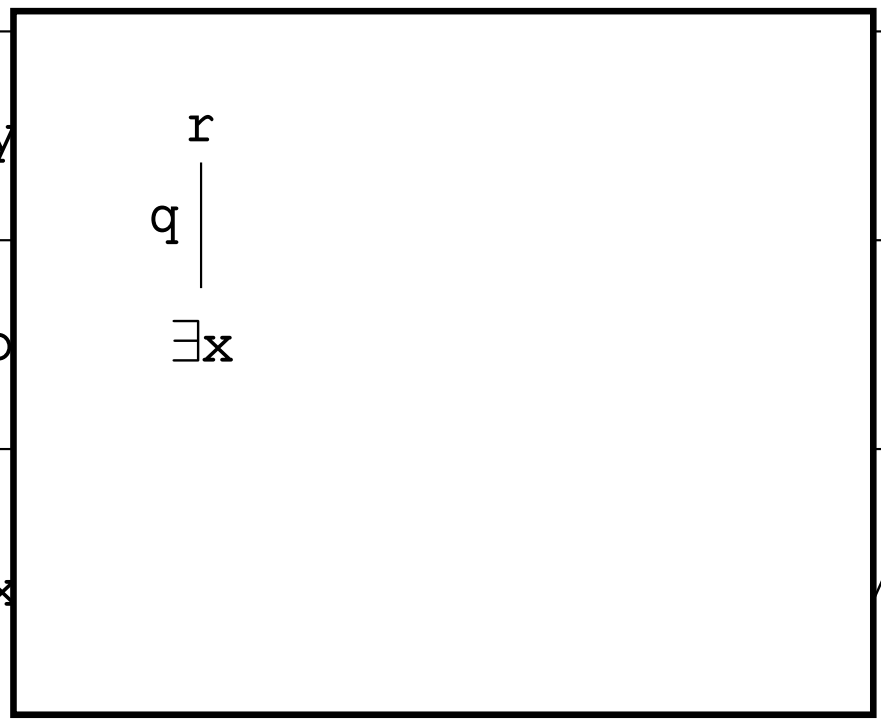
$\exists y$

Error: no parent

no

Error: parent is not a directory

$\exists x$



$\wedge\ r = r'$

Example Specification: mkdir q/f

Success

$$\exists x, x', y' \cdot$$
$$\texttt{resolve}(r, \texttt{cwd}, q, x) \wedge \texttt{dir}(x) \wedge x[f]\uparrow$$
$$\wedge\ \texttt{similar}(r, r', \texttt{cwd}, q, x, x') \wedge x \sim_{\{f\}} x'$$
$$\wedge\ \texttt{dir}(x') \wedge x'[f]y' \wedge \texttt{dir}(y') \wedge y'[\varnothing]$$

Error: file exists

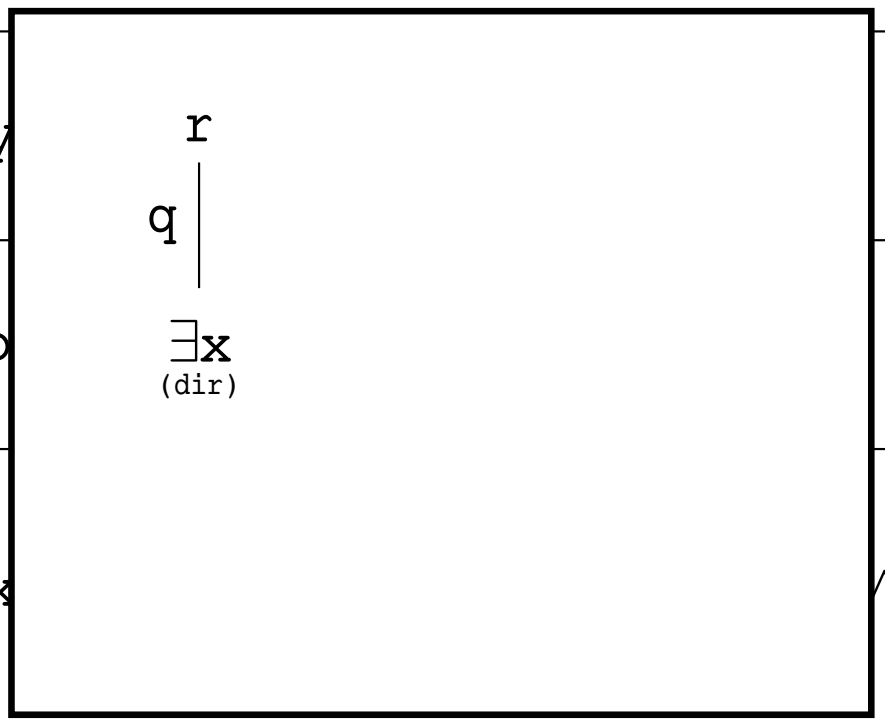
$\exists y$

Error: no parent

no

Error: parent is not a directory

$\exists x$



$\wedge\ r = r'$

Example Specification: mkdir q/f

Success

$$\exists x, x', y' \cdot$$
$$\texttt{resolve}(r, \texttt{cwd}, q, x) \wedge \texttt{dir}(x) \wedge x[f]\uparrow$$
$$\wedge\ \texttt{similar}(r, r', \texttt{cwd}, q, x, x') \wedge x \sim_{\{f\}} x'$$
$$\wedge\ \texttt{dir}(x') \wedge x'[f]y' \wedge \texttt{dir}(y') \wedge y'[\varnothing]$$

Error: file exists

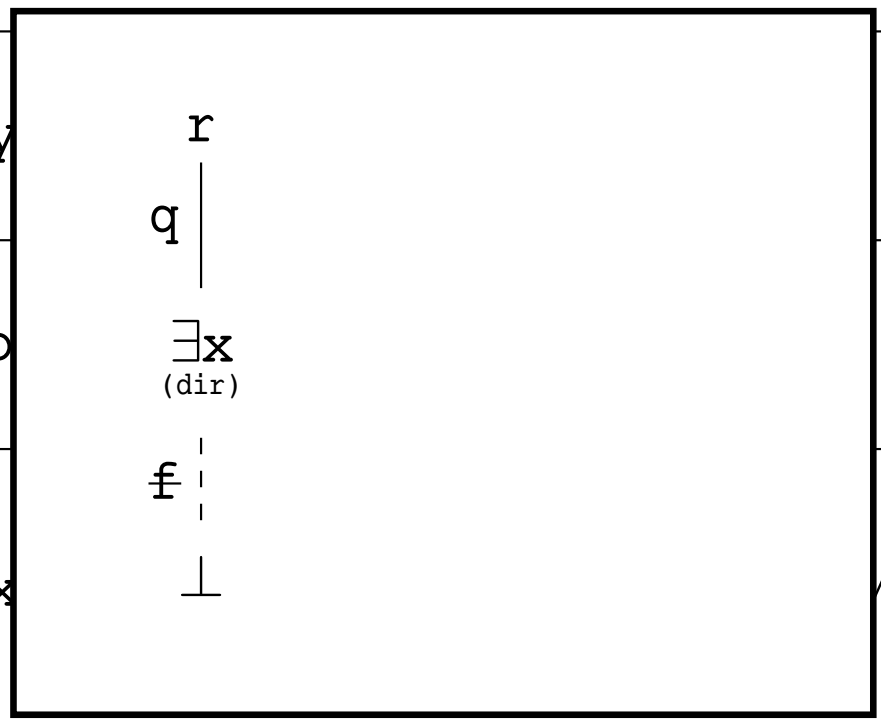
$\exists y$

Error: no parent

no

Error: parent is not a directory

$\exists x$



$\wedge\ r = r'$

Example Specification: mkdir q/f

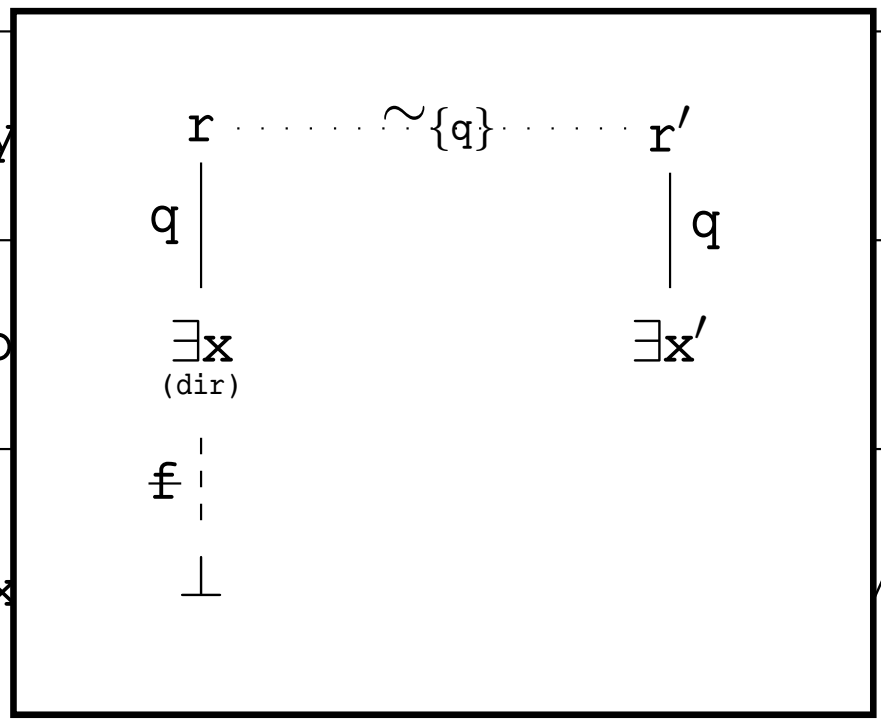
Success

$$\exists \mathtt{x}, \mathtt{x}', \mathtt{y}' \cdot$$
$$\mathtt{resolve}(\mathtt{r}, \mathtt{cwd}, \mathtt{q}, \mathtt{x}) \wedge \mathtt{dir}(\mathtt{x}) \wedge \mathtt{x}[\mathtt{f}]\uparrow$$
$$\wedge\ \mathtt{similar}(\mathtt{r}, \mathtt{r}', \mathtt{cwd}, \mathtt{q}, \mathtt{x}, \mathtt{x}') \wedge \mathtt{x} \sim_{\{\mathtt{f}\}} \mathtt{x}'$$
$$\wedge\ \mathtt{dir}(\mathtt{x}') \wedge \mathtt{x}'[\mathtt{f}]\mathtt{y}' \wedge \mathtt{dir}(\mathtt{y}') \wedge \mathtt{y}'[\varnothing]$$

Error: file exists $\exists \mathtt{y}$

Error: no parent no

Error: parent is not a directory $\exists \mathtt{x}$ $\wedge\ \mathtt{r} = \mathtt{r}'$



Example Specification: mkdir q/f

Success

$$\exists x, x', y' \cdot$$
$$\texttt{resolve}(r, \texttt{cwd}, q, x) \wedge \texttt{dir}(x) \wedge x[f]\uparrow$$
$$\wedge\, \texttt{similar}(r, r', \texttt{cwd}, q, x, x') \wedge x \sim_{\{f\}} x'$$
$$\wedge\, \texttt{dir}(x') \wedge x'[f]y' \wedge \texttt{dir}(y') \wedge y'[\varnothing]$$

Error: file exists

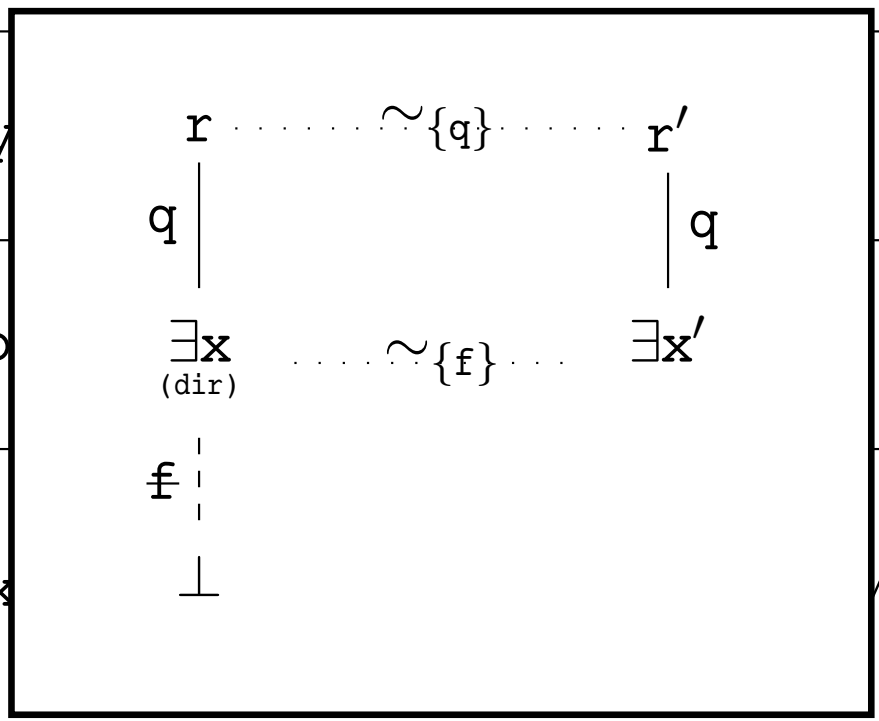
$\exists y$

Error: no parent

no

Error: parent is not a directory

$\exists x$



$\wedge\, r = r'$

Example Specification: mkdir q/f

Success

$$\exists x, x', y' \cdot$$
$$\texttt{resolve}(r, \texttt{cwd}, q, x) \wedge \texttt{dir}(x) \wedge x[f]\uparrow$$
$$\wedge\ \texttt{similar}(r, r', \texttt{cwd}, q, x, x') \wedge x \sim_{\{f\}} x'$$
$$\wedge\ \texttt{dir}(x') \wedge x'[f]y' \wedge \texttt{dir}(y') \wedge y'[\varnothing]$$

Error: file exists

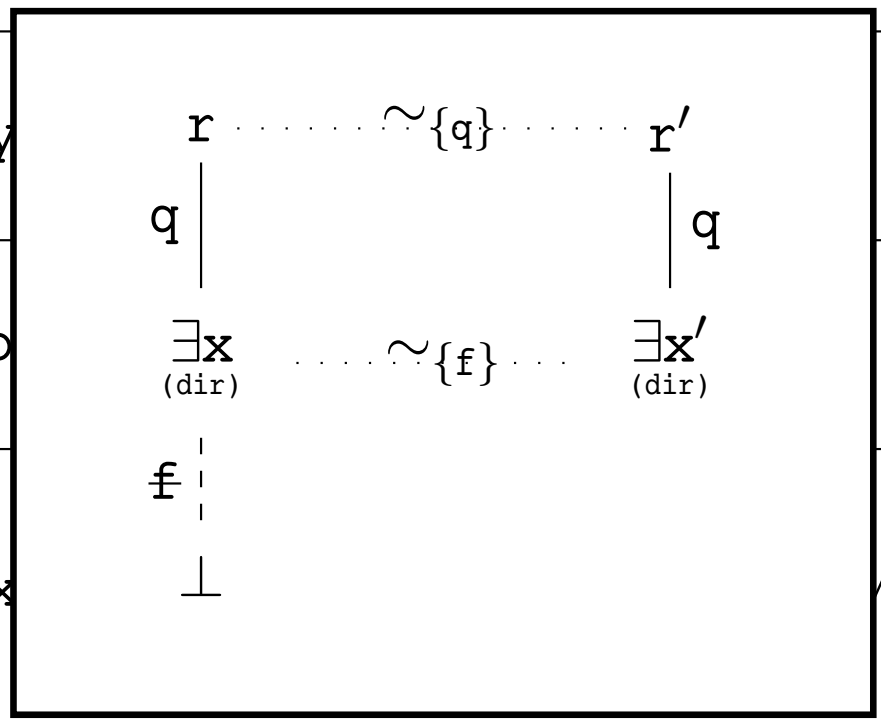
$\exists y$

Error: no parent

no

Error: parent is not a directory

$\exists x$



$\wedge\ r = r'$

Example Specification: mkdir q/f

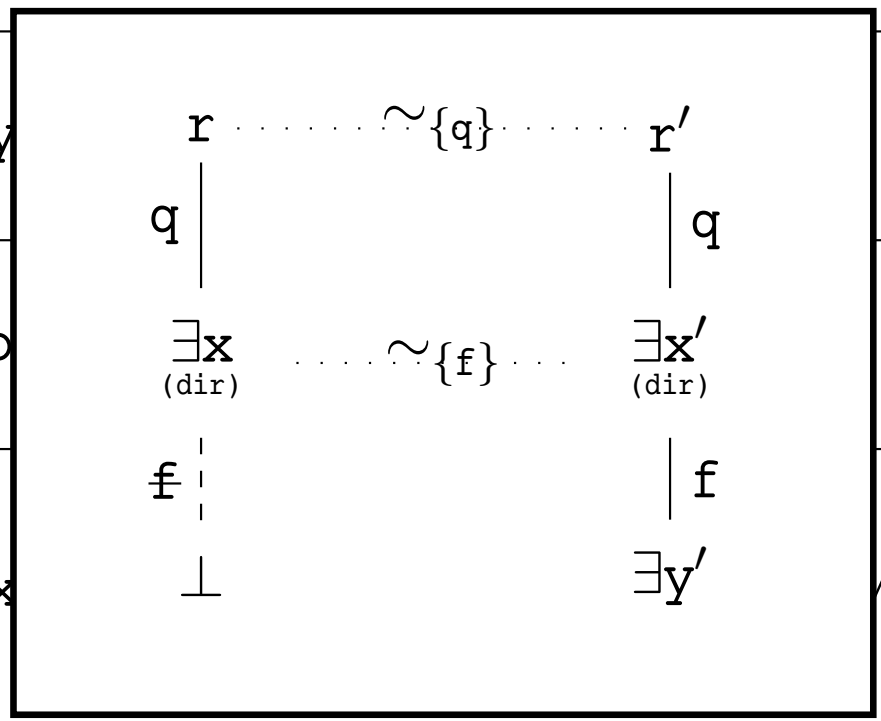
Success

$$\exists \mathtt{x}, \mathtt{x}', \mathtt{y}' \cdot$$
$$\mathtt{resolve}(\mathtt{r}, \mathtt{cwd}, \mathtt{q}, \mathtt{x}) \wedge \mathtt{dir}(\mathtt{x}) \wedge \mathtt{x}[\mathtt{f}]\uparrow$$
$$\wedge\, \mathtt{similar}(\mathtt{r}, \mathtt{r}', \mathtt{cwd}, \mathtt{q}, \mathtt{x}, \mathtt{x}') \wedge \mathtt{x} \sim_{\{\mathtt{f}\}} \mathtt{x}'$$
$$\wedge\, \mathtt{dir}(\mathtt{x}') \wedge \mathtt{x}'[\mathtt{f}]\mathtt{y}' \wedge \mathtt{dir}(\mathtt{y}') \wedge \mathtt{y}'[\varnothing]$$

Error: file exists $\exists \mathtt{y}$

Error: no parent no

Error: parent is not a directory $\exists \mathtt{x}$ $\wedge\, \mathtt{r} = \mathtt{r}'$



Example Specification: mkdir q/f

Success

$$\exists x, x', y' \cdot$$
$$\texttt{resolve}(r, \texttt{cwd}, q, x) \wedge \texttt{dir}(x) \wedge x[f]\uparrow$$
$$\wedge\, \texttt{similar}(r, r', \texttt{cwd}, q, x, x') \wedge x \sim_{\{f\}} x'$$
$$\wedge\, \texttt{dir}(x') \wedge x'[f]y' \wedge \texttt{dir}(y') \wedge y'[\varnothing]$$

Error: file exists

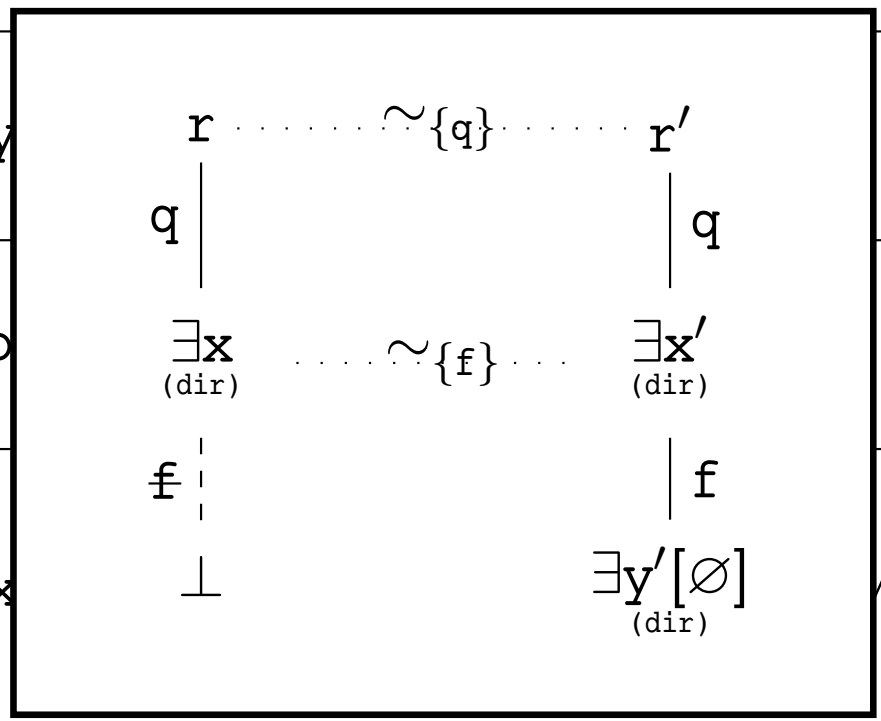
$\exists y$

Error: no parent

no

Error: parent is not a directory

$\exists x$



$\wedge\, r = r'$

Chaining Specifications

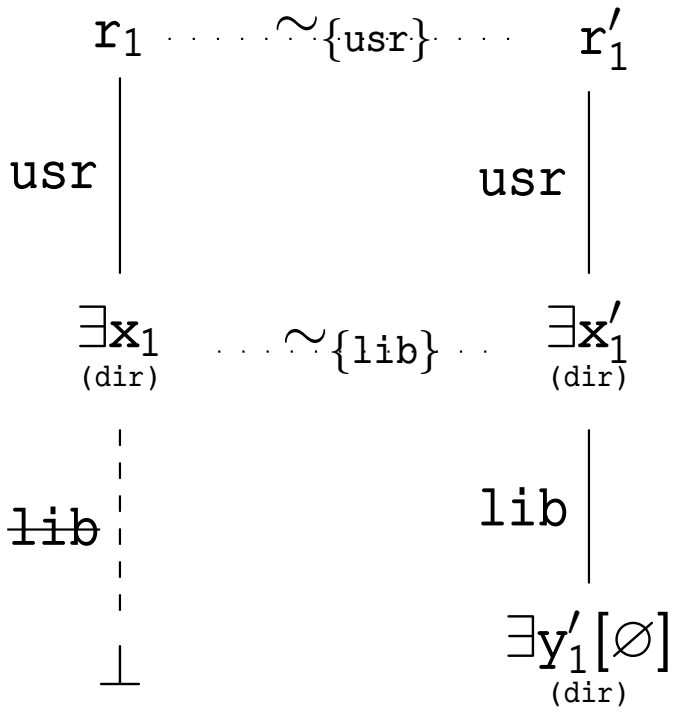
mkdir /usr/lib
(success)

mkdir /usr/lib/foo
(success)

Chaining Specifications

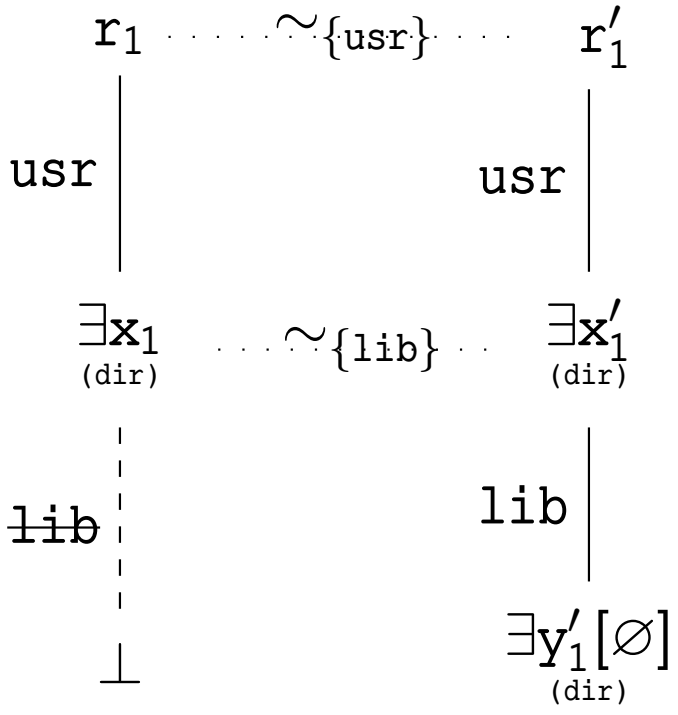
mkdir /usr/lib
(success)

mkdir /usr/lib/foo
(success)

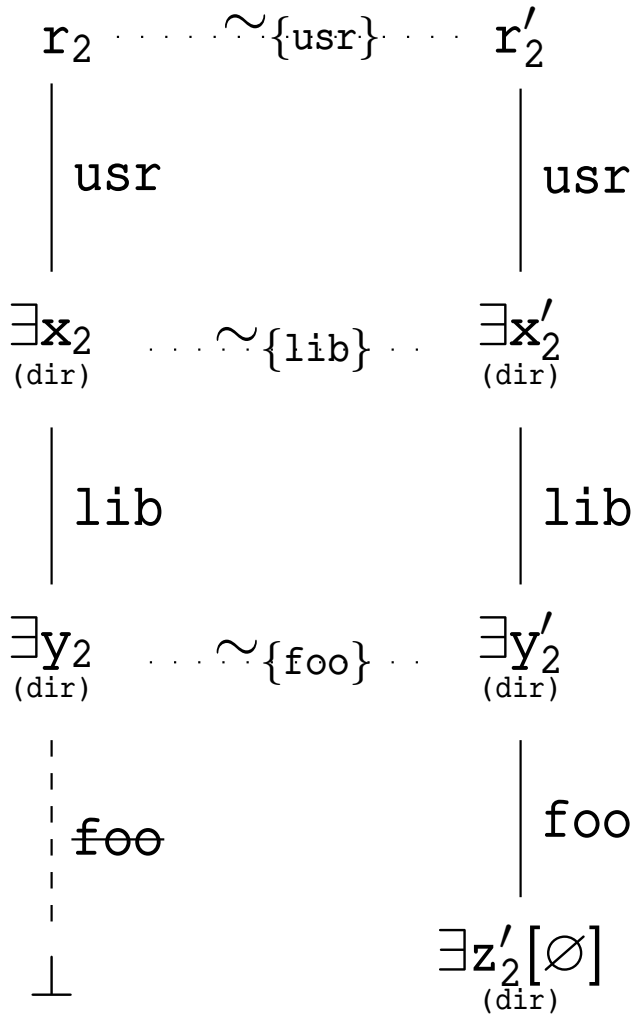


Chaining Specifications

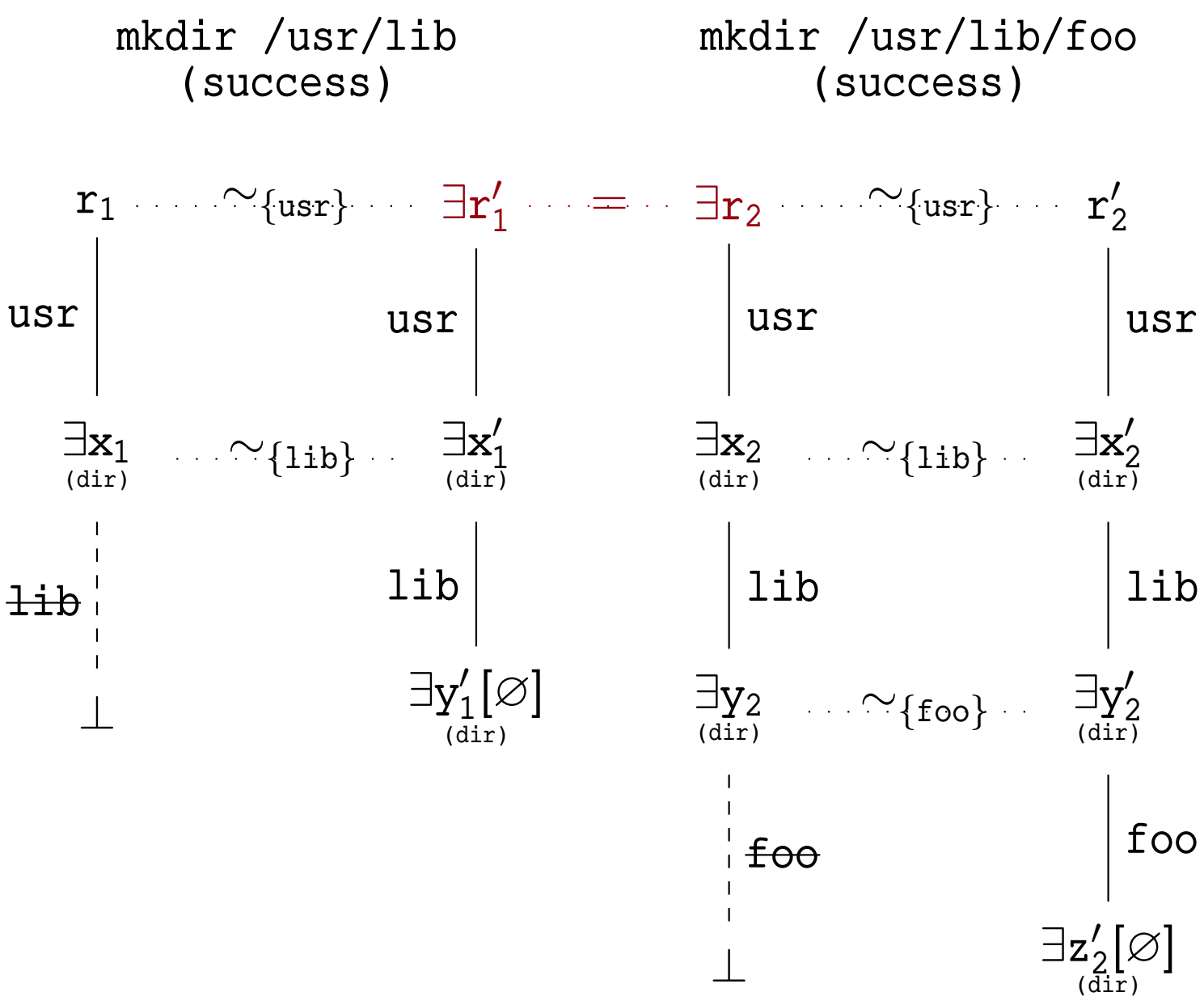
mkdir /usr/lib
(success)



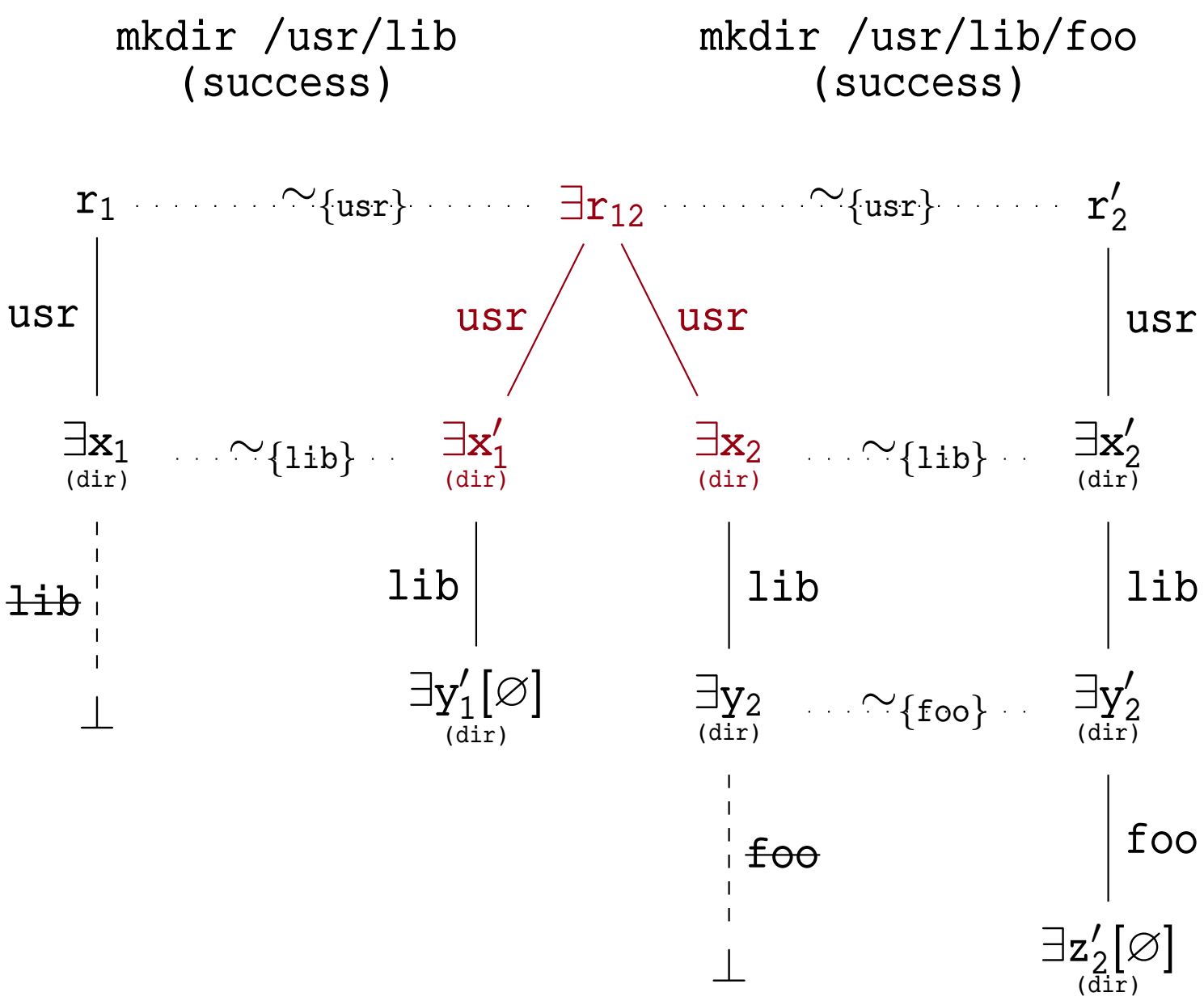
mkdir /usr/lib/foo
(success)



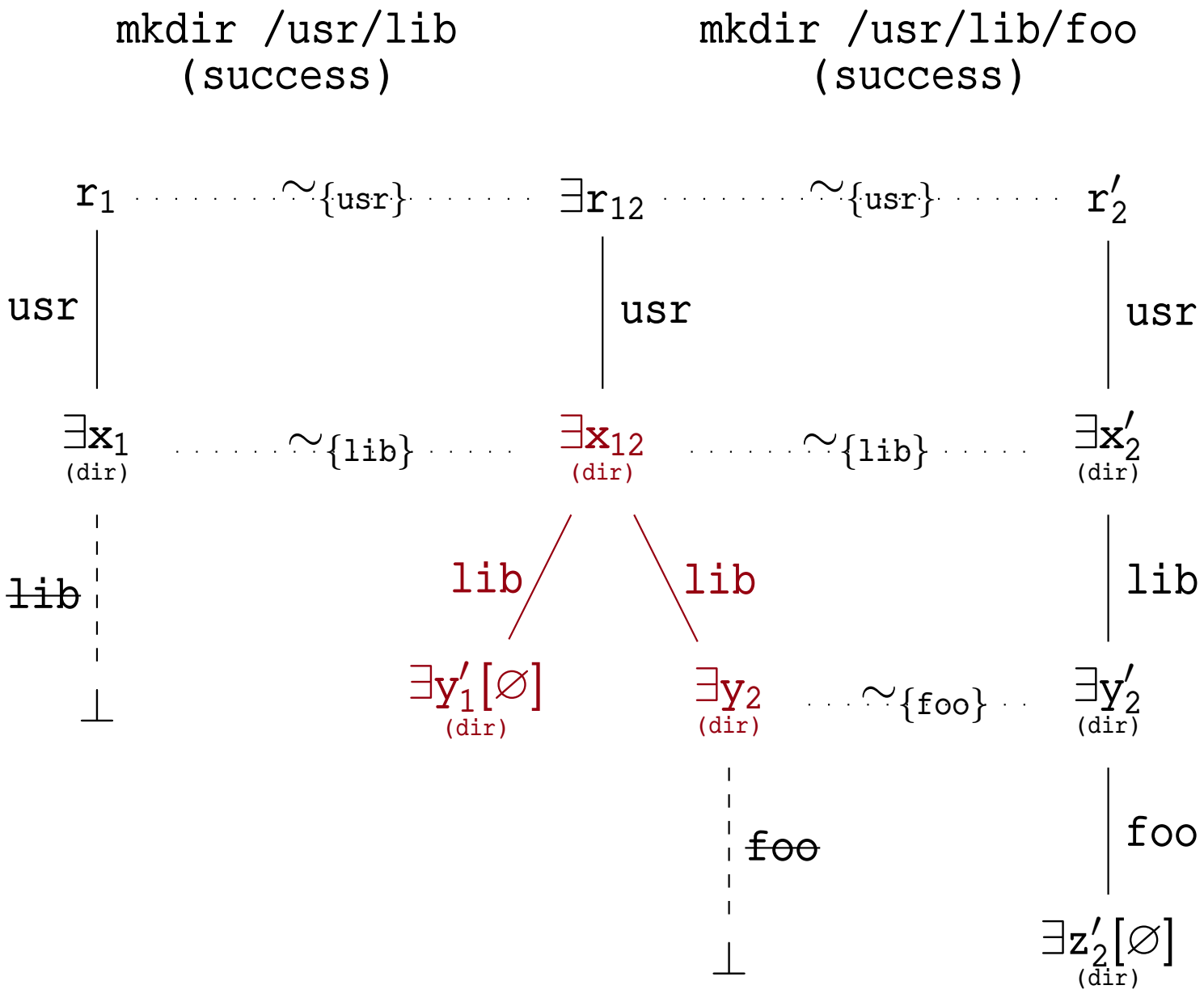
Chaining Specifications



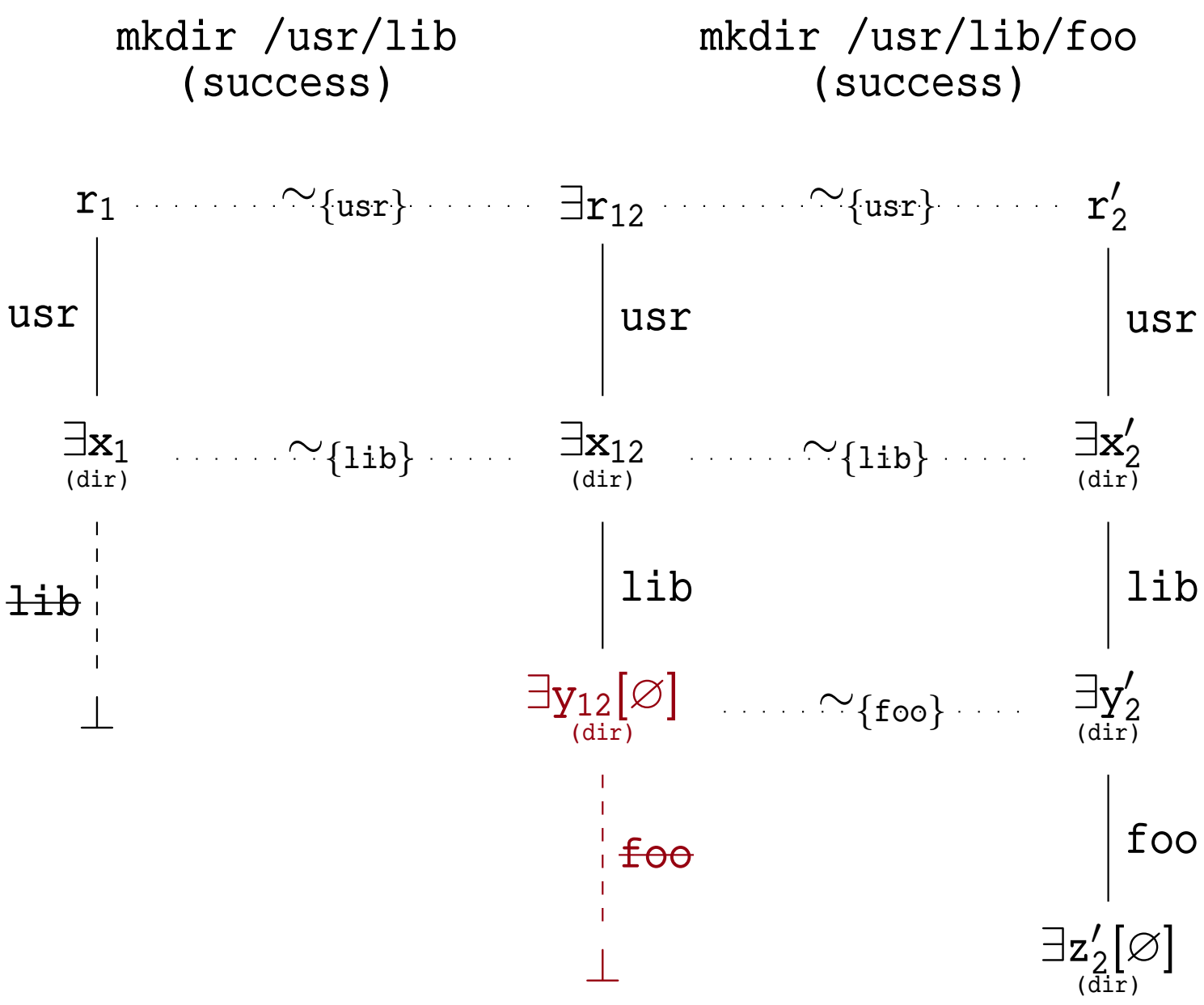
Chaining Specifications



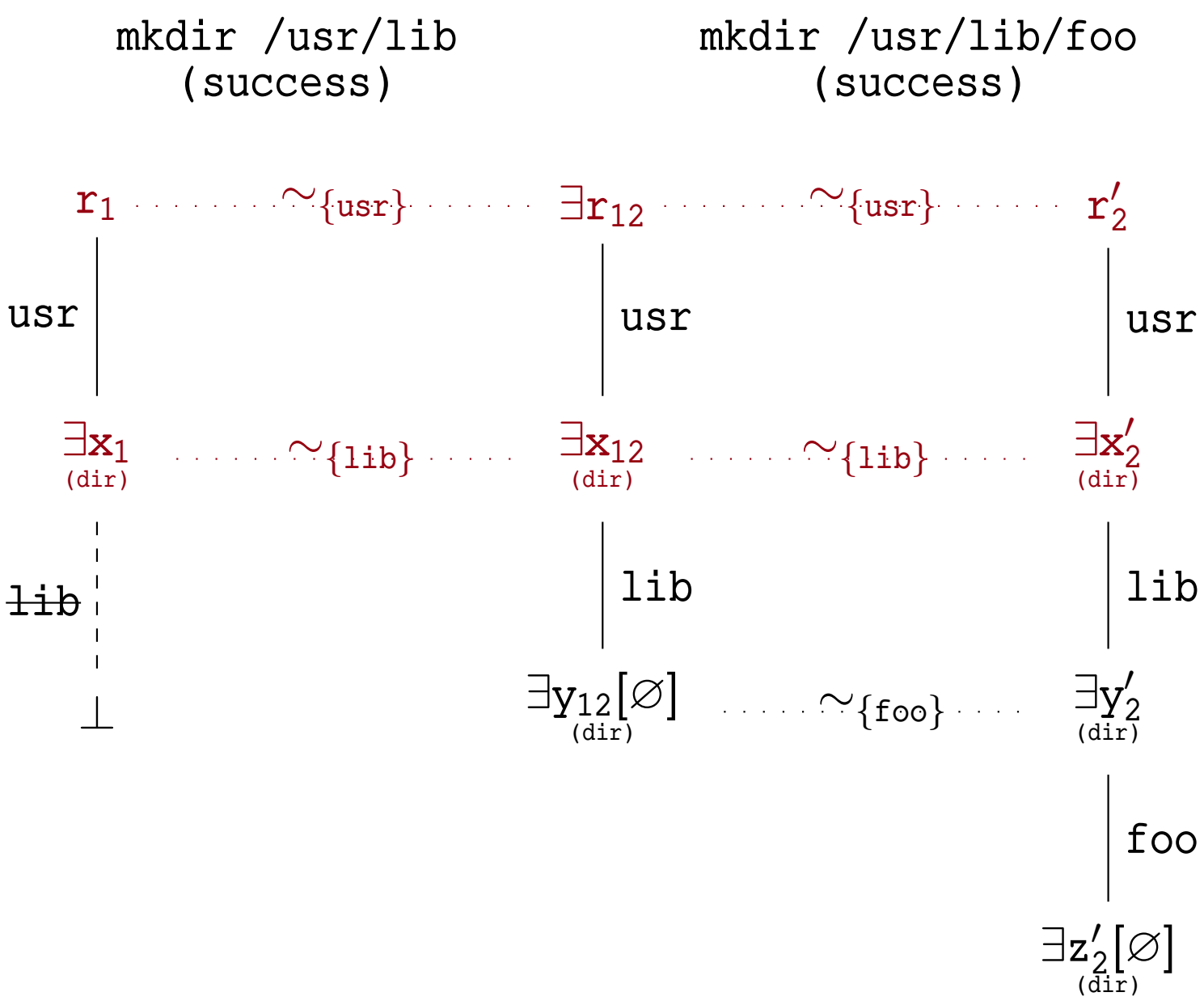
Chaining Specifications



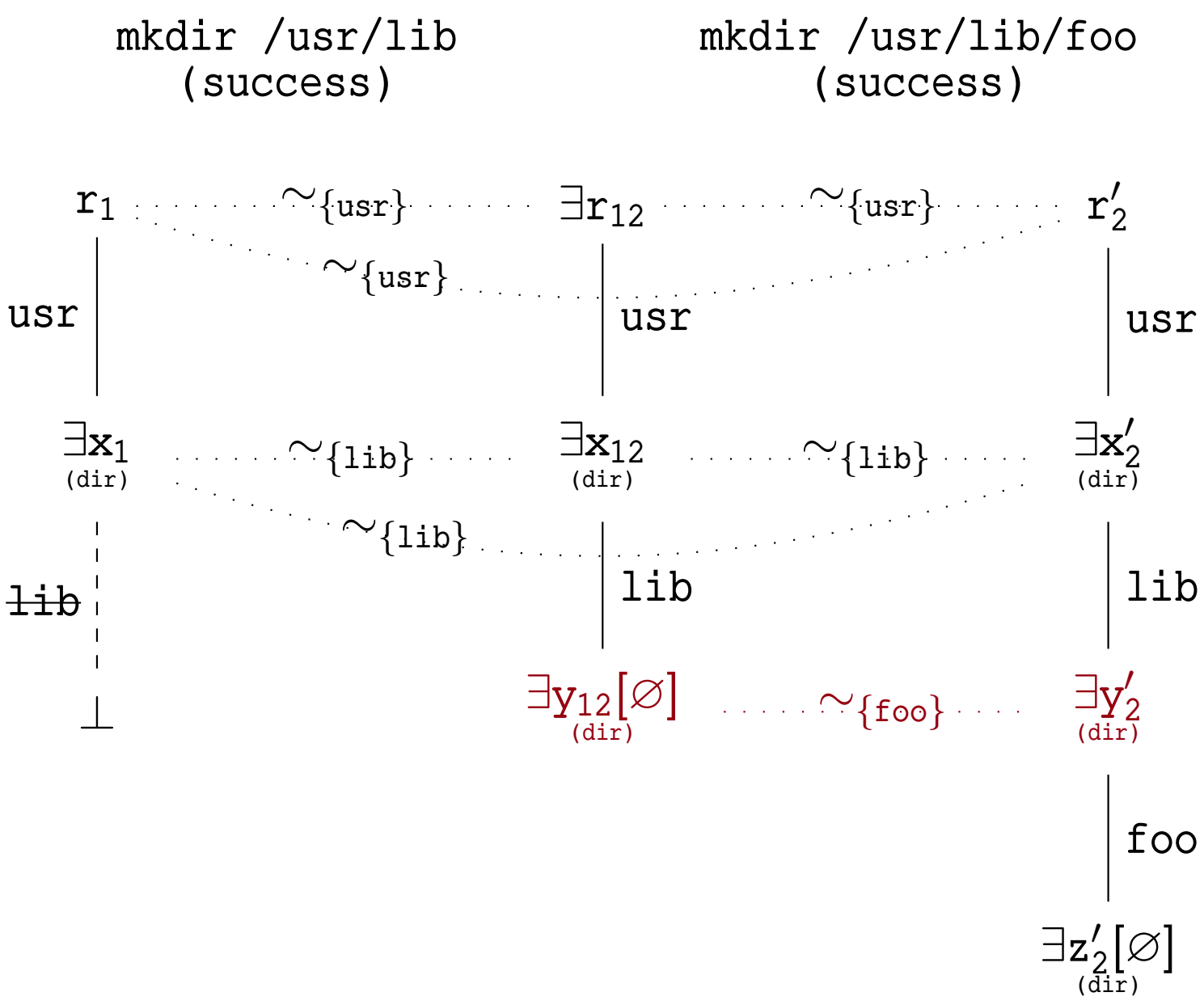
Chaining Specifications



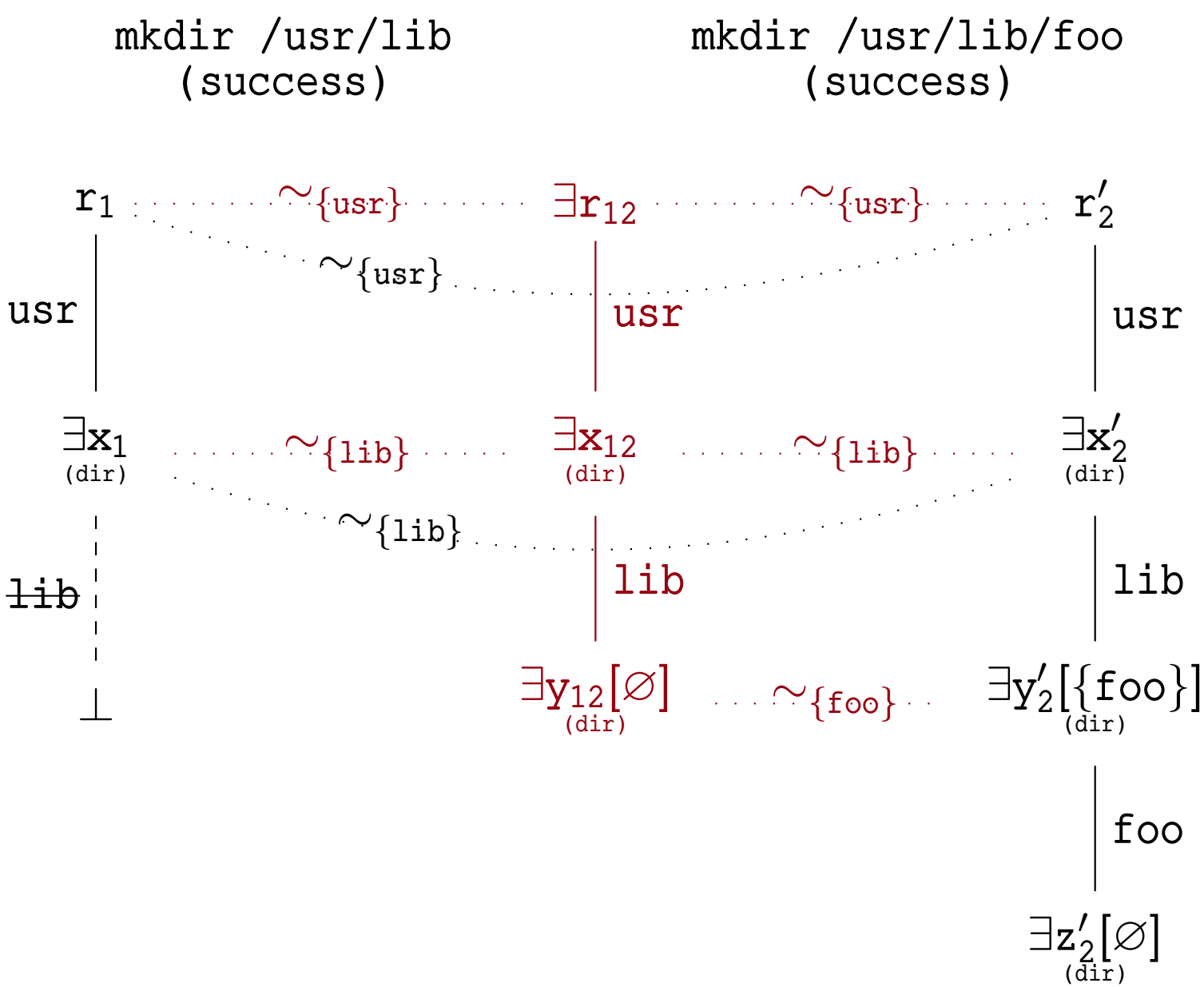
Chaining Specifications



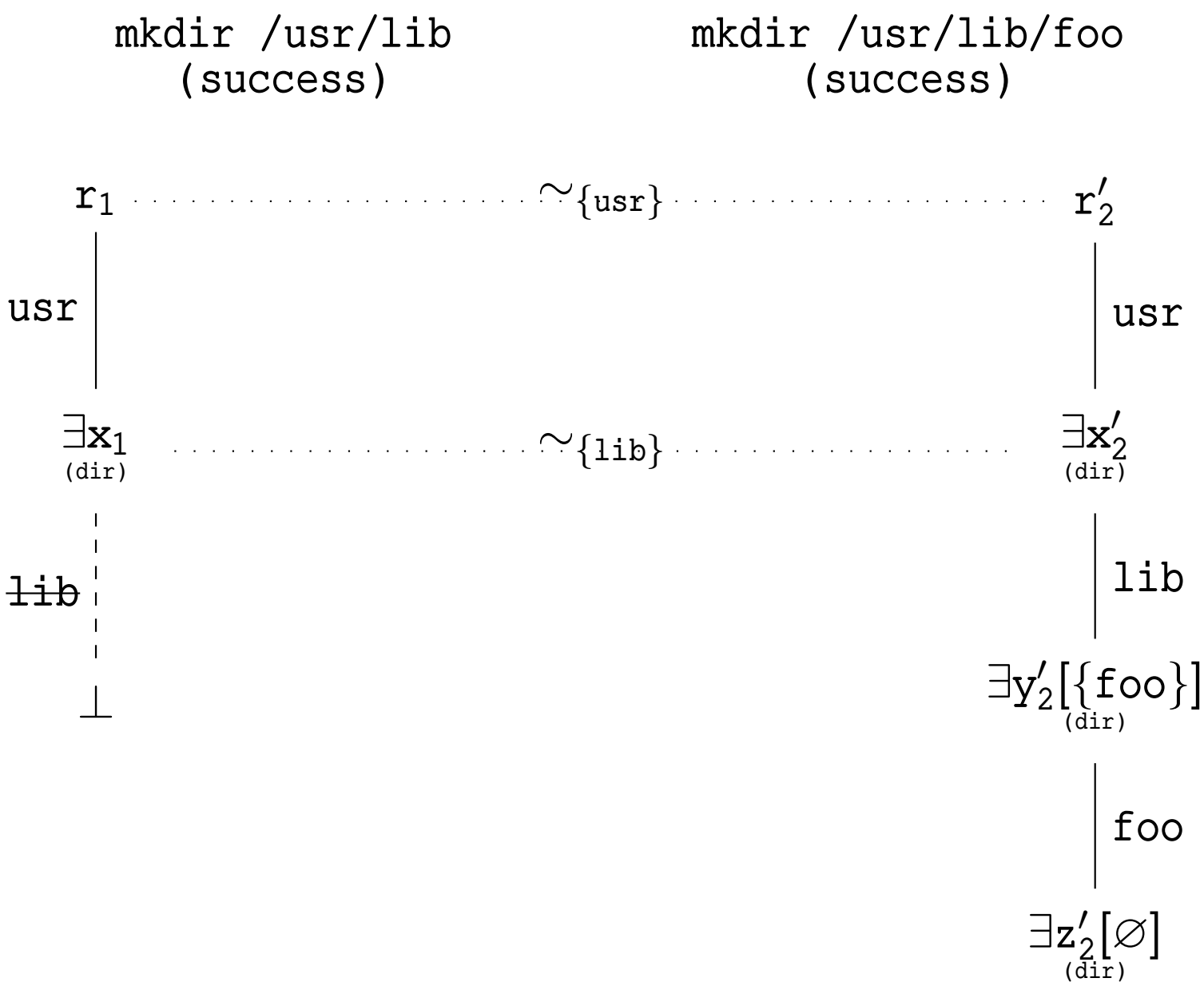
Chaining Specifications



Chaining Specifications



Chaining Specifications



Chaining Specifications

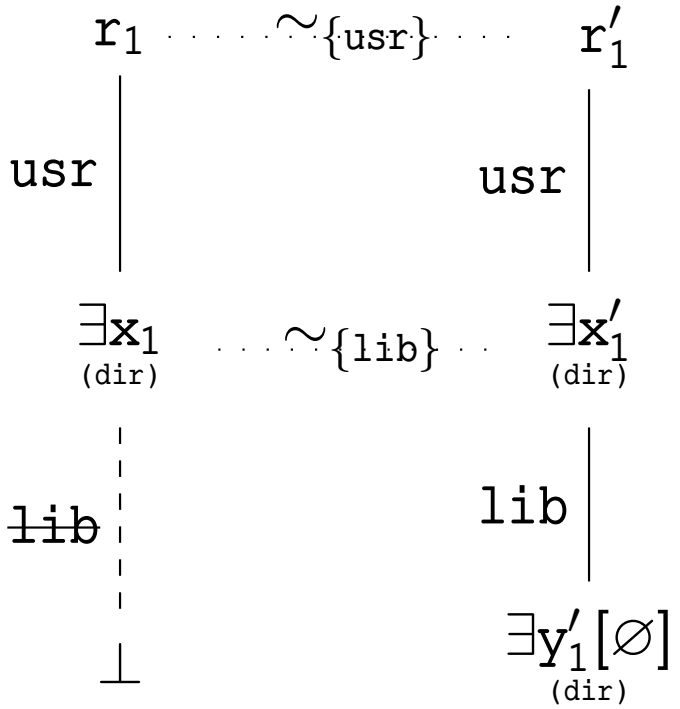
```
mkdir /usr/lib
  (success)
```

```
mkdir /usr/lib/foo
(error: file exists)
```

Chaining Specifications

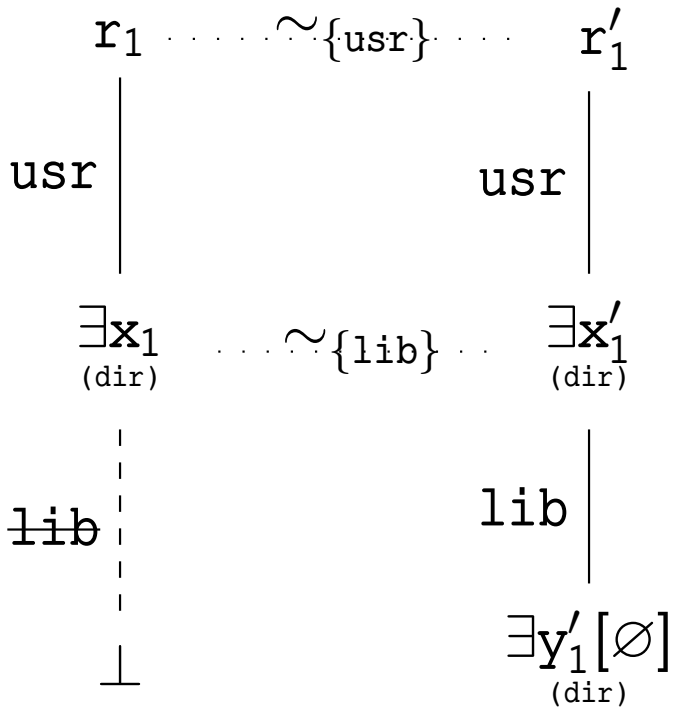
mkdir /usr/lib
(success)

mkdir /usr/lib/foo
(error: file exists)

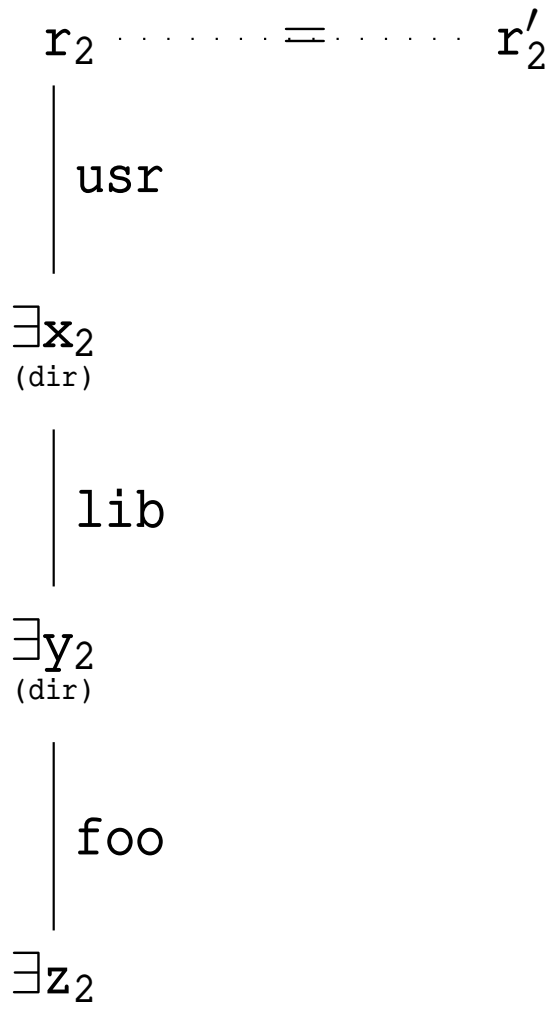


Chaining Specifications

mkdir /usr/lib
(success)



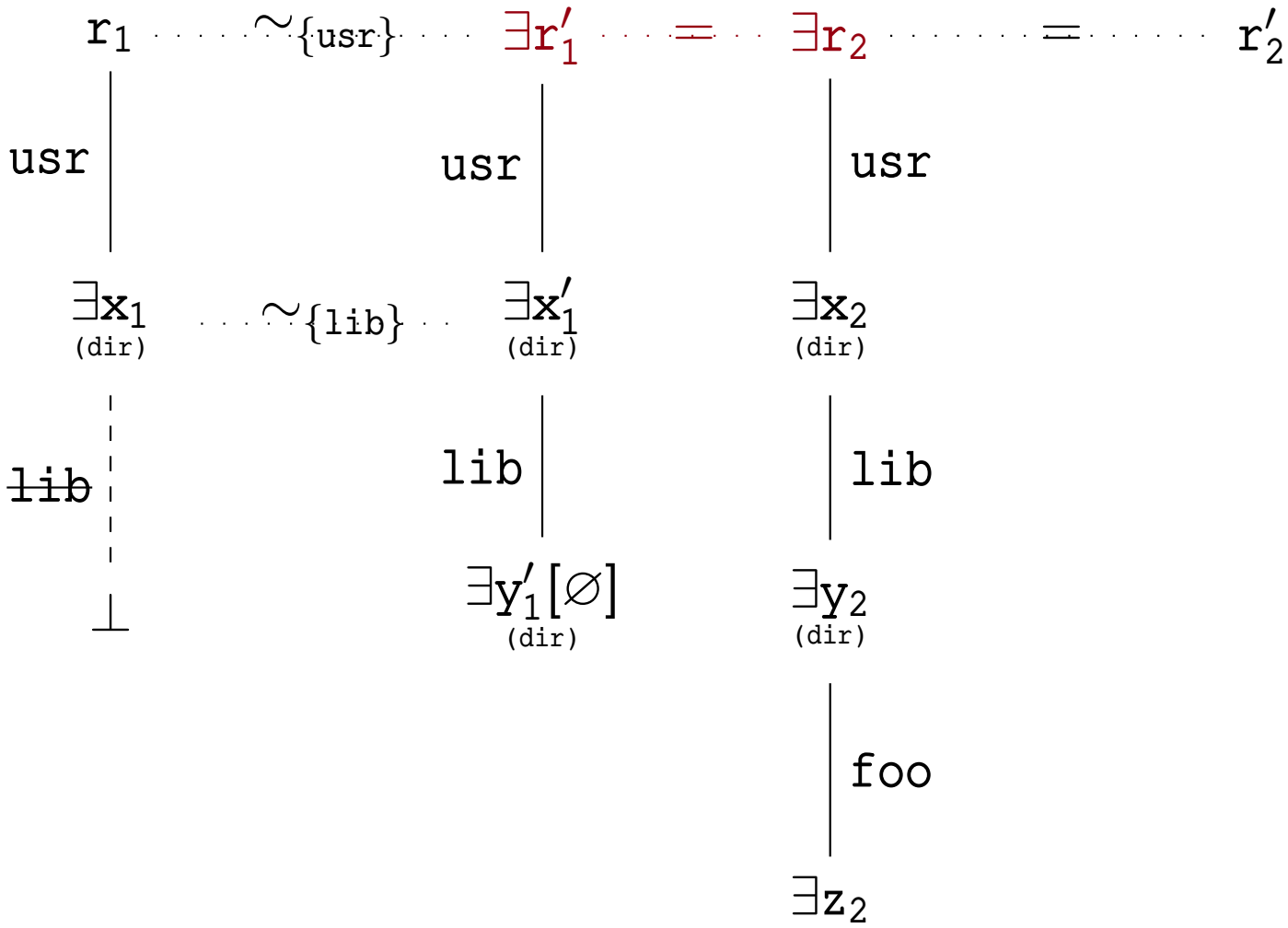
mkdir /usr/lib/foo
(error: file exists)



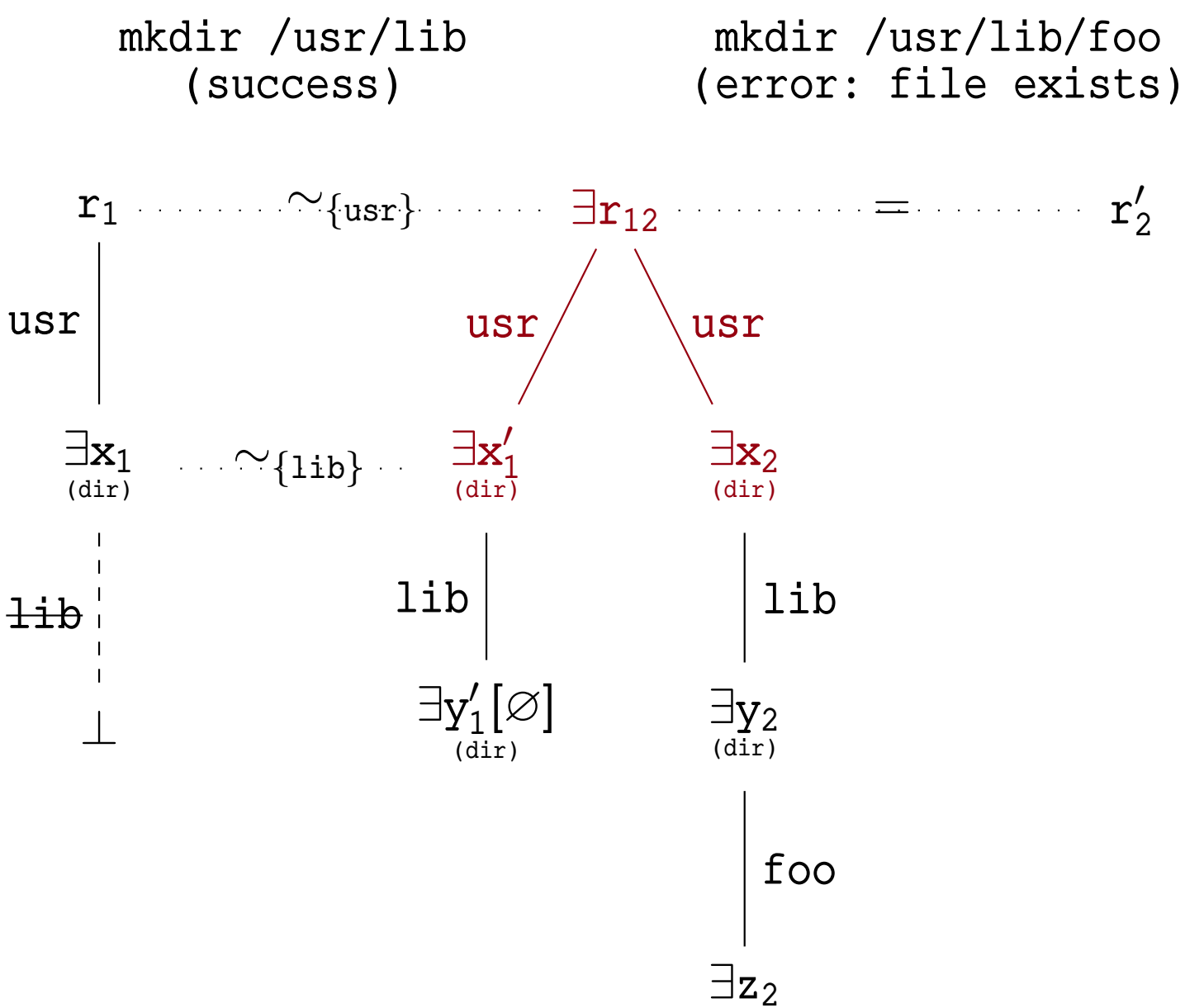
Chaining Specifications

mkdir /usr/lib
(success)

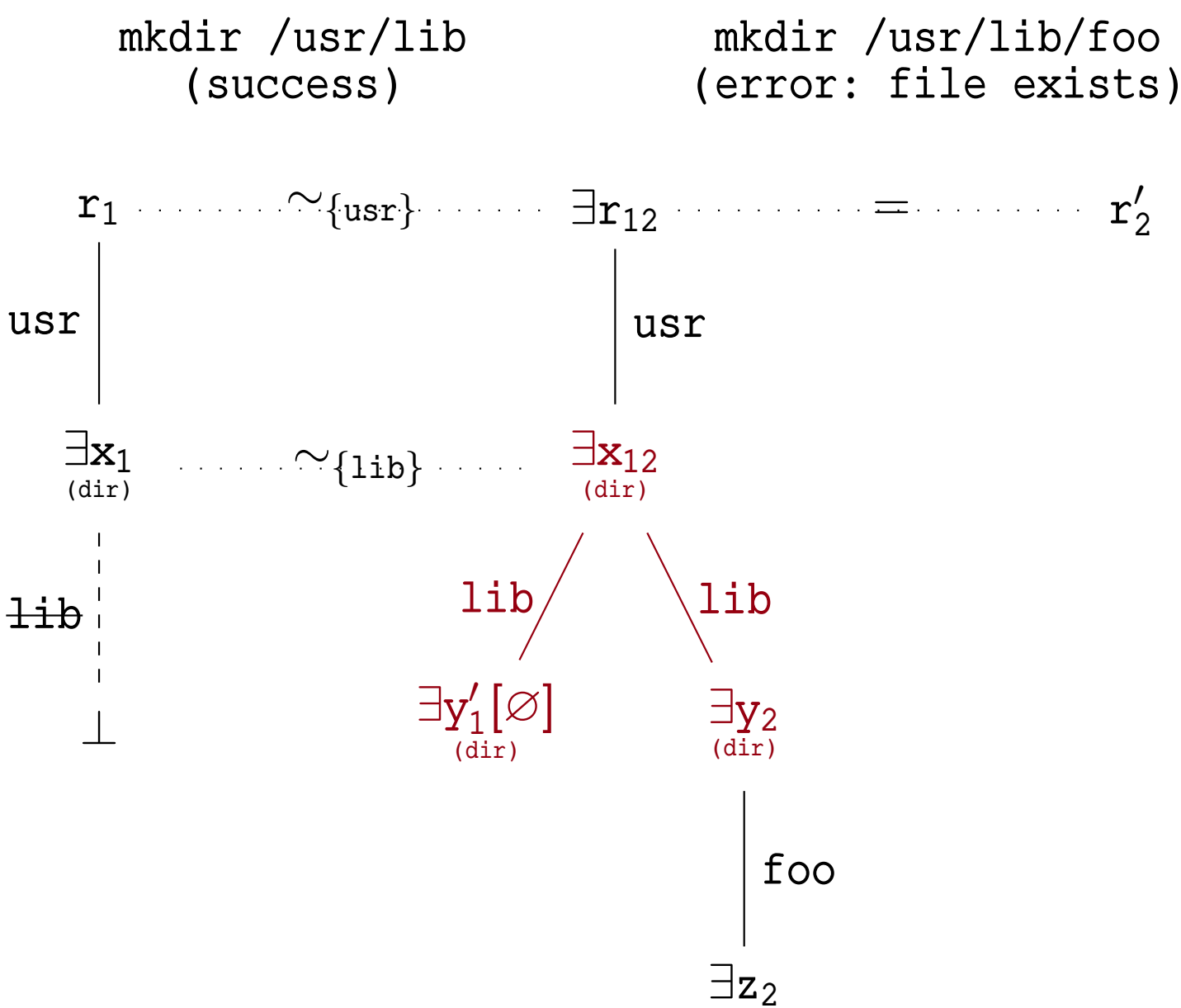
mkdir /usr/lib/foo
(error: file exists)



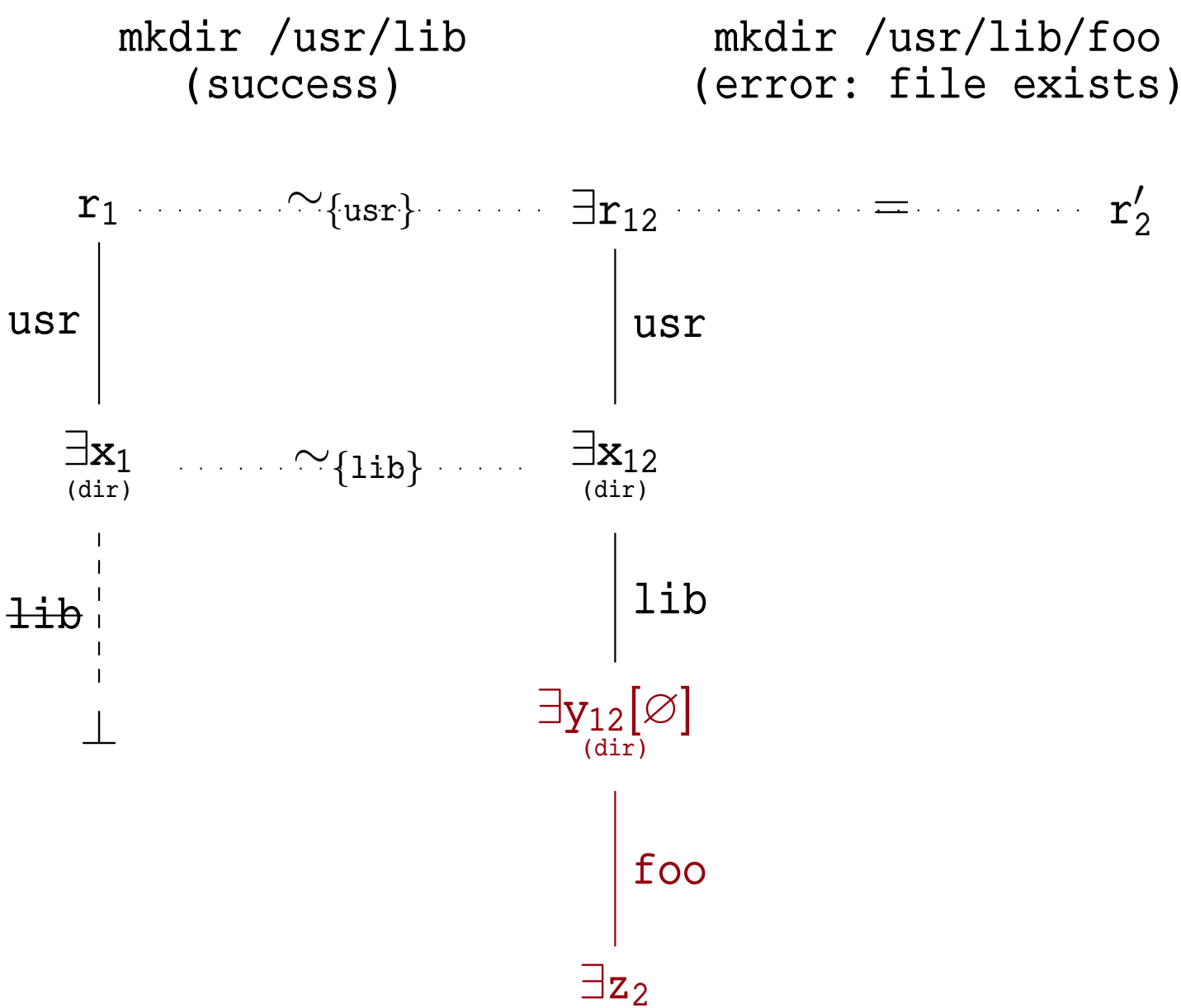
Chaining Specifications



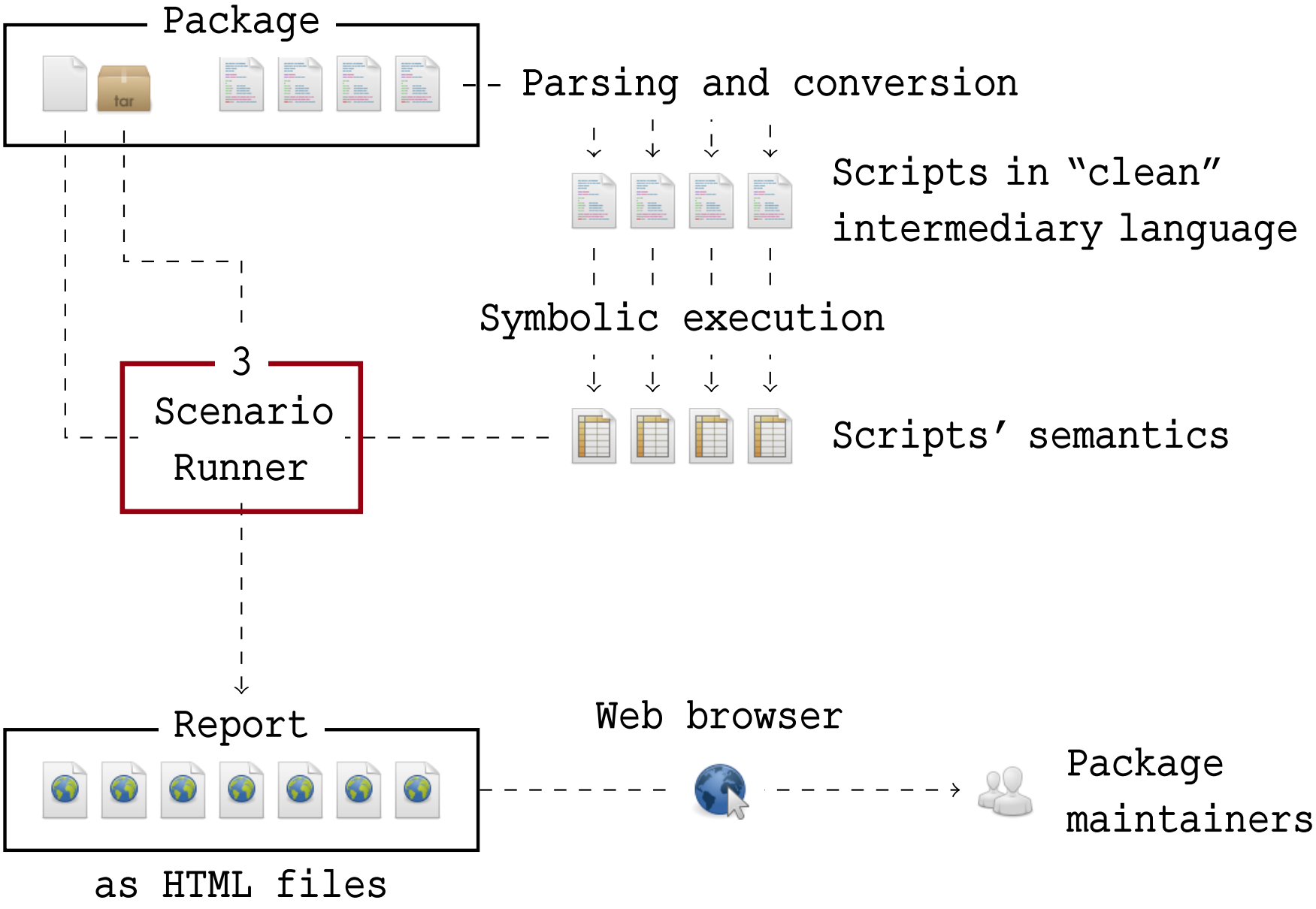
Chaining Specifications



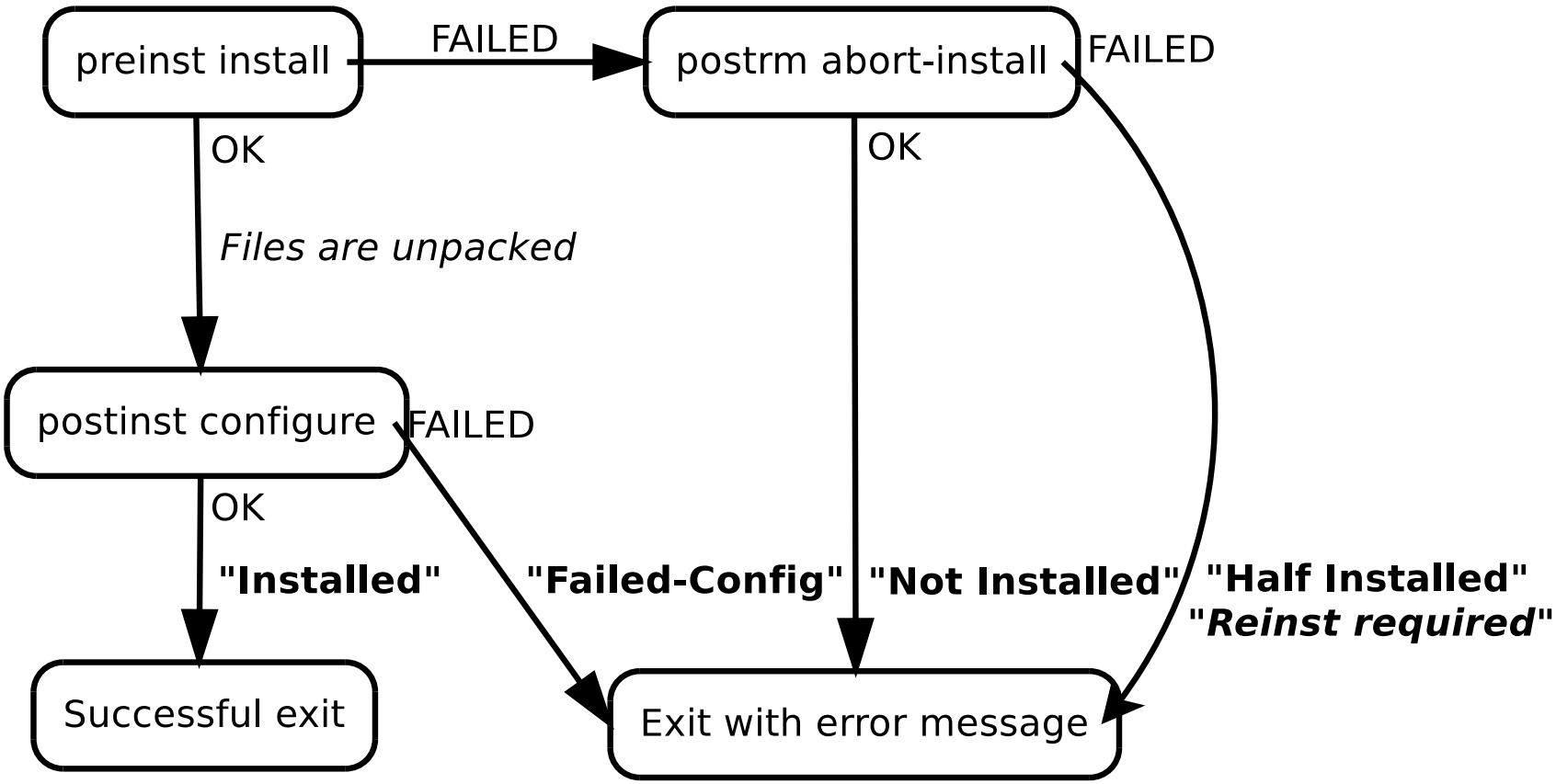
Chaining Specifications



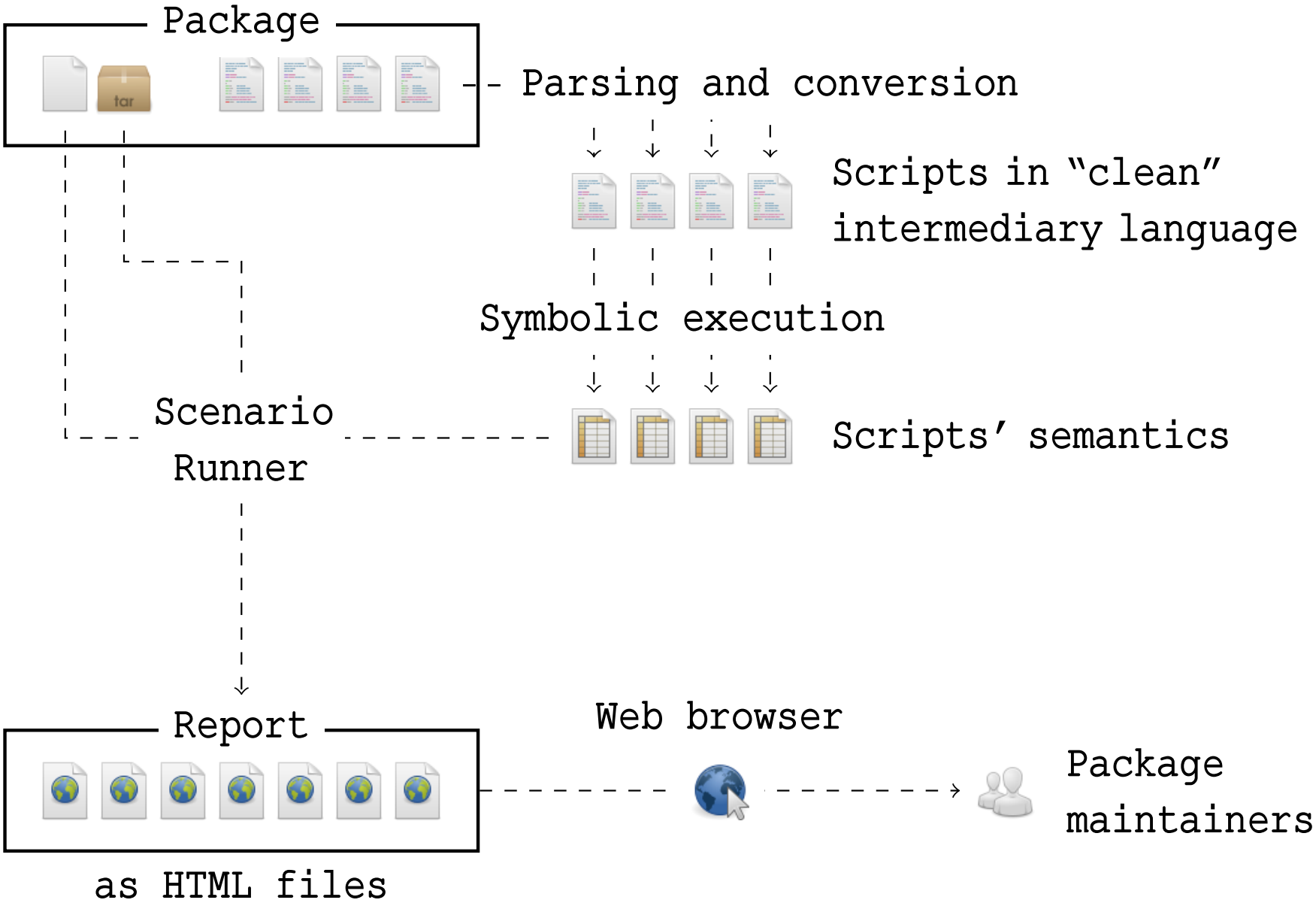
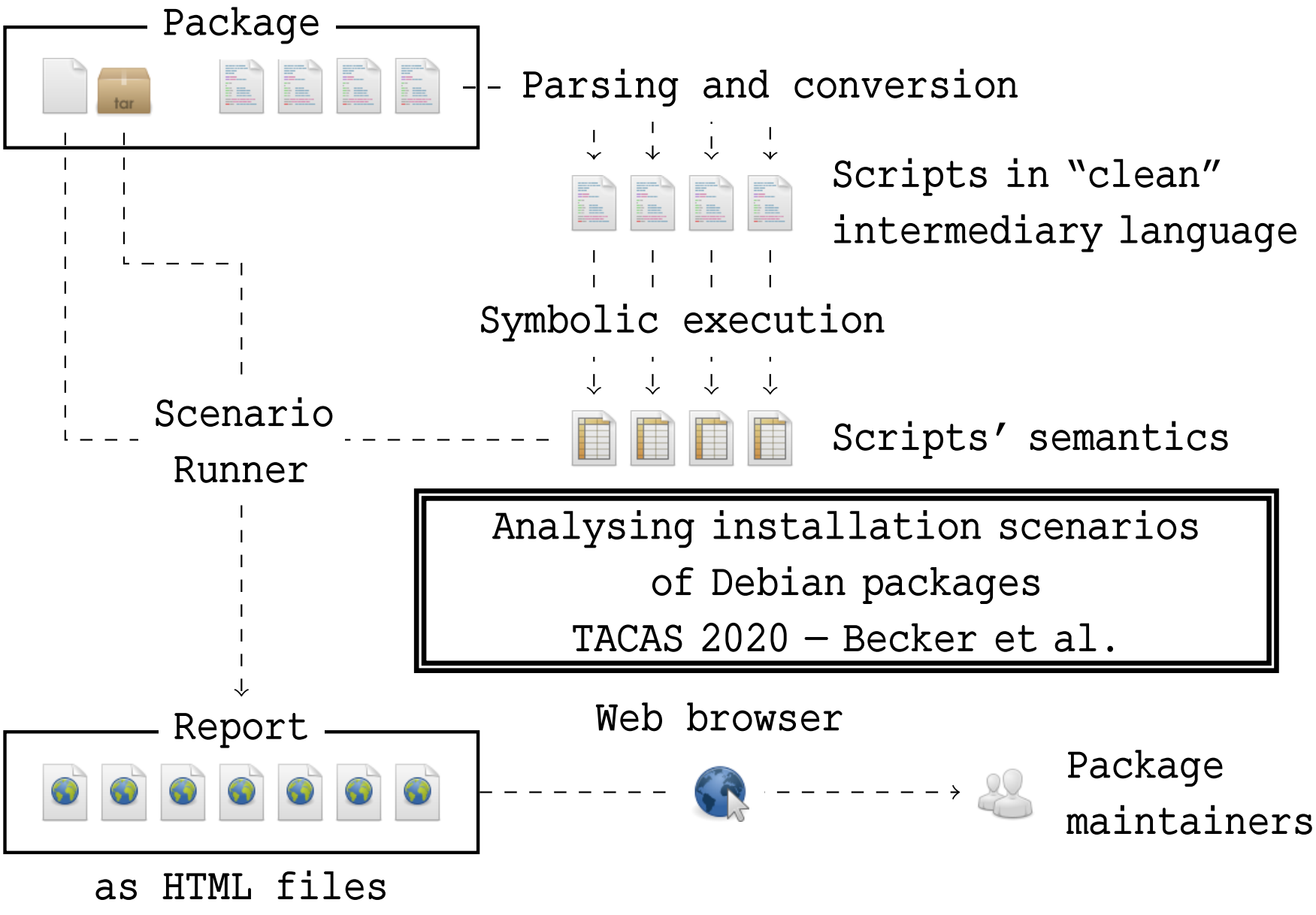
Battle Plan


Package
tar
Parsing and conversion
Scripts in "clean"
intermediary language
Symbolic execution
3
Scenario
Runner
Scripts' semantics
Report
Web browser
Package
maintainers
as HTML files

Installation Scenario



Thank You For Your Attention!



Thank You For Your Attention!