

# 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

December 14, 2020

IRIF Verification Seminar

- > 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 amd64 74.0.1-1 [51.3 MB]
Fetched 51.3 MB in 5s (9,569 kB/s)
(Reading database ... 140834 files and directories currently installed.)
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



firefox\_74.0-1\_amd64.deb





control.tar.xz




data.tar.xz

# 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

 firefox\_74.0-1\_amd64.deb


 control.tar.xz


 data.tar.xz

  control  
 postinst  
 prerm  
...


 `/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

 firefox\_74.0-1\_a

 control.tar.xz

 control

 postinst

 prein

...

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

 firefox\_74.0-1\_a

 control.tar.xz

 control

 postinst

 prerm

...

```
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 User Request
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 installed.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd64 74.0.1-1 [51.3 MB]
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 not installed.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd64 74.0.1-1 [51.3 MB]
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  
↓

# 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 installed.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd64 74.0.1-1 [51.3 MB]
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



# 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 installed.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd64 74.0.1-1 [51.3 MB]
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

# 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 installed.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd64 74.0.1-1 [51.3 MB]
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 not installed.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd64 74.0.1-1 [51.3 MB]
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

Run postinst

# 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 installed.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd64 74.0.1-1 [51.3 MB]
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

Run postinst

Process Triggers

# 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 installed.
Need to get 51.3 MB of archives.
Get:1 http://deb.debian.org/debian unstable/main amd64 firefox amd64 74.0.1-1 [51.3 MB]
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  
Run postinst  
Process Triggers  
Done

# 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 installed.
Need to get 51.9 MB of archives.
Get:1 http://deb.debian.org/debian/main amd64/firefox 74.0.1-1 amd64.deb
Fetched 51.9 MB in 35s (1,505 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

Run postinst

Process Triggers

Done

We are running Shell scripts

The diagram illustrates the sequence of operations during the installation of the Firefox package. It starts with a 'User Request' to install 'firefox'. This leads to 'Resolve Dependencies', which involves reading package lists and building a dependency tree. The next step is 'Download Package', where the package file is fetched from the repository. This is followed by 'Run preinst', 'Unpack files', and 'Run postinst', which are collectively represented by the box 'We are running Shell scripts'. The final steps are 'Process Triggers' and 'Done'.

# 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 installed.
Need to get 10.4 MB of archives.
Get:1 http://deb.debian.org/debian/main amd64/firefox 74.0.1-1 amd64.deb
Fetched 10.4 MB in 1s (10.4 MB/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

Run postinst

Process Triggers

Done

We are running Shell scripts with full privileges.

# 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 path.el business (which is also unnecessary)?



# The CoLiS Project

> Correctness of Linux Scripts

# The CoLiS Project

- > Correctness of Linux Scripts
- > ANR project from October 2015 to March 2021.

# The CoLiS Project

- > Correctness of Linux Scripts
- > ANR project from October 2015 to March 2021.
- > Goal: applying formal methods to the quality assessment of Debian Packages.

# The CoLiS Project

- > Correctness of Linux Scripts
- > ANR project from October 2015 to March 2021.
- > 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 March 2021.
- > 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 March 2021.
- > 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 March 2021.
- > 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 March 2021.
- > 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.

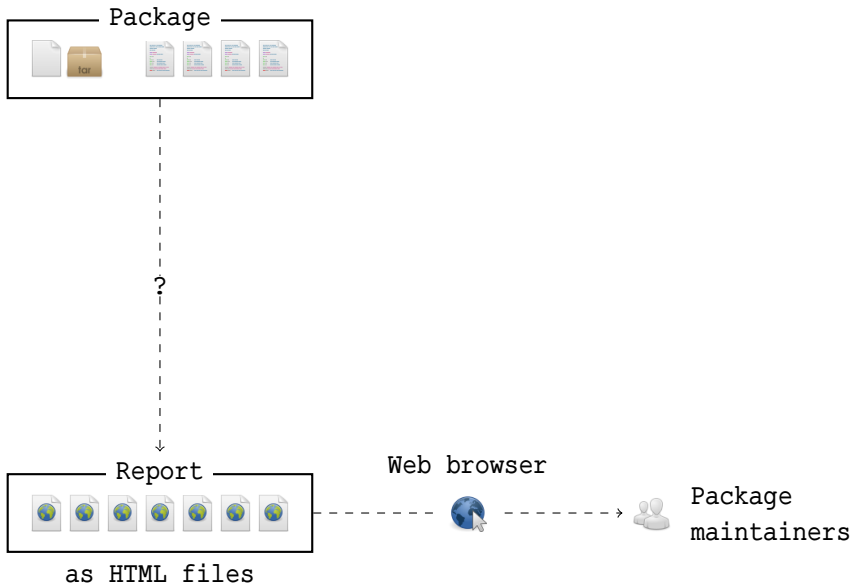


# Battle Plan

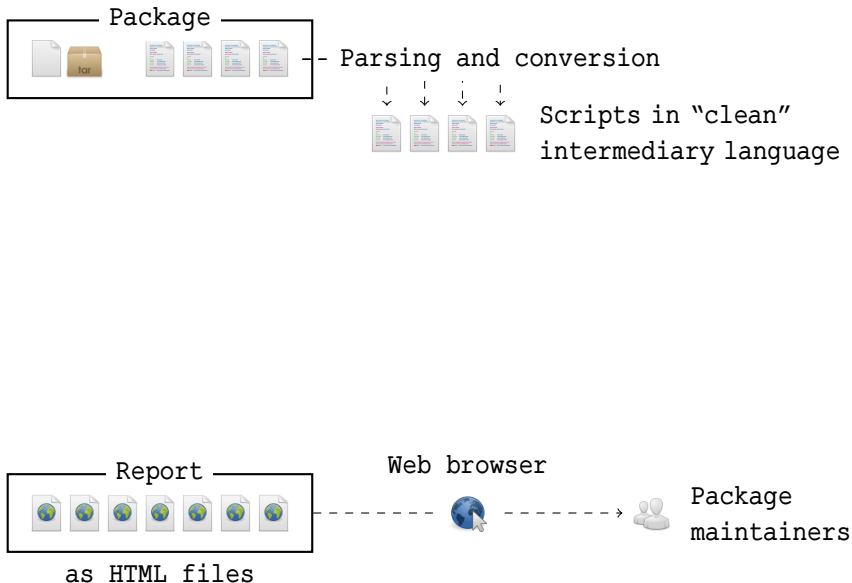
Package



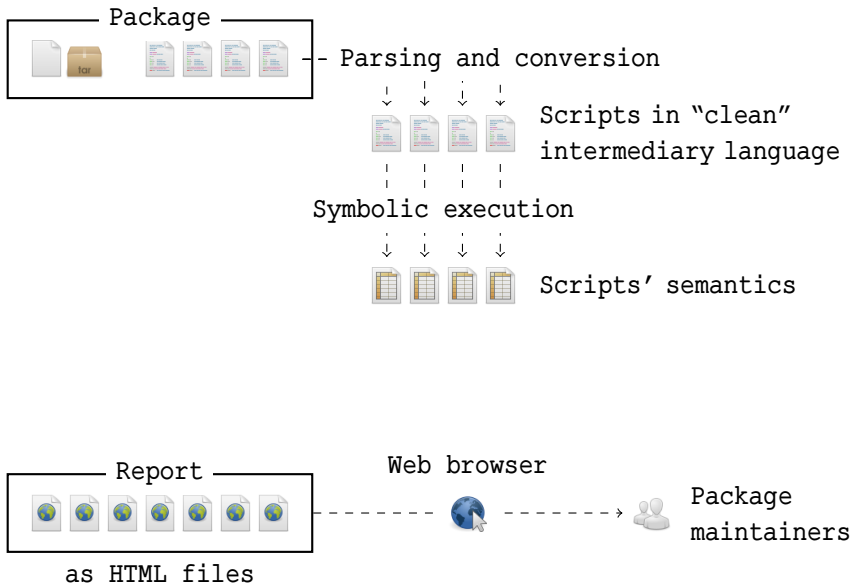
# Battle Plan



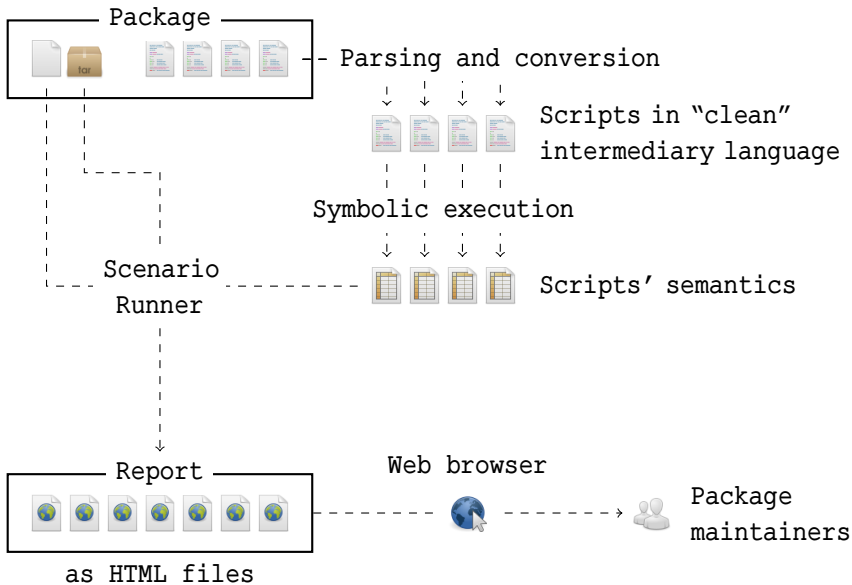
# Battle Plan



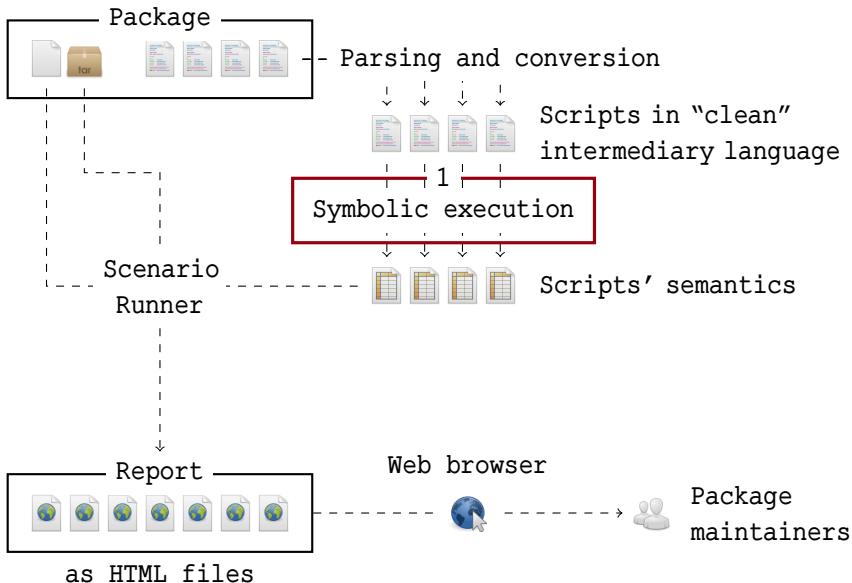
# Battle Plan



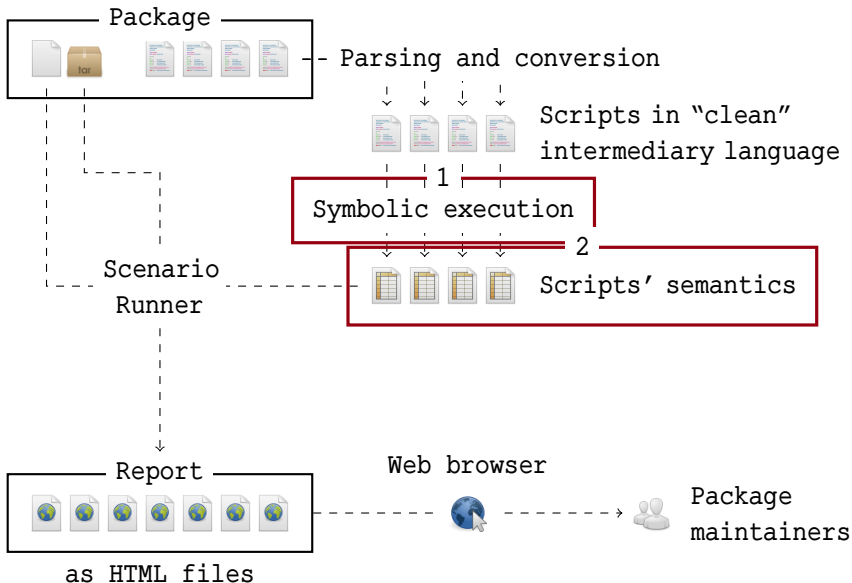
# Battle Plan



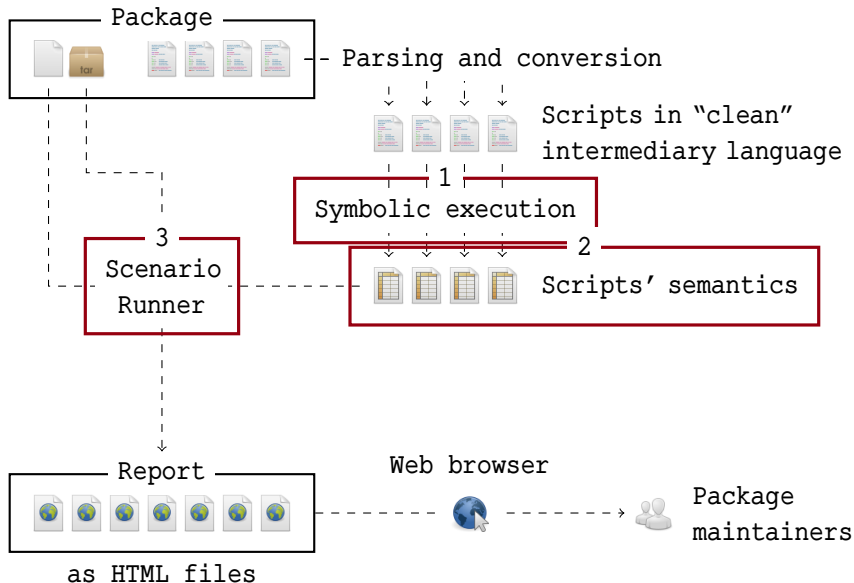
# Battle Plan



# Battle Plan

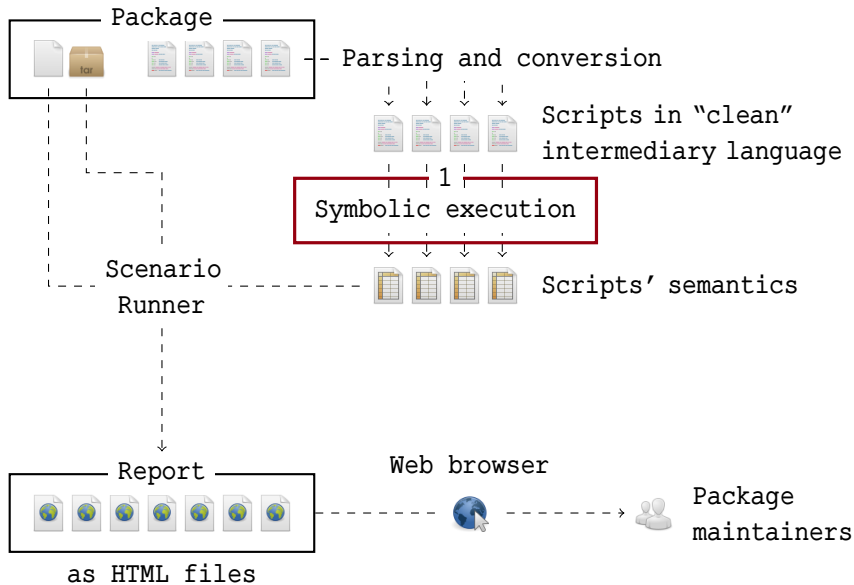


# Battle Plan





# Battle Plan



# Symbolic Execution

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

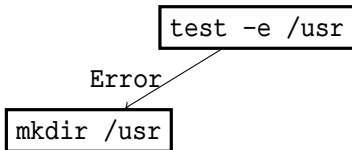
# Symbolic Execution

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

test -e /usr

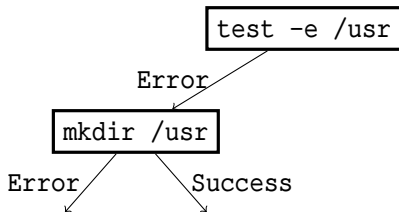
# Symbolic Execution

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



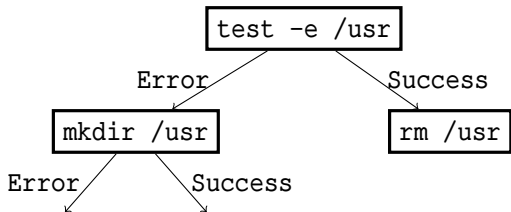
# Symbolic Execution

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



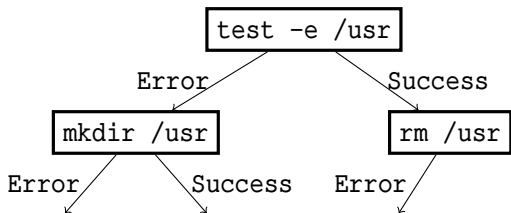
# Symbolic Execution

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



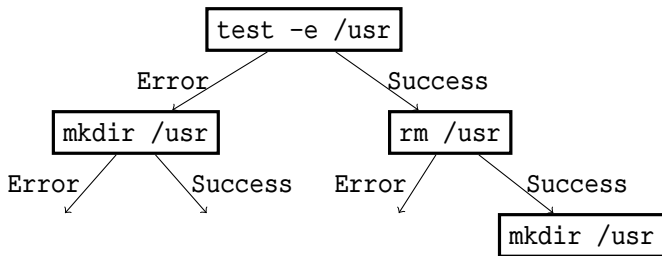
# Symbolic Execution

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



# Symbolic Execution

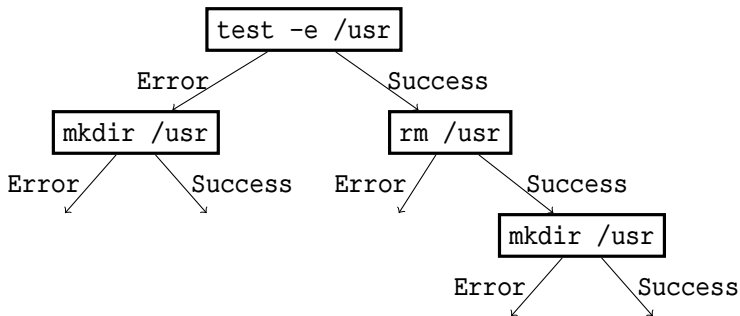
```
if test -e /usr; then
  rm /usr
fi
mkdir /usr
```





# Symbolic Execution

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



# Symbolic Execution

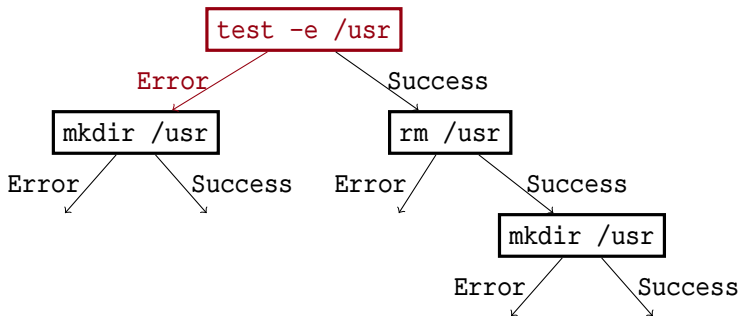
test -e /usr:

Success: /usr existed;

nothing changed

Error: /usr did not exist;

nothing changed



# Symbolic Execution

test -e /usr:

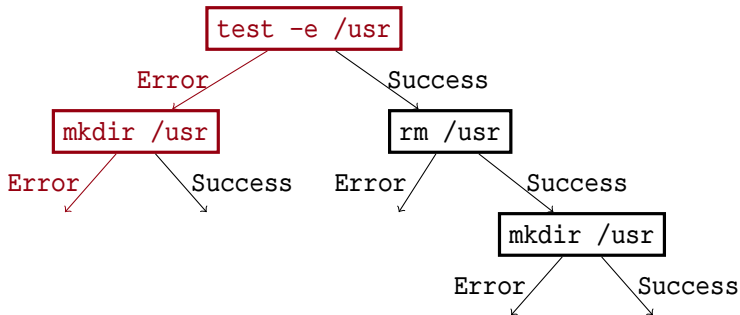
Success: /usr existed;  
nothing changed

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:

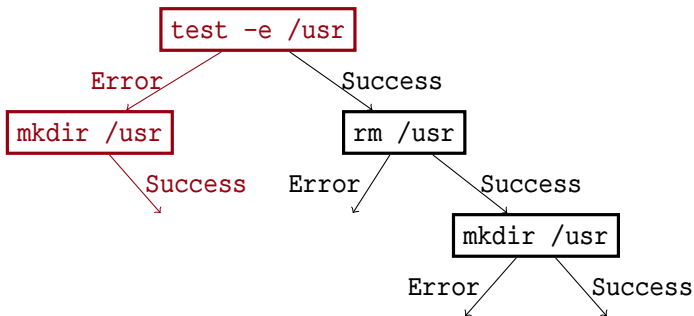
Success: /usr existed;  
nothing changed

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:

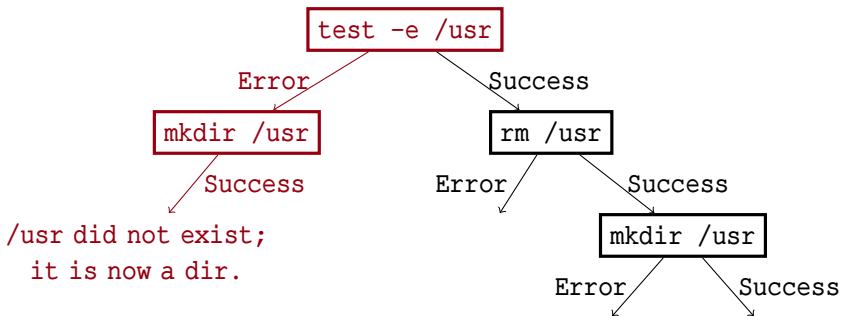
Success: /usr existed;  
nothing changed

Error: /usr did not exist;  
nothing changed

mkdir /usr:

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

Error: /usr existed; nothing changed

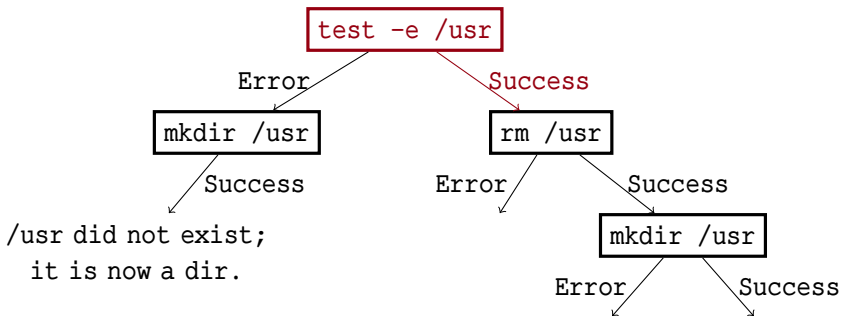


# Symbolic Execution

test -e /usr:

Success: /usr existed;  
nothing changed

Error: /usr did not exist;  
nothing changed



# Symbolic Execution

test -e /usr:

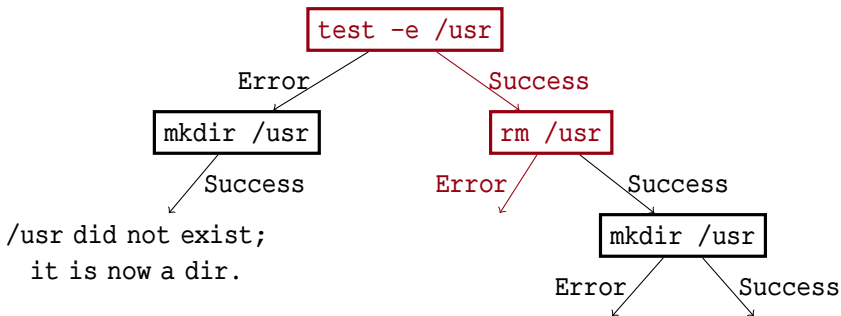
Success: /usr existed;  
nothing changed

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:

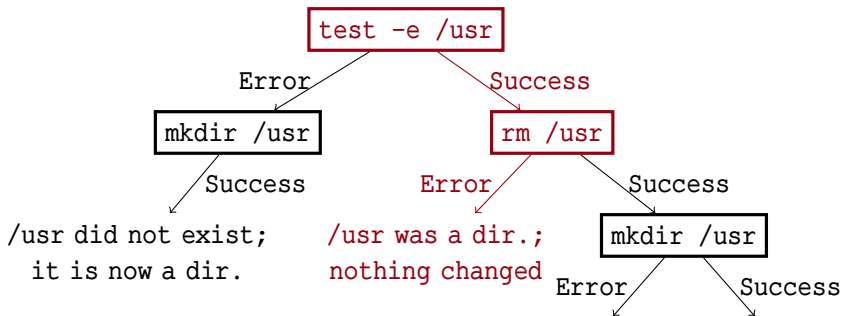
Success: /usr existed;  
nothing changed

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:

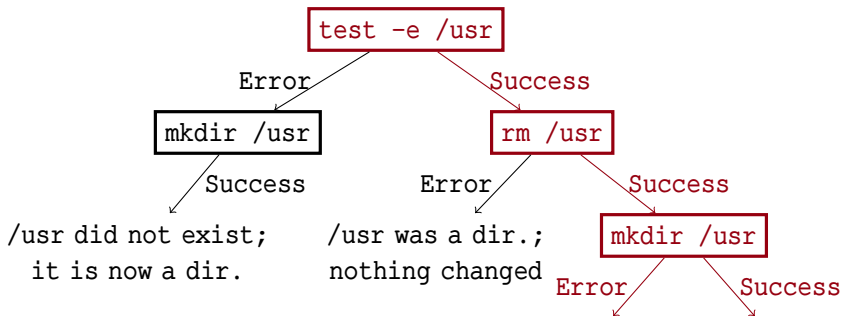
Success: /usr existed;  
nothing changed

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:

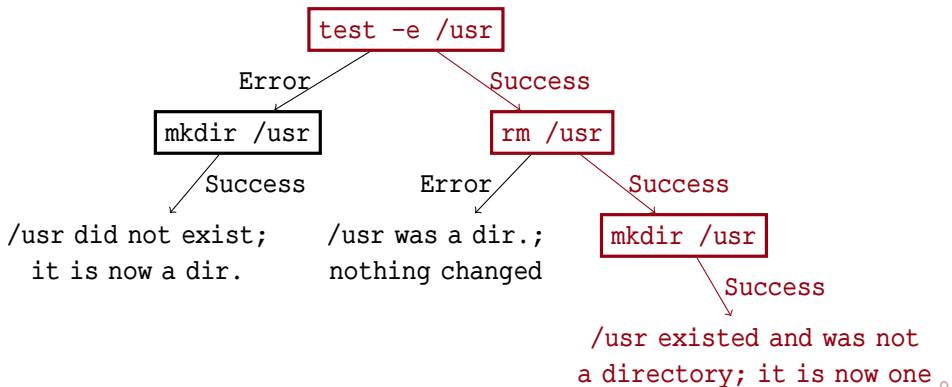
Success: /usr existed;  
nothing changed

Error: /usr did not exist;  
nothing changed

rm /usr:

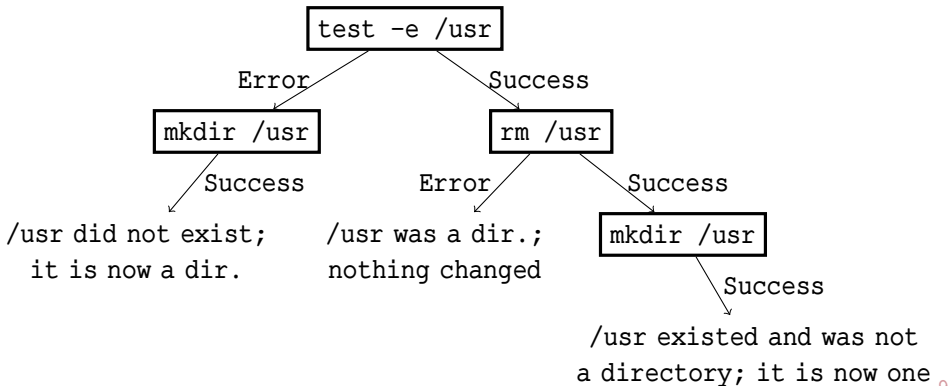
Success: /usr existed and was not a  
directory; it does not exist anymore

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 | $\exists r' \cdot \phi_1(r_1, r') \wedge \phi_2(r', r_2)$ |
| 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 | $\exists r' \cdot \phi_1(r_1, r') \wedge \phi_2(r', r_2)$ |
| Detection of impossible cases                             | emptiness of the domain    |                                                           |
| Transformation of a relation in a more understandable one |                            |                                                           |

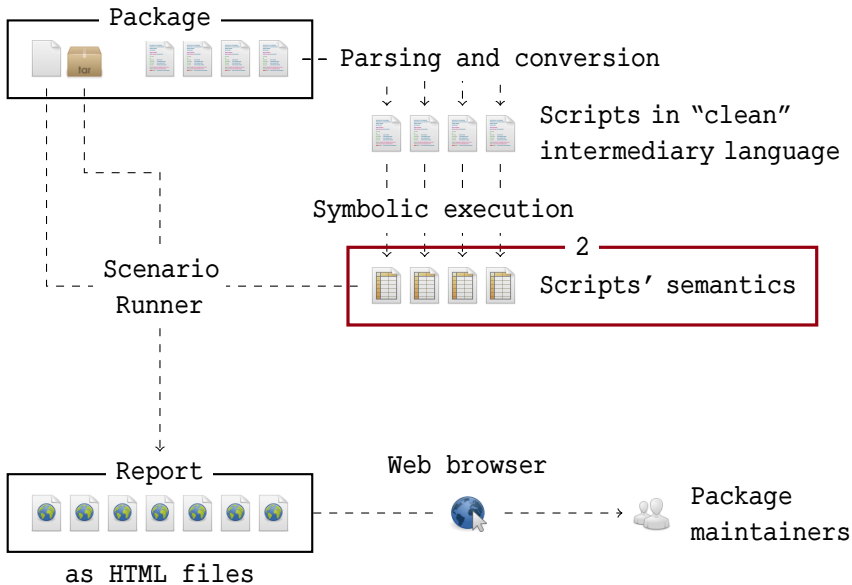
# Backend Requirements

|                                                           | Tree Transducers           | Feature Tree Logics                                       |
|-----------------------------------------------------------|----------------------------|-----------------------------------------------------------|
| Tree relations                                            | by definition              | if two free variables                                     |
| Expressivity to specify POSIX utilities                   | ?                          | ?                                                         |
| Composition of relations                                  | composition of transducers | $\exists r' \cdot \phi_1(r_1, r') \wedge \phi_2(r', r_2)$ |
| 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 | $\exists r' \cdot \phi_1(r_1, r') \wedge \phi_2(r', r_2)$ |
| Detection of impossible cases                             | emptiness of the domain    | unsatisfiability                                          |
| Transformation of a relation in a more understandable one | ?                          | ?                                                         |

# Battle Plan



# Feature Trees

```
  .  
 / \  
lib/ share  
dir  dir
```

```
  .  
 / \  
bin/ usr  
dir  .  
     / \  
    lib/ share  
    dir  dir
```

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

# Feature Trees

```
  .  
 / \  
lib/ share  
dir  dir
```

```
  .  
 / \  
bin/ usr  
dir  .  
     / \  
    lib/ share  
    dir  dir
```

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

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

# Basic Constraints

# Basic Constraints

Equality

$$x = y$$



## Basic Constraints

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

# Basic Constraints

$\rho$  is a model if

Equality

$$\mathbf{x} = \mathbf{y}$$

$$\rho(\mathbf{x}) = \rho(\mathbf{y})$$

Feature

$$\mathbf{x}[\mathbf{f}]\mathbf{y}$$

# Basic Constraints

$\rho$  is a model if

Equality

$$\mathbf{x} = \mathbf{y}$$

$$\rho(\mathbf{x}) = \rho(\mathbf{y})$$

Feature

$$\mathbf{x}[\mathbf{f}]\mathbf{y}$$

$$\rho(\mathbf{x})(\mathbf{f}) = \rho(\mathbf{y})$$

# Basic Constraints

$\rho$  is a model if

Equality

$\mathbf{x} = \mathbf{y}$

$\rho(\mathbf{x}) = \rho(\mathbf{y})$

Feature

$\mathbf{x}[\mathbf{f}]\mathbf{y}$

$\rho(\mathbf{x})(\mathbf{f}) = \rho(\mathbf{y})$

Absence

$\mathbf{x}[\mathbf{f}]\uparrow$

# Basic Constraints

|          |                                    | $\rho$ is a model if                              |
|----------|------------------------------------|---------------------------------------------------|
| Equality | $\mathbf{x} = \mathbf{y}$          | $\rho(\mathbf{x}) = \rho(\mathbf{y})$             |
| Feature  | $\mathbf{x}[\mathbf{f}]\mathbf{y}$ | $\rho(\mathbf{x})(\mathbf{f}) = \rho(\mathbf{y})$ |
| Absence  | $\mathbf{x}[\mathbf{f}]\uparrow$   | $\mathbf{f} \notin \text{dom}(\rho(\mathbf{x}))$  |

# Basic Constraints

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

# Basic Constraints

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

# Basic Constraints

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



# Basic Constraints

|            |                                           | $\rho$ is a model if                                                                        |
|------------|-------------------------------------------|---------------------------------------------------------------------------------------------|
| Equality   | $\mathbf{x} = \mathbf{y}$                 | $\rho(\mathbf{x}) = \rho(\mathbf{y})$                                                       |
| Feature    | $\mathbf{x}[\mathbf{f}]\mathbf{y}$        | $\rho(\mathbf{x})(\mathbf{f}) = \rho(\mathbf{y})$                                           |
| Absence    | $\mathbf{x}[\mathbf{f}]\uparrow$          | $\mathbf{f} \notin \text{dom}(\rho(\mathbf{x}))$                                            |
| Fence      | $\mathbf{x}[\mathbf{F}]$                  | $\text{dom}(\rho(\mathbf{x})) \subseteq \mathbf{F}$                                         |
| Similarity | $\mathbf{x} \sim_{\mathbf{F}} \mathbf{y}$ | $\rho(\mathbf{x}) _{\mathbb{C}_{\mathbf{F}}} = \rho(\mathbf{y}) _{\mathbb{C}_{\mathbf{F}}}$ |

# Basic Constraints

|            |                                           | $\rho$ is a model if                                                                        |
|------------|-------------------------------------------|---------------------------------------------------------------------------------------------|
| Equality   | $\mathbf{x} = \mathbf{y}$                 | $\rho(\mathbf{x}) = \rho(\mathbf{y})$                                                       |
| Feature    | $\mathbf{x}[\mathbf{f}]\mathbf{y}$        | $\rho(\mathbf{x})(\mathbf{f}) = \rho(\mathbf{y})$                                           |
| Absence    | $\mathbf{x}[\mathbf{f}]\uparrow$          | $\mathbf{f} \notin \text{dom}(\rho(\mathbf{x}))$                                            |
| Fence      | $\mathbf{x}[\mathbf{F}]$                  | $\text{dom}(\rho(\mathbf{x})) \subseteq \mathbf{F}$                                         |
| Similarity | $\mathbf{x} \sim_{\mathbf{F}} \mathbf{y}$ | $\rho(\mathbf{x}) _{\mathbb{C}_{\mathbf{F}}} = \rho(\mathbf{y}) _{\mathbb{C}_{\mathbf{F}}}$ |
| Directory  | $\text{dir}(\mathbf{x})$                  |                                                                                             |

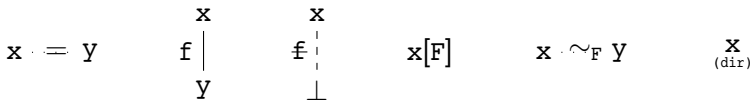
# Basic Constraints

|            |                                           | $\rho$ is a model if                                                                        |
|------------|-------------------------------------------|---------------------------------------------------------------------------------------------|
| Equality   | $\mathbf{x} = \mathbf{y}$                 | $\rho(\mathbf{x}) = \rho(\mathbf{y})$                                                       |
| Feature    | $\mathbf{x}[\mathbf{f}]\mathbf{y}$        | $\rho(\mathbf{x})(\mathbf{f}) = \rho(\mathbf{y})$                                           |
| Absence    | $\mathbf{x}[\mathbf{f}]\uparrow$          | $\mathbf{f} \notin \text{dom}(\rho(\mathbf{x}))$                                            |
| Fence      | $\mathbf{x}[\mathbf{F}]$                  | $\text{dom}(\rho(\mathbf{x})) \subseteq \mathbf{F}$                                         |
| Similarity | $\mathbf{x} \sim_{\mathbf{F}} \mathbf{y}$ | $\rho(\mathbf{x}) _{\mathbf{G}_{\mathbf{F}}} = \rho(\mathbf{y}) _{\mathbf{G}_{\mathbf{F}}}$ |
| Directory  | $\text{dir}(\mathbf{x})$                  | $\rho(\mathbf{x}) = \text{dir}$                                                             |

# Basic Constraints

$\rho$  is a model if

|            |                                           |                                                                                             |
|------------|-------------------------------------------|---------------------------------------------------------------------------------------------|
| Equality   | $\mathbf{x} = \mathbf{y}$                 | $\rho(\mathbf{x}) = \rho(\mathbf{y})$                                                       |
| Feature    | $\mathbf{x}[\mathbf{f}]\mathbf{y}$        | $\rho(\mathbf{x})(\mathbf{f}) = \rho(\mathbf{y})$                                           |
| Absence    | $\mathbf{x}[\mathbf{f}]\uparrow$          | $\mathbf{f} \notin \text{dom}(\rho(\mathbf{x}))$                                            |
| Fence      | $\mathbf{x}[\mathbf{F}]$                  | $\text{dom}(\rho(\mathbf{x})) \subseteq \mathbf{F}$                                         |
| Similarity | $\mathbf{x} \sim_{\mathbf{F}} \mathbf{y}$ | $\rho(\mathbf{x}) _{\mathbf{G}_{\mathbf{F}}} = \rho(\mathbf{y}) _{\mathbf{G}_{\mathbf{F}}}$ |
| Directory  | $\text{dir}(\mathbf{x})$                  | $\rho(\mathbf{x}) = \text{dir}$                                                             |



## 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

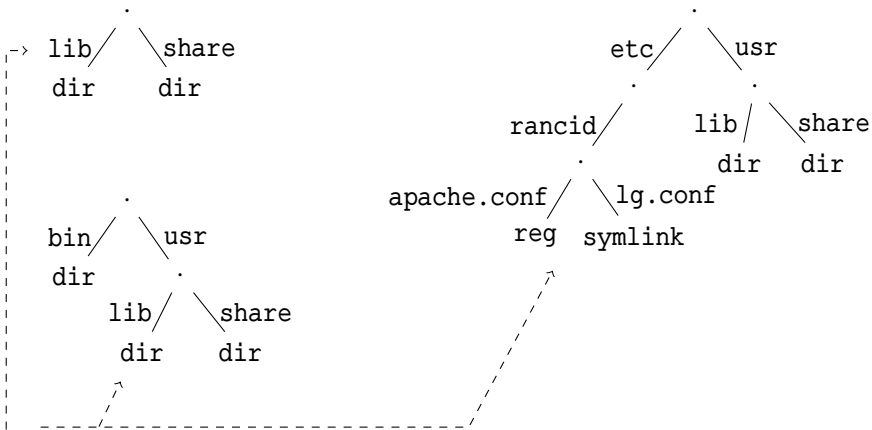
```
  .  
lib/ \ share  
dir   dir
```

```
  .  
bin/ \ usr  
dir   .  
      .  
      lib/ \ share  
      dir   dir
```

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

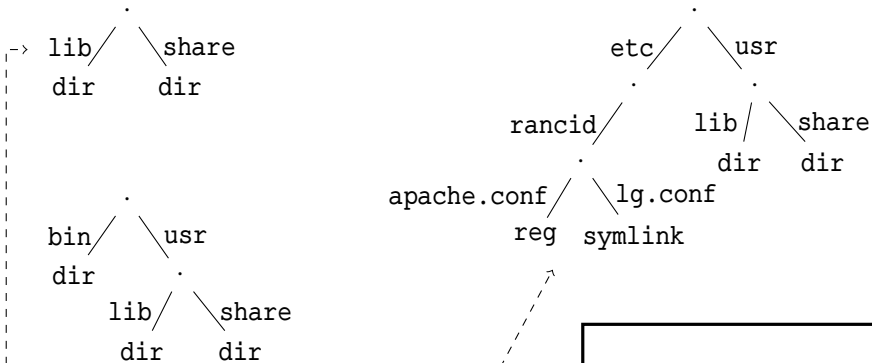
$$x[usr]z \wedge z[etc]\uparrow$$
$$\wedge \exists v \cdot y[bin]v \wedge x \sim_{\{bin,etc\}} Y$$

# An Example



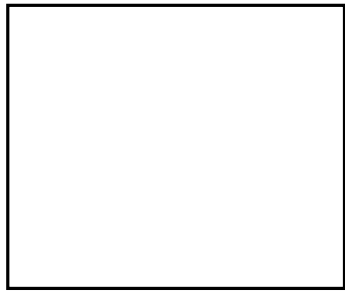
$$[x, Y, z] \models x[usr]z \wedge z[etc]\uparrow \\ \wedge \exists v \cdot y[bin]v \wedge x \sim_{\{bin, etc\}} Y$$

# An Example



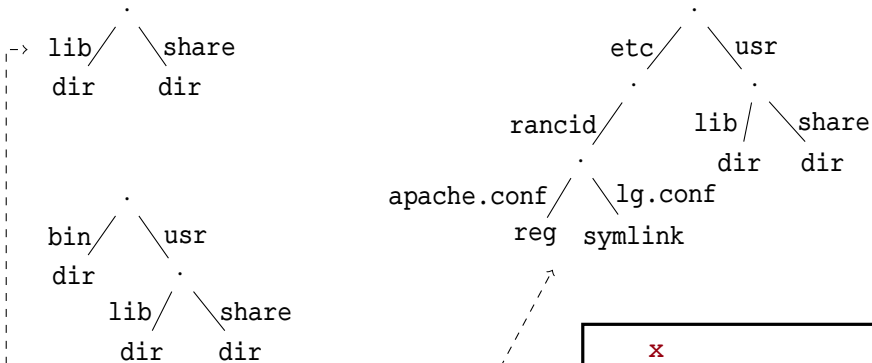
$$[x, Y, z] \models x[\text{usr}]z \wedge z[\text{etc}] \uparrow$$

$$\wedge \exists v \cdot y[\text{bin}]v \wedge x \sim_{\{\text{bin}, \text{etc}\}} Y$$

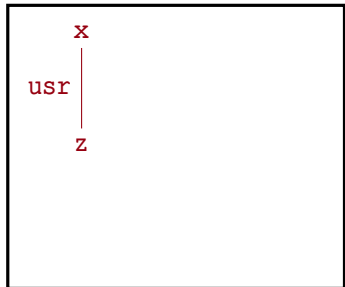




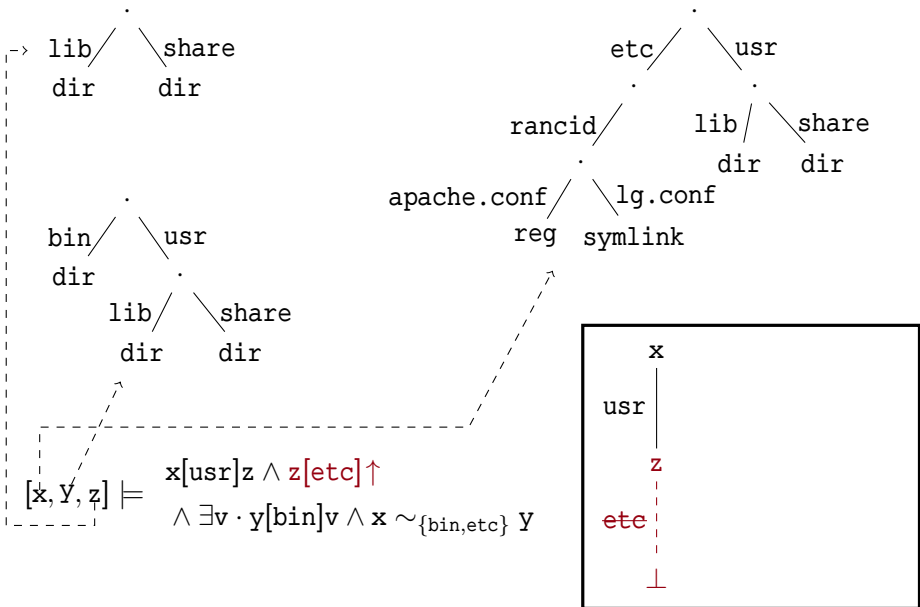
# An Example



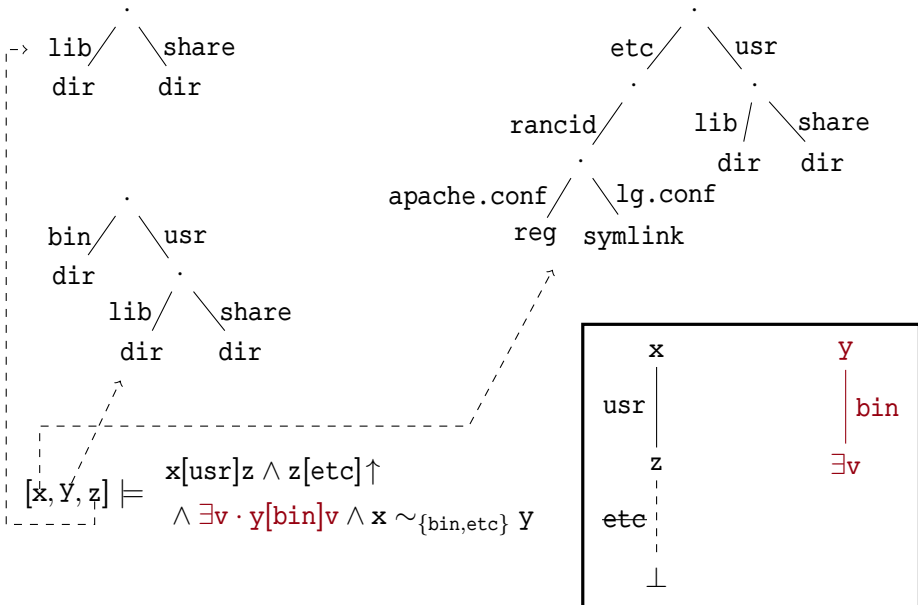
$$\begin{aligned}
 [x, Y, z] \models & \quad x[usr]z \wedge z[etc] \uparrow \\
 & \quad \wedge \exists v \cdot y[bin]v \wedge x \sim_{\{bin, etc\}} Y
 \end{aligned}$$



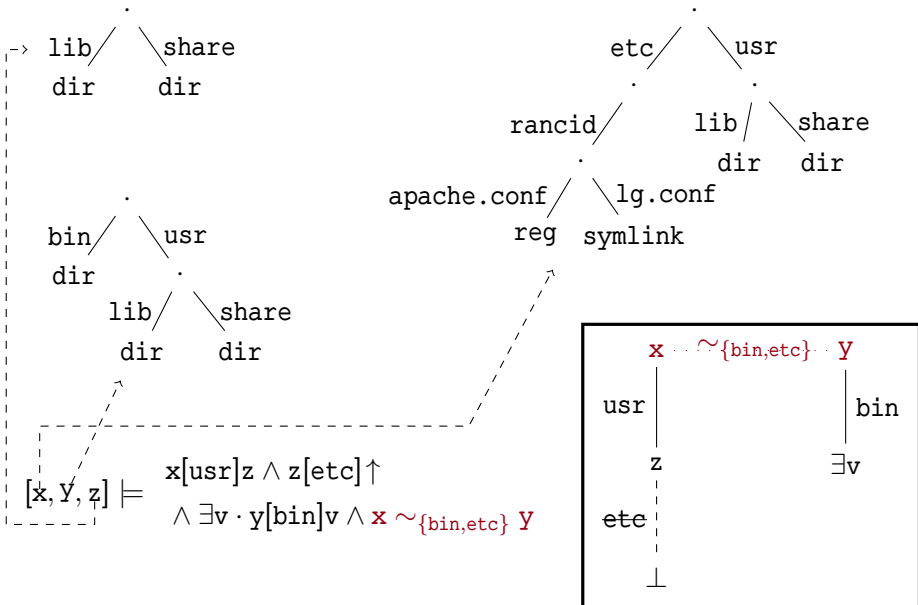
# An Example



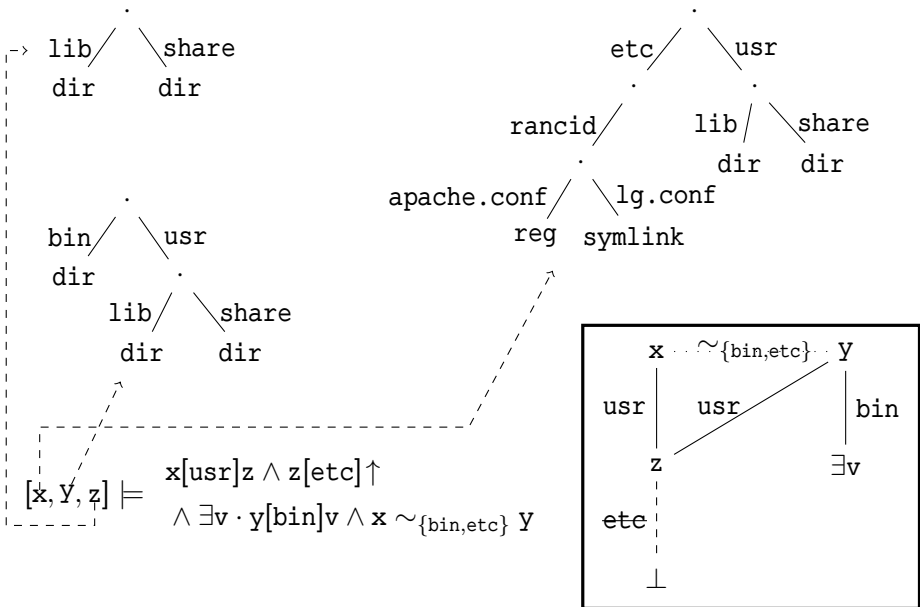
# An Example



# An Example



# An Example



# Example Transformation Rule

$$\mathbf{x[f]z} \wedge \mathbf{x} \sim_{\mathbf{F}} \mathbf{y}$$

$$(\mathbf{f} \notin \mathbf{F})$$

$$\begin{array}{c} \mathbf{x} \cdots \sim_{\mathbf{F}} \cdots \mathbf{y} \\ \mathbf{f} \mid \\ \mathbf{z} \end{array}$$

$$(\mathbf{f} \notin \mathbf{F})$$

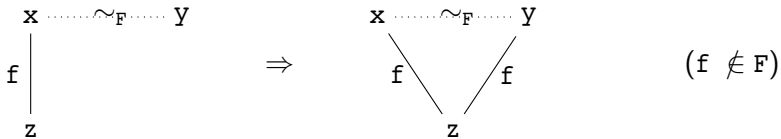
# Example Transformation Rule

$$\mathbf{x[f]z} \wedge \mathbf{x} \sim_{\mathbf{F}} \mathbf{y} \quad \Rightarrow \quad \mathbf{x[f]z} \wedge \mathbf{x} \sim_{\mathbf{F}} \mathbf{y} \wedge \mathbf{y[f]z} \quad (\mathbf{f} \notin \mathbf{F})$$

$$\begin{array}{c} \mathbf{x} \cdots \sim_{\mathbf{F}} \cdots \mathbf{y} \\ | \\ \mathbf{f} \\ | \\ \mathbf{z} \end{array} \quad (\mathbf{f} \notin \mathbf{F})$$

# Example Transformation Rule

$$\mathbf{x[f]z} \wedge \mathbf{x} \sim_{\mathbf{F}} \mathbf{y} \quad \Rightarrow \quad \mathbf{x[f]z} \wedge \mathbf{x} \sim_{\mathbf{F}} \mathbf{y} \wedge \mathbf{y[f]z} \quad (\mathbf{f} \notin \mathbf{F})$$





## Example Clash Rule

$$\mathbf{x[F]} \wedge \mathbf{x[f]z}$$
$$(\mathbf{f} \notin \mathbf{F})$$
$$\begin{array}{c} \mathbf{x[F]} \\ | \\ \mathbf{f} \\ | \\ \mathbf{z} \end{array}$$
$$(\mathbf{f} \notin \mathbf{F})$$

## Example Clash Rule

$$\mathbf{x[F]} \wedge \mathbf{x[f]z} \quad \Rightarrow \quad \perp \quad (\mathbf{f} \notin \mathbf{F})$$

$$\begin{array}{c} \mathbf{x[F]} \\ | \\ \mathbf{f} \\ | \\ \mathbf{z} \end{array} \quad (\mathbf{f} \notin \mathbf{F})$$

## Example Clash Rule

$$\mathbf{x[F]} \wedge \mathbf{x[f]z} \quad \Rightarrow \quad \perp \quad (\mathbf{f} \notin \mathbf{F})$$

$$\begin{array}{c} \mathbf{x[F]} \\ \mathbf{f} \mid \\ \mathbf{z} \end{array} \quad \Rightarrow \quad \perp \quad (\mathbf{f} \notin \mathbf{F})$$

## Example Specification: mkdir q/f

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Success                          | $\begin{aligned} & \exists \mathbf{x}, \mathbf{x}', \mathbf{y}'. \\ & \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow \\ & \wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}' \\ & \wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f] \mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset] \end{aligned}$ |
| Error: file exists               | $\exists \mathbf{y} \cdot \text{resolve}(r, \text{cwd}, q/f, \mathbf{y}) \wedge r = r'$                                                                                                                                                                                                                                                                                                                                                               |
| Error: no parent                 | $\text{noresolve}(r, \text{cwd}, q) \wedge r = r'$                                                                                                                                                                                                                                                                                                                                                                                                    |
| Error: parent is not a directory | $\exists \mathbf{x} \cdot \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \neg \text{dir}(\mathbf{x}) \wedge r = r'$                                                                                                                                                                                                                                                                                                                              |

# Example Specification: mkdir q/f

Success

$$\begin{aligned} & \exists \mathbf{x}, \mathbf{x}', \mathbf{y}'. \\ & \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow \\ & \wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}' \\ & \wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f] \mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset] \end{aligned}$$

Error: file exists

$\exists \mathbf{y}$

Error: no parent

no

Error: parent is not  
a directory

$\exists \mathbf{x}$

$\wedge r = r'$

# Example Specification: mkdir q/f

Success

$\exists \mathbf{x}, \mathbf{x}', \mathbf{y}'.$

$\text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow$

$\wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}'$

$\wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f]\mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset]$

Error: file exists

$\exists \mathbf{y}$

$r$   
|  
 $q$

Error: no parent

no

$\exists \mathbf{x}$

Error: parent is not  
a directory

$\exists \mathbf{x}$

$\wedge r = r'$

# Example Specification: mkdir q/f

Success

$$\begin{aligned} & \exists \mathbf{x}, \mathbf{x}', \mathbf{y}'. \\ & \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow \\ & \wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}' \\ & \wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f] \mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset] \end{aligned}$$

Error: file exists

$\exists \mathbf{y}$

$r$   
|  
 $q$

Error: no parent

no

$\exists \mathbf{x}$   
(dir)

Error: parent is not  
a directory

$\exists \mathbf{x}$

$\wedge r = r'$

# Example Specification: mkdir q/f

Success

$$\begin{aligned} & \exists \mathbf{x}, \mathbf{x}', \mathbf{y}'. \\ & \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow \\ & \wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}' \\ & \wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f] \mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset] \end{aligned}$$

Error: file exists

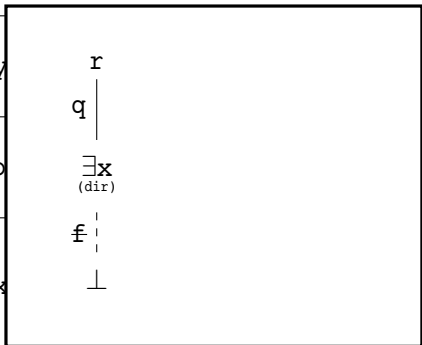
$\exists \mathbf{y}$

Error: no parent

no

Error: parent is not  
a directory

$\exists \mathbf{x}$



$\wedge r = r'$



# Example Specification: mkdir q/f

Success

$$\begin{aligned} & \exists \mathbf{x}, \mathbf{x}', \mathbf{y}'. \\ & \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow \\ & \wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}' \\ & \wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f] \mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset] \end{aligned}$$

Error: file exists

$\exists \mathbf{y}$

$$\begin{array}{ccc} r & \dots \sim_{\{q\}} \dots & r' \\ | & & | \\ q & & q \end{array}$$

Error: no parent

no

$$\begin{array}{ccc} \exists \mathbf{x} & & \exists \mathbf{x}' \\ \text{(dir)} & & \end{array}$$

Error: parent is not  
a directory

$\exists \mathbf{x}$

$$\begin{array}{c} f \\ \vdots \\ \perp \end{array}$$

$\wedge r = r'$

# Example Specification: mkdir q/f

Success

$$\begin{aligned} & \exists \mathbf{x}, \mathbf{x}', \mathbf{y}'. \\ & \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow \\ & \wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}' \\ & \wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f] \mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset] \end{aligned}$$

Error: file exists

$$\exists \mathbf{y} \quad \begin{array}{ccc} r & \dots \sim_{\{q\}} \dots & r' \\ q \mid & & \mid q \end{array}$$

Error: no parent

$$\text{no} \quad \begin{array}{ccc} \exists \mathbf{x} & \dots \sim_{\{f\}} \dots & \exists \mathbf{x}' \\ (\text{dir}) & & \end{array}$$

Error: parent is not a directory

$$\begin{array}{ccc} \exists \mathbf{x} & \begin{array}{c} f \vdots \\ \perp \end{array} & \wedge r = r' \end{array}$$

# Example Specification: mkdir q/f

Success

$$\begin{aligned} & \exists \mathbf{x}, \mathbf{x}', \mathbf{y}'. \\ & \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow \\ & \wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}' \\ & \wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f] \mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset] \end{aligned}$$

Error: file exists

$\exists \mathbf{y}$

$$\begin{array}{ccc} r & \dots \sim_{\{q\}} \dots & r' \\ | & & | \\ q & & q \end{array}$$

Error: no parent

no

$$\begin{array}{ccc} \exists \mathbf{x} & \dots \sim_{\{f\}} \dots & \exists \mathbf{x}' \\ (\text{dir}) & & (\text{dir}) \end{array}$$

Error: parent is not a directory

$\exists \mathbf{x}$

$$\begin{array}{c} f \\ \vdots \\ \perp \end{array}$$

$\wedge r = r'$

# Example Specification: mkdir q/f

Success

$$\begin{aligned} & \exists \mathbf{x}, \mathbf{x}', \mathbf{y}'. \\ & \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow \\ & \wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}' \\ & \wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f] \mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset] \end{aligned}$$

Error: file exists

$\exists \mathbf{y}$

$$\begin{array}{ccc} r & \dots \sim_{\{q\}} \dots & r' \\ | & & | \\ q & & q \end{array}$$

Error: no parent

no

$$\begin{array}{ccc} \exists \mathbf{x} & \dots \sim_{\{f\}} \dots & \exists \mathbf{x}' \\ (\text{dir}) & & (\text{dir}) \end{array}$$

Error: parent is not  
a directory

$\exists \mathbf{x}$

$$\begin{array}{ccc} f & \vdots & f \\ | & & | \\ \perp & & \exists \mathbf{y}' \end{array}$$

$\wedge r = r'$

# Example Specification: mkdir q/f

Success

$$\begin{aligned} & \exists \mathbf{x}, \mathbf{x}', \mathbf{y}'. \\ & \text{resolve}(r, \text{cwd}, q, \mathbf{x}) \wedge \text{dir}(\mathbf{x}) \wedge \mathbf{x}[f] \uparrow \\ & \wedge \text{similar}(r, r', \text{cwd}, q, \mathbf{x}, \mathbf{x}') \wedge \mathbf{x} \sim_{\{f\}} \mathbf{x}' \\ & \wedge \text{dir}(\mathbf{x}') \wedge \mathbf{x}'[f] \mathbf{y}' \wedge \text{dir}(\mathbf{y}') \wedge \mathbf{y}'[\emptyset] \end{aligned}$$

Error: file exists

$\exists \mathbf{y}$

$$\begin{array}{ccc} r & \dots \sim_{\{q\}} \dots & r' \\ | & & | \\ q & & q \end{array}$$

Error: no parent

no

$$\begin{array}{ccc} \exists \mathbf{x} & \dots \sim_{\{f\}} \dots & \exists \mathbf{x}' \\ (\text{dir}) & & (\text{dir}) \end{array}$$

Error: parent is not a directory

$\exists \mathbf{x}$

$$\begin{array}{ccc} f & \vdots & f \\ | & & | \\ \perp & & \exists \mathbf{y}'[\emptyset] \\ & & (\text{dir}) \end{array}$$

$\wedge r = r'$

# Chaining Specifications

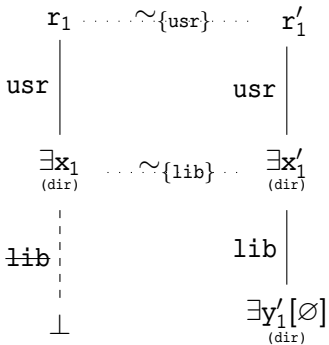
```
mkdir /usr/lib  
(success)
```

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

# Chaining Specifications

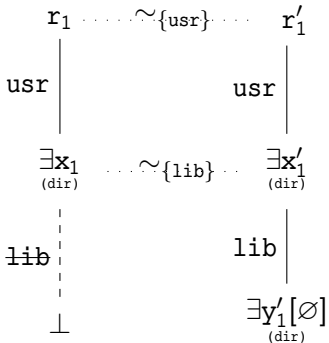
mkdir /usr/lib  
(success)

mkdir /usr/lib/foo  
(success)

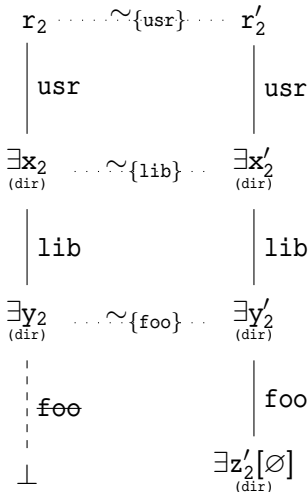


# Chaining Specifications

mkdir /usr/lib  
(success)



mkdir /usr/lib/foo  
(success)

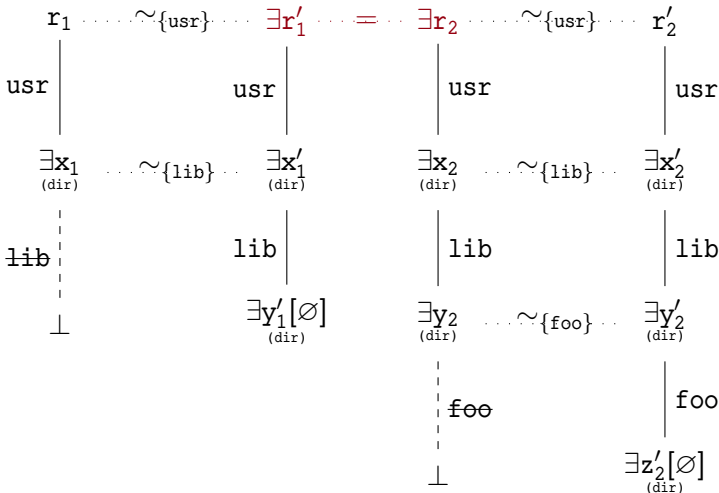




# Chaining Specifications

mkdir /usr/lib  
(success)

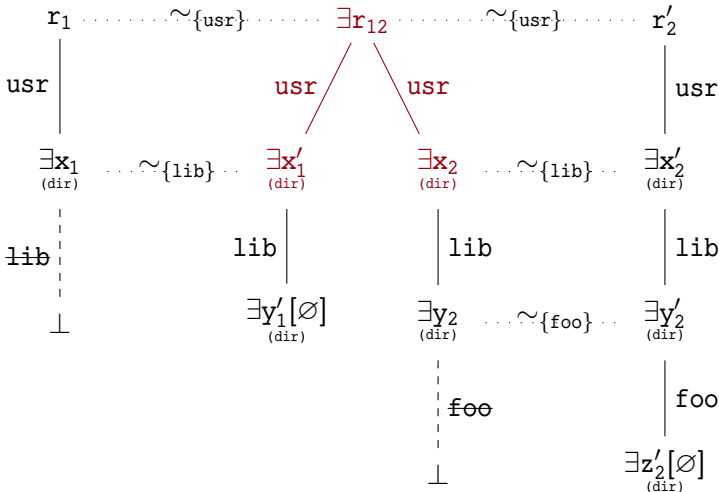
mkdir /usr/lib/foo  
(success)



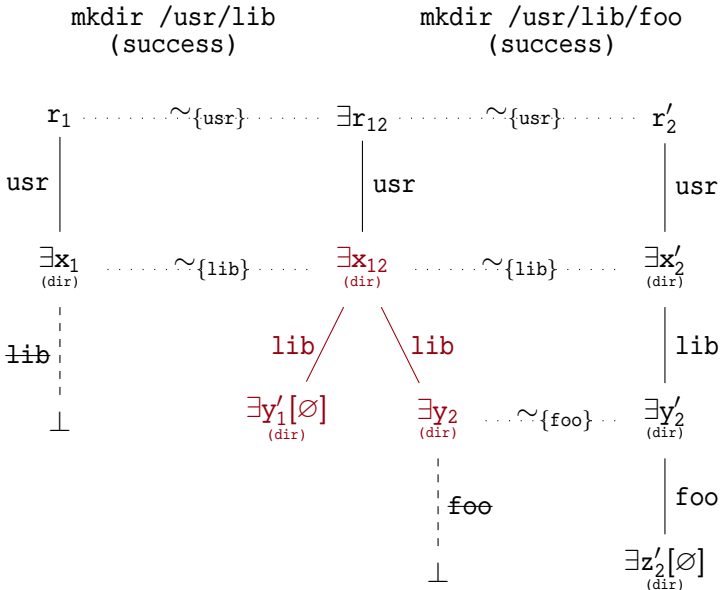
# Chaining Specifications

mkdir /usr/lib  
(success)

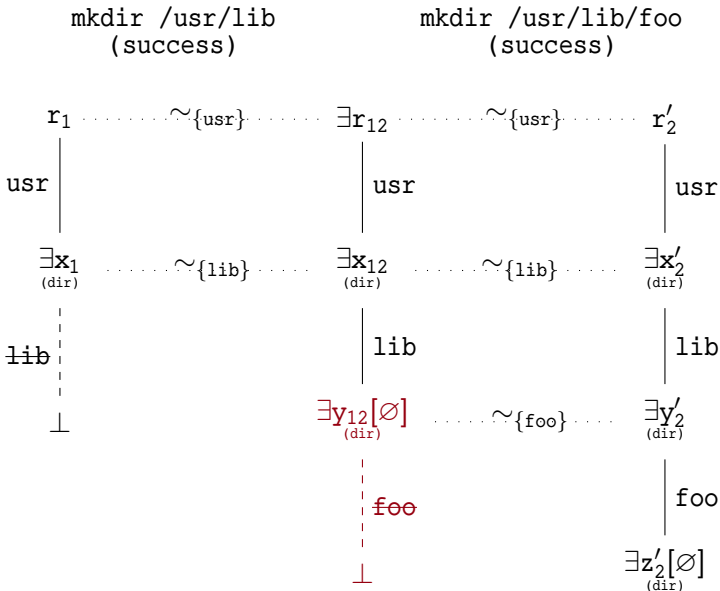
mkdir /usr/lib/foo  
(success)



# Chaining Specifications



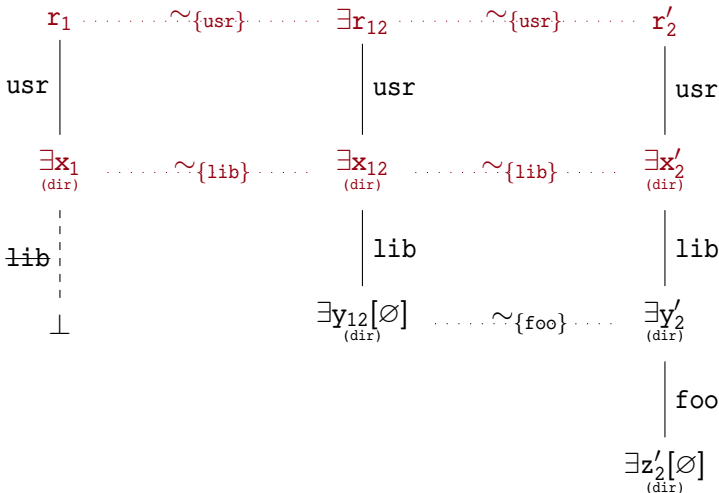
# Chaining Specifications



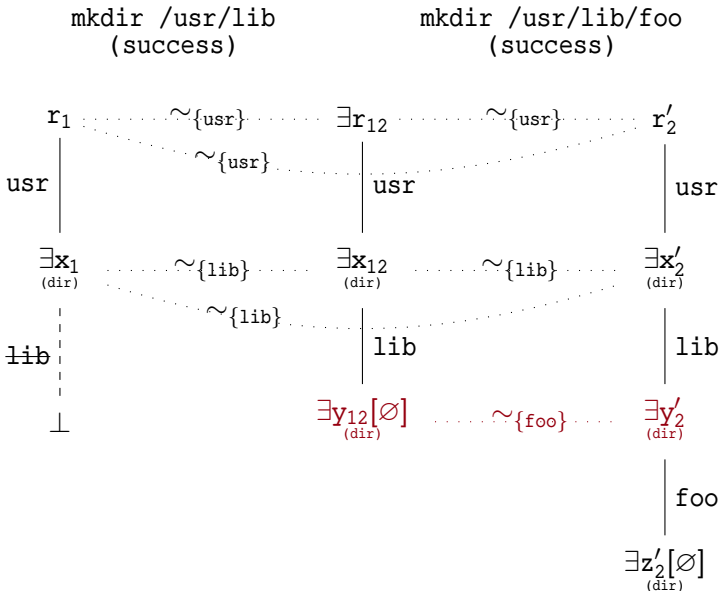
# Chaining Specifications

mkdir /usr/lib  
(success)

mkdir /usr/lib/foo  
(success)



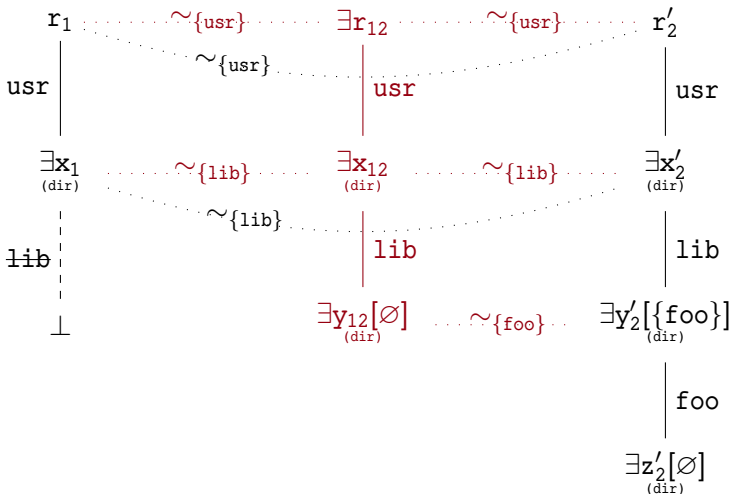
# Chaining Specifications



# Chaining Specifications

mkdir /usr/lib  
(success)

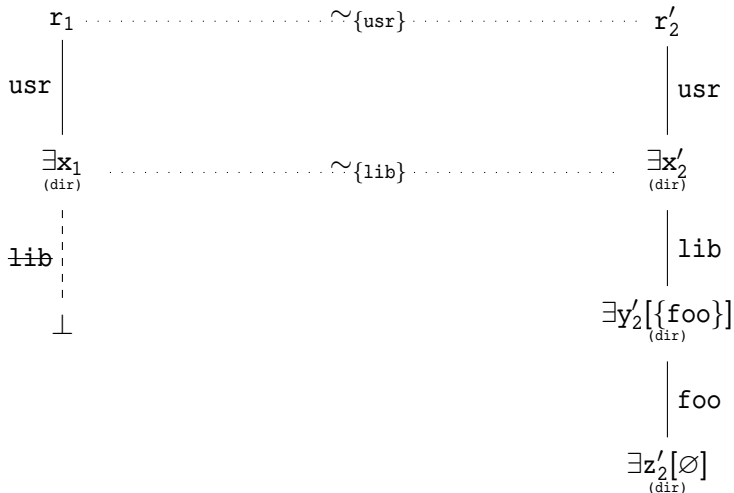
mkdir /usr/lib/foo  
(success)



# Chaining Specifications

mkdir /usr/lib  
(success)

mkdir /usr/lib/foo  
(success)





# Chaining Specifications

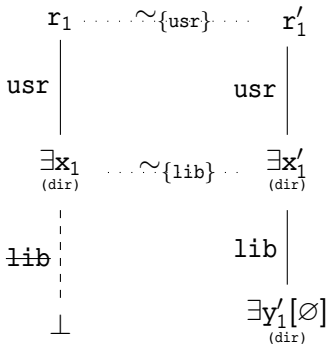
```
mkdir /usr/lib  
(success)
```

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

# Chaining Specifications

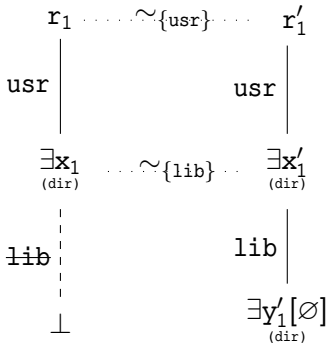
mkdir /usr/lib  
(success)

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

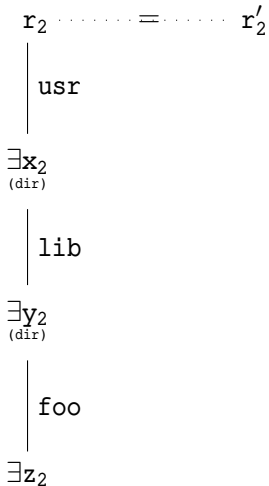


# Chaining Specifications

mkdir /usr/lib  
(success)



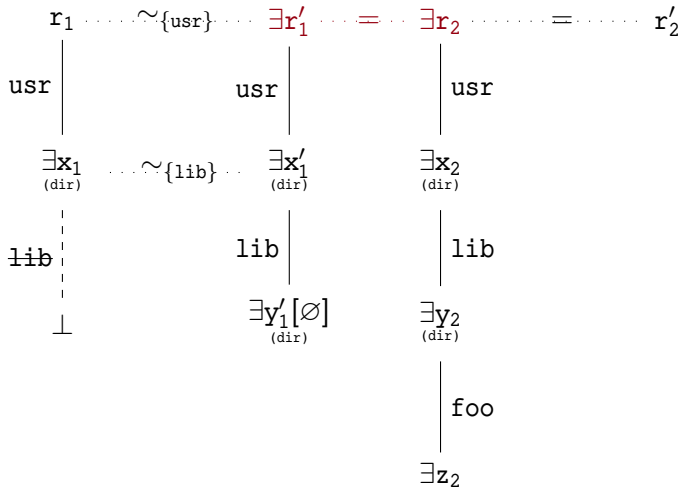
mkdir /usr/lib/foo  
(error: file exists)



# Chaining Specifications

mkdir /usr/lib  
(success)

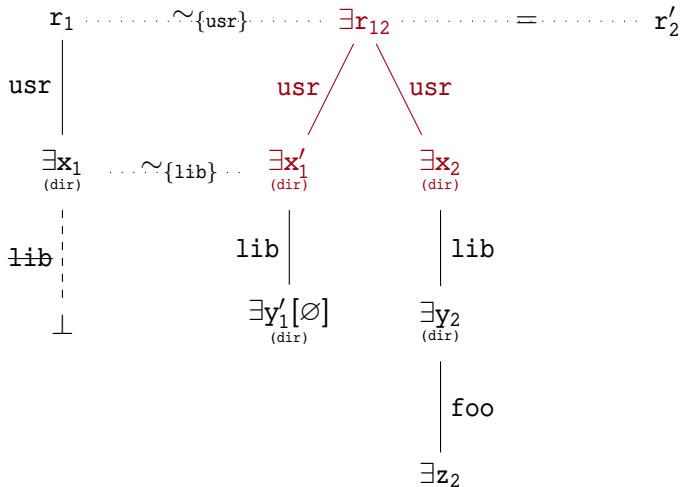
mkdir /usr/lib/foo  
(error: file exists)



# Chaining Specifications

mkdir /usr/lib  
(success)

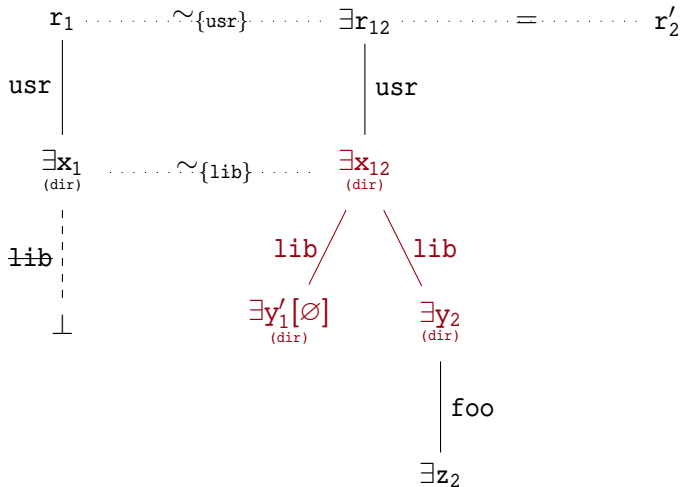
mkdir /usr/lib/foo  
(error: file exists)



# Chaining Specifications

mkdir /usr/lib  
(success)

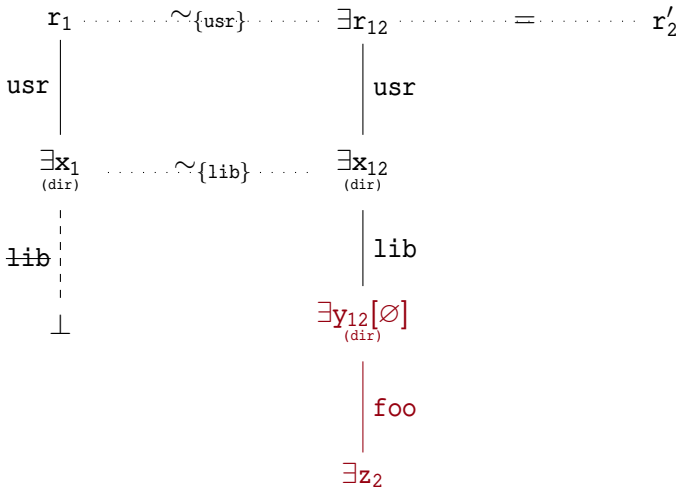
mkdir /usr/lib/foo  
(error: file exists)



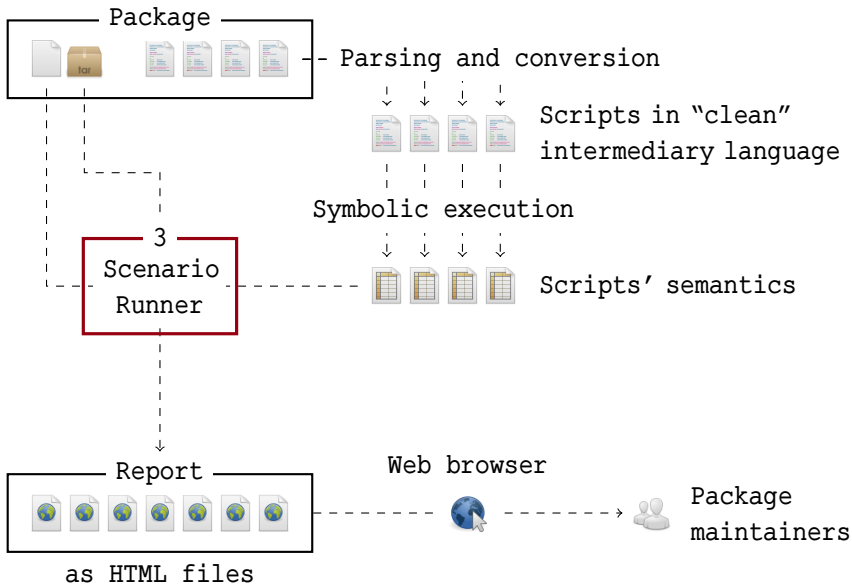
# Chaining Specifications

mkdir /usr/lib  
(success)

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

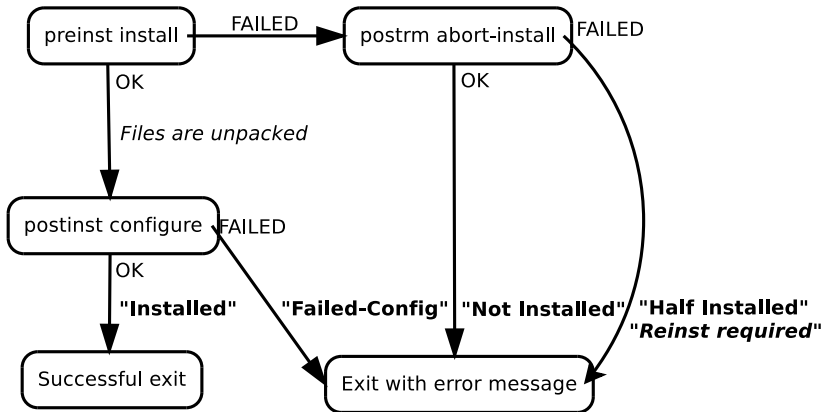


# Battle Plan

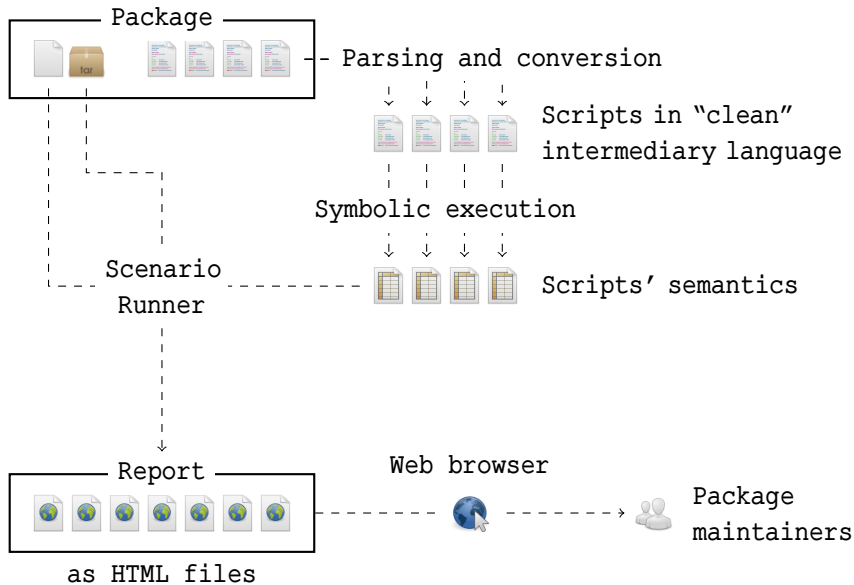




# Installation Scenario



# Thank You For Your Attention!



# Thank You For Your Attention!

