# Nix: A Safe and Policy-Free System for Software Deployment

Eelco Dolstra  Merijn de Jonge  Eelco Visser

Institute of Information & Computing Sciences
Utrecht University, The Netherlands

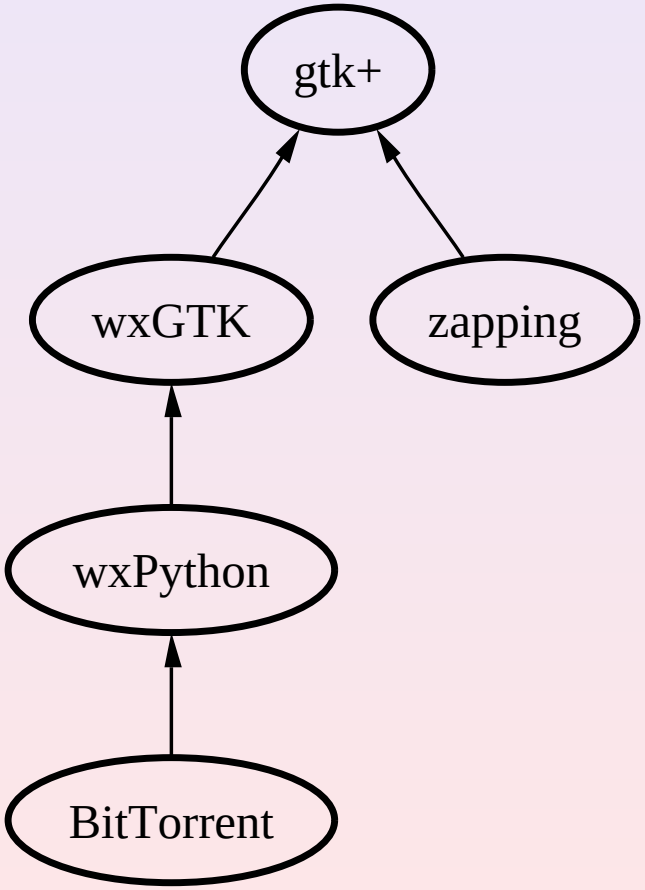
November 17, 2004

# Software deployment

- Software deployment: the art of **transferring software** (packages) from one machine to another (and managing it).
- The hard part: packages should **work the same** on the target machine.
  - "DLL hell"
  - "Dependency hell"

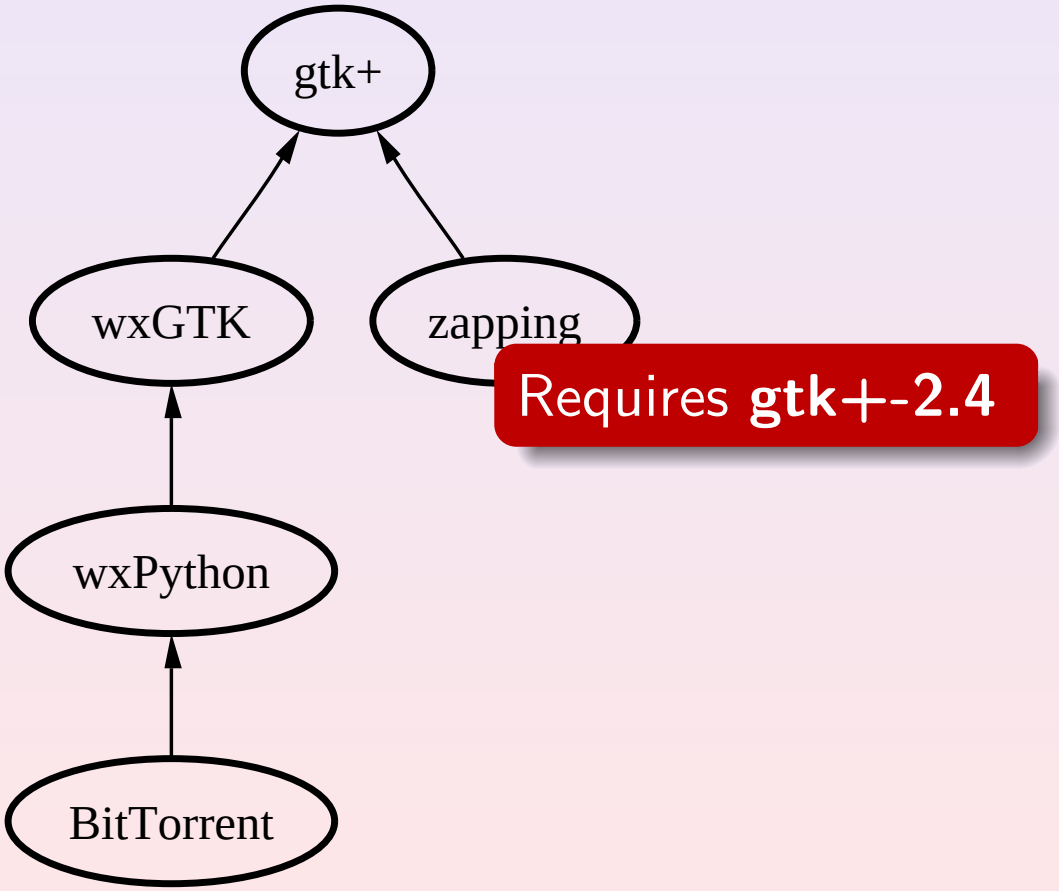
# So why is this hard?

- Difficult to have multiple versions; but we want this to
  - Test upgrades
  - Deal with conflicting dependencies
  - Support different user / service requirements



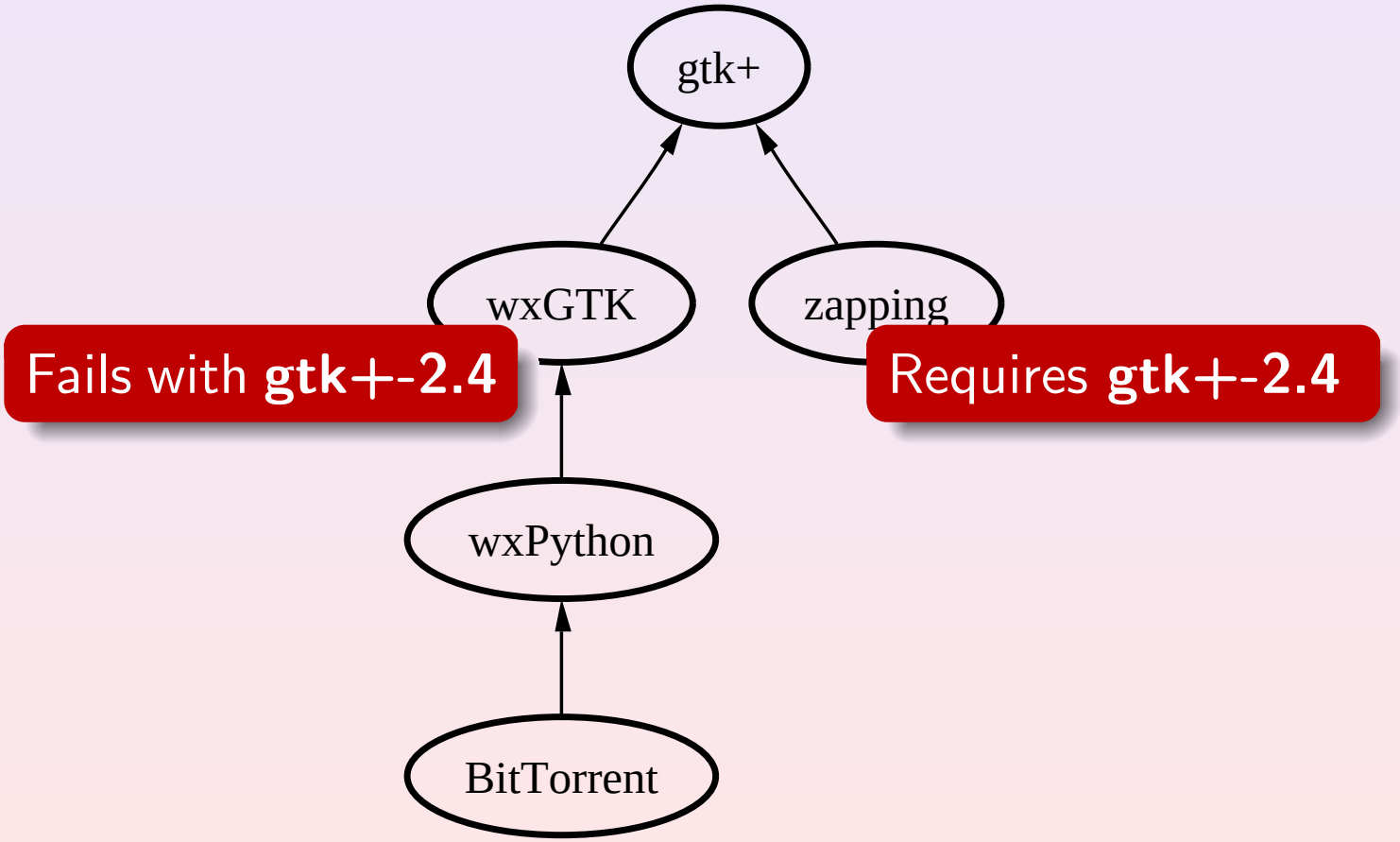
# So why is this hard?

- Difficult to have multiple versions; but we want this to
  - Test upgrades
  - Deal with conflicting dependencies
  - Support different user / service requirements



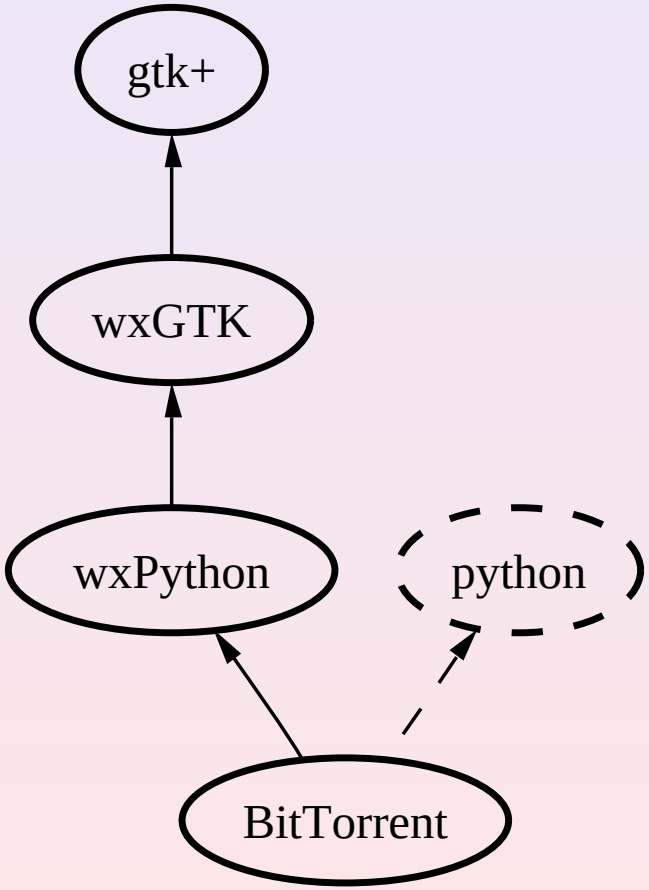
# So why is this hard?

- Difficult to have multiple versions; but we want this to
  - Test upgrades
  - Deal with conflicting dependencies
  - Support different user / service requirements



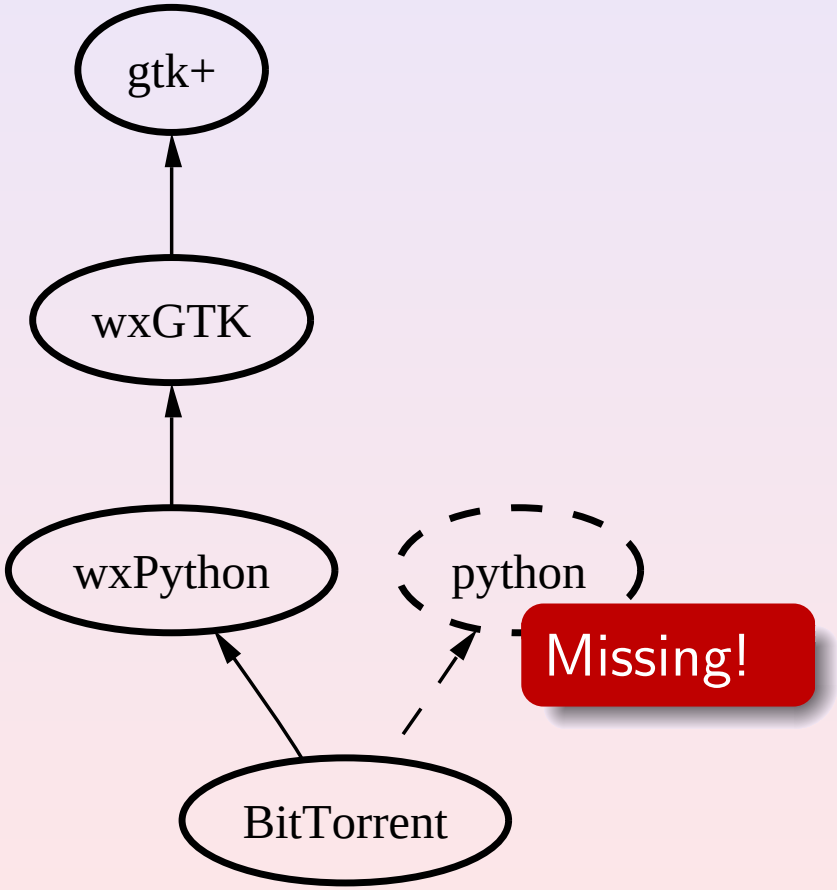
# So why is this hard?

- Unreliable dependency information
  - What packages are needed?
  - What versions?

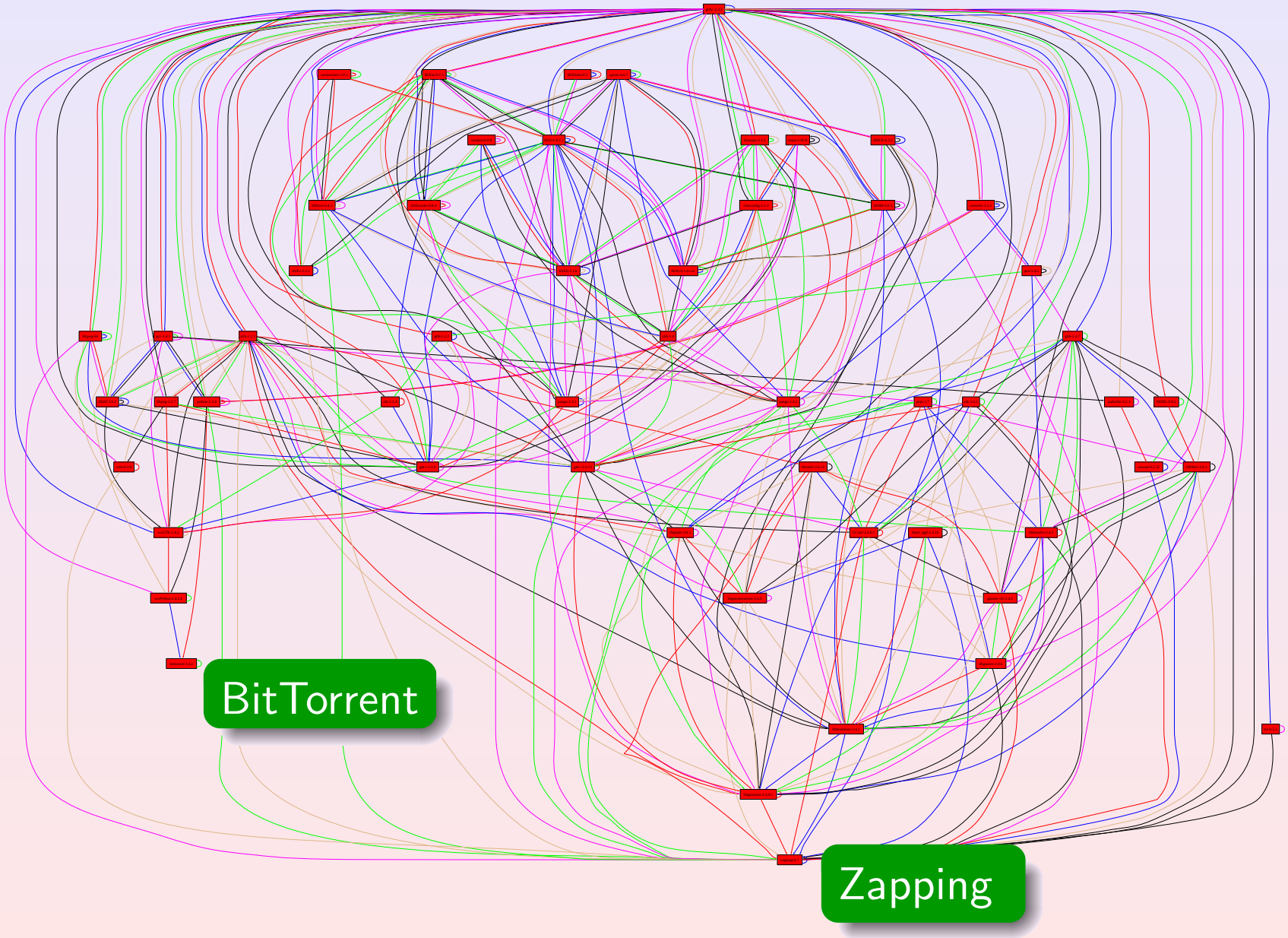


# So why is this hard?

- Unreliable dependency information
  - What packages are needed?
  - What versions?



# So why is this hard?



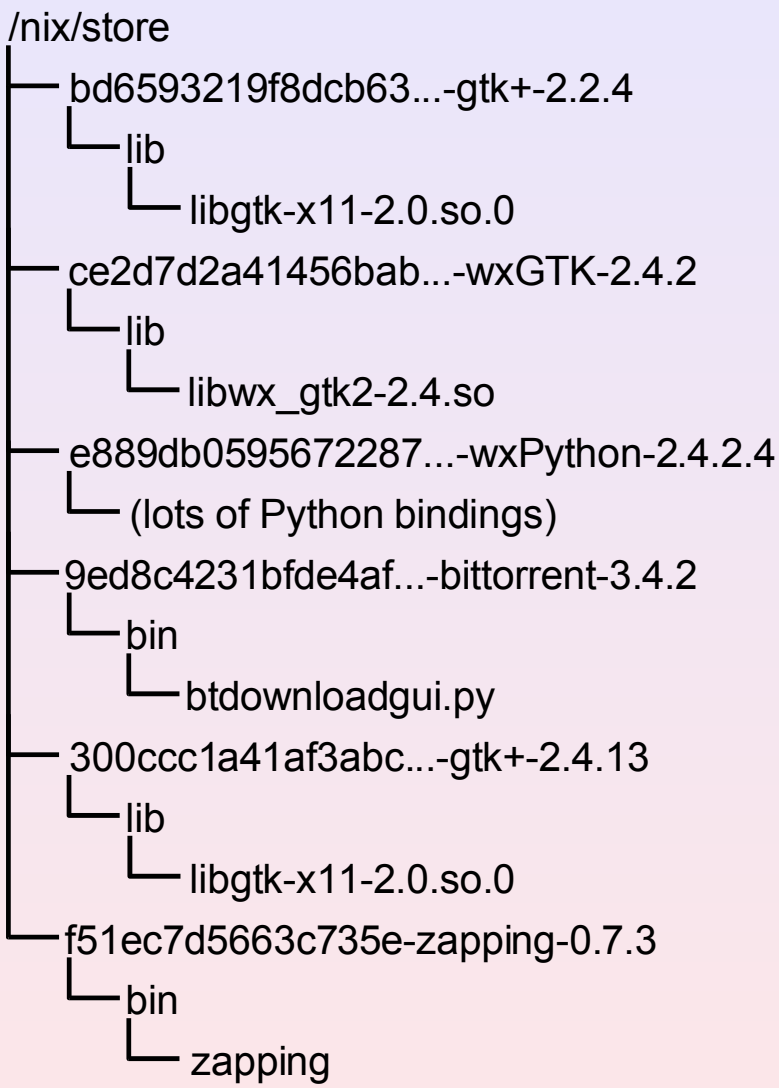
# The Nix Deployment System

- Central idea: store all packages in isolation.
- Unique paths:

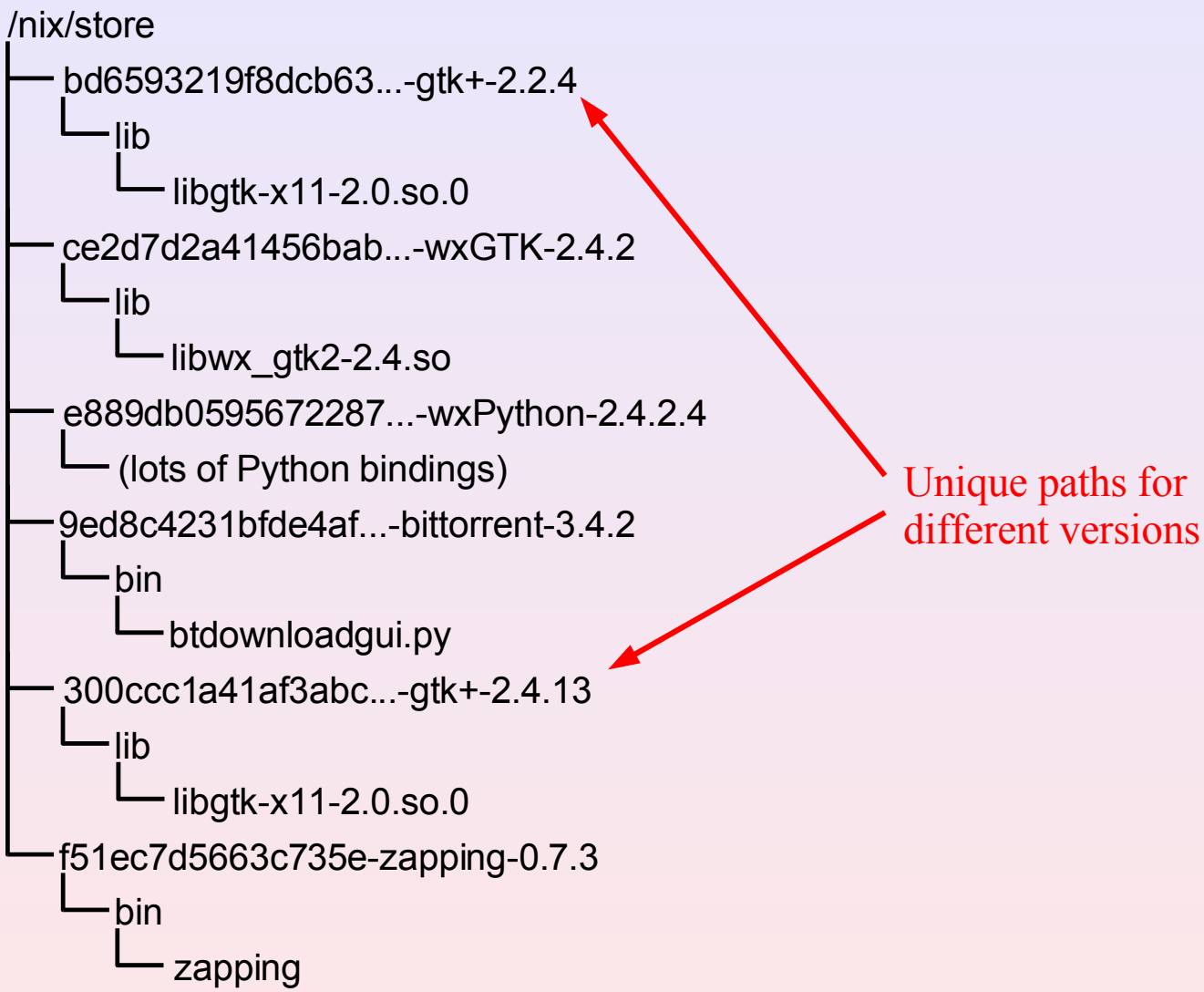
```
/nix/store/605332199533e73b...-gtk+-2.2.4
```

  which is an MD5 hash of **all** inputs used to build the package:
  - Libraries
  - Compilers
  - Build scripts
  - Build parameters
  - System type
  - ...
- **Prevent** undeclared **build time** dependencies.
- **Scan** for **runtime** dependencies.
- Deploy only **closures** under the **depends-on** relation.

# Nix store


/nix/store
bd6593219f8dcb63...-gtk+-2.2.4
lib
libgtk-x11-2.0.so.0
ce2d7d2a41456bab...-wxGTK-2.4.2
lib
libwx_gtk2-2.4.so
e889db0595672287...-wxPython-2.4.2.4
(lots of Python bindings)
9ed8c4231bfde4af...-bittorrent-3.4.2
bin
btdownloadgui.py
300ccc1a41af3abc...-gtk+-2.4.13
lib
libgtk-x11-2.0.so.0
f51ec7d5663c735e-zapping-0.7.3
bin
zapping

# Nix store


/nix/store
bd6593219f8dcb63...-gtk+-2.2.4
lib
libgtk-x11-2.0.so.0
ce2d7d2a41456bab...-wxGTK-2.4.2
lib
libwx_gtk2-2.4.so
e889db0595672287...-wxPython-2.4.2.4
(lots of Python bindings)
9ed8c4231bfde4af...-bittorrent-3.4.2
bin
btdownloadgui.py
300ccc1a41af3abc...-gtk+-2.4.13
lib
libgtk-x11-2.0.so.0
f51ec7d5663c735e-zapping-0.7.3
bin
zapping
Unique paths for
different versions

# Nix expressions

## hello/default.nix

```
{stdenv, fetchurl, perl}:

stdenv.mkDerivation {
  name = "hello-2.1.1";
  builder = ./builder.sh;
  src = fetchurl {
    url =
      ftp://ftp.gnu.org/pub/gnu/hello/hello-2.1.1.tar.gz;
    md5 = "70c9ccf9fac07f762c24f2df2290784d";
  };
  inherit perl;
}
```

# Nix expressions

## hello/default.nix

```
{stdenv, fetchurl, perl}:

stdenv.mkDerivation {
  name = "hello-2.1.1";
  builder = ./builder.sh;
  src = fetchurl {
    url =
      ftp://ftp.gnu.org/pub/gnu/hello/hello-2.1.1.tar.gz;
    md5 = "70c9ccf9fac07f762c24f2df2290784d";
  };
  inherit perl;
}
```

Function arguments

# Nix expressions

## hello/default.nix

```
{stdenv, fetchurl, perl}:

stdenv.mkDerivation {
  name = "hello-2.1.1";
  builder = ./builder.sh;
  src = fetchurl {
    url =
      ftp://ftp.gnu.org/pub/gnu/hello/hello-2.1.1.tar.gz;
    md5 = "70c9ccf9fac07f762c24f2df2290784d";
  };
  inherit perl;
}
```

Function arguments

Build attributes

# Nix expressions

## hello/builder.sh

```
. $stdenv/setup

PATH=$perl/bin:$PATH

tar xvfz $src
cd hello-*
./configure --prefix=$out
make
make install
```

# Nix expressions

## hello/builder.sh

```
. $stdenv/setup

PATH=$perl/bin:$PATH

tar xvfz $src
cd hello-*
./configure --prefix=$out
make
make install
```

Environment initially empty; prevents undeclared dependencies

# Nix expressions

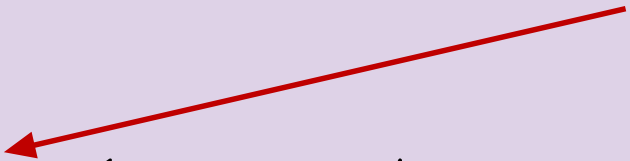
## system/all-packages-generic.nix

```
hello = (import ../applications/misc/hello/ex-1 {
  inherit fetchurl stdenv perl;
};

perl = (import ../development/interpreters/perl) {
  inherit fetchurl stdenv;
};

fetchurl = (import ../build-support/fetchurl) {
  inherit stdenv; ...
};

stdenv = ...;
```

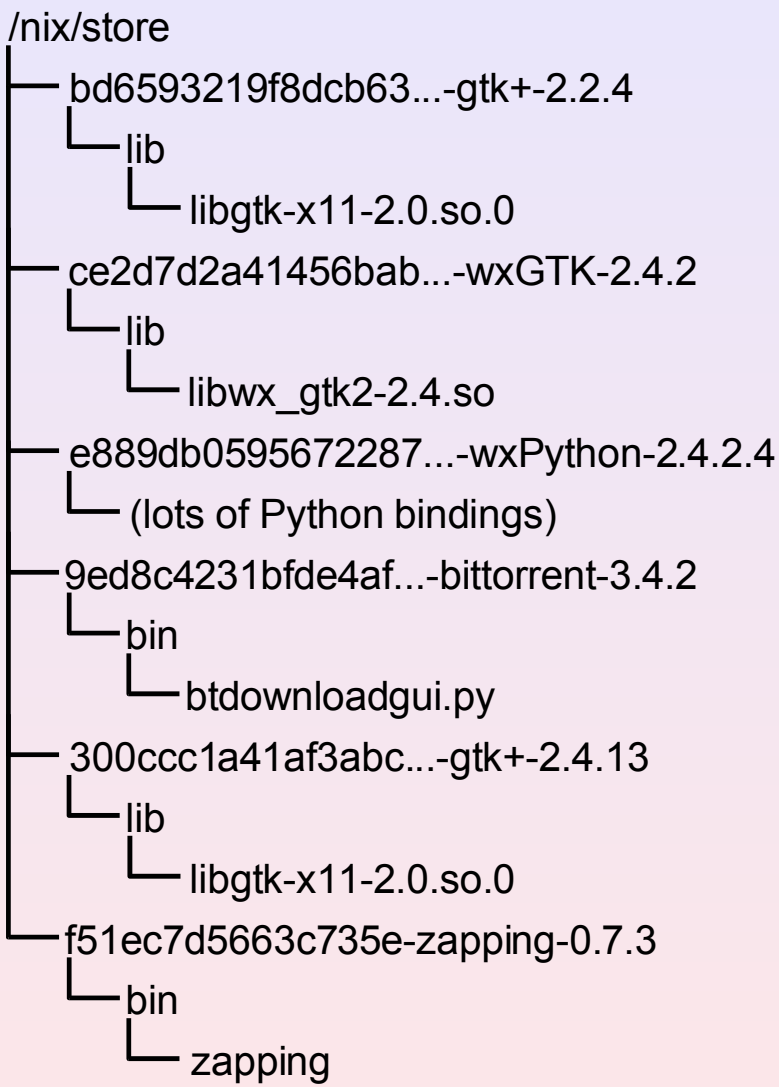
# Nix expressions

## system/all-packages-generic.nix

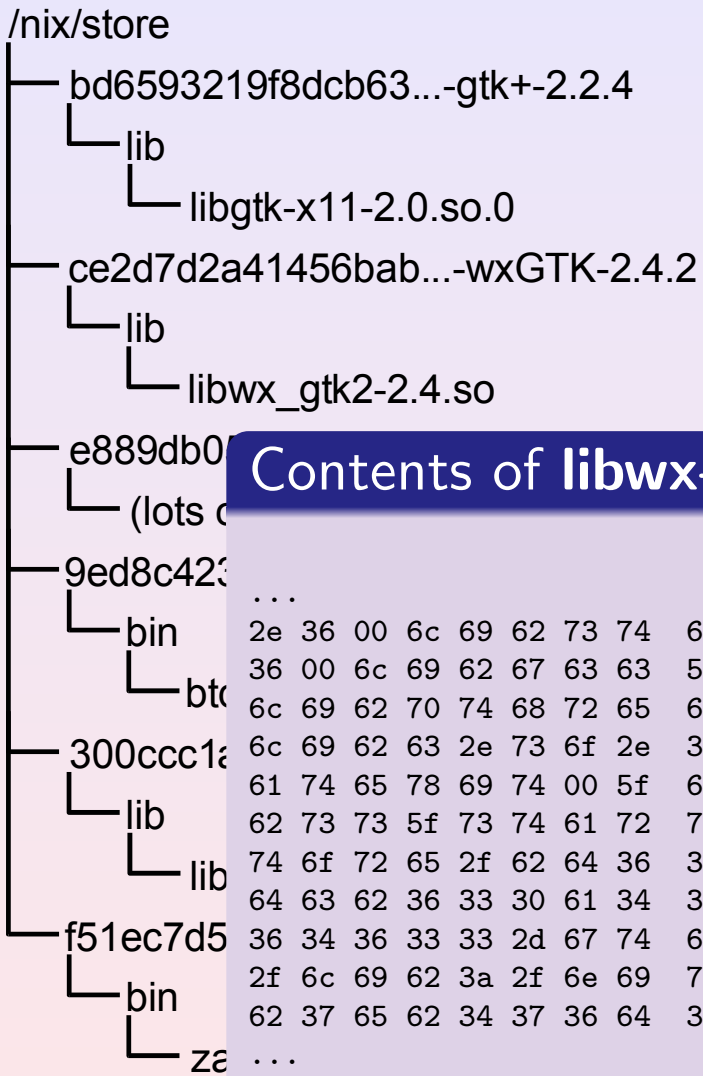
```
hello = (import ../applications/misc/hello/ex-1 {
  inherit fetchurl stdenv perl;
};

perl = (import ../development/interpreters/perl) {
  inherit fetchurl stdenv;
};

fetchurl = (import ../build-support/fetchurl) {
  inherit stdenv; ...
};

stdenv = ...;
```



# Finding runtime dependencies



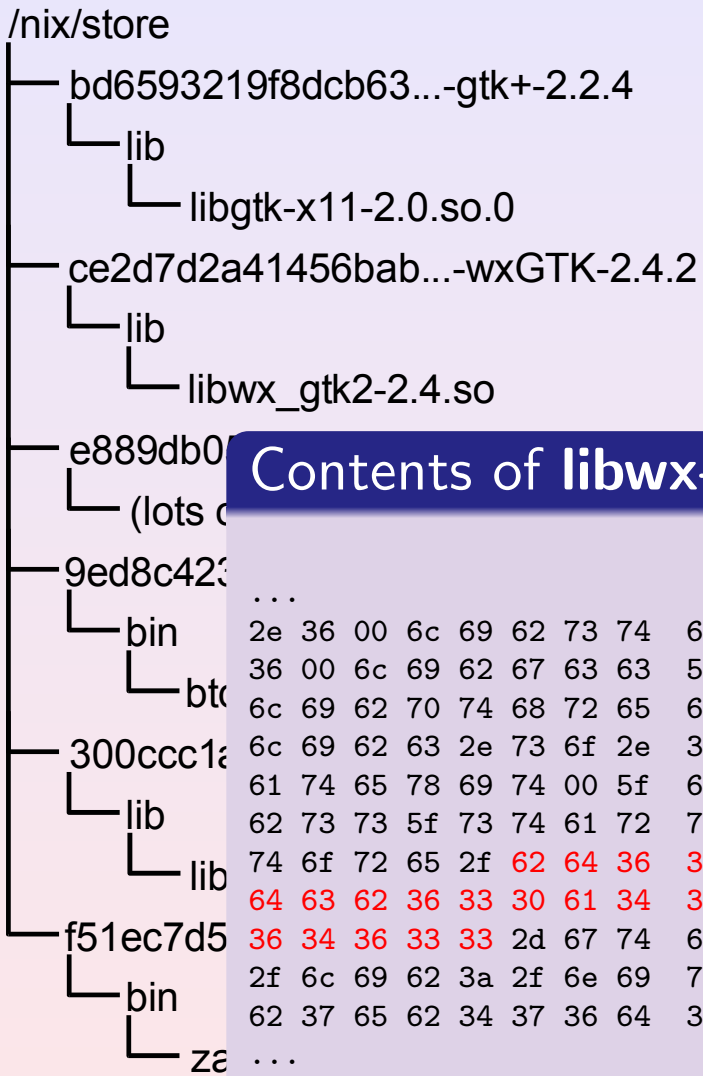
# Finding runtime dependencies




## Contents of **libwx-gtk2-2.4.so**

```
...
2e 36 00 6c 69 62 73 74  64 63 2b 2b 2e 73 6f 2e  |.6.libstdc++.so.|
36 00 6c 69 62 67 63 63  5f 73 2e 73 6f 2e 31 00  |6.libgcc_s.so.1.|
6c 69 62 70 74 68 72 65  61 64 2e 73 6f 2e 30 00  |libpthread.so.0.|
6c 69 62 63 2e 73 6f 2e  36 00 5f 5f 63 78 61 5f  |libc.so.6.__cxa_|
61 74 65 78 69 74 00 5f  65 64 61 74 61 00 5f 5f  |atexit._edata.__|
62 73 73 5f 73 74 61 72  74 00 2f 6e 69 78 2f 73  |bss_start./nix/s|
74 6f 72 65 2f 62 64 36  35 39 33 32 31 39 66 38  |tore/bd6593219f8|
64 63 62 36 33 30 61 34  35 35 62 31 61 35 37 66  |dcb630a455b1a57f|
36 34 36 33 33 2d 67 74  6b 2b 2d 32 2e 32 2e 34  |64633-gtk+-2.2.4|
2f 6c 69 62 3a 2f 6e 69  78 2f 73 74 6f 72 65 2f  |/lib:/nix/store/|
62 37 65 62 34 37 36 64  36 32 62 61 65 38 62 63  |b7eb476d62bae8bc|
...
```

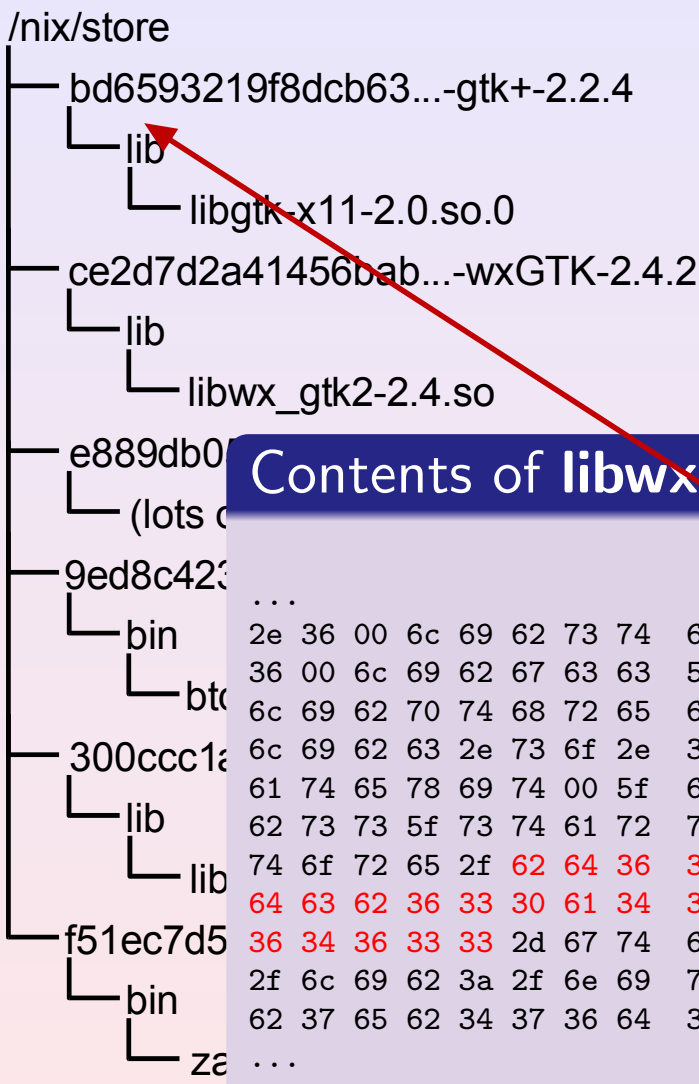
# Finding runtime dependencies




## Contents of **libwx-gtk2-2.4.so**

```
...
2e 36 00 6c 69 62 73 74  64 63 2b 2b 2e 73 6f 2e  |.6.libstdc++.so.|
36 00 6c 69 62 67 63 63  5f 73 2e 73 6f 2e 31 00  |6.libgcc_s.so.1.|
6c 69 62 70 74 68 72 65  61 64 2e 73 6f 2e 30 00  |libpthread.so.0.|
6c 69 62 63 2e 73 6f 2e  36 00 5f 5f 63 78 61 5f  |libc.so.6.__cxa_|
61 74 65 78 69 74 00 5f  65 64 61 74 61 00 5f 5f  |atexit._edata.__|
62 73 73 5f 73 74 61 72  74 00 2f 6e 69 78 2f 73  |bss_start./nix/s|
74 6f 72 65 2f 62 64 36  35 39 33 32 31 39 66 38  |tore/bd6593219f8|
64 63 62 36 33 30 61 34  35 35 62 31 61 35 37 66  |dcb630a455b1a57f|
36 34 36 33 33 2d 67 74  6b 2b 2d 32 2e 32 2e 34  |64633-gtk+-2.2.4|
2f 6c 69 62 3a 2f 6e 69  78 2f 73 74 6f 72 65 2f  |/lib:/nix/store/|
62 37 65 62 34 37 36 64  36 32 62 61 65 38 62 63  |b7eb476d62bae8bc|
...
```

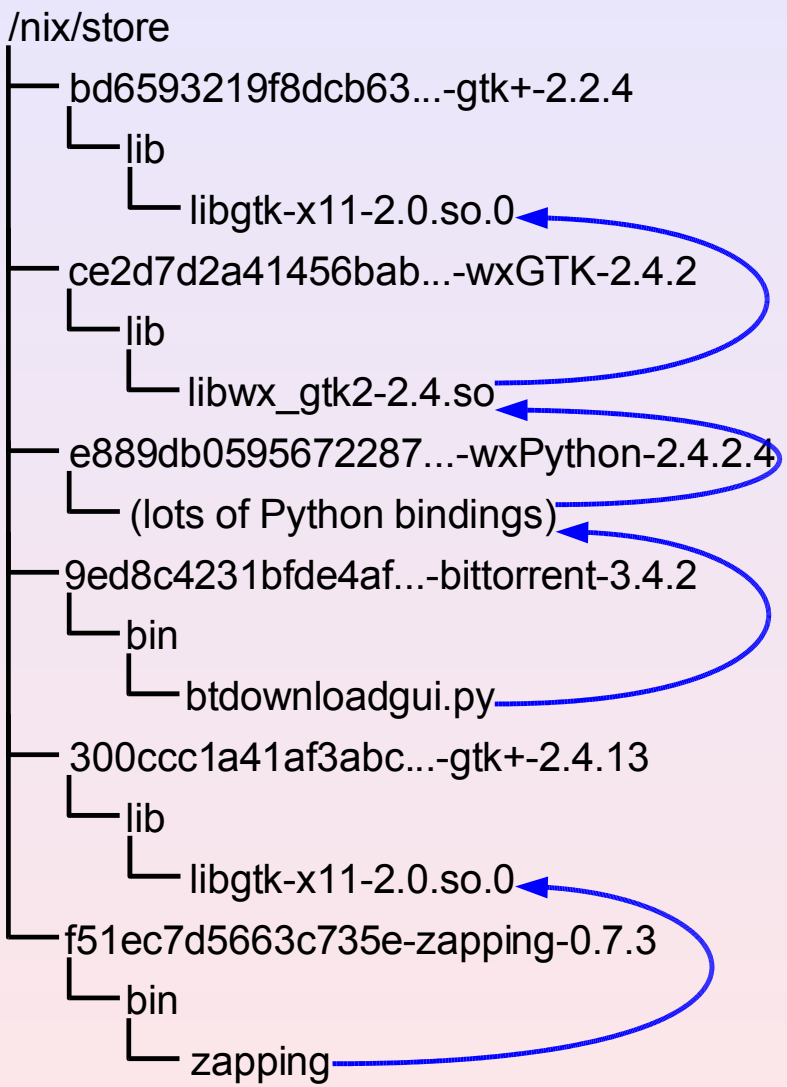
# Finding runtime dependencies



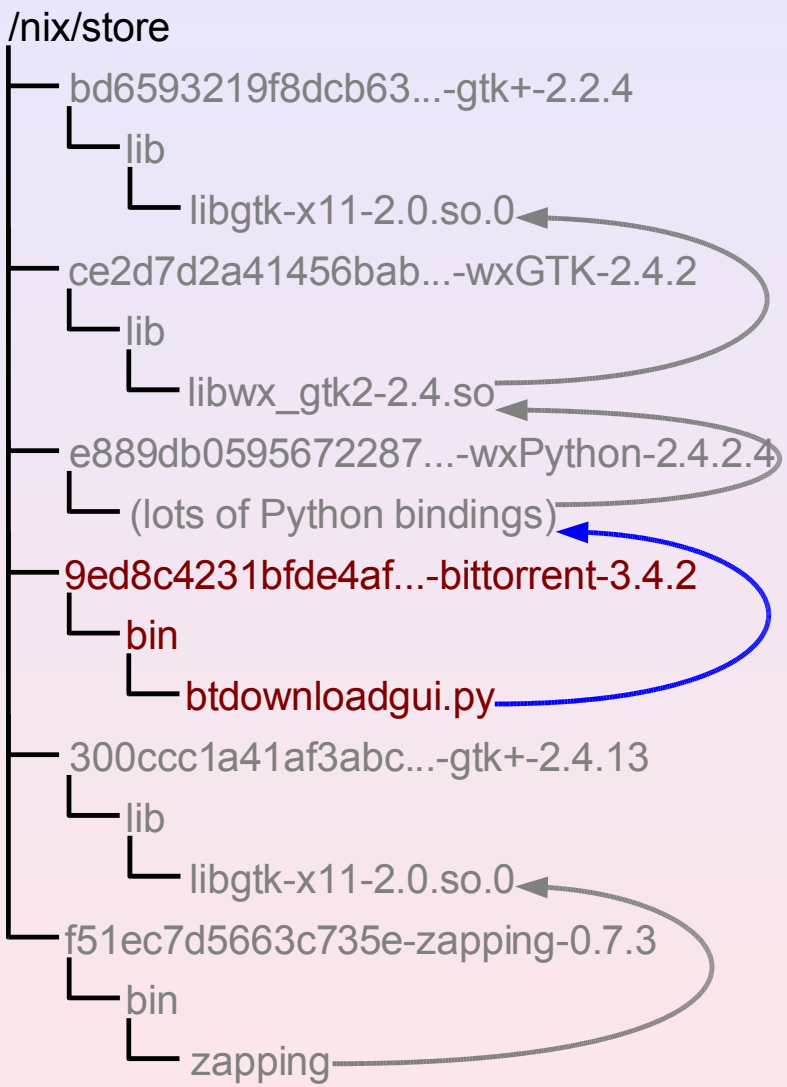

## Contents of **libwx-gtk2-2.4.so**

```
...
2e 36 00 6c 69 62 73 74  64 63 2b 2b 2e 73 6f 2e  |.6.libstdc++.so.|
36 00 6c 69 62 67 63 63  5f 73 2e 73 6f 2e 31 00  |6.libgcc_s.so.1.|
6c 69 62 70 74 68 72 65  61 64 2e 73 6f 2e 30 00  |libpthread.so.0.|
6c 69 62 63 2e 73 6f 2e  36 00 5f 5f 63 78 61 5f  |libc.so.6.__cxa_|
61 74 65 78 69 74 00 5f  65 64 61 74 61 00 5f 5f  |atexit._edata.__|
62 73 73 5f 73 74 61 72  74 00 2f 6e 69 78 2f 73  |bss_start./nix/s|
74 6f 72 65 2f 62 64 36  35 39 33 32 31 39 66 38  |tore/bd6593219f8|
64 63 62 36 33 30 61 34  35 35 62 31 61 35 37 66  |dcb630a455b1a57f|
36 34 36 33 33 2d 67 74  6b 2b 2d 32 2e 32 2e 34  |64633-gtk+-2.2.4|
2f 6c 69 62 3a 2f 6e 69  78 2f 73 74 6f 72 65 2f  |/lib:/nix/store/|
62 37 65 62 34 37 36 64  36 32 62 61 65 38 62 63  |b7eb476d62bae8bc|
...
```

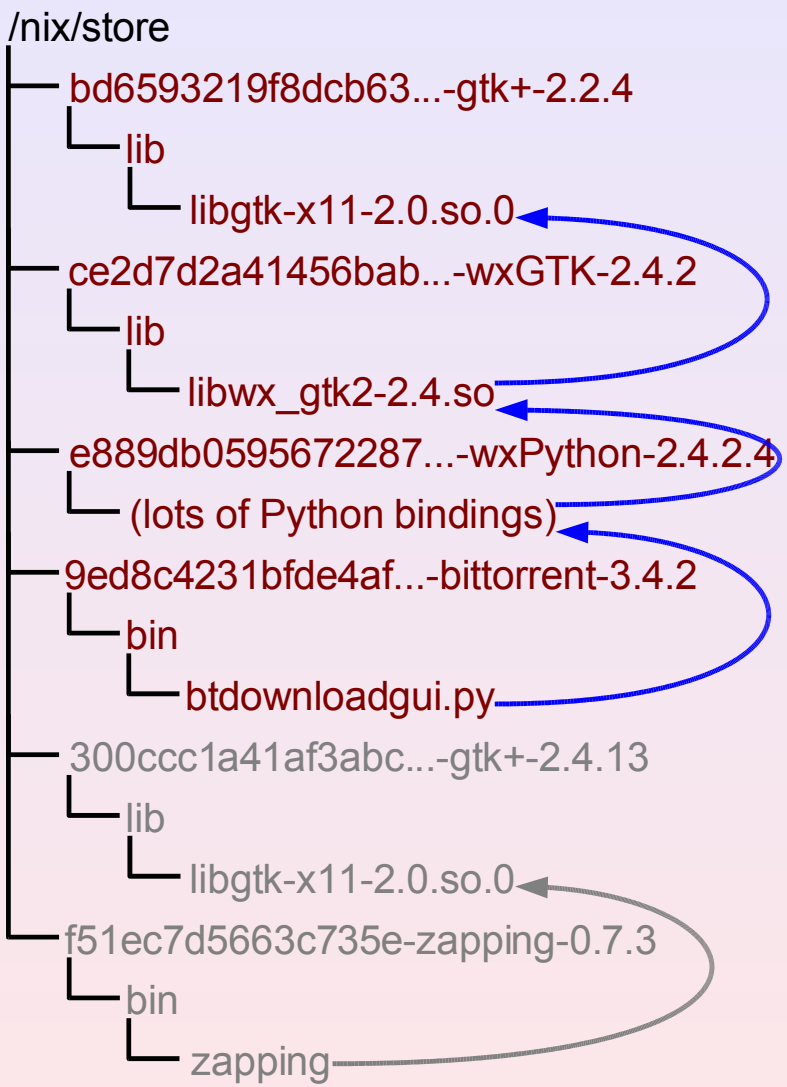
# Finding runtime dependencies



# Finding runtime dependencies



# Finding runtime dependencies



# User operations

- To build and install Hello:

```
$ nix-env -if .../all-packages.nix hello
```

- When a new version comes along:

```
$ nix-env -uf .../all-packages.nix hello
```

- If it doesn't work:

```
$ nix-env --rollback
```

- Delete unused packages:

```
$ nix-collect-garbage
```

# User operations

- To build and install Hello:

```
$ nix-env -if .../all-packages.nix hello
```

- When a new version comes along:

```
$ nix-env -uf .../all-packages.nix hello
```

- If it doesn't work:

```
$ nix-env --rollback
```

- Delete unused packages:

```
$ nix-collect-garbage
```

# User operations

- To build and install Hello:

```
$ nix-env -if .../all-packages.nix hello
```

- When a new version comes along:

```
$ nix-env -uf .../all-packages.nix hello
```

- If it doesn't work:

```
$ nix-env --rollback
```

- Delete unused packages:

```
$ nix-collect-garbage
```

# User operations

- To build and install Hello:

```
$ nix-env -if .../all-packages.nix hello
```

- When a new version comes along:

```
$ nix-env -uf .../all-packages.nix hello
```

- If it doesn't work:

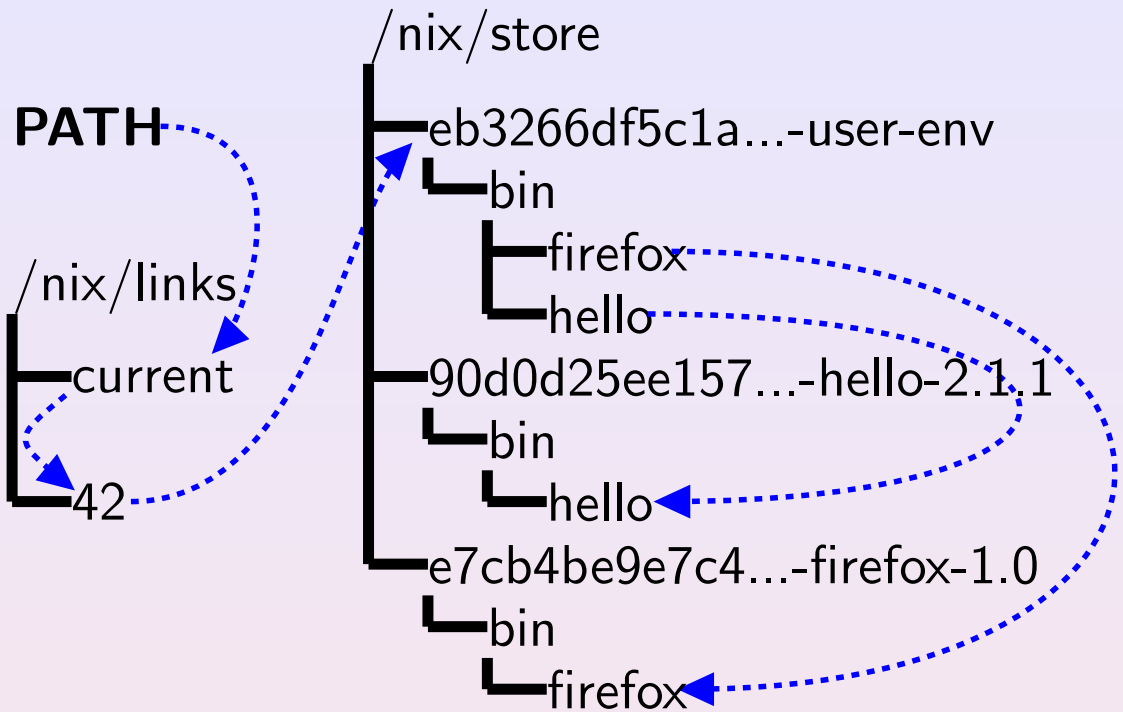
```
$ nix-env --rollback
```

- Delete unused packages:

```
$ nix-collect-garbage
```

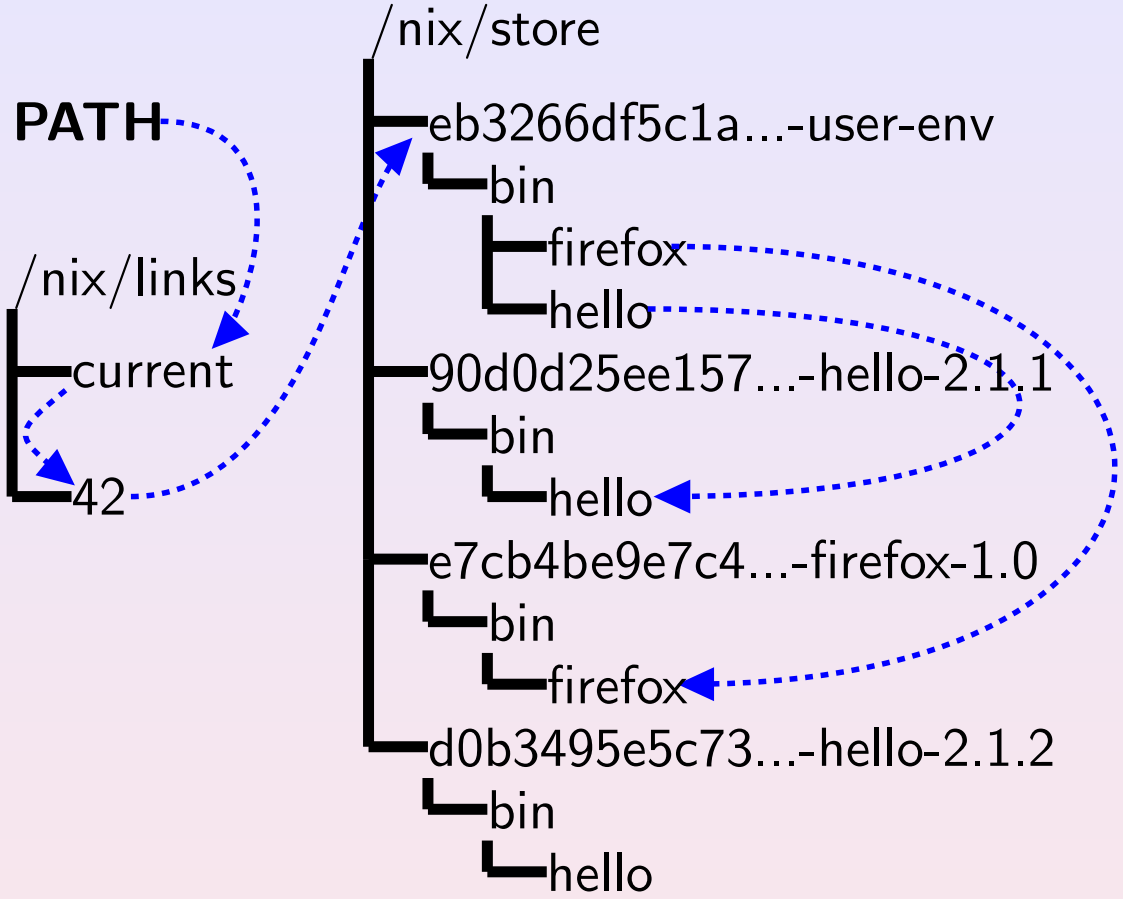
# User environments

- Users can have different sets of installed applications.
- **nix-env** operations create new **user environments** in the store.
- We can atomically switch between them.
- These are roots of the garbage collector.



# User environments

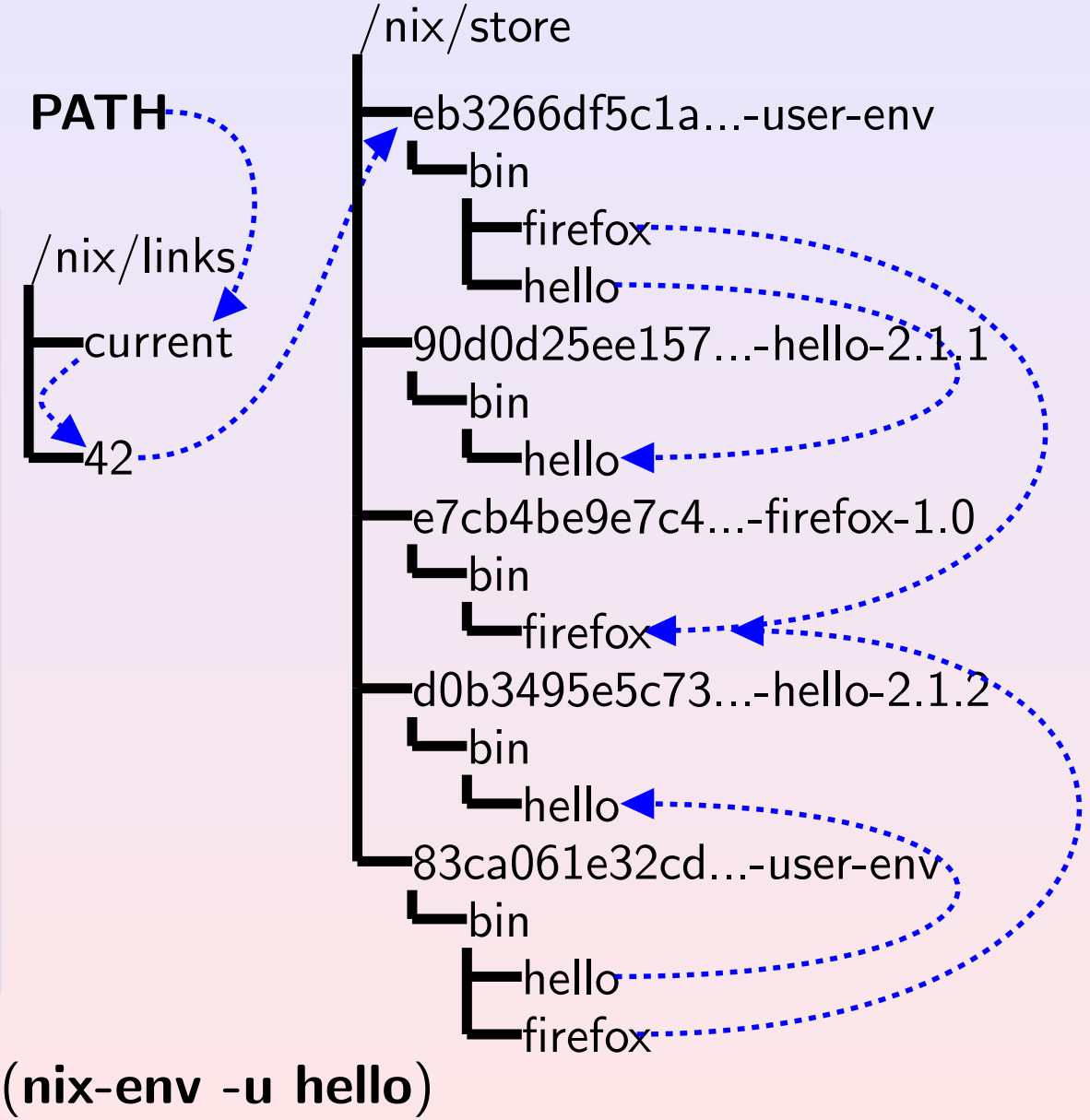
- Users can have different sets of installed applications.
- **nix-env** operations create new **user environments** in the store.
- We can atomically switch between them.
- These are roots of the garbage collector.




**(nix-env -u hello)**

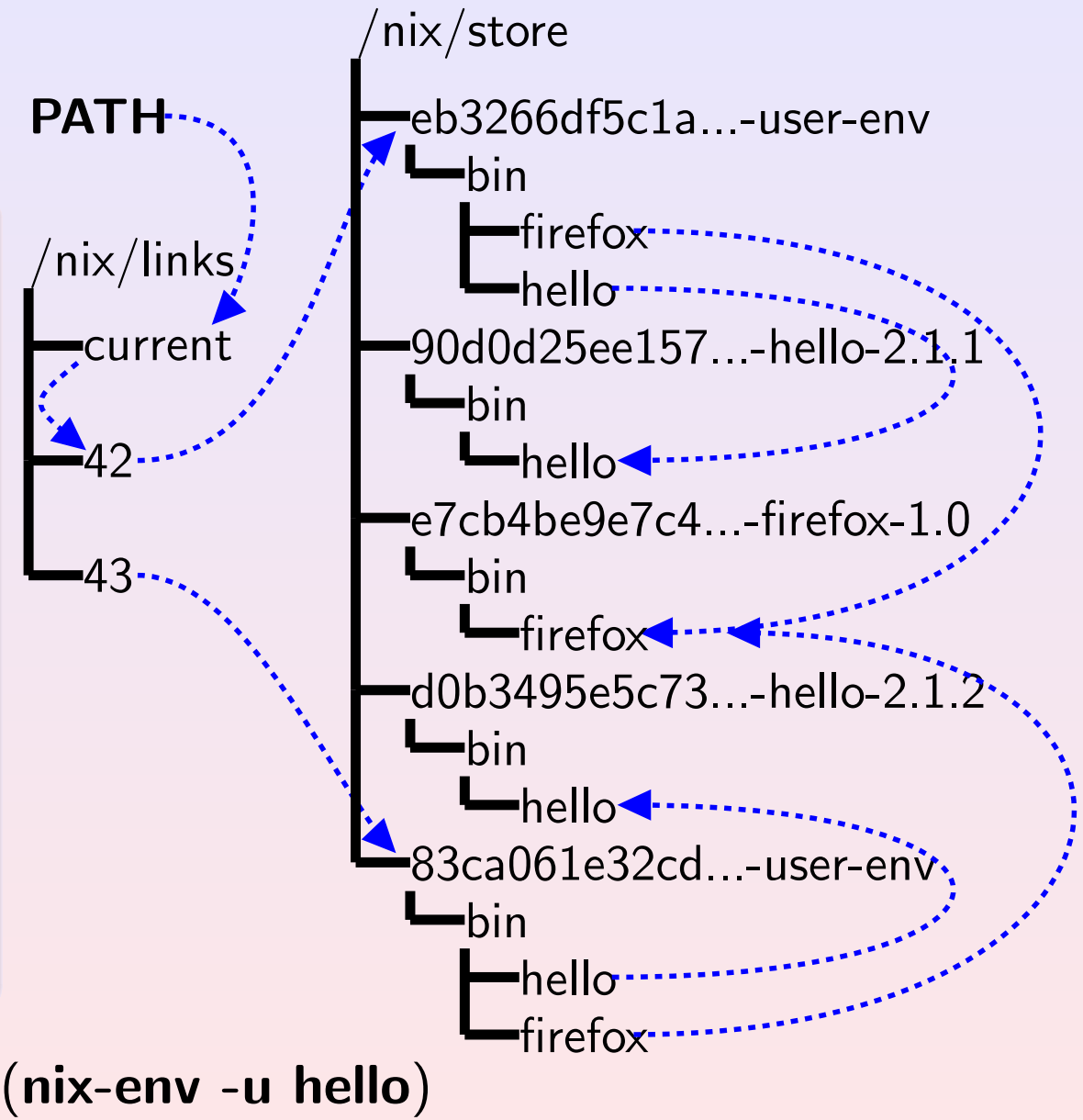
# User environments

- Users can have different sets of installed applications.
- **nix-env** operations create new **user environments** in the store.
- We can atomically switch between them.
- These are roots of the garbage collector.



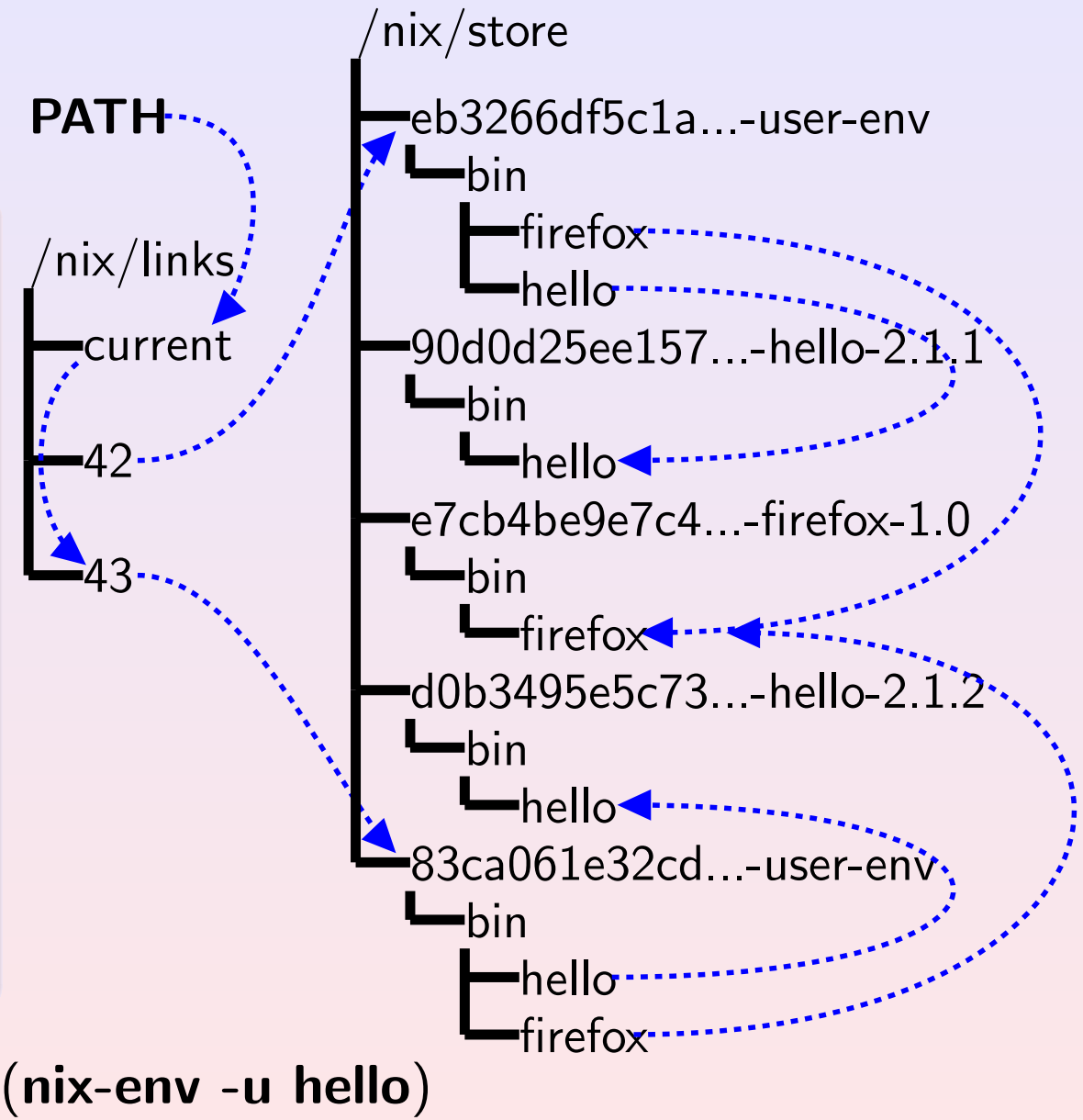
# User environments

- Users can have different sets of installed applications.
- **nix-env** operations create new **user environments** in the store.
- We can atomically switch between them.
- These are roots of the garbage collector.



# User environments

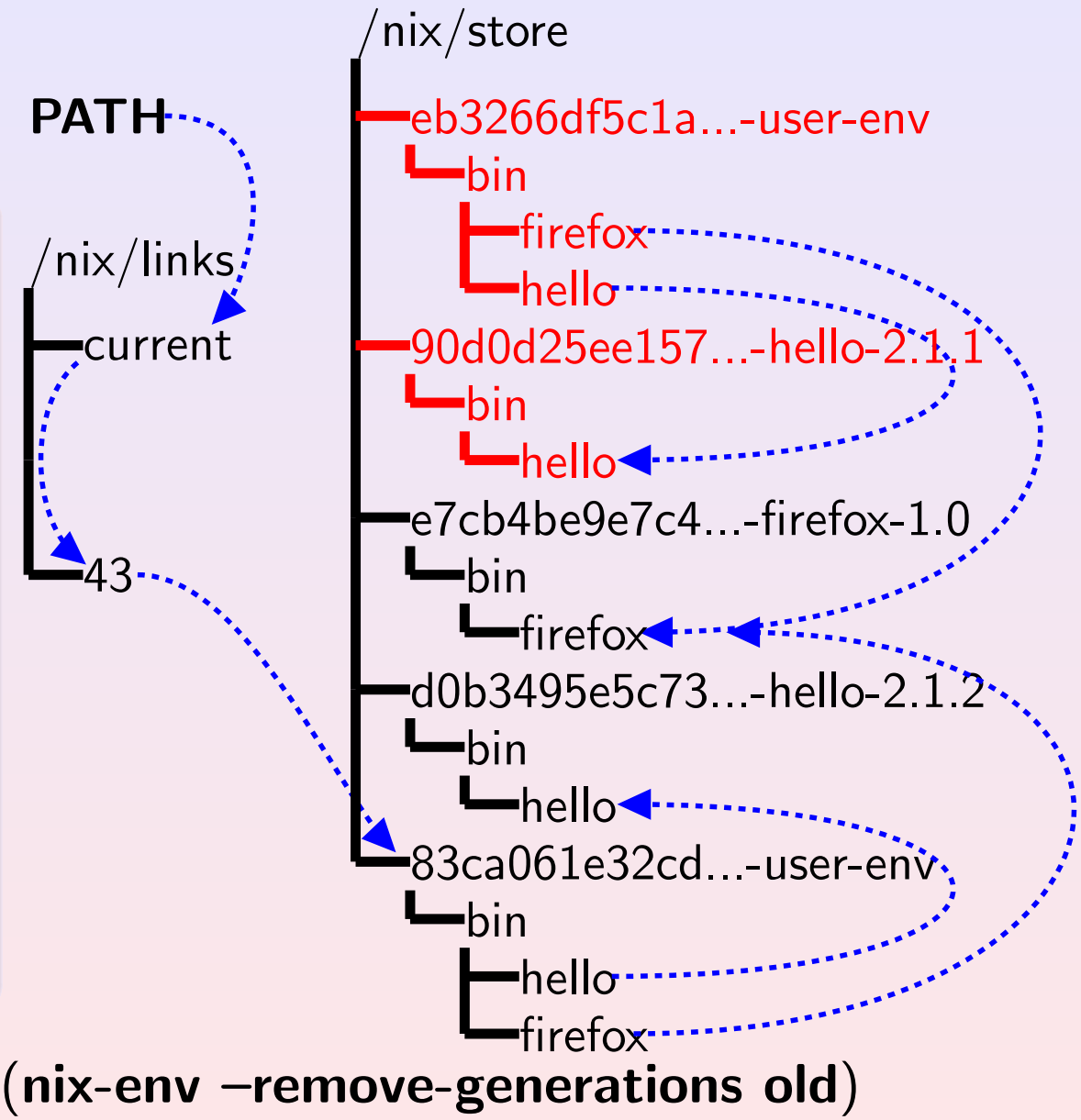
- Users can have different sets of installed applications.
- **nix-env** operations create new **user environments** in the store.
- We can atomically switch between them.
- These are roots of the garbage collector.




**(nix-env -u hello)**

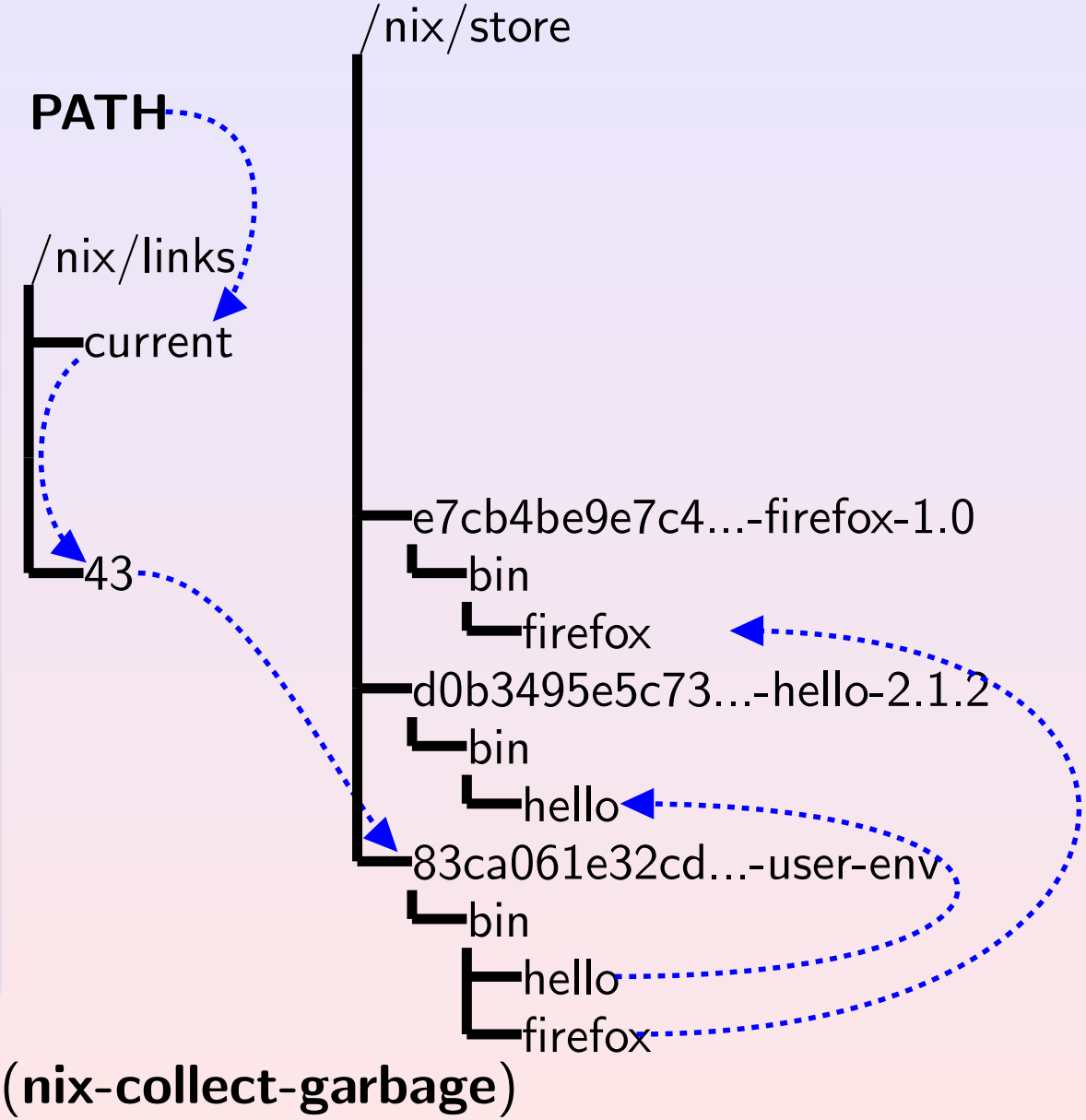
# User environments

- Users can have different sets of installed applications.
- **nix-env** operations create new **user environments** in the store.
- We can atomically switch between them.
- These are roots of the **garbage collector**.



# User environments

- Users can have different sets of installed applications.
- **nix-env** operations create new **user environments** in the store.
- We can atomically switch between them.
- These are roots of the **garbage collector**.



# Deployment using Nix

- This is conceptually a **source deployment model**.
- We get **binary deployment** by sharing pre-built packages.
- On the producer side:

```
$ nix-push $(nix-instantiate .../all-packages.nix) \
    http://server/cache
```

- On the client side:

```
$ nix-pull http://server/cache
```

- Installation will now reuse pre-built packages, **iff** they are exactly the same.

# Deployment using Nix

- This is conceptually a **source deployment model**.
- We get **binary deployment** by sharing pre-built packages.
- On the producer side:

```
$ nix-push $(nix-instantiate .../all-packages.nix) \
   http://server/cache
```

- On the client side:

```
$ nix-pull http://server/cache
```

- Installation will now reuse pre-built packages, **iff** they are exactly the same.

# Deployment using Nix

- This is conceptually a **source deployment model**.
- We get **binary deployment** by sharing pre-built packages.
- On the producer side:

```
$ nix-push $(nix-instantiate .../all-packages.nix) \
   http://server/cache
```

- On the client side:

```
$ nix-pull http://server/cache
```

- Installation will now reuse pre-built packages, **iff** they are exactly the same.

# An example deployment policy: channels

- Channels allow Nix expressions to be updated automatically.
- Subscribe to a channel:

```
$ nix-channel --add http://.../channels/nixpkgs-unstable
```

- Fetch latest channel instance:

```
$ nix-channel --update
```

- Update all installed packages:

```
$ nix-env -u '*'
```

# An example deployment policy: channels

- Channels allow Nix expressions to be updated automatically.
- Subscribe to a channel:

```
$ nix-channel --add http://.../channels/nixpkgs-unstable
```

- Fetch latest channel instance:

```
$ nix-channel --update
```

- Update all installed packages:

```
$ nix-env -u '*'
```

# An example deployment policy: channels

- Channels allow Nix expressions to be updated automatically.
- Subscribe to a channel:

```
$ nix-channel --add http://.../channels/nixpkgs-unstable
```

- Fetch latest channel instance:

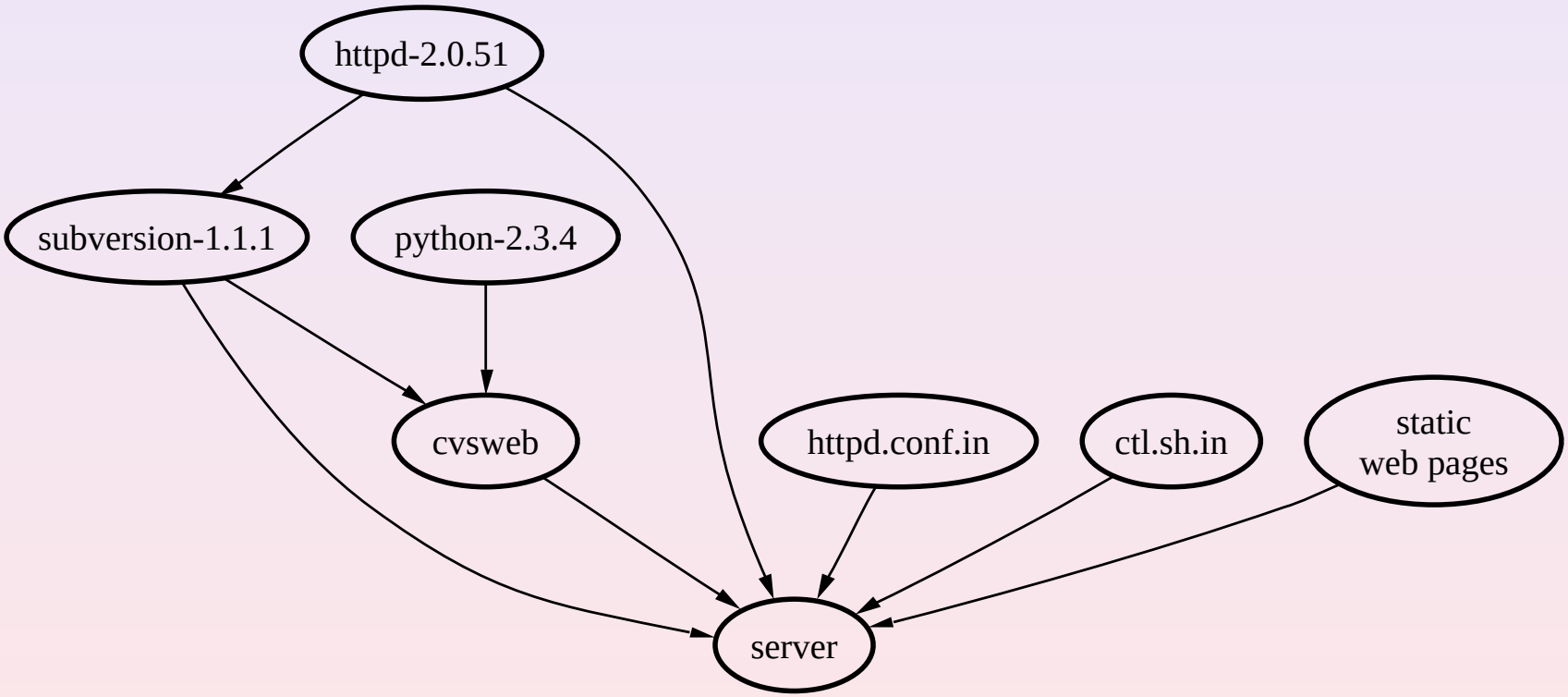
```
$ nix-channel --update
```

- Update all installed packages:

```
$ nix-env -u '*'
```

# Service deployment

- Deploying a service is (almost) the same as deploying software.
- Example: Subversion server at **svn.cs.uu.nl**.



# Conclusions

- Contributions:
  - Safe, automatic coexistance of versions/variants.
  - Reliable dependencies.
  - Multiple concurrent configurations.
  - Atomic upgrades/rollbacks.
  - Safe garbage collection.
  - Binary deployment is automatic.
  - Can accomodate many deployment policies.
  - Useful for service deployment.
- Available at `http://www.cs.uu.nl/groups/ST/Trace/Nix`.

# FAQ

"How to handle security patches (e.g., in the C library)? There you *do* want destructive updates."

- No you don't. How to roll-back if the patch breaks things?
- Just deploy the new components; to the extent that there is sharing with old ones, no rebuilds / redownloads are necessary.
- In the case of dynamic libraries, wrapper packages can be used to prevent a mass rebuild.