Building a
Proof Assistant

Favonia

Assistants based on dependent type theory

Coq, Agda, Lean, ...

Like a compiler, but...

Interactivity is prime focus

Code generation: less so

Bottleneck: type checking

RedPRL Team

Carlo Angiuli

Evan Cavallo

Favonia

Hazel Levine

Matthew McQuaid

Reed Mullanix

Jon Sterling

RedPRL   redtt   cooltt   algaett

Buld Yet⁴ Another Proof Assistant

NbE* —— check whether two terms are equal
*Normalization by Evaluation

Refiner —— check whether a term is well-typed

Kernel —— the "trusted" part

Elaborator — surface syntax to core syntax

Driver —— imports, definitions, etc.

Parser —— strings to surface syntax

NbE*
Refiner

Kernel
Elaborator
Driver
Parser

Yuujinchou: namespaces

Bantorra: library management

Asai: compiler diagnostics

base/utility

algaeff: algebraic effects

bwd: backward lists

type theory

mugen: universe levels

kado: cofibrations in Cartesian cubical type theory

Dream

Prototype good proof assistants for new type theories

Yuujinchou

namespaces and name modifiers

Expressiveness: all common features

Explicit sequencing: unambiguous modifiers

Implicit namespaces: definition injection

Detecting typos

Small kernel

Algebraic effects

```
open M
  using (a)
  renaming (a to b)
  hiding (b)
```

Agda code: what would happen?

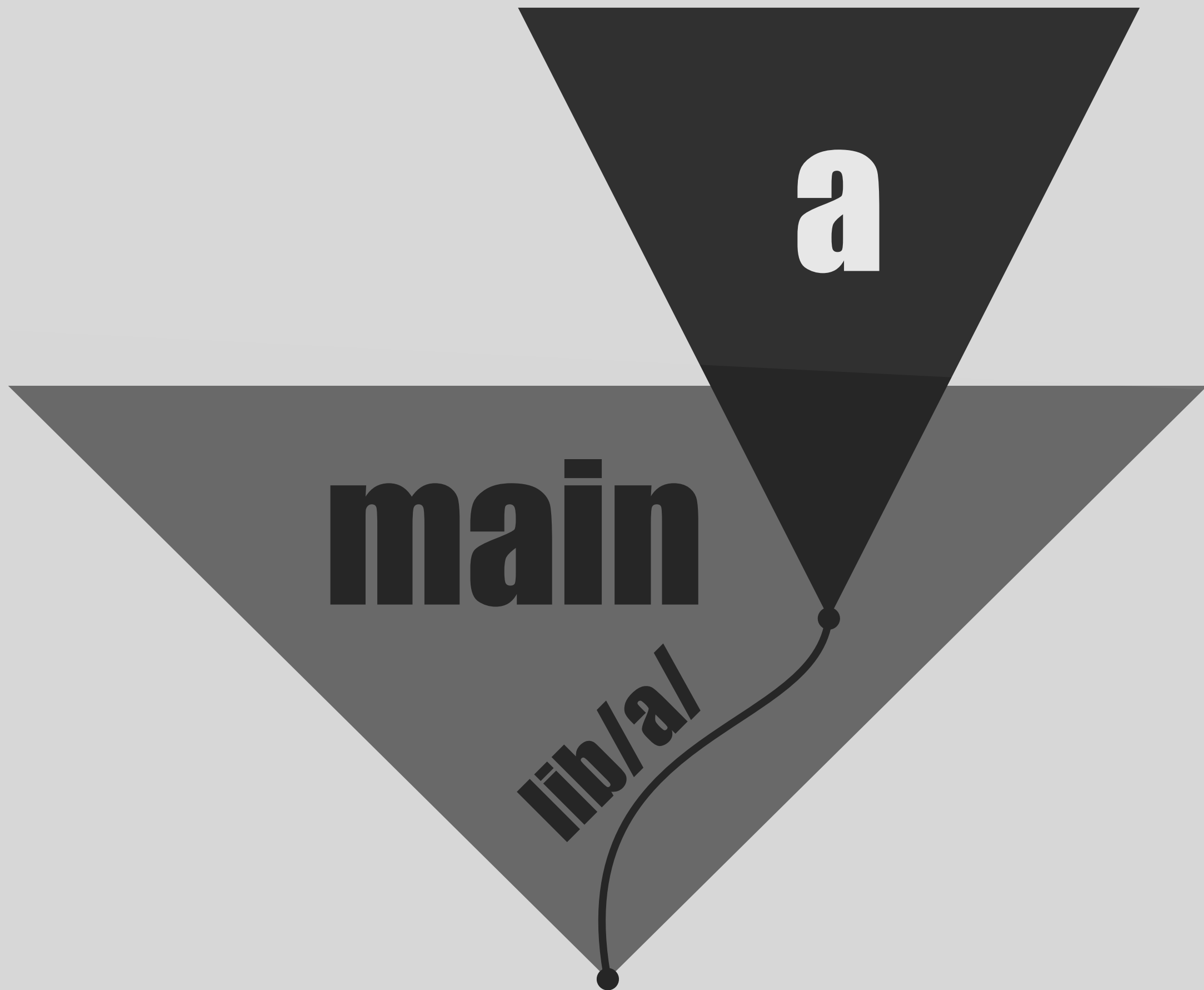# Bantorra

library management

Recursive POSIX-style mounting
Flexible library resultion
Built-in routers: local dir, git, index, ...
Built-in combinators: dispatch, rewrite, ...
Thread safety
Algebraic effects

Asai
compiler diagnostics

Great Unicode support: no column numbers

Multiple backends: LSP*, Terminal, ...

*currently broken

Backtraces

Multi-span highlighting

Algebraic effects

Asai API Design

Terminating now? emit v.s. fatal

Classification for formatting (to end users)

Short, Google-able code

Detailed messages and backtraces

All above, while being uncluttered

Mugen
universe levels

McBride's "Crude but Effective Stratification"

We generalized natural numbers to "displacement algebras"

Conditionally accepted by POPL 2023 on its theory

[me, Carlo Angiuli & Reed Mullanix]

Mugen

Negative levels: each universe contains a smaller one

Rational levels: always a level between any two levels

Fractal levels: embedding itself between any two levels

Kado

cofibrations

Heavily optimized; used in cooltt

Natural numbers replaced by "displacement algebras"

Used to implement unfolding control

More to Come

Pretty Printing
Records
Meta/Staged Programming
Controlled Unfolding
...