# Pinvis

Brian Pittman - CPE631 - 4/23/12

# The Problem

- Analysis of binary executables is difficult
- Existing tools focus on debugging or performance tuning
- Source code is not always available

# Enter Pinvis

Pinvis is not a debugger. Pinvis is not a performance analysis tool.

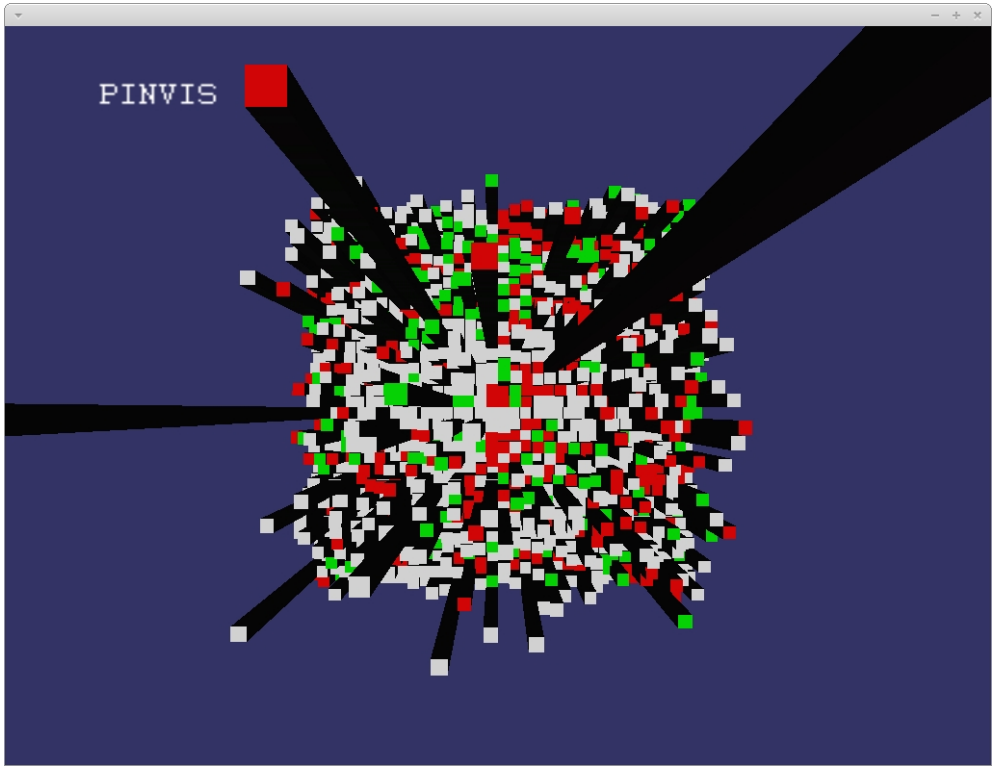
Pinvis is an attempt to visualize all relevant aspects of a binary executable file, with a focus on providing an intuitive description of what is happening at the lowest levels.

# Pinvis Structure

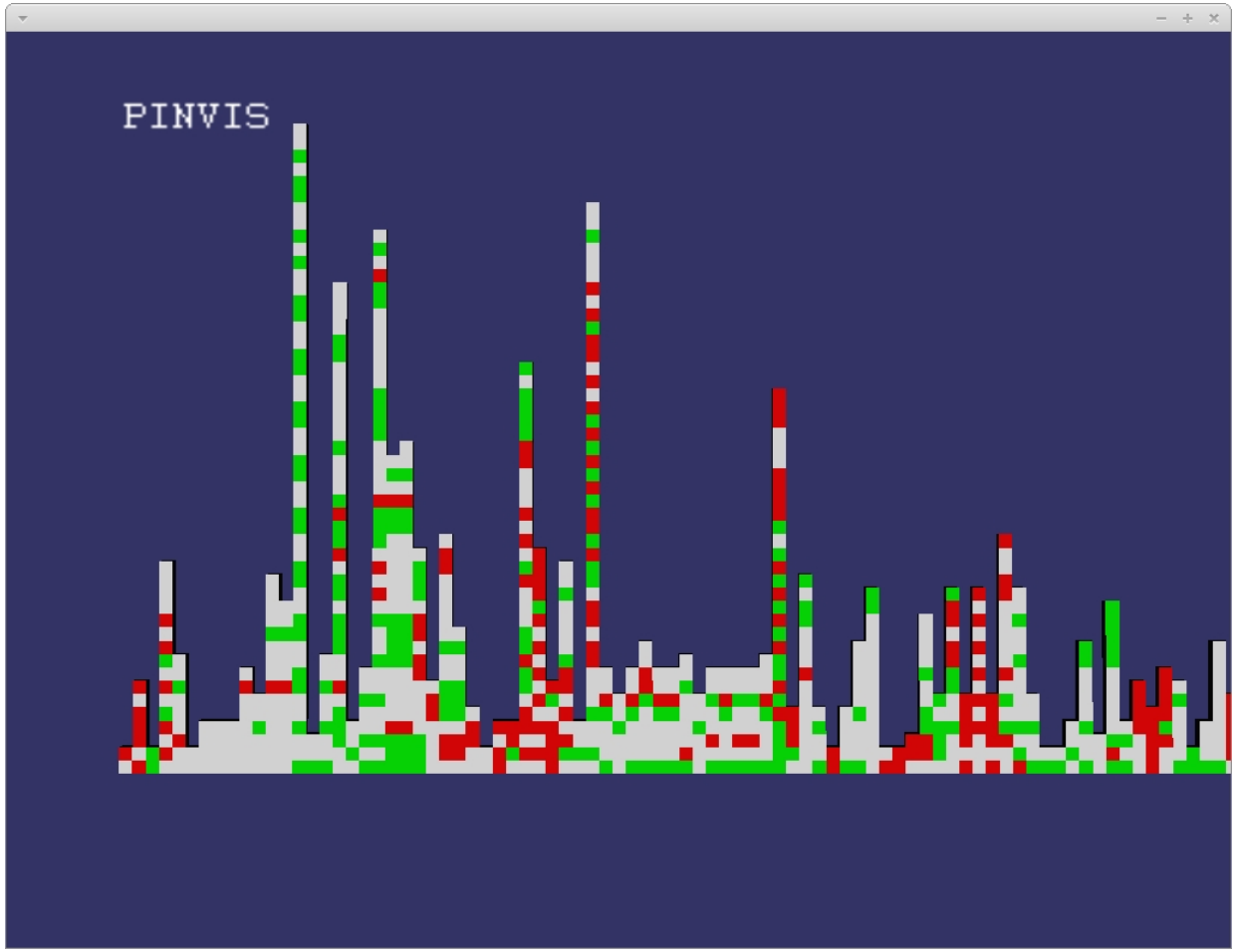
- Pintool writes a file containing:
  - dynamic streams
  - memory read/writes
  - image/function names
  - timeline of stream execution
- Visualization program: reads pintool output
  - 3D rendering using OpenSceneGraph library
  - Organize streams in grids or rows
  - Step through timeline of execution
  - Filter streams on the fly
  - Color streams

# Features: Grid layout

- Each column is 1 dynamic stream
- Each cube is 1 instruction in the stream

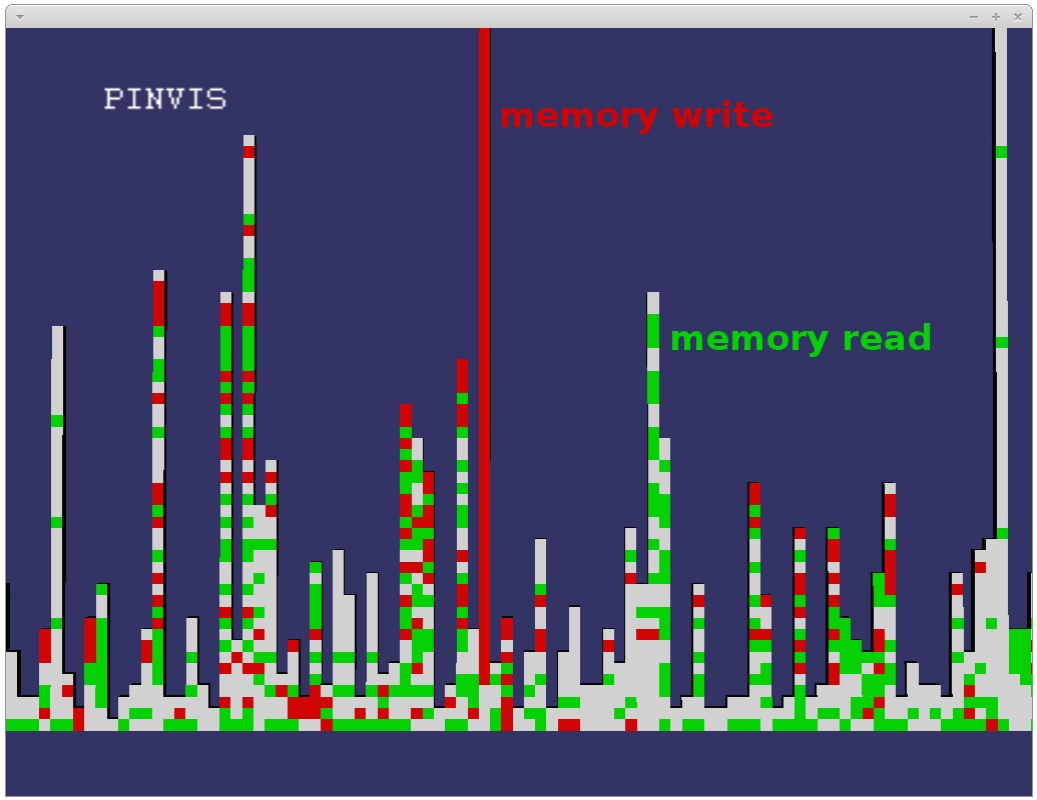


# Features: Row layout



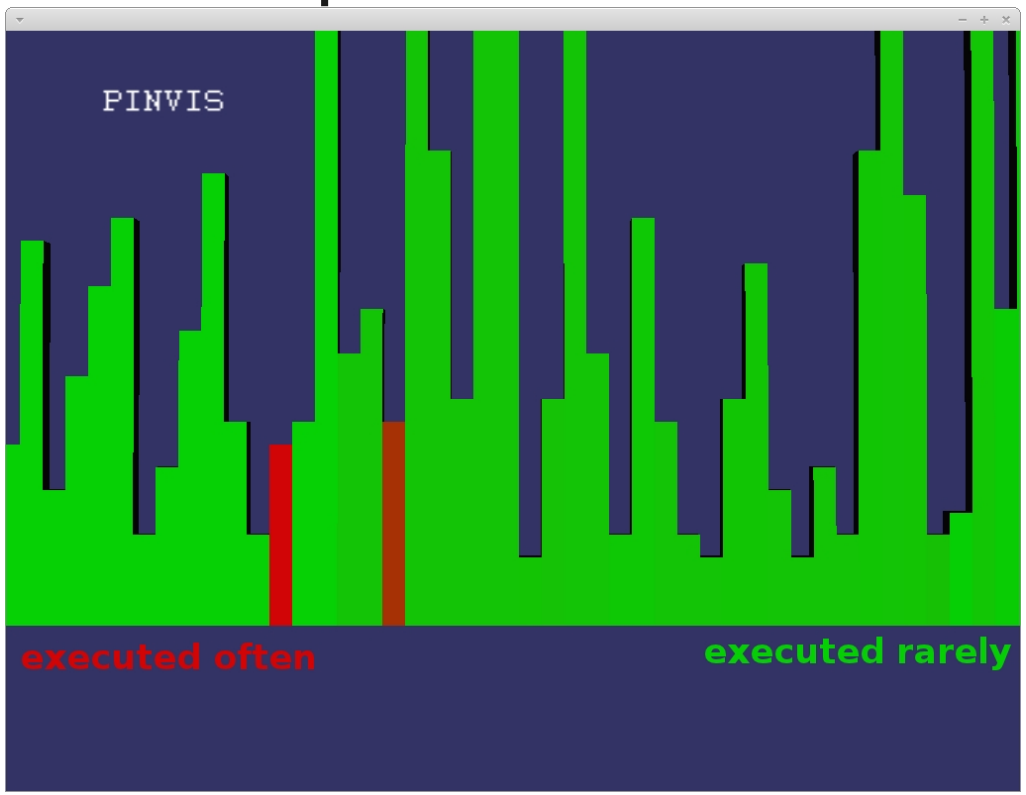
# Features: Color by memory access

- Green = read
- Red = write



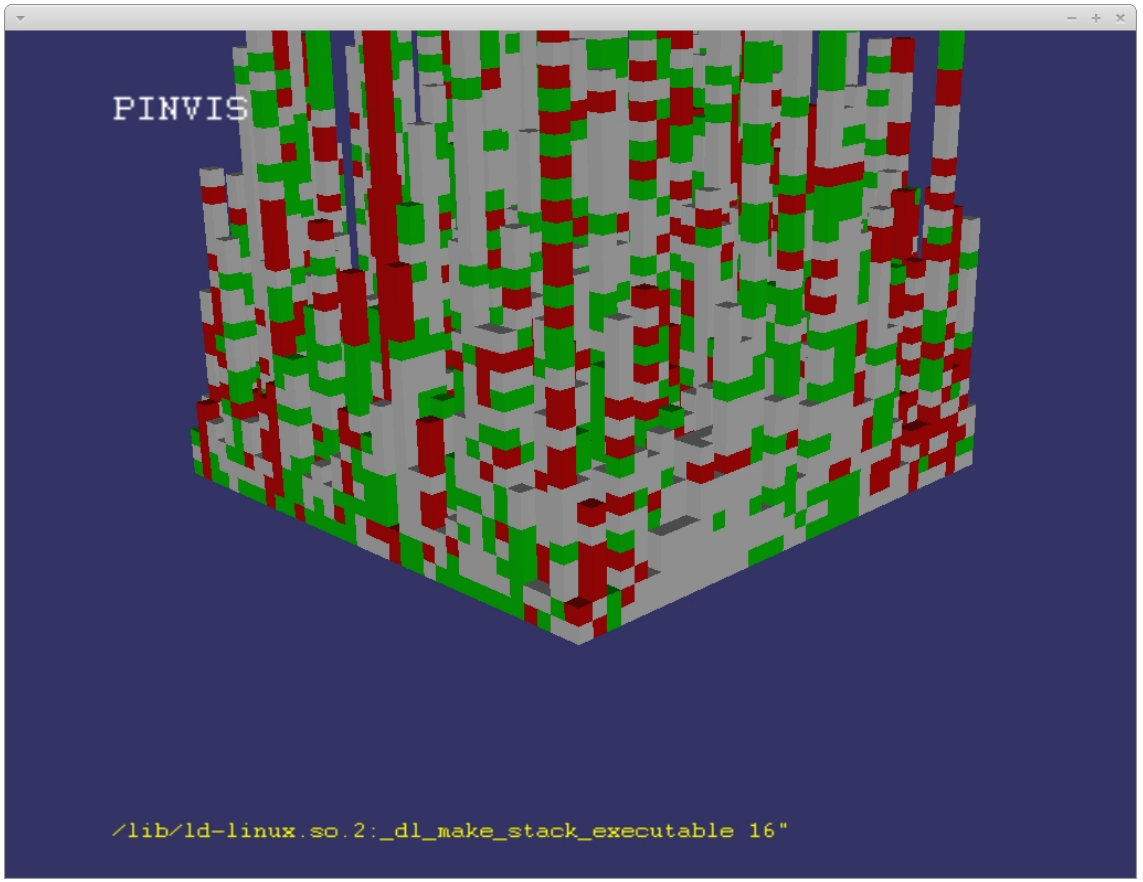
# Features: Color by execution freq

- Green = least frequent
- Red = most frequent



# Features: Image/Function names

- Click a stream to show its image/function name

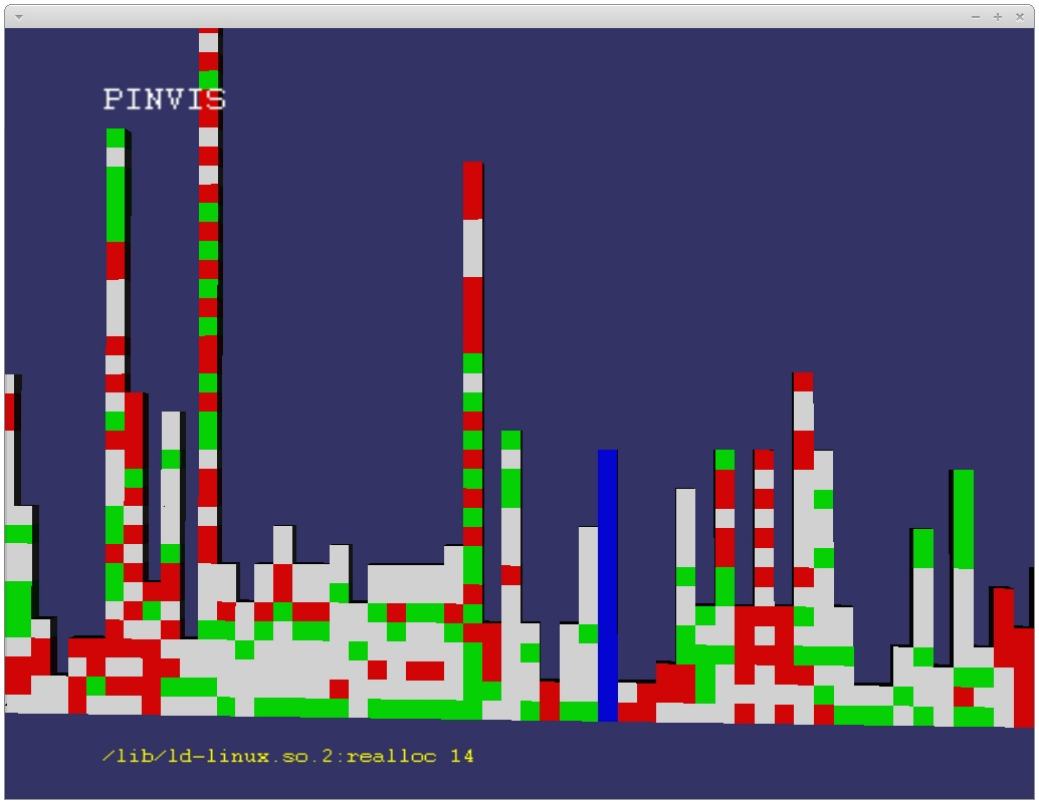


# Features: Filtering

- Click a stream and press 'h' to hide all streams in that image (or 'u' to hide all others)

# Features: Timeline

- Press 'n' to highlight the next stream in program execution order



# Demo video

http://www.youtube.com/watch?v=d8NPgr5jvN4

# Future Work/TODO

- Filter on pintool side
- UI improvements
- Memory heat map
- Visualize "next" streams
- Direct connection between pintool and visualization program for "realtime" visualization