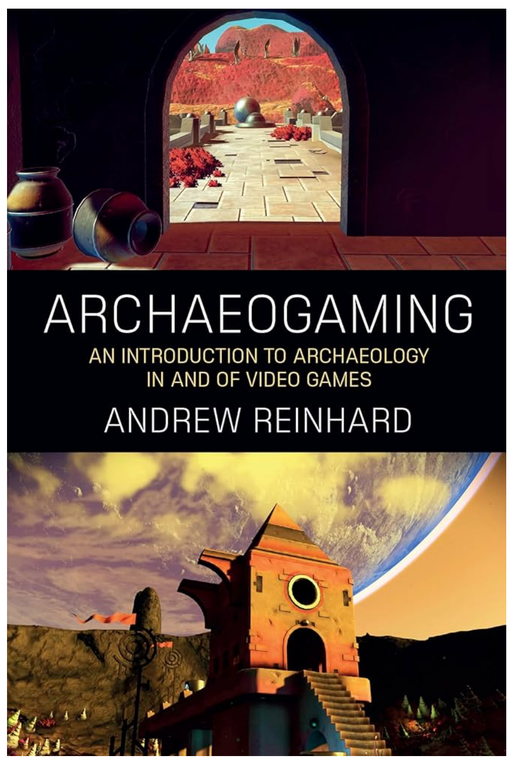
Reverse-Engineering Video Games at Scale

Aly Cerruti

Why Do We Care?

- 2023 report from Video Game History Foundation: "**87%** of classic video games released in the United States are critically endangered"
- This gives us a technical basis for performing archaeology on video games
- "Archaeogaming [includes reverse engineering] games to understand underlying code and structures and the materials that house them."



Traces

- Traces avoid major downsides of traditional analysis
  - Static analysis: execution patterns, external events
  - Dynamic analysis: requires a running instance
- Traces can be "replayed" infinite times

A Lava Trace

```
...
R 00cdfe5a f468 4d
W 00cdfe5a d00a 00
I SNAPSHOT 9 cdfe5a
D 00cdfe60 0140 f0f1 fee8 f14b cbe8 d0 54 f468 TSTA
...
```

Why Database?

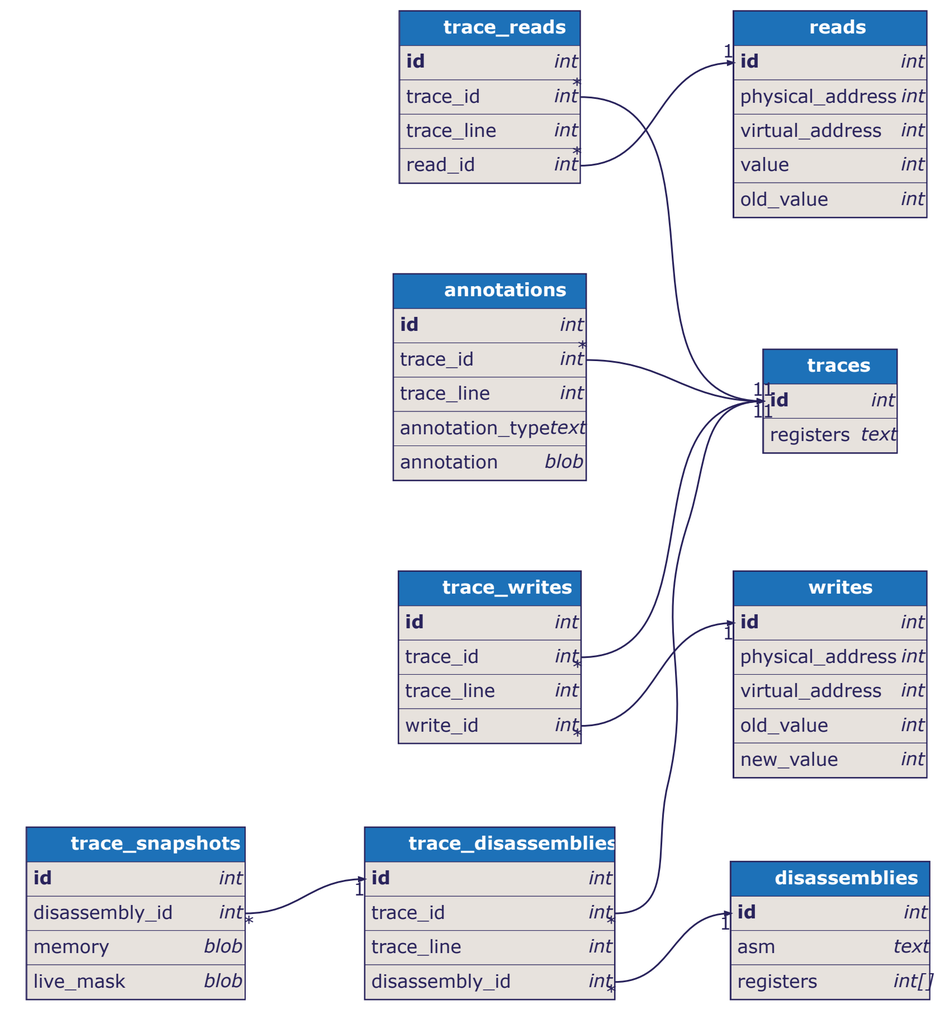
Code and execution paths are highly duplicated:

sample-trace-minestorm	sample-trace-minestorm.zst
File	File
2.58 GB	112 MB

Take advantage of duplication with foreign keys.

- Database of multiple traces enables analysis **over a whole corpus**
- Run analyzers independently then consider annotations as a whole

Trace DB Structure



Example Query

```
INSERT INTO annotations
  (trace_id, trace_line, annotation_type)
SELECT trace_id, trace_line, 's0_read'
FROM trace_reads
JOIN reads ON trace_reads.read_id = reads.id
WHERE reads.virtual_address = 0x2002
AND (reads.value & 0x20) <> 0;
```

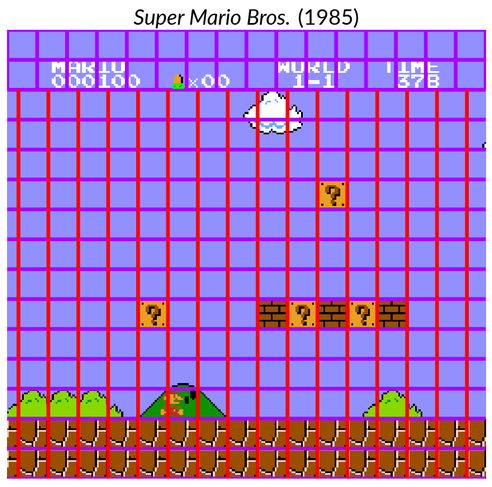
Cross-Game Analysis: NES example

Default (zero) scroll (tiles are aligned)

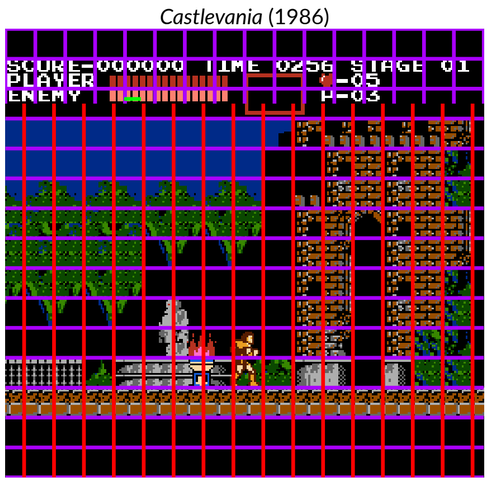
Nonzero scroll (tiles are offset)

Sprite #0

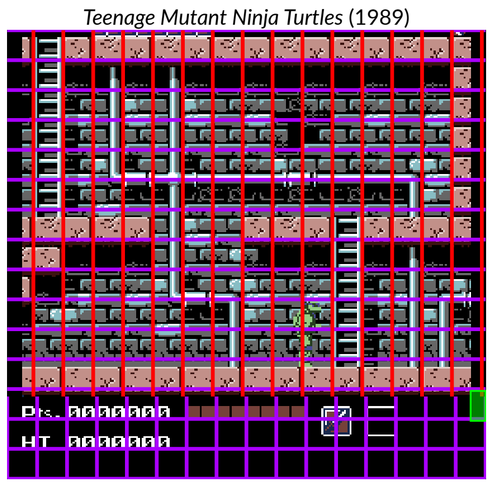
Super Mario Bros. (1985)



Castlevania (1986)



Teenage Mutant Ninja Turtles (1989)



- Goal: find games that have both a scrolling tile section and a static UI section
- Known scrolling method: change background scroll register after drawing Sprite #0

Analyzers to run with the tool:

- Annotate all Sprite #0 hits (reads from address `$2002` with bit 6 set)
- Annotate all starts of VBLANK (jumps to NMI handler, reads from `$2002` with bit 7 set)
- Annotate writes to the background scroll register (`$2005`)
- Likely candidates: annotations form a cyclic pattern

Games that are known to have static UI layers but do not fit the pattern may be interesting RE targets!