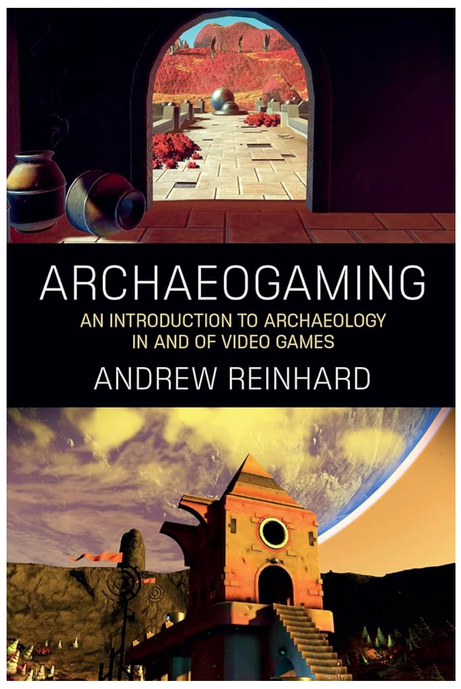
大規模ビデオゲームリバースエンジニアリング

余漁

研究の意義

- 2023年のビデオゲーム歴史財団（VGHF）によるレポート：「アメリカでリリースされたクラシックビデオゲームのうち、**87%**が絶滅危惧」
- 本研究はビデオゲームの考古学『アーキオゲーミング』を実践するための技術的基盤
- 「アーキオゲーミングは〔リバースエンジニアリングにより〕ゲームの基盤コードと構造、および格納媒体の解析を含む。」



トレース

- トレース解析は従来の解析の弱点を回避
  - 静的解析：実行パターン、外部イベントの考慮
  - 動的解析：実行中のインスタンスが必要
- トレースは無限回の「再生」が可能

LAVAトレースの例

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

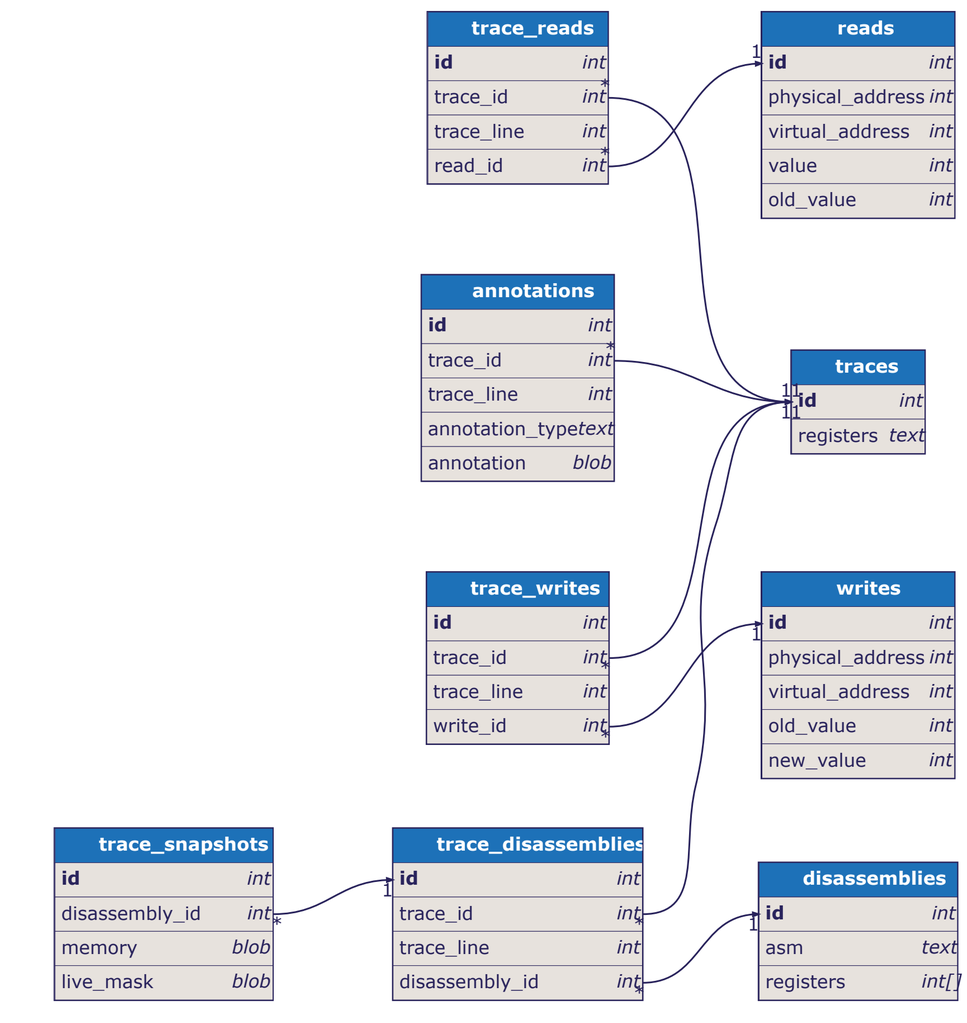
なぜデータベースなのか

コードおよび実行パスは高度に重複している：

外部キーを用いて、この重複を活用する。

- 複数のトレースを含むDBにより**コーパス全体にわたる**分析が可能
- アナライザーを個別に実行し、注釈の集合を全体として評価

トレースDB構造



クエリの例

```
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;
```

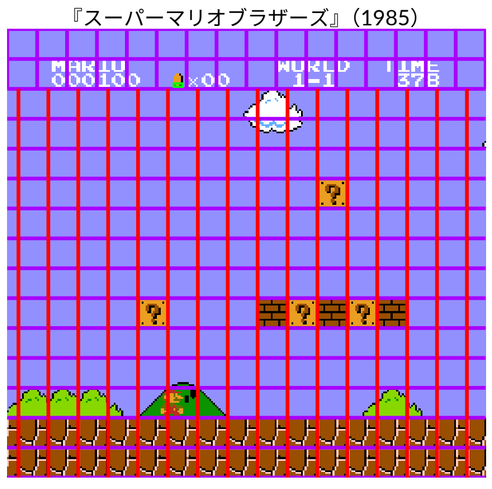
ゲーム間比較分析サンプル：ファミコン

背景スクロールなし
（画面とタイルが一致）

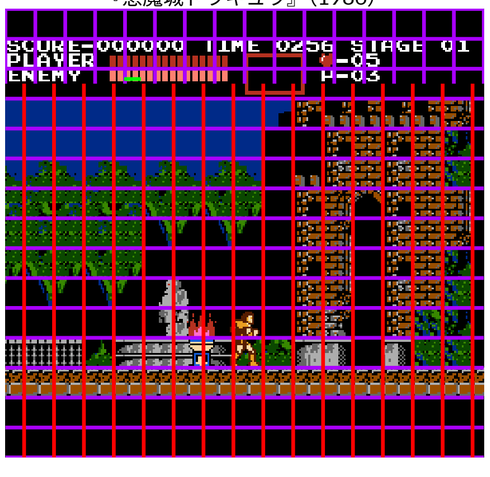
背景スクロールある
（画面とタイルが相違）

０番スプライト

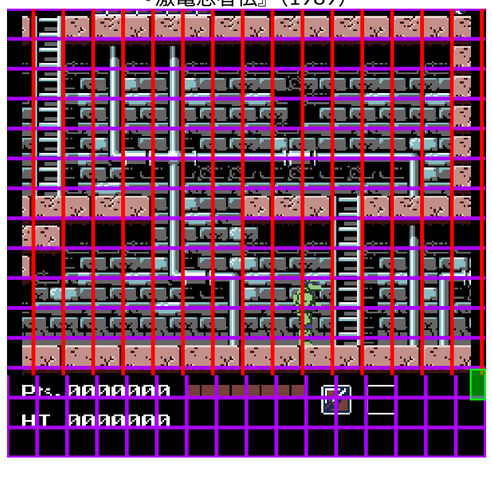
『スーパーマリオブラザーズ』（1985）



『悪魔城ドラキュラ』（1986）



『激亀忍者伝』（1989）



- 目的：スクロールする背景部分と静的なUI部分の両方を持つゲームを特定
- 既知のスクロール手法：０番スプライトが描画された後、背景スクロールレジスタに設定

使用するアナライザー：

- ０爆弾の判定（bit6が立っていてアドレス$2002のリード）のすべてを注釈
- VBLANKの開始（NMIハンドラーへのジャンプ・bit7が立っていて$2002のリード）のすべてを注釈
- 背景スクロールレジスタ($2005)のセットのすべてを注釈
- 有力な候補：周期的なパターンが現れる

静的なUI部分を持つにもかかわらずこのパターンに当てはまらないゲームは、興味深いリバースエンジニアリングの対象になる可能性がある！