Reverse engineering hardware, backing up ROMs, hardware emulation including use of JIT and dynamic recompilers, and emulation of retro video game systems

Adam Boult (www.bou.lt)

April 30, 2025

Contents

Preface

This is a live document, and is full of gaps, mistakes, typos etc.

Part I

Reverse engineering hardware

Part II

Hardware emulation

Chapter 1

Emulation

1.1 Low-level emulation

1.1.1 Emulating memory

big array of bytes hex numbers of some length

1.1.2 Emulating processors

emulation. cpu has operations. need to emulate them. convert to native. table with lookup for clock cycle requirements, mode etc.

1.2 High-level emulation

1.3 Containers

1.4 Virtualisation

Part III

Backing up ROMS, including CD (bin/cue) and DVD (iso), and mounting them (can mount ISO with "mount", cdemu for CDs)

Part IV

Lossless compression of ROMS, including regular zip, chd, gz, rvz

Part V

NES

Part VI

Game Boy

Part VII

Game Boy Advance

Part VIII

SNES

Part IX

N64

Part X

Arcade systems

Part XI

Sony consoles

Part XII

Sega consoles

Part XIII

Field-programmable gate array (FPGA)