# Emulacja procesora 8086 oparta na nowoczesnym standardzie języka C++

## Instrukcje, opcode i argumenty w x86

Patryk Kaniewski

2021-05-24

# Słownik

- opcode - zakodowanie działanie (instrukcja)
- operand - argument instrukcji

# CISC

complex instruction set computer - jest to komputer w którym jedna instrukcja może wykonać wiele operacji wewnętrznie

## Przyklad x86

MOV - wiele trybów adresowanie, dzialanie na rejestrach i pamięci

# RISC

reduced instruction set computer - jest to komputer w którym jedna instrukcja wykonuję jedna operacje

## Przykład ARM

LDR - load register - wartość -> rejestr X

# Kodowanie instrukcji

- fixed-length
- variable-length

# fixed-length

MIPS - R-format, J-format, I-format

## R format

Instrukcja składa się z tych samych elementów

opcode funct rd rs rt shift

mnemonic destination operand 1 operand 2

- add $8, $9, $10

# variable-length

x86 - wiele róznych formatów od 1 do 6 bajtów (8086)

## mov

| | | |
|---|---|---|
| mov ax, [bx] | -> | 8B 07 |
| mov bx, 37h | -> | BB 37 00 |

| byte | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 1 | opcode | | | | | | d | w |
| 2 | mod | | reg | | | r/m | | |
| 3 | [optional] | | | | | | | |
| 4 | [optional] | | | | | | | |
| 5 | [optional] | | | | | | | |
| 6 | [optional] | | | | | | | |

- d - direction
- w - word/byte
- mod - mode
- reg - register
- r/m - register/memory

# demo

demo

# Referencje


## Verifying x86 Instruction Implementations

https://arxiv.org/abs/1912.10285

## Intel 8086 Family User's Manual

https://edge.edx.org/c4x/BITSPilani/EEE231/asset/8086_family_Users_Manual_1_.pdf

## Apple ][ Emulation on an AVR Microcontroller

https://kola.opus.hbz-nrw.de/opus45-kola/frontdoor/deliver/index/docId/858/file/thesis_strauch_final.pdf

# Referencje (kont.)


## The INTEL® 8087 numeric data processor

https://dl.acm.org/doi/10.1145/1500518.1500674

## Formal Specification of the x86 Instruction Set Architecture

https://publikationen.sulb.uni-saarland.de/handle/20.500.11880/26394

## Emu8086

Implementacja referencyjna