V8&Node.Js RoadMap

陆亚涵
PLCT LAB
yahan@iscas.ac.cn
2023/12/15

大纲

1. V8过去一年的工作
2. V8未来工作
3. NodeJs 工作介绍
4. Chroium upstream 状态

V8过去一年工作

总提交量:

commit:125

added lines: 13369, removed lines: 8387, total lines: 4982

V8过去一年工作

- V8编译器sparkplug/liftoff/turbofan rv64gc和rv32gc移植完成，主要是常态化维护修复Bug，跟随上游更新
- RV64 B 扩展中Zbb/Zba/Zbs汇编器实现
- RV64 PointerCompress/Sandbox/Static Roots特性在riscv64上实现

  chromium-review中增加rv64 pointer compress 的CI bot

- 完成对RVV archcode重构，减少archcode数量

V8未来工作

- 增加对B/Zicond 扩展的指令选择优化支持
- 模拟器支持RVV更多的XLEN配置

目前V8自带的模拟器仅支持RVV XLEN=128, 但标准里XLEN可以从 128 到 1024

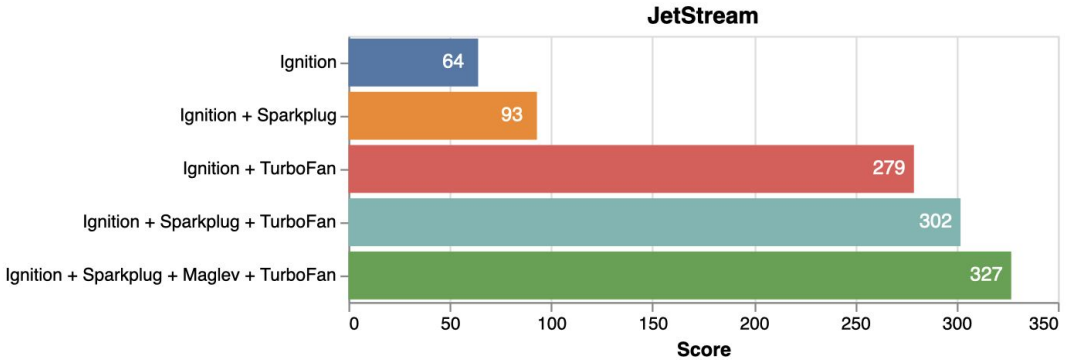
V8未来工作

- Turboshaft

  a new ir for turbofan

- Melgav

  V8’s Fastest Optimizing JIT
  A Simple SSA-Based



V8未来工作

- Webassembly Stack Switching
  a. Support for Asynch/await programming pattern.
  b. Support for green threads(scheduled by a runtime library).
  c. Support for yield-style generators.

  V8 中实现Stack Switching依赖三个builtin

- 安卓支持

  实现安卓需要的某些特性

NodeJs工作介绍

测试状态

- v8-embedded simulator: almost all regression pass
- qemu-user: fail 140+ cases
- qemu-system: fail 65+ cases

提交Patch

NodeJs新增flag:v8_enable_simulator

https://github.com/nodejs/node/pull/50653

非x64/x86 架构的node.js可以运行回归测试在x86/x64机器上

未来

查清不同环境下测试样例出现不同结果的原因

Chromium upstream 状态

Chromium在linux发行版中编译需要四个组件的补丁:

- angle (已合入upstream)
- base(已合入upstream)
- sandbox
- ffmpeg

谢　谢