

verl 仓库周报 · 2026 第 23 周 (06-01 至 06-07)

verl-project/verl

周期: 2026-06-01 至 2026-06-07

来源 PR: 36 · 重点 PR: 24 · 自动生成

原文链接: <http://prhub.com.cn/verl-project/verl/reports/2026-06-01-to-2026-06-07>

执行摘要

本周 (2026-06-01 至 2026-06-07) 仓库进入密集重构与修复阶段, 共合并 36 个 PR (其中 24 个重点 PR)。最显著的变化是平台抽象层 (#6086) 和 SkipManager (#6097) 两大基础设施重构落地, 标志着仓库向多硬件可扩展性和统一调试能力迈出重要一步。同时, NPU 适配持续深化 (MXFP8、Qwen3.5-122B、CANN 升级), 多项关键 Bugfix (安全 RCE、显存泄漏、资源泄漏) 显著提升系统稳定性, CI 系统也完成了 pip→uv 迁移、模型升级和日志路径统一。Megatron Checkpoint 管理器重构 (#6014) 进一步提升了可维护性与兼容性。

本周重点变化

基础设施重构

- 平台抽象层 (#6086): 引入 PlatformBase 和 PlatformRegistry, 通过装饰器动态注册新硬件平台; EngineRegistry 改为 last-writer-wins 策略, 允许外部插件覆写引擎实现。为 NVIDIA、Ascend、Cambricon 等多芯片提供统一可扩展接口。
- SkipManager (#6097): 创建 BaseSkip 基类和 SkipManager 装饰器, 统一管理 rollout 等环节的调试跳过方案, 替代原有 RolloutSkip, 支持同步 / 异步模式, 并预留扩展点。
- Megatron Checkpoint 重构 (#6014): 采用分层构建器重写 MegatronCheckpointManager, 引入 v2 目录结构 (model/、optimizer/、extra/), 新增迁移脚本一键升级旧版 checkpoint; 将 use_dist_checkpointing 重命名为 use_mbridge 提升 API 清晰度。

NPU 适配增强

- MXFP8 训练修复 (#6562): 修复 Ascend NPU 上 MXFP8 训练的量化缓存重置、导入失败和自动检测误判问题, 引入独立环境变量 VLLM_ASCEND_TASK_QUEUE_ENABLE。
- Qwen3.5-122B 支持 (#6582): 新增 Ascend 上运行 Qwen3.5-122B MoE GRPO 的脚本, 通过自动检测设备实现 GPU/NPU 配置分离。
- CANN 升级 (#6520): NPU 环境从 CANN 8.5.0 升级至 9.0.0, 同步适配 transformers 5.3.0 中 MoE 权重存储格式变化。
- CI 工具链升级: Ascend CI 工作流中 pip 迁移为 uv pip (#6535), NPU 测试模型从 Qwen2.5 切换至 Qwen3 (#6554), 日志路径统一 (#6600)。

关键 Bugfix

- 安全漏洞修复 (#6542) : 修复 Qwen3 工具解析器因使用 eval 导致的 RCE 漏洞, 替换为 ast.literal_eval 并添加 CPU 测试。
- 显存泄漏修复 (#6447) : Megatron ref 模型 offload 时 GPU 显存未释放, 通过同步拷贝和 storage().resize_(0) 修复。
- FSDP2 检查点修复 (#6604) : 当使用 CPUOffloadPolicy 时 save_checkpoint 崩溃, 添加 _uses_fsdp2_cpu_offload_policy 判断。
- Worker 计数泄漏 (#6544) : NaiveRouter 在请求重试失败后未释放 worker 计数, 通过 try/finally 确保释放。
- MTP 损失 NaN 修复 (#6464) : 上下文并行中 num_tokens=0 导致 NaN, 使用 clamp 到 1 修复, 并校正 per-token 损失梯度归一化。
- 多模态缓存重置 (#6522) : 权重更新后同时重置多模态和编码器缓存, 避免特征错误。

CI 改进

- 稳定主 CI (#6568) : 修复 fully async FSDP2 OOM, 添加缺失的依赖安装步骤。
- FSDP actor/critic CI 修复 (#6550) : 增加序列并行与 use_remove_padding 的运行时校验。
- VeOmni 安装测试修复 (#6557) : 简化模拟模块缺失的方式, 提高测试可靠性。

模块与主题趋势

本周 PR 标签分布显示 bugfix (14 个) 居首, 其次是 infra 和 npu (各 12 个), ci (8 个) 和 megatron (5 个) 紧随其后。这表明团队在追求新功能的同时, 重点在于修复既有问题、加固基础设施和适配 NPU 硬件。模型支持方面, Qwen3 系列成为主力, Qwen2.5 测试被逐步替换。作者方面, wuxibin89 (5 个)、daikang6 (4 个)、hustmf (3 个) 贡献最多, 社区参与活跃。热点文件集中在 Ascend CI 配置 (e2e_ascend.yml、nightly_ascend.yml)、Megatron 工具函数 (megatron_utils.py) 和文档索引 (docs/index.rst), 反映出 CI 稳定性、Megatron 支持和文档组织是当前迭代重点。

风险观察

1. 核心路径变更风险: 平台抽象层和 SkipManager 均涉及 engine 和 rollout 核心路径, 虽然已通过 code review, 但大规模重构后可能出现隐藏的兼容性问题, 建议下周安排专项回归测试。
2. 测试覆盖不足: 多个重要 Bugfix (如 #6544 worker 泄漏、#6447 显存泄漏) 没有附加单元测试, 依赖人工审查, 可能遗漏边界情况。建议后续补全测试。
3. 配置兼容性: SkipManager 引入新配置体系, 旧配置 (如 RolloutSkip) 已被删除, 用户需迁移; 当前 main_ppo_sync 尚未适配。
4. 未解决 Review 问题: 部分 NPU 脚本 (#6582、#6554) 存在硬编码路径、Ref 模型配置缺失等未采纳的建议, 可能影响实际运行稳定性。
5. CI 环境变化: pip→uv 迁移和 CANN 升级可能带来依赖解析行为变化或兼容问题, 需持续监控 CI 通过率。

重点 PR 速览

- #6086 (平台抽象层, 重要性 9.4) : 定义 PlatformBase 和 PlatformRegistry, 支持通过装饰器注册新硬件平台; EngineRegistry 允许外部插件覆写。Review 中接受了复用 VERL_USE_EXTERNAL_MODULES、移除 CPU 后端等建议。
- #6097 (SkipManager, 重要性 9.4) : 创建 BaseSkip 基类和 SkipManager 装饰器, 统一管理 rollout skip, 替代原有 RolloutSkip。修复了验证批次污染、属性初始化等问题。当前 main_ppo_sync 尚未适配。
- #6014 (Megatron 重构, 重要性 9.4) : 采用分层构建器重构 MegatronCheckpointManager, 引入 v2 目录结构, 新增迁移脚本。Review 中讨论了命名和安全性问题, 部分建议已采纳。
- #6542 (安全漏洞修复, 重要性 7.4) : 修复 Qwen3 工具解析器 RCE 漏洞, 用 ast.literal_eval 替换 eval, 并添加 CPU 测试。直接获批合并。
- #6612 (VeOmni 内存优化, 重要性 8.2) : 将专家重配内存从 $O(E)$ 降至 $O(E/ep_size)$, 通过 broadcast 循环替代 all_gather。Review 指出 group_src 参数和 buffer 共享问题未解决, 需关注。
- #6447 (显存泄漏修复, 重要性 7.0) : 在 Megatron ref 模型 offload 中, 通过同步拷贝和 storage().resize_(0) 释放 GPU 存储, 并添加安全检查。建议补充单元测试。
- #6562 (Ascend MXFP8 修复, 重要性 6.9) : 修复 MXFP8 训练三大问题, 引入重置函数和环境变量。Review 中防御性检查已采纳。
- #5760 (Profiling 窗口, 重要性 9.0) : 支持部分 token profiling 窗口配置, 减少 trace 数据量, 映射到 vLLM 和 SGLang 参数。验证逻辑重复问题待重构。

后续建议

1. 加强重构后验证: 平台抽象层和 SkipManager 变更较大, 建议下周安排专项回归测试, 覆盖主要训练流程 (GRPO、PPO) 和硬件配置 (GPU/NPU)。
2. 补充缺失测试: 针对 #6544、#6447 等关键 Bugfix 开发对应单元测试, 防止回归。
3. 跟进未解决 Review 问题: PR #6582 的 Ref 模型配置缺失、#6612 的 buffer 共享风险、#6550 的 model_config 类型兼容性等应在后续 PR 中修复。
4. 推广 CI 改进经验: uv 迁移和模型升级效果稳定后可推广到更多工作流; 日志路径统一做法可规范化为标准实践。
5. 提升 NPU 脚本质量: 对存在硬编码路径和未采纳最佳实践的脚本进行统一审查和修复。
6. 版本规划: 版本已升至 0.9.0.dev, 下周可考虑进入 RC 阶段, 集中解决剩余风险点, 为正式发布做准备。