WIELD: SYSTEMATIC REINFORCEMENT LEARNING WITH PROGRESSIVE RANDOMIZATION

Michael Schaarschmidt 1 Kai Fricke 2 Eiko Yoneki 1

ABSTRACT

Reinforcement learning frameworks have introduced abstractions to implement and execute algorithms at scale. They assume standardized simulator interfaces but are not concerned with identifying suitable task representations. We present Wield, a first-of-its kind system to facilitate task design for practical reinforcement learning. Through software primitives, Wield enables practitioners to decouple system-interface and deployment-specific configuration from state and action design. To guide experimentation, Wield further introduces a novel task design protocol and classification scheme centred around staged randomization to incrementally evaluate model capabilities.

1 INTRODUCTION

Following high profile successes in domains like games and robotics, interest in applications of deep reinforcement learning (RL) has seen explosive growth. In computer systems, RL has found applications across a diverse range of domains such as scheduling (Mao et al., 2019b), networking (Valadarsky et al., 2017), database management (Marcus & Papaemmanouil, 2018; Marcus et al., 2019), and device placement optimization (Mirhoseini et al., 2017; 2018).

Essential for the proliferation of RL applications have been open source implementations of popular algorithms. Algorithmic frameworks like RLlib (Liang et al., 2019), RLgraph (Schaarschmidt et al., 2019) or OpenAI baselines (Dhariwal et al., 2017) allow practitioners to execute off-the-shelf algorithms at scale. These frameworks standardize task execution through shared interfaces such as OpenAI gym (Brockman et al., 2016). They do not concern themselves with identifying problem representations.

In consequence, RL applications in systems have seen limited standardization. While a multitude of experimental successes have been reported in controlled environments, real-world data processing systems are yet to widely utilize RL. Experimental research often relies on highly customized benchmarks, hardware setups, state-action representations, and proprietary simulators. Moreover, assessing evaluations is complicated by the use of fixed workloads and limited reporting on the impact of random seeds and workload variation. Hence, applied research is fragmented, and novel approaches are difficult to reproduce. Their viability across larger deployments or different tasks remains unclear.

RL algorithms suffer from known limitations due to large sample requirements, sensitivity to hyper-parameters (Henderson et al., 2017), random weight initialization, and small input perturbations (Kansky et al., 2017). In this paper, we argue that another root cause of limited real-world progress is a lack of shared evaluation protocols and design tools. Specifically, both reinforcement learning agents and systems workloads can exhibit several degrees of non-determinism.

For example, RL agents have been used in blackbox optimization settings where an agent is trained to optimize a single fixed workload instance (e.g. a single computation graph (Mirhoseini et al., 2018)). Within a blackbox setting, experiments with varied random seeds can each perform on the same fixed task (fixed blackbox), or sample a random task instance per experiment to illustrate robustness to task variation (randomized blackbox). Similar evaluation modes can be applied to generalization problems, with additional consideration for within- and out-of-distribution evaluation.

To begin addressing these difficulties, we present Wield, a first-of-its-kind system towards systematic task design and evaluation in applied RL. Wield makes two contributions:

First, Wield provides a small set of reusable software primitives which decouple system interface and RL representation from deployment-specific configuration and proprietary simulators. These primitives are coordinated through standardized task evaluation protocols which help researchers explore new state, action, and reward models independent of system-specifics.

Second, we introduce progressive randomization, a novel task evaluation protocol and classification scheme which explicitly delineates sources of non-determinism. Progressive
randomization enables practitioners to communicate evaluation assumptions, and to incrementally evaluate model capabilities.

In the remainder of the paper, we first introduce Wield’s design abstractions and discuss common issues around model design in systems-RL (RL applied to systems). We then introduce progressive randomization and use it to review recent work in systems-RL. In the evaluation, we demonstrate Wield’s utility by reviewing the device placement problem, a popular task in systems-RL. We reproduce prior work to classify its capabilities through progressive randomization, and subsequently implement a novel placer with Wield. Our results illustrate the true cost of evaluating RL solutions, and further call into question common evaluation practices on fixed datasets.

2 WIELD

2.1 Overview

Delineating practical progress requires systematic assessment and comparison of approaches. The aim of Wield is to provide re-usable abstractions to standardize task design for systems applications of reinforcement learning.

Figure 1 gives a conceptual overview of Wield. On a high level, Wield acts as an interface between a data-processing system (e.g. database, scheduler, distributed execution engine) and a reinforcement learning framework such as RL graph or RLlib, auto-tuners, or any implementation exposing a task interface. We implemented our Wield prototype using RLgraph’s agent implementations (Schaarschmidt et al., 2019). The highest level abstraction in Wield are workflows which coordinate execution of online (interacting with a system) or offline (e.g. log data) training, evaluation, and serialization of data and models.

Models use task graphs to describe hierarchies of tasks wherein a single node may be a single differentiable agent architecture, a blackbox auto-tuner, or a supervised model. Tasks use converters to map between agent and system view of data, and schemas to standardize programmatic layouts of input states and actions. By separating representation design and system-specifics, task architectures can be used across similar systems or problem structures which only differ in the system interface (e.g. different databases with distinct query languages).

2.2 Task design abstractions

Wield’s task abstractions unify workflow streams via standardized task and data layouts. Layout refers to the concrete dimensions, data types and processing steps for all inputs and outputs of an RL agent. As a running example, we use the popular problem of placing a computational graph (e.g. a TensorFlow graph) across a heterogeneous set of devices to minimize runtime of the update operation (Mirhoseini et al., 2017; 2018; Addanki et al., 2019).

2.3 Task schemas

State design. Task schemas are motivated by the observation that states for systems problems need to be explicitly designed. In contrast, game simulators like Atari have fixed state dimensions (e.g. 640 × 480 images) across games. All methods can rely on a fixed base representation (i.e. the original game frame) for reproducible and comparable experiments. Wield schemas encapsulate input-dependent state and action layout construction.

Consider a state model for encoding an operation in a computational graph. The state may encode various types of semantic problem information such as operator type embeddings, tensor shapes, current device, and topology of the local graph neighborhood (Mirhoseini et al., 2018). While iteratively exploring different representations, schemas capture the layout of the resulting states. Moreover, different resource types and layouts, i.e. dimensions of state arrays, may be required per deployment due to different number of devices and nodes. Schemas allow developers to express a state layout as a function of system parameters. In practice, developers may implement multiple schemas to iteratively compare representations.

States can also encode bias towards decision horizons. For example, Tesauro et al. describe a choice of state encoding in the context of server resource allocation via a discretized mean request arrival rate (Tesauro et al., 2006). Their state includes both the current mean arrival rate and the one from the prior observation interval to relate the impact of actions to arrival rate. In workload management tasks, the
workload generating process is generally unknown, and future workloads (e.g. request rates or job size) may be independent or correlated to current decisions. State features and preprocessing, e.g. temporal smoothing, must encode such assumptions. In the device placement problem, states are deterministically computed as the graph is traversed in topological order.

In summary, state design for systems-RL is an iterative process which differs from feature design for supervised learning as the state must also capture transition dynamics. To help researchers explore, compare and version state designs, Wield standardizes them through schemas.

**Action design.** Similar to state design, action structure must be designed manually as agent outputs need to be translated to structured system calls, e.g. by generating a special query to update the state of a database. Simple action representations include single binary or categorical decisions where an action selects one of a small number of resources or task slots, e.g. which task to schedule next from a task queue, or which device to assign to an operation on a single node. The term “action structure” refers to interpreting the outputs of a neural network. For example, in Q-learning, a neural network used to represent the Q-function is designed by creating a final action selection layer with one neuron per possible integer action. The outputs are interpreted as Q-values. To output multiple distinct actions, multiple action layers may be created. RL practitioners must explicitly consider how decision problems can be mapped to convenient (i.e. as few distinct actions as possible) representations.

Such representations may not scale to larger problem instances if the number of actions directly corresponds to problem size. Consider a device placement problem scheduling a large computational graph across a cluster with tens of thousands of devices where each device would then correspond to an action. Without an informative prior, an agent would have to first observe performance dependencies across all types of devices. This would require an impractical number of samples to explore action combinations.

This is in contrast to well-conditioned continuous action spaces (e.g. for a physical actuator) where small changes in output correlate to small and predictable changes in the state trajectory. Large discrete action spaces may require task decomposition. If similarity between actions in large discrete action spaces is known in advance, actions can also be selected in a multi-stage approach whereby first an action in a promising region of the action space is selected, and a nearest-neighbor lookup is subsequently performed to identify a fitting local action (Dulac-Arnold et al., 2015).

Listing 1 shows two simplified single-task schemas for the device placement problem. One schema defines a one-dimensional input-array for a recurrent architecture (Mirho-

```python
def _build_inputs(self, input_graph, devices):
    num_ops = count_ops(input_graph)
    num_options = len(NODE_OPTIONS)
    return Dict(
        'embeddings': FloatBox(
            shape=(num_ops, num_options + len(devices))),
        'current_node_num': IntBox(low=0, high=num_ops),
        'in_neighbors': IntBox(shape=(num_ops, MAX_NEIGHBORS),
        'out_neighbors': IntBox(shape=(num_ops, MAX_NEIGHBORS))
    )

Listing 1. Task schemas define programmatic layout based on deployment-specific parameters.

seini et al., 2018) while the other defines layouts for a graph neural network (Addanki et al., 2019). Both share the same action layout based on available input devices. The example illustrates how system-specific configurations are used to define layouts for states and actions.

In summary, schemas define physical layouts of states and actions, and decouple them from transition dynamics.

### 2.4 Converters

Where schemas correspond to physical layouts, converters are adapters expressing how system metrics, configuration parameters, and query languages or custom protocols correspond to numerical representations within an optimization.

There is a many-to-many relationship between schemas and converters. A schema specifying a layout can be used by different converters, and a converter may work with different schemas. Schemas constrain how decision model is encoded structurally (layout), converters specify how this encoding is achieved from raw system information (content). Listing 2 shows the conversion API provided by Wield with an example implementation for device placement. Workflows invoke the converter API to translate between system and agent representation.

### 2.5 Task architectures

Schemas and converters help decouple system-specifics from task representation in RL for a single task. Task graphs organize tasks into independent sub- and multi-task architectures.

**Shared-parameter tasks** are multi-task architectures
where a single end-to-end differentiable architecture has multiple task output networks which each emit separate actions per step. **Independent tasks** are task architectures where separate learners focus on different sub-tasks, e.g. in the case of hierarchical decomposition or parallel independent tasks.

Non-trivial task graphs occur through task decomposition (Figure 2). Hierarchical task decomposition refers to tasks organized as directed acyclic graphs where outputs from single tasks (vertices) are used as input states (edges) to other task vertices. Independent tasks refers to a scenario where multiple learners interact with an environment, possibly learning at different time scales. Hierarchical reinforcement learning has been studied in a variety of contexts with the most well known approach being the options framework (Sutton et al., 1999). There, a top-level policy chooses between different sub-policies (options) to execute over a time-frame (until the sub-task terminates). In Wield, we focus on work flows where users manually identify task hierarchies as a means of encoding domain knowledge.

Hierarchical designs to organize resources at different granularities are also a core element of systems research (e.g. cache hierarchies, hierarchical scheduling). However, hierarchical RL has found limited attention in the systems community as a means to manage large state and action spaces. This could be due to most open source implementations focusing on single-agent scenarios or unstructured collections of policies (e.g. RLlib (Liang et al., 2018)).

Task graphs in Wield simplify factorization of tasks into different sub-tasks which may train and act jointly, or at different time-scales. Task objects primarily encapsulate distinct agents or any other optimization implementing OpenAI gym (Brockman et al., 2016) interfaces. Hierarchical tasks often require to transform the output of one task before inputting it to a subsequent task, e.g. by enriching it with additional environment information or preparing a specific input format. Nodes in a task graph hence further encapsulate pre-and post-processing for each sub-task. Edges in the graph are implicitly created by creating one task as a sub-task of another task in the same task-graph. When performing inference, task outputs are routed through the task graph based on user-defined directed edges between tasks, and the results of all tasks during execution are returned.

In this section, we introduced a light-weight set of software primitives for modularized task design. Next, we present progressive randomization as the guidance mechanism to evaluate representations.

## 3 Progressive Randomization

### 3.1 The case for task randomization

A key obstacle when assessing model capabilities is the use of fixed workloads. In domains like database management, query processing benchmarks often focus on narrow application scenarios with small query sets (e.g. TPC-H, TPC-C). Leis et al. proposed the Join Order Benchmark which contains 113 queries specifically designed to investigate join estimation capabilities in query optimisers (Leis et al., 2015). In device placement, researchers have relied on fixed graphs of standard architectures which may differ in implementations (Mirhoseini et al., 2018), custom variants of common architectures (Addanki et al., 2019), or proprietary datasets (Paliwal et al., 2019).

While hand-designed workloads can highlight particular weaknesses or strengths of a system, they nevertheless are prone to over-fitting small test sets. We argue that the design of RL mechanisms for systems can benefit from synthetic workload mechanisms with configurable task difficulty as a means to understand both training and inference behaviour.
Reasoning about non-determinism when evaluating stochastic optimization mechanisms requires distinguishing deterministic and non-deterministic elements in both workload and optimization procedure (network weight initialization). In Wield, we construct workloads from the perspective of changing between several evaluation and randomization modes. We distinguish between blackbox and generalization mode. In blackbox mode, a single workload instance (e.g. a single set of queries or jobs) is generated and a model is trained and evaluated on that same instance. In generalization mode, training is executed on different instances than the ones used in the final evaluation.

Both modes can be executed with varying levels of randomization. Workload determinism refers to deterministic behaviour of task instances. Training determinism refers to deterministic initialization and sampling during training. For example, in blackbox mode the generation of the single task instance and the training initialization can both be deterministic. Similarly, in generalization, both the instances used during training and the final test instances can be randomly generated or held fixed. This invites problematic practices such as cherry-picking and presenting only successful combinations of workloads and weight initialization values (while omitting this selection).

In the RL literature, all combinations of blackbox and generalization modes can be found. Comparing results is difficult if authors do not to report which workload elements are held fixed or are subject to randomization, or why a particular sample was chosen.

### 3.2 Progressive randomization

**Overview.** Progressive randomization is based on the observation that different randomization modes can serve different phases of design. For example, holding a workload fixed to study robustness against random initialization is valuable when a designer is uncertain if a model design can solve a task at all. Conversely, using a fixed optimization can be useful to study the impact of workload parameters on optimization outcomes. Evaluation difficulties are not inherent to a specific mode of randomization or evaluation. They arise when conflating sources of performance variation or misinterpreting model capabilities.

In supervised learning, projects such as DAWNBench (Coleman et al., 2018) have suggested metrics like time-to-accuracy to compare model designs and hardware choices to understand trade-offs in deep learning systems. In contrast, shared RL tasks such as the Malmo Minecraft challenge (Johnson et al., 2016) or Unity agents (Juliani et al., 2018) are focused on performance in simulated worlds where randomization is incidental. That is, workloads may include some degree of randomization and generalization but these are not varied to analyse their contribution to agent performance (or lack thereof). Task variation in these scenarios is further constrained by experimental cost. The purpose of randomization is to evaluate model robustness to both subtle and fundamental changes in workloads. For example, in systems-RL, this requires gathering evidence about plausible workload distributions a controller may encounter.

Table 1 lists the different evaluation modes in the protocol and their purpose. It also lists example applications. Fixed optimization parameters in practice refer to the random weight initialization strategies in neural networks, and further to the random seed used when sampling mini-batches for stochastic gradient descent as well as policy decisions. Fixed blackbox refers to always training on the same workload or problem instance, while fixed generalization refers to an unseen but fixed test task. Randomized generalization implies that for each reported experiment result, a new test instance was generated.

Not all possible combinations of non-determinism are present in the protocol. Fixed optimization parameters on fixed workloads are initially useful to produce repeatable results and debug non-optimization components of a task (C_0). For subsequent evaluation concerns, they should be randomized to avoid cherry-picking ‘lucky’ seeds. In C_1

| Class | Optimization seed | Workload randomization | Example use cases |
|-------|-------------------|------------------------|-------------------|
| C_0   | Fixed             | Fixed blackbox task    | Iterate and debug representation |
| C_1   | Random            | Fixed blackbox task    | Weight initialization sensitivity |
| C_2   | Random            | Randomized blackbox task | Model sensitivity to task parameters |
| C_3   | Random            | Fixed in-distribution generalization | Understand sample requirements |
| C_4   | Random            | Randomized in-distribution generalization | Customized production use |
| C_5   | Random            | Fixed out-of-distribution generalization | Robustness against unforeseen inputs |
| C_6   | Random            | Randomized out-of-distribution generalization | Production use without customization |
and \( C_2 \), weight initialization and workload instance (e.g. a set of jobs sampled from a workload distribution) are incrementally randomized.

**Generalization.** Subsequent levels evaluate performance on unseen problem instances. *In-distribution generalization* refers to workload assumptions where the test task is taken from the same distribution training tasks were generated from. For example, the device placement problem can be randomized by varying batch size and sequence unroll lengths on the same architecture (Addanki et al., 2019) (in-distribution), or by testing on entirely new architectures (out-of-distribution). Generalization semantics are complicated by task-specific concerns. For fixed or randomized generalization tasks, there may be no useful measures of how different test tasks are from training examples. Parts or the entire test task could be seen during training, unless the test task is held out and rejected.

Nonetheless, the description of a model to e.g. be in \( C_3 \) for a certain task gives useful indication of expected behaviour. We refer to being in a class as to meeting application-specific assumptions. For example, a model in \( C_2 \) which meets randomized blackbox objectives can be used as a direct search tool in practice without requiring to retune hyper-parameters, whereas a model in \( C_1 \) tuned for a fixed blackbox objective is customized to a single deployment or task context. Distinguishing model classes sets expectations and allows researchers to effectively communicate evaluation designs.

Generalization concerns in deep reinforcement learning are poorly understood. They are not well captured analytically but rather empirically per task. This is primarily a consequence of limited understanding on generalization capabilities of neural networks as policy vehicles. A model may be in different classes depending on the number the samples is trained on. In particular, researchers at OpenAI highlighted in their work on competitive DOTA that massively increasing model and sample size can induce qualitatively different generalization behaviour (OpenAI, 2018). Moreover, even for the same hyper-parameters, a large fraction of random weight initialization and optimization seeds may vary drastically in performance (Henderson et al., 2017).

We propose to describe models based on the these empirical properties. Progressive randomization classification thus includes (i) the number of state transitions experienced during training \( n \), (ii) the number of random seeds used for weight initialization and optimizations \( s_r \), and (iii) the observed frequency \( f \) where learning objectives were achieved.

For example, a model may be described as \( C_1(n = 10^7, s = 10, f = 0.4) \) to communicate empirical success when training 10 million samples and trying 10 different random seeds, where 4 of 10 trials met the objective. In the following notation, we omit \( s \) and \( f \) from notation when only discussing sample count or class membership. Communicating success rates is especially important when considering the training cost on single-tasks without generalization.

As sample collection cost varies drastically between tasks, conditioning class membership on sample size is useful for estimates on model transfer on tasks with different sample collection cost. For example, the same model may be in \( C_1(n = 10^4) \) but in \( C_3(n = 10^6) \) as robustness to inputs increases with experiences seen during training. The number of sample trajectories seen during training may also correlate with the observed frequency of reaching an objective.

**Limitations.** Progressive randomization encourages shared understanding of model capabilities across problem domains. Practitioners can use it to incrementally test new

---

**Table 2. Progressive randomization protocol overview.** Each class specifies a different level of non-determinism. If a range is given without an approximate estimate, this refers to different data sets being reported at different sample sizes. A * refers to researchers reporting median or mean across random optimization seeds.

| Work                          | Objective                                      | Highest \( C_i \) reported |
|-------------------------------|------------------------------------------------|--------------------------|
| Neural packet classification  | Classification time/memory                     | \( C_0(n = 10^7, s = ?, f = ?) \) |
| Device placement              | SGD iteration time                              | \( C_1(n = 10^3, s = ?, f = ?) \) |
| Device placement              | SGD iteration time                              | \( C_1(n = 2 \times 10^5, s = 4, f = 1.0)^* \) |
| Join order                    | Query execution time                            | \( C_3(n = 10^7, s = ?, f = ?) \) |
| Device placement              | SGD iteration time                              | \( C_3(n = 10^5 - 10^6, s = ?, f = ?) \) |
| Cardinality predictions       | Prediction error                                | \( C_3(n = 10^4, s = ?, f = ?) \) |
| Language to program           | Program generation                              | \( C_3(n = 10^4, s = 5, f = 1.0)^* \) |
| Spark scheduling              | Spark job completion times                      | \( C_4(n = 10^8, s = ?, f = ?) \) |
| Congestion control            | Throughput, latency                             | \( C_4(n = 10^6 - 10^7, s = ?, f = ?) \) |
| Query Optimizer               | Improve query latency                           | \( C_5(n = 10^4 - 10^6, s = 50, f = 1.0)^* \) |
| Computation graph rewriting   | Memory usage                                    | \( C_5(n = 4 \times 10^5, s = 20, f = ?) \) |
| AlphaZero                     | Win game of chess                               | \( C_5(n = 10^9, s = ?, f = ?) \) |
implementations. Several dimensions regarding model scale, the cost of featurization, and other hidden cost are not captured. The protocol also does not replace standard considerations on experiment design or statistical analysis. The classification system is intentionally simple to serve as a low-overhead summary of design assumptions. While only a starting point, progressive randomization constitutes the first explicit evaluation protocol for focused on delineating workload randomization.

3.3 Prior work viewed through progressive randomization

We use progressive randomization as a lens on prior work in research and applied RL. Table 2 classifies selected prior work, sorted by class membership. The classification immediately illustrates problem progress. For example, in the device placement problem, Mirhoseini et al.’s initial work (Mirhoseini et al., 2017) with manual operation grouping required orders of magnitudes more samples than their subsequent work using a hierarchical approach (Mirhoseini et al., 2018). Both operated in a fixed blackbox setting. Addanki’s et al.’s (Addanki et al., 2019) and Paliwal et al’s recent work (Paliwal et al., 2019) utilizing graph neural networks then illustrates progress towards generalization through permutation-invariant representations.

In our survey, we found subtle differences in evaluation randomization which can be made make explicit through progressive randomization. For example, Addanki et al. generate random variations of computation graphs for training and testing, but both sets are fixed ($C_3$).

A similar progress pattern can be observed in database tasks. In their first work on join order enumeration, Marcus et al. (Marcus & Papaemmanouil, 2018) used a policy optimization method on a fixed set of training and test queries, the Join Order Benchmark (JOB) (Leis et al., 2015). Training with randomized optimization parameters yields $C_3(n \approx 10^5)$. In subsequent work, Marcus et al. proposed a learned query optimiser (Marcus et al., 2019) which they evaluate on several tasks, including a fixed set of out-of-distribution queries $C_5(n \approx 10^4 - 10^6, s = 50, f = 1.0)$. We also observe that training workloads in database applications were often generated by augmenting fixed existing query sets (TPC-H, IMDB). It would be desirable for the systems-RL community to develop shared standards on training and test randomization.

Many approaches do not report explicitly how workload randomization and optimization parameters were selected which makes classification difficult. If a fixed task is presented without reporting number of training trials, seeds, or randomization assumptions (i.e. a potentially cherry picked single random seed), we assume $C_0$.

Few of the applied works we surveyed explicitly report on failure modes, despite often using appendices to communicate other training hyper-parameters. This highlights the need for more explicit evaluation protocols. Evaluation times for systems-RL can vary drastically between microseconds and minutes. Sample-size classification helps researchers evaluate if a simulator may be needed.

Finally, prior systems applications of RL are not typically defined through a binary objective such as winning a game or reaching a score threshold. Performance objectives are explorative, e.g. outperforming problem-specific baselines. This can obfuscate practical utility without cost-benefit analysis on implementation cost.

![Figure 3](https://example.com/figure3.png)

Figure 3. Reproducing the hierarchical placer on the fixed NMT graph. Top: Fixed seed. Bottom: Random seed sampled per trial.

4 Evaluation

We illustrate systematic assessment on the device placement problem. We then subsequently implement a competing model and again incrementally evaluate it.

4.1 Reproducing prior work

We use progressive randomization to evaluate the open source TensorFlow device placer (’Grappler’) available as part of the grappler module¹ (Mirhoseini et al., 2018).

Setup. As a benchmark, we use the neural machine transla-

¹https://github.com/tensorflow/tensorflow/tree/master/tensorflow/python/grappler
tion (NMT) architecture evaluated by all prior device placement work. While some models were trained in a distributed setting, reported NMT results ((Mirhoseini et al., 2018), Figure 3) illustrate strong performance improvements within hours of training using a single node. NMT is an attractive benchmark task because the variants tested consist of an encoder-decoder architecture with multiple LSTM layers. Prior work shows placements must split training batches non-trivially across GPUs and time dimensions.

The open source placer was not able to run evaluations on Google’s NMT implementation with its own evaluation utilities. Serialization of a number of related metagraph components failed. The results presented here were obtained by directly instantiating the TF graph and calling training operations. This significantly increases cost per measurement. Each measurement was given one warm-up run, and the subsequent measurement was reported to the controller. The open source hierarchical placer decays its learning rate to 0 within 1000 updates, corresponding to the results reported in the paper. Here, all results were run at least 1000 steps.

**Fixed blackbox.** We begin with the fixed random seed, fixed workload setting ($C_0$). Figure 3 (top) illustrates runtime of the training operation (i.e. a single iteration of mini-batch stochastic gradient descent). Results are averaged across runs, shaded areas indicate 1 standard deviation confidence intervals. We used the random seed supplied by the default configuration in the open source implementation (1234), and repeated the experiment 10 times.

The placer identified improved placements in most runs with a mean final improvement (measured as the mean of the final 10 steps against the initial runtime) of 52%. One run failed to substantially improve in the end (5%). Invalid placements were removed from the figures (assigned runtime value 100 in the implementation).

We break down both the final relative improvements and the best-seen solution during training in Table 3. Results show that i) all trials identified significant improvements during training, and ii) some trials diverged. Divergence even occurs with a fixed random seed and a fixed workload, likely due to noise in the reward. We also contrast learned values against entirely random placements and groupings in Figure 3 (top) which fail to find good placements.

In Figure 3 (bottom), the same graph is evaluated on 10 randomly chosen seeds (fixed workload, randomised optimization parameters, $C_1$). Mean improvement was 72% with all random seeds achieving over 70% improvement. The fixed seed led to higher variance than the random seeds.

While restricted to a single graph, reproduced results confirm the paper’s claims of reliable improving runtimes in black-box settings. With a success criterion of at least 30% improvement (minimum improvement in paper 35.9%), we report $C_1(n = 1000, s = 10, f = 1.0)$.

**Randomized blackbox.** In Figure 4 (top), we modify task parameters by varying batch size and unroll lengths in the recurrent network to create a randomized blackbox setting ($C_2$) where both graph and optimization seed are varied. Best runtimes are expected to differ due to different graph sizes. Of six trials, three succeeded, one failed entirely (1), and one (5) diverged from an effective configuration ($C_2(n = 1000, s = 6, f = 0.83)$).

```
Table 3. Fixed blackbox improvements found by Grappler.

| Trial | Final model | Best seen |
|-------|-------------|-----------|
| Trial 1 | 57.0%       | 69.0%     |
| Trial 2 | 67.0%       | 71.0%     |
| Trial 3 | 25.0%       | 69.0%     |
| Trial 4 | 51.0%       | 73.0%     |
| Trial 5 | 5.0%        | 74.0%     |
| Trial 6 | 70.0%       | 73.0%     |
| Trial 7 | 69.0%       | 69.0%     |
| Trial 8 | 47.0%       | 73.0%     |
| Trial 9 | 68.0%       | 70.0%     |
| Trial 10 | 66.0%      | 69.0%     |
```

Figure 4. Randomized blackbox evaluation. Top: Random blackbox, random seed. Bottom: Repeats of failed trial 2.

Did trial 2 fail due to posing a more difficult placement task, or due to random initialization? In case of unclear failures, we decrease randomization levels and re-evaluate the failed task. We repeated the failed trial as a fixed blackbox task...
with randomized optimization parameters. Figure 4 (bottom) shows results of rerunning the same task nine more times for a total of ten trials. Results include more fails and diverged results but also succeeding runs. Three trials failed to improve placements significantly. Performance variation is further higher than in the published result, as graph variations affect failure rate.

**Fixed in-distribution generalization.** Next, we consider generalization capabilities. We first evaluate the final trained model in each trained randomized graph against all other trials’ graphs. Figure 5 show two examples of cross-graph comparisons. Final models perform significantly worse against the best seen solutions when training specifically on the respective graph, with overheads against the best solution ranging between 20% - 50%. Analysis of placements shows (i) during training on a particular graph, non-trivial placements using all devices are identified during exploration, and (ii) diverged final placements default to single-device (CPU only) or single-GPU. When evaluating generalization, placements for slightly varied graphs frequently defaulted to trivial single-GPU decisions.

![Figure 5. Generalization overhead example.](image)

The failure to identify non-trivial placements for varied graphs is hence both a result of models diverging and limited model capability. We compare detailed generalization results and classify against our placer in the next section.

### 4.2 Implementing a placer with Wield

Next, we use Wield’s primitives to implement and evaluate a new placer. Our implementation combines insights from the open source hierarchical placer and Addanki’s recent work on using graph neural networks (Addanki et al., 2019). Addanki et al. rely on manual grouping and identify effective generalizable placements based on i) incremental evaluation of placements, and ii) a neighborhood embedding in a graph neural network based on computing parallel, parent, and child-operation groups.

Our goal is to investigate if Wield’s abstractions can be used to re-implement customized architectures. We loosely combine both approaches using Wield’s task graph abstraction to implement an hierarchical graph network placer. Grouper and placer are proximal policy optimization agents (Schulman et al.) learning independently at different time scales.

![Figure 6. Open source hierarchical placer versus Wield placer.](image)

We repeat the same NMT experiments used on the hierarchical placer. To calibrate hyper-parameters, we ran five trial experiments to identify effective learning rate schedules and incremental reward modes before final experiments. Our main finding was that the grouper required a more aggressive learning rate schedule, because initially random groupings caused the neighborhood computation in the placer to diverge (all groups were connected to all others).

Figure 6 compares operation runtimes over the course of training. Due to cost, we terminated some experiments early after no more improvement was observed. Both implementations frequently found their best placements within 500 graph evaluations. We repeated the randomized blackbox experiment with 6 new graphs ($C_2$) to evaluate sensitivity to graph variations. In table 4, we compare relative runtime improvements across trials between Grappler and Wield. Mean improvements are similar and differences not statistically significant (for $p < 0.05$).

| Trial | Grappler best | Wield best |
|-------|---------------|------------|
| Trial 1 | 22.6% | 37.4% |
| Trial 2 | 37.4% | 38.2% |
| Trial 3 | 37.8% | 32% |
| Trial 4 | 36.7% | 37.4% |
| Trial 5 | 37.2% | 41.5% |
| Trial 6 | 34.5% | 48% |
| Mean  | 34.4% (5.4%) | 39.1% (4.9%) |

Finally, we also repeated the cross-graph generalization experiment to investigate generalization capabilities of the structured neural network representation. Since the network computes a permutation invariant embedding of operation neighborhood, higher robustness to input variants should be observed. We show a detailed breakdown of both approaches’ generalization capability by showing how the final model trained on a graph (rows) performs in terms of relative runtime improvement on another graph (columns) (Tables 5 and 6). Grappler’s placer only in few instances significantly improved the initial placement (> 30%), with a
We also showed that using Wield, a competitive placer could be implemented by combining off-the-shelf algorithmic components. In both placers, models diverged after identifying effective placements, and learning rate schedules would need to be tuned to high precision to prevent this. Both the true cost of such calibrations and the impact of workload randomization have not been widely discussed in the systems-RL community. With Wield and progressive randomization, we aim to simplify randomization through standardized workflows.

## 5 Related Work

Our work is inspired by the observations around evaluation difficulties in deep RL in various prior lines of research. Henderson et al. observed how subtle implementation issues and random initialization drastically affect performance (Henderson et al., 2017) across implementations. Mania et al. subsequently demonstrated that an augmented random search outperformed (Mania et al., 2018) several policy optimization algorithms on supposedly difficult control tasks. Further recent work on policy gradient algorithms observed that the performance of popular algorithms may depend on implementation heuristics (e.g. learning rate annealing, reward normalization) which are not part of the core algorithm (Ilyas et al., 2018). For real-world RL, Dulac-Arnold et al. (Dulac-Arnold et al., 2019) recently summarized a set of nine core challenges needed to safely reach production.

In the wake of identifying evaluation challenges around Atari games, researchers have proposed specialized simulators to benchmark specific properties such as generalization capabilities (CoinRun (Cobbe et al., 2018)) or agent safety (e.g. DeepMind safety gridworlds (Leike et al., 2017)). Bsuite (Osband et al.) is a novel benchmark for analyzing agent behavior which varies random seeds to score agent performance but which does not distinguish different generalization modes or randomized tasks.

To interface open source algorithm implementations, practitioners have adopted OpenAI gym interfaces in novel simulators. For example, Siemens introduced a benchmark for industrial control tasks (Hein et al., 2017). Others have built gym-bridges and new problem scenarios on top of existing simulators such as the ns3 networking simulator (ns3-gym (Gawlowicz & Zubow, 2018)). In systems-RL, Park is a benchmarking framework providing a common interface to a variety of problems in query processing, networking, or scheduling (Mao et al., 2019a). Park takes a first step towards shared task-design but does not explicitly include randomization and distinct blackbox and generalization modes.

## 6 Conclusion

We introduced Wield, a new tool towards systematic task construction and model evaluation for applied RL. Wield decouples application-specific protocols from task representation. We also introduced progressive randomization, an instructive evaluation protocol and classification scheme to analyze model capabilities under different randomization assumptions. Our assessment highlights the exciting recent progress in systems-RL, while demonstrating the substantial cost of delineating model capabilities.
ACKNOWLEDGMENTS

Michael Schaarschmidt is supported by a Google PhD Fellowship. We are also grateful for receiving research credits from Google Cloud.

REFERENCES

Addanki, R., Venkatakrishnan, S. B., Gupta, S., Mao, H., and Alizadeh, M. Placeto: Learning generalizable device placement algorithms for distributed machine learning. CoRR, abs/1906.08879, 2019. URL http://arxiv.org/abs/1906.08879.

Brockman, G., Cheung, V., Pettersson, L., Schneider, J., Schulman, J., Tang, J., and Zaremba, W. Openai gym. CoRR, abs/1606.01540, 2016. URL http://arxiv.org/abs/1606.01540.

Cobbe, K., Klimov, O., Hesse, C., Kim, T., and Schulman, J. Quantifying generalization in reinforcement learning. arXiv preprint arXiv:1812.02341, 2018.

Coleman, C., Kang, D., Narayanan, D., Nardi, L., Zhao, T., Zhang, J., Bailis, P., Olukotun, K., Ré, C., and Zaharia, M. Analysis of dawnbench, a time-to-accuracy machine learning performance benchmark. CoRR, abs/1806.01427, 2018. URL http://arxiv.org/abs/1806.01427.

Dhariwal, P., Hesse, C., Klimov, O., Nichol, A., Plappert, M., Radford, A., Schulman, J., Sidor, S., Wu, Y., and Zhokhov, P. Openai baselines. https://github.com/openai/baselines, 2017.

Dulac-Arnold, G., Evans, R., van Hasselt, H., Sunehag, P., Lillicrap, T., Hunt, J., Mann, T., Weber, T., Degris, T., and Coppin, B. Deep reinforcement learning in large discrete action spaces. 2015.

Dulac-Arnold, G., Mankowitz, D. J., and Hester, T. Challenges of real-world reinforcement learning. CoRR, abs/1904.12901, 2019. URL http://arxiv.org/abs/1904.12901.

Gawlowicz, P. and Zubow, A. ns3-gym: Extending openai gym for networking research. CoRR, abs/1810.03943, 2018. URL http://arxiv.org/abs/1810.03943.

Guu, K., Pasupat, P., Liu, E. Z., and Liang, P. From language to programs: Bridging reinforcement learning and maximum marginal likelihood. In Barzilay, R. and Kan, M. (eds.), Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics, ACL 2017, Vancouver, Canada, July 30 - August 4, Volume 1: Long Papers, pp. 1051–1062. Association for Computational Linguistics, 2017. doi: 10.18653/v1/P17-1097.

Hein, D., Depeweg, S., Tokic, M., Udluft, S., Hentschel, A., Runkler, T. A., and Sterzing, V. A benchmark environment motivated by industrial control problems. arXiv preprint arXiv:1709.09480, 2017.

Henderson, P., Islam, R., Bachman, P., Pineau, J., Precup, D., and Meger, D. Deep reinforcement learning that matters. CoRR, abs/1709.06560, 2017. URL http://arxiv.org/abs/1709.06560.

Ilyas, A., Engstrom, L., Santurkar, S., Tsipras, D., Janoos, F., Rudolph, L., and Madry, A. Are deep policy gradient algorithms truly policy gradient algorithms? CoRR, abs/1811.02553, 2018. URL http://arxiv.org/abs/1811.02553.

Jay, N., Rotman, N. H., Godfrey, B., Schapira, M., and Tamar, A. A deep reinforcement learning perspective on internet congestion control. In Chaudhuri, K. and Salakhutdinov, R. (eds.), Proceedings of the 36th International Conference on Machine Learning, ICML 2019, 9-15 June 2019, Long Beach, California, USA, volume 97 of Proceedings of Machine Learning Research, pp. 3050–3059. PMLR, 2019. URL http://proceedings.mlr.press/v97/jay19a.html.

Johnson, M., Hofmann, K., Hutton, T., and Bignell, D. The malmo platform for artificial intelligence experimentation. In IJCAI, pp. 4246–4247, 2016.

Juliani, A., Berges, V.-P., Vckay, E., Gao, Y., Henry, H., Mattar, M., and Lange, D. Unity: A general platform for intelligent agents. arXiv preprint arXiv:1809.02627, 2018.

Kansky, K., Silver, T., Mély, D. A., Eldawy, M., Lázaro-Gredilla, M., Lou, X., Dorfman, N., Sidor, S., Phoenix, S., and George, D. Schema networks: Zero-shot transfer with a generative causal model of intuitive physics. 2017.

Leike, J., Martic, M., Krakovna, V., Ortega, P. A., Everitt, T., Lefrancq, A., Orseau, L., and Legg, S. AI safety gridworlds. CoRR, abs/1711.09883, 2017. URL http://arxiv.org/abs/1711.09883.

Leis, V., Gubichev, A., Mirchev, A., Boncz, P., Kemper, A., and Neumann, T. How good are query optimizers, really? Proceedings of the VLDB Endowment, 9(3):204–215, 2015.

Liang, E., Liaw, R., Nishihara, R., Moritz, P., Fox, R., Goldberg, K., Gonzalez, J., Jordan, M., and Stoica, I. Rllib: Abstractions for distributed reinforcement learning. In International Conference on Machine Learning, pp. 3059–3068, 2018.

Liang, E., Zhu, H., Jin, X., and Stoica, I. Neural packet classification. CoRR, abs/1902.10319, 2019. URL http://arxiv.org/abs/1902.10319.
Mania, H., Guy, A., and Recht, B. Simple random search provides a competitive approach to reinforcement learning. *CoRR*, abs/1803.07055, 2018. URL http://arxiv.org/abs/1803.07055.

Mao, H., Schwarzkopf, M., Venkatakrishnan, S. B., Meng, Z., and Alizadeh, M. Learning scheduling algorithms for data processing clusters. *arXiv preprint arXiv:1810.01963*, 2018.

Mao, H., Negi, P., Narayan, A., Wang, H., Yang, J., Wang, H., Marcus, R., Addanki, R., Khani, M., He, S., et al. Park: An open platform for learning augmented computer systems. *Reinforcement Learning for Real Life Workshop, ICML*, 2019a. URL https://github.com/park-project/park.

Mao, H., Schwarzkopf, M., Venkatakrishnan, S. B., Meng, Z., and Alizadeh, M. Learning scheduling algorithms for data processing clusters. In Wu, J. and Hall, W. (eds.), *Proceedings of the ACM Special Interest Group on Data Communication, SIGCOMM 2019*, Beijing, China, August 19-23, 2019, pp. 270–288. ACM, 2019b. doi: 10.1145/3341302.3342080.

Marcus, R. and Papaemmanouil, O. Deep reinforcement learning for join order enumeration. In Bordawekar, R. and Shmueli, O. (eds.), *Proceedings of the First International Workshop on Exploiting Artificial Intelligence Techniques for Data Management, aiDM@SIGMOD 2018*, Houston, TX, USA, June 10, 2018, pp. 3:1–3:4. ACM, 2018. doi: 10.1145/3211954.3211957.

Marcus, R., Negi, P., Mao, H., Zhang, C., Alizadeh, M., Kraska, T., Papaemmanouil, O., and Tabul, N. Neo: A Learned Query Optimizer. *arXiv e-prints*, art. arXiv:1904.03711, Apr 2019.

Mirhoseini, A., Pham, H., Le, Q. V., Steiner, B., Larsen, R., Zhou, Y., Kumar, N., Norouzi, M., Bengio, S., and Dean, J. Device placement optimization with reinforcement learning. *arXiv preprint arXiv:1706.04972*, 2017.

Mirhoseini, A., Goldie, A., Pham, H., Steiner, B., Le, Q. V., and Dean, J. Hierarchical planning for device placement. 2018. URL https://openreview.net/pdf?id=Hkc-TeZOW.

OpenAI. OpenAI Five DOTA. Website, June 2018. URL https://blog.openai.com/openai-five/.

Ortiz, J., Balazinska, M., Gehrke, J., and Keerthi, S. S. Learning state representations for query optimization with deep reinforcement learning. In Schelter, S., Seufert, S., and Kumar, A. (eds.), *Proceedings of the Second Workshop on Data Management for End-To-End Machine Learning, DEEM@SIGMOD 2018*, Houston, TX, USA, June 15, 2018, pp. 4:1–4:4. ACM, 2018. doi: 10.1145/3209889.3209890.

Osband, I., Doron, Y., Hessel, M., Aslanides, J., Sezener, E., Saraiva, A., McKinney, K., Lattimore, T., Szepesvari, C., Singh, S., Roy, B. V., Sutton, R., Silver, D., and Hasselt, H. V. Behaviour suite for reinforcement learning.

Paliwal, A., Gimeno, F., Nair, V., Li, Y., Lubin, M., Kohli, P., and Vinyals, O. REGAL: transfer learning for fast optimization of computation graphs. *CoRR*, abs/1905.02494, 2019. URL http://arxiv.org/abs/1905.02494.

Schurschmidt, M., Mika, S., Fricke, K., and Yoneki, E. RL-graph: Modular Computation Graphs for Deep Reinforcement Learning. In *Proceedings of the 2nd Conference on Systems and Machine Learning (SysML)*, April 2019.

Schulman, J., Abbeel, P., and Chen, X. Equivalence between policy gradients and soft q-learning.

Silver, D., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., Lanctot, M., Sifre, L., Kumaran, D., Graepel, T., Lillicrap, T., Simonyan, K., and Hassabis, D. A general reinforcement learning algorithm that masters chess, shogi, and go through self-play. *Science*, 362(6419):1140–1144, 2018. ISSN 0036-8075. doi: 10.1126/science.aar6404. URL https://science.sciencemag.org/content/362/6419/1140.

Sutton, R. S., Precup, D., and Singh, S. P. Between mdps and semi-mdps: A framework for temporal abstraction in reinforcement learning. *Artif. Intell.*, 112(1-2):181–211, 1999. doi: 10.1016/S0004-3702(99)00052-1.

Tesauro, G., Jong, N. K., Das, R., and Bennani, M. N. A hybrid reinforcement learning approach to autonomic resource allocation. In *Proceedings of the 2006 IEEE International Conference on Autonomic Computing*, ICAC ’06, pp. 65–73, Washington, DC, USA, 2006. IEEE Computer Society. ISBN 1-4244-0175-5. doi: 10.1109/ICAC.2006.1662383. URL http://dx.doi.org/10.1109/ICAC.2006.1662383.

Valadarsky, A., Schapira, M., Shahaf, D., and Tamar, A. A machine learning approach to routing. *arXiv preprint arXiv:1708.03074*, 2017.
A EXPERIMENT HYPERPARAMETERS

We list all hyperparameters used in Wield’s hierarchical placer. Table 7 lists grouper parameters.

Table 7. Training parameters used for Wield’s grouper agent.

| Parameter            | Value          |
|----------------------|----------------|
| clip ratio           | 0.25           |
| discount             | 1.0            |
| GAE λ                | 1.0            |
| batch size           | num ops in graph |
| update iterations per batch | 10          |
| num groups           | 20             |
| policy layer size    | 32             |
| num hidden layers    | 2              |
| layer activation     | tanh           |
| value function       | same as policy |
| optimizer            | Adam           |
| learning rate        | [0.01, 0.00001]|
| linear decay steps   | 600            |

Table 8 lists placer parameters. The embedding implementation is a faithful implementation of Addanki et al.’s description (Addanki et al., 2019). The main difference is that their work relies on manual grouping. When we tested initially random groupings produced by the grouper, neighborhood embeddings diverged due to large neighborhood sets. We hence used tanh activations instead of rectified linear units, and configured the grouper to a more aggressive learning rate schedule.

Table 8. Training parameters used for Wield’s placer agent.

| Parameter                        | Value          |
|----------------------------------|----------------|
| clip ratio                       | 0.2            |
| discount                         | 1.0            |
| GAE λ                            | 1.0            |
| batch size                       | 10             |
| update iterations per batch      | 1              |
| layer size (all layers)          | num groups     |
| num in neighbors                 | 5              |
| num out neighbors                | 5              |
| neighborhood aggregation rounds  | 10             |
| layer activation                 | tanh           |
| value function                   | same as policy |
| optimizer                        | Adam           |
| learning rate                    | [0.0003, 0.0001]|
| linear decay steps               | 1000           |
| groups placed per graph evaluation | 10            |

The NMT architecture was taken from Google’s NMT implementation\(^2\). We used the ‘normed_bahdanau’ attention layer with the ‘gnmt_v2’ architecture.

\(^2\)https://github.com/tensorflow/nmt