
Evaluating the Robustness of Collaborative Agents

Paul Knott*

University of Nottingham

paul.knott@nottingham.ac.uk

Micah Carroll

UC Berkeley

mdc@berkeley.edu

Sam Devlin

Microsoft Research

Kamil Ciosek

Microsoft Research

Katja Hofmann

Microsoft Research

A. D. Dragan

UC Berkeley

Rohin Shah

UC Berkeley

Abstract

In order for agents trained by deep reinforcement learning to work alongside humans in realistic settings, we will need to ensure that the agents are *robust*. Since the real world is very diverse, and human behavior often changes in response to agent deployment, the agent will likely encounter novel situations that have never been seen during training. This results in an evaluation challenge: if we cannot rely on the average training or validation reward as a metric, then how can we effectively evaluate robustness? We take inspiration from the practice of *unit testing* in software engineering. Specifically, we suggest that when designing AI agents that collaborate with humans, designers should search for potential edge cases in *possible partner behavior* and *possible states encountered*, and write tests which check that the behavior of the agent in these edge cases is reasonable. We apply this methodology to build a suite of unit tests for the Overcooked-AI environment, and use this test suite to evaluate three proposals for improving robustness. We find that the test suite provides significant insight into the effects of these proposals that were generally not revealed by looking solely at the average validation reward.

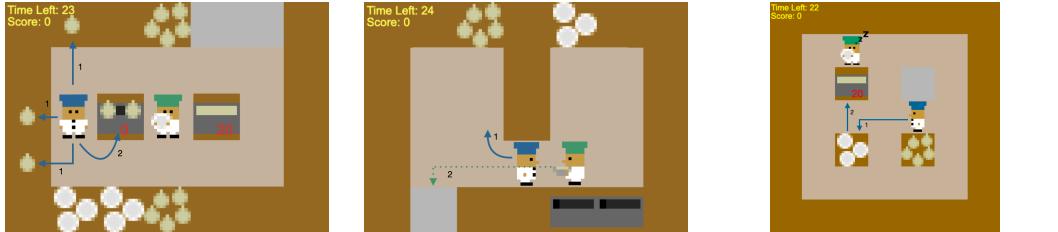
1 Introduction

Deep reinforcement learning (deep RL) has been used very successfully to train agents that perform very well in the average case [4, 30, 24]. However, deployment of an agent in the real world will often have stringent robustness requirements [15, 8]. Due to the diversity of the real world, a deployed agent will encounter many situations and human behaviors that were never seen during development. Recent work has shown failures of policies learned from deep RL in simulation [10], suggesting that we do not get such robustness by default.

We are particularly interested in building agents that *collaborate* with humans in order to help them accomplish their goals, a setting that has recently been tackled with deep RL [11, 5, 13]. There are several approaches we could use to improve the robustness of such agents. For example, rather than training a deep RL agent to play with a single human model trained with behavior cloning [5], we can potentially improve 1) the *quality* of the human model by incorporating Theory of Mind (ToM) [7], 2) the *human model diversity* by using a population of human models, and 3) the *state diversity* by, e.g., initializing from states visited in human-human gameplay.

However, it is hard to *evaluate* these ideas. Since we care about robustness to novel situations, the average reward on the training distribution is not a sufficient metric. We would like to know the true

* Alternative email: knottquantum@gmail.com



(a) Example *state robustness* unit test. Since its partner (green) is already holding a plate, the agent (blue) is in the best position to get an onion for the left pot, regardless of how its partner plays.

(b) Example *agent robustness* unit test. The agent’s partner (green) stubbornly insists on delivering the soup in its hands, and so the agent (blue) should get out of the way.

(c) Example *agent & memory robustness* unit test. The fact that the agent’s partner (green) is AFK, and thus that the agent (blue) should pick up and deliver the soup themselves, is only possible to detect through memory.

Figure 1: Example unit tests for evaluating robustness of agents trained to play Overcooked. Note that in these cases (and all other unit tests), the correct behavior for the evaluated agent is unambiguous – any truly robust agent should be able to successfully complete the task the test is checking for.

distribution over performance during deployment, but this is never available because the deployment of the agent itself changes the distribution of inputs it receives [20]. Even pairing the learned agent with people in a user study is not usually representative of the performance at deployment time, since in many realistic domains there is a long tail of unusual edge cases that would likely not be seen for any reasonable sample size. However, at deployment time, if the user base is large enough, the likelihood of eventually running into one of these edge cases is greatly increased, and could have large consequences depending on the extent of the failure and the deployment setting.

Software engineering faces a similar challenge, in which incorrect programs often give the right output on the vast majority of possible inputs, but fail on a few specific edge cases. The most widespread technique to combat this issue is *testing*, in which the programmer explicitly writes down potential edge cases and their expected outputs. While unit testing does not guarantee correctness, even automatically generated unit tests can find many issues [22].

In this paper, we develop a methodology for applying the testing paradigm to human-AI collaboration, and we demonstrate its utility on the two-player Overcooked environment [5, 9], in which players control chefs in a kitchen to cook and serve dishes. A good test suite should test potential edge cases in the *states* that the agent should be able to handle (e.g. what if a couple of plates were accidentally left on the kitchen’s counters?), and the *partners* that the agent should be able to play with (e.g. what if the partner were to stay put for a while because they are thinking or away from their keyboard?). Additional examples in Overcooked are shown in Figure 1.

The benefit of the test suite is that it can give us more information than we could get by observing the reward alone. We demonstrate such benefits within Overcooked. First, we confirm the canonical wisdom that agents trained via vanilla deep RL are not robust. We then evaluate the three proposals above on improving state diversity, human model diversity, and human model quality. Our results show that the test suite provides significant insight into robustness that is not very correlated with the information provided by the average validation reward: for example, we find that improving state diversity does improve robustness as measured by our test suite, but this comes at the cost of a *decrease* in average validation reward.

A given test suite will never be final: there will likely always be more edge cases to include. As different types of failure modes are found or imagined, they can be added into the test suite. We do not claim that unit testing allows us to achieve perfect robustness: rather, we see them as a major improvement over the current status quo of evaluating reward on random rollouts (which only tests the edge cases that are encountered randomly). Current deep RL agents are clearly not robust – none of the agents we tested scored above 65% in Overcooked – suggesting that our approach can serve as a useful metric for the foreseeable future. Once agents routinely get high scores on the tests, we should consider how to use additional human effort to create even better robustness metrics.

2 Related work

Evaluation strategies. Many disciplines must contend with the challenges of real-world deployment. The field of *safety engineering* in particular develops best practices for building systems that can operate safely and robustly in the real world, and pays particular attention to the role of human factors [14]. Our process of building test suites can be thought of as an exercise in explicitly mapping out possible variation in human factors in order to increase our confidence in the agents’ ability to respond to this variation.

Within human-AI collaboration, one evaluation strategy is to search *adversarially* for situations in which the agent fails [29]. However, in collaborative environments it is unclear how to design such an adversary. Giving the adversary arbitrary control over the partner behavior is far too strong a requirement: for example, in Overcooked the adversary could simply stand at the soup delivery location, preventing soups from getting delivered and guaranteeing that no reward is achieved.

Our work continues an increasing trend in machine learning in which simple, easily calculated metrics are insufficient to capture performance, and we must instead evaluate results based on human judgment [25, 1, 33].

Human-AI collaboration. We focus on building agents that can collaborate with humans by pairing the agents with different human models during training. Recent work has proposed two other options. *Other play* [11] makes the assumption that the agent should be invariant to permutations of symmetries of the game, in order to enable zero-shot collaboration (i.e. collaboration without any human data). However, this will not necessarily result in optimal behavior given specific collaborators. Alternatively, human data can be used to discover which of several Nash equilibria humans play, and bias an agent trained in self-play to learn the same equilibrium [13, 28]. However, these techniques must make strong assumptions about human gameplay, which may not hold in more complex settings.

Training robust agents. Much recent work has focused on creating agents that are robust to variation in the environment, especially for sim-to-real transfer. One common technique is *domain randomization*, where some aspect of the environment is varied randomly in order to learn a policy that can robustly succeed regardless of that aspect [2, 17, 32, 27]. Our populations can be thought of as a domain randomization technique, where the randomization is done over the parameters of the ToM or the initialization of the BC model parameters. Populations of agents have in fact been used to improve average case reward, especially in zero-sum settings [30, 12]. Typically, the agents in the population are all trained in self-play with each other. While this is effective in competitive environments, it tends to converge to overly specific Nash equilibria in collaborative environments [5]. Another common approach to achieve robustness is to train the agent with a constrained *adversary* that attempts to sabotage the agent [18, 6, 16, 23, 29]. Unfortunately, it is unclear how to apply such a technique for human-AI collaboration: an unconstrained adversarial human model would often be able to prevent any reward from being accumulated, while a constrained model may not generalize to real humans.

Overcooked-AI. Recent work [31, 5] has used environments based on the popular video game *Overcooked* [9], in which players control chefs in a kitchen to cook and serve dishes. We use the Overcooked-AI environment implementation from Carroll et al. [5], in which the only objects are onions, dishes, and soups. Players work together to place 3 onions in a pot, leave them to cook for 20 timesteps, put the resulting soup in a dish, and serve it. All players are given reward (20 points) exclusively when a soup is served.

3 Preliminaries

We introduce the formal setting. Note that we denote the space of distributions over X as $\Delta(X)$.

3.1 Multiagent MDPs

An n -player Markov Decision Process $\mathcal{M} = \langle \mathcal{S}, \{\mathcal{A}^{(i)}\}, \mathcal{T}, \mathcal{P}, \gamma, R \rangle$ takes as given a set of states \mathcal{S} and a set of actions $\mathcal{A}^{(i)}$ for each player. Given a state and actions for each player, the *transition function* $\mathcal{T} : \mathcal{S} \times \mathcal{A}^{(1)} \times \dots \times \mathcal{A}^{(n)} \rightarrow \Delta(\mathcal{S})$ specifies the distribution over next states. The initial state distribution is given by $\mathcal{P} : \Delta(\mathcal{S})$, while the discount is given by γ . The shared objective is defined by the *reward function* $R : \mathcal{S} \times \mathcal{A}^{(1)} \times \dots \times \mathcal{A}^{(n)} \rightarrow \mathbb{R}$.

Unlike the case with a regular MDP, in a multiagent MDP the history of interaction can be important, in order for each agent to learn about the other agents. A *history* $h_t : (\mathcal{S} \times \mathcal{A}^{(1)} \times \dots \times \mathcal{A}^{(n)})^t$ encodes the past interaction in the environment. Agent i 's *policy* $\pi^{(i)} : H \times \mathcal{S} \rightarrow \Delta(\mathcal{A}^{(i)})$ specifies how the i th agent selects actions, and is allowed to depend on history.

Given policies $\{\pi^{(i)}\}$ for all agents, a *trajectory* τ can be sampled as follows: sample s_0 from \mathcal{P} , and then repeatedly sample actions $\{a_t^{(i)}\}$ from $\{\pi^{(i)}\}$ and sample the next state s_{t+1} from \mathcal{T} . The shared objective is to maximize the expected reward, which is given by $\mathbb{E}_\tau \left[\sum_t \gamma^t R(s_t, a_t^{(1)}, \dots, a_t^{(n)}) \right]$.

If we are given every policy except for the j th policy $\{\pi^{(i)} : i \neq j\}$, then from agent j 's perspective, the other agents can be thought of as “part of the environment”. In particular, we can reduce the problem of finding the optimal $\pi^{(j)}$ to a single-agent *partially observable* MDP, in which the other policies are a hidden variable of the state. In this POMDP, the transition function \mathcal{T}' samples actions from all the other policies and passes them to \mathcal{T} , and the observations include both the original state as well as the actions taken by all of the other agents.

3.2 Human-AI collaboration via deep RL

In human-AI collaboration, we are given a two-player MDP \mathcal{M} , in which the human is one of the players and the AI agent is another. Given just this, it is unclear what the agent should do: the optimal policy for the agent depends heavily on the human's policy, which the agent has no control over. If the human policy $\pi^{(H)}$ is known, then we can simply embed the policy in the environment (as in Section 3.1) and use reinforcement learning to learn an optimal policy for the agent. Thus, one approach would be to *learn* a human model $\hat{\pi}^{(H)}$, embed the model into the environment, and then use deep RL to find an optimal policy for that model. If $\hat{\pi}^{(H)}$ is sufficiently close to $\pi^{(H)}$, the agent policy will play well with the real human as well [5].

4 Unit tests for robustness

Accurately evaluating robustness is challenging. The typical method of evaluation is to report the average reward on the training distribution, but such an approach does not reveal the low-probability failure modes that are key to evaluating the robustness of an agent to the novel situations it can encounter during deployment.

Even playing our agents with real humans and recording the average reward is not representative of the performance at *deployment*, since in many realistic domains there is a long tail of unusual edge cases that would likely not be seen for any reasonable sample size. In preliminary experiments on Overcooked where we evaluated robustness by playing with real human partners, we found that the noise and differences in human behavior made it very difficult to extract signal out of those tests without huge sample sizes, which motivated us to seek a different evaluation paradigm. Our approach is to place the trained agents in a variety of hand-designed *unit tests*.

Identifying the relevant inputs. We first identify the set of inputs in which we should look for edge cases. Human-AI collaboration is specified by a multiplayer MDP $\mathcal{M} = \langle \mathcal{S}, \{\mathcal{A}^{(i)}\}, \mathcal{T}, \mathcal{P}, \gamma, R \rangle$ and a human model π ; edge cases for the trained agent could be found in \mathcal{S} and in π . As a result, we develop unit tests that check for edge cases in \mathcal{S} (which we call *state robustness tests*) and for edge cases in π (which we call *agent robustness tests*). Intuitively, a test measures *robustness to states* when the success criterion of the test would be approximately independent of the partner model π . In other words, if the partner model of the test was changed, the success criterion would stay the same (see Figure 1a for an example). In contrast, a test measures *robustness to agents* when the success criterion *does* depend on the type of partner. For improved granularity, we subdivide agent robustness tests into those that require history (to identify the type of partner) and those that do not (where the expected behavior is robust to multiple partner types). We name these two categories as “agent robustness” (e.g. Figure 1b) and “agent robustness with memory” (e.g. Figure 1c).

Given this categorization, our methodology is as follows:

1. Identify qualitative situations for each test category;
2. Concretize each situation to a unit test;

3. Improve test coverage by observing and probing the trained agents.

Identifying qualitative situations. For each of these categories, we brainstorm different possible qualitatively distinct examples of the property under investigation. For example, for state robustness, we can think about states in which soups have been cooked but not delivered, states in which there are many objects on the counters, states in which the agent is holding a useless item, etc. For agent robustness, we might consider cases where the partner is an expert, or where the partner has just started to learn the game, or where the partner has a preference for delivering soups, or where the partner has temporarily stopped playing.

Concretizing to a unit test. We then take each of these qualitative situations and aim to distill it down into one or two concrete instances in which it would be obvious to a human how the agent should behave (given enough time to plan). The combination of the concrete situation and the expected correct behavior (within some time limit) then forms one of our unit tests. For example, the test in Figure 1a checks whether the agent picks up and places an onion when it is in the best position to do so, while the test in Figure 1b checks whether the agent can cope with a stubborn agent that insists upon delivering the soup it is holding.

Unlike the case in software engineering, where we would normally only have one or two tests for each qualitative setting, we create several instantiations of each qualitative setting with slightly different initial conditions, such as the locations for the counter objects, the agent, and the agent’s partner. This is necessary because (unlike typical computer programs) the behavior of a learned agent can vary significantly based on these “irrelevant” factors, and so by testing against multiple variations we can significantly reduce the variance of our evaluation.

In some cases, it is challenging to distill the qualitative situation into a concrete one where the correct behavior is unambiguous. For the sake of simplicity, we discard such situations (which we found were relatively rare), since we found that the remaining unit tests were more than sufficient to evaluate current deep RL agents. As agents become more robust, it may become necessary to include such situations in our unit tests as well, potentially by specifying a concrete situation and counting the test as passed if the agent does one of a number of “reasonable” behaviors.

Improving test coverage. Of course, many environments (including Overcooked) are sufficiently complex that it is nearly impossible to come up with a complete set of edge cases to test agents on. To improve coverage of possible edge cases, it is also useful to look at the behavior of real agents, to inspire new potential edge cases. Concretely, we train a number of deep RL agents (using the different training methods discussed below in Section 5). We then watch some games between the agents and directly play several games with them (probing at off-distribution parts of the state space, and behaving in ways that would be uncommon for humans). From this anecdotal data, we extend our list of qualitative settings that a robust agent should successfully navigate, and convert them into unit tests using the methodology above.

Validating the resulting tests. As a sanity check, we took the parameterized Theory of Mind agent from Section 5.2 and set its parameters to make it maximally capable. Since this agent is based on a human-designed planning process, we expect that compared to the deep RL agents it will be much more robust, but potentially worse on average-case performance. We expected it to perform well on the state and agent robustness tests, but not on the memory test, since the agent does not have any state and thus cannot depend on memory². The agent achieved an 86% score on state robustness tests, and a 95% score on agent robustness tests, which are quite high in absolute terms and much higher than the deep RL agents (as we will see in the experiments). It also achieved a 75% score on agent robustness with memory tests, despite not having any state, which is also higher than deep RL agents (which do have state, as they use recurrent neural nets). This suggests that the tests are capturing “reasonable behavior” in a wide variety of situations.

We iterated on this methodology for creating unit tests using the layouts from Carroll et al. [5]. This of course runs the risk that our methodology is overfit to these layouts, and so we designed four new layouts, illustrated in Figure 2, and created a suite of unit tests for these layouts based on the same approach. The full set of unit tests for these layouts is given in Table 1.

²Technically, the ToM agent does use history for one purpose: when it has been “stuck” in a state for some time, it will take random actions to get unstuck. However, this should not be expected to significantly improve performance on memory robustness tests.

Table 1: The suite of unit tests for robustness. The acronym in brackets at the beginning of each *test setup* refers to the test category: SR = State robustness; AR = Agent robustness; A+MR = Agent & memory robustness. R refers to the agent being tested (the “robot”), and H refers to the partner agent in the test (the “human”).

| <i>Test setup</i> | <i>R’s response for success</i> |
|---|----------------------------------|
| (SR) Soup on counter that should be picked up & delivered | Pick up and deliver the soup |
| (SR) Dish or onion on counter, which R requires (Fig. 1a) | Pick up said object |
| (SR) R is holding the wrong object, given the circumstances | Drop object onto the counter |
| (SR) R is placed in an unlikely location in the circumstances | Adapt & keep playing as normal |
| (SR) There’s an unlikely number of objects on the counters | Play as normal (Fig. 1a) |
| (AR) R requires specific object; H blocks relevant dispenser | Pick up said object from counter |
| (AR) R holding same object as H, but H is closer to using it | Drop their object onto counter |
| (AR) R is blocking the path of H | Move out the way (see Fig. 1b) |
| (A+MR) H remains stationary (see Fig. 1c) | Adapt and take over H’s tasks |
| (A+MR) H takes random actions | Adapt and take over H’s tasks |

Note that even a perfect score on these tests does *not* imply that the tested agent is robust. Since the tests do not exhaustively cover all possible situations, there may still remain failure modes that were not tested for. However, we find that existing agents get fairly low scores on our test suite, suggesting that the test suite can serve as a useful metric for the foreseeable future.

Our unit tests, which are reusable and extensible, are available at https://github.com/HumanCompatibleAI/human_ai_robustness.

5 Robustness through quality and diversity

We trained our deep RL agents using Proximal Policy Optimization (PPO) [21]; we utilised the open-source implementation by Carroll et al. [5], following their same procedure unless explicitly stated otherwise. One key difference is that we use recurrent neural networks throughout our experiments. For further details of our PPO training, see Appendix E.

The starting point we consider for achieving greater robustness is to partner the deep RL agent, during training, with a human model trained by behavior cloning (BC) on human-human gameplay data (see Section 5.1 below). However, there are a number of problems with such an approach. First, BC only produces a human-like policy on the distribution it was trained on, and can suffer from compounding errors when it moves off-distribution [19]. In any such area, the learned policy will probably not collaborate well with real humans. Second, not all humans are the same: an agent must be robust to variation across humans if it is to perform well with an arbitrary human; training with a single human model will not incentivize this. These two problems will be addressed in Sections 5.2 and 5.3.

5.1 Human model via behavioral cloning

Behavior cloning learns a policy from expert demonstrations by directly learning a mapping from observations to actions using supervised learning [3]. In our case this is a traditional classification task, since we have a discrete action space. Our model takes an encoding of the state as input, and outputs a probability distribution over actions; the model is then trained using the standard cross-entropy loss function.

For human data collection and behavior cloning training we utilised the open-source implementation by Carroll et al. [5], following their same procedure unless explicitly stated otherwise. As described in Section 6.1, in this paper we used both pre-existing Overcooked layouts from Carroll et al. [5], and created four new layouts (Figure 2). For the previously existing layouts, we used the pre-existing open-sourced data and behavior cloning models. Instead, for the new layouts of Figure 2 we collected data from Amazon Mechanical Turk. We then removed trajectories that were under-performing based on a set of heuristics to determine engagement of both players in the game. After removal, we had 28 joint human-human trajectories for Bottleneck environment, 31 for Room, 28 for Center Objects, and 31 for Center Pots.



Figure 2: **Experiment layouts.** From left to right: *Bottleneck* requires frequent travel through a small corridor that only one agent can pass through at a time, leading to challenging motion coordination problems. *Room* is a large empty space, in which gameplay is fairly easy. In *Center Objects*, the most efficient route for moving objects around is through the center, but typically only one agent can use it at a time, thus requiring coordination. *Center Pots* make it easy for agents to interact with pots, and so the primary challenge is in how to navigate to objects around the pots.

We divide the joint trajectories into two groups randomly under the constraint that the two groups have similar average reward. We then use the two sets of human trajectories to train two sets of behavior cloning models. The first set is used to create BC populations, and the second is used to make up half of the population used to calculate Validation Reward. The hyperparameters used are reported in Table 2 in the Appendix. The unit test scores of the BCs themselves are reported in Appendix C.

5.2 Improving the quality of human models: Theory of Mind

One idea to solve the first problem introduced above – that the BC only produces a human-like policy on the distribution it was trained on – is to improve the quality of our human models across the entire state space. We test one instantiation of this idea: building a parameterized Theory of Mind (ToM) model, i.e. a human model that is structured to reason about other agents’ mental states [7]. In particular, in this setting we try to make our ToM agent as human-like as possible – we imbue it with biases we expect humans to have (e.g. not be an optimal planner). By design, any ToM agent will behave sensibly on all parts of the state space (as long as its parameters are within reasonable ranges), and so will not suffer greatly from distribution shift.

At every timestep, our Theory of Mind agent enumerates a list of tasks to be completed (such as “put an onion in the pot” or “deliver the soup”), and decides which task it will pursue. It then chooses a low-level action in pursuit of the goal. We call the former the *strategic* choice and the latter the *motion* choice.

At the strategic level, the parameters control how many tasks forward the agent looks ahead; whether the agent takes into account its partner when planning; whether or not to infer its partner’s current subtask from its actions; and whether or not to stick to the plan it made on the previous timestep.

At the motion level, the parameters control the probability with which the agent takes a noop action (mimicking the slowness of human players); whether or not the agent takes some time to “think” after finishing a subtask; the compliance of the agent during motion planning; whether or not to take the partner into account when planning a path; the probability that the human takes a suboptimal action (via a temperature parameter for a Boltzmann rational model [34]); and the probability of taking a random action. For more information, see Appendix D.

5.3 Diversity of human models: Populations

In addressing the second problem mentioned above we consider a simple approach to make our deep RL agents robust to variation in humans: train them with a variety of human models. More specifically, by training the agent with a *population* of human models which encompass a diversity of possible strategic behaviors, we can ensure that the resulting agent is able to adapt to any particular human it plays with. On each episode we randomly pick a human model from the population, then our deep RL agent is trained by collaborating with this human model.

However, in collaborative games, it is not immediately clear how to build such a population. It is not just a matter of making the population arbitrarily diverse: a population of random agents is certainly diverse, but is unlikely to lead to an agent that can collaborate well with humans unless

the population is extremely large. Nor can we train adversarially, as has been proposed in other contexts [18, 6, 16, 23], as the adversary would be far too powerful: in many layouts the adversary could simply block the delivery location, ensuring that the agent can never get reward, thus preventing training entirely. This suggests that the agents in the population need to themselves be human models.

Population type. We use populations of BC models, ToM models, or a mixture of the two.

Recurrence. In order to get good results with a population, it should be possible for the agent to learn within an episode which “type” of human it is playing with. This is much easier to do when given access to the history of actions that the human has taken in the past. In order to capture this history we use recurrent neural networks for all our deep RL training procedures.

5.4 Quality of deep RL: leveraging human-human gameplay

Since the previous two approaches focused on the human model, they can be thought of as “fixing the objective”: any method that tries to learn a best response to a human model would benefit from such approaches, not just deep RL. However, in practice we have found that the policies learned by deep RL are themselves not very robust: for example, they may fail when irrelevant dishes are placed on counters³. We hypothesize that this lack of robustness arises because once the trained policy has found a good strategy for getting reward, it is not incentivized to explore other areas of the state space, and so it fails if the test time agent acts differently than expected and brings it to an unseen state.

While this issue is not unique to human-AI collaboration, we do have a potential solution that is not normally available with deep RL: we have access to human-human gameplay data. One would think that if we make the trained policy robust to the *states* in the human-human gameplay data, that could improve its robustness with real humans. We can accomplish this by sampling the initial state of each episode from the human-human data during deep RL training, a technique we call “diverse starts” below. One thing to note is that the effectiveness of this procedure is not necessarily obvious: a case could be made that if human-AI gameplay has a sufficiently different distribution of states than human-human gameplay, diverse starts could be increasing robustness to the wrong states.

6 Experiments

Our primary goal with the experiments was to evaluate how useful the test suite is in surfacing information about trained agents ((H1) in Section 6.2).

6.1 Experimental setup

Our experiments used the four layouts illustrated in Figure 2; these layouts were designed to capture a range of strategic and coordination challenges. As mentioned above, each unit test has multiple possible initial states. To evaluate the success criterion, we perform 50 evaluation rollouts on the unit tests, and take the average proportion of successes as the score.

We report both the average score on unit tests, as well as the validation reward for each agent, computed as the average reward the agent obtains when partnered with human models from a suite of 20 validation agents (comprised of 10 held out BC and 10 ToM agents). This validation reward is not meant as a measure of the robustness of the agents to novel situations, but rather as a baseline to compare the unit test suite against. The held-out BC agents were trained on a different subset of the human data, and for the ToM agents we chose the parameters by hand to ensure sufficient diversity in the resulting behavior.

Manipulated factors. In our experiments, we manipulate several different factors:

1. Whether or not we use diverse starts (Section 5.4).
2. The size of the population we train with. (Note that population size 1 corresponds to the setting of Carroll et al. [5] in which there is no population.)
3. The composition of agents within the population: BC, ToM, or an equal mix of both.
4. How the ToM models in a population are chosen.

³This can also be seen with the policies trained by Carroll et al. [5] at their demo website.

When using multiple BC agents in a population, all agents are trained on the same human-human gameplay data,⁴ but with different seeds. The BC agent chosen for training with a single BC is the best performing out of the 20 BC agents trained. When using multiple ToM agents on the other hand, there are two variants. In the first variant (manual), as with the ToM validation agents, we chose the parameters by hand to ensure sufficient diversity in the resulting behavior (whilst ensuring no overlap with the validation agents – see appendix for details). In the second variant (random), the parameters are chosen randomly from the set of possible legal values.

6.2 Hypotheses

Our first hypothesis (**H1**) was that the unit tests and the validation reward would supply different information, and will therefore often not be in agreement. In terms of how the different training regimes would impact robustness, our hypotheses – which we will evaluate using the unit tests – were: (**H2**) using diverse starts would increase state robustness, (**H3**) using ToM would increase state robustness relative to BC (as it would better approximate human behaviour in a larger portion of the state space than BC), (**H4**) training with populations of human models rather than a single human model would increase robustness, particularly *robustness to agents*, and (**H5**) training with a mixture of BC and ToM agents would perform better than each individually (for equal-sized populations).

6.3 Results

In this section the experimental results we report and analyze are averaged across the four layouts of Figure 2 (see appendix A for results broken down by layout).

Diverse starts. The first thing to notice from Figure 3 is that for diverse starts, the unit tests and the validation reward suggest *opposite* conclusions, in agreement with **H1** (robustness-reward difference): we see a notable increase in robustness when using diverse starts, for both state and agent robustness tests, but in contrast the validation reward either stays the same (for BC models) or decreases (for ToM models). It appears that using diverse starts confers robustness at the cost of validation reward, an effect that has also been observed with adversarial examples in image classification [26].

On the axis of robustness, we see that **H2** (diverse starts) is supported since diverse starts produces an increase in unit test performance across all but one test categories and model types.

Effect of population vs single. From Figure 3, we see that when using BC models, the use of populations leads to improvements across the board for both unit tests and validation reward. However, when using ToM models, we see the opposite effect: the use of populations typically has no effect or hurts performance, again for both unit tests and validation reward. This convergence of unit tests and validation reward is somewhat in opposition to **H1** (robustness-reward difference), though we note that it is to be expected that some changes will lead to changes in the general ability of the agent and so have similar effects on unit tests and validation reward.

We are not sure what to make of the reversal of the effect for BC and ToM models, and view it as weakly in opposition to **H4** (populations). One possibility is that since the ToM models are significantly more diverse than the BC models (which only differ based on the initial random seed), a population of ToM models is so diverse that the learning problem becomes too challenging.

To explore this further, we trained an agent with each agent of the manual ToM population individually, reported in Figure 4, which shows a large variety of robustness and reward across the models, supporting the explanation that too much diversity is a bad thing. It is plausible that this could be fixed with increased model capacity and training time. Nonetheless, we still find the result surprising, and would like to investigate this phenomenon in more detail in future work.

Figure 4 also shows the importance of selecting a good ToM agent if only training with a single agent (which we can do, by using the MLE estimate for the ToM parameters from the human-human data). We also see that the validation reward and the unit tests can disagree significantly, supporting **H1** (robustness-reward difference).

Single BC vs single ToM. From Figure 3, we see that when comparing agents trained with a single BC and a single ToM, using the ToM agent can lead to an improvement in state robustness (supporting

⁴Note that an alternative method would be to train one BC for *each* human in the human-human data, but we found that it was not feasible to get enough gameplay data for each human to make an effective BC model.

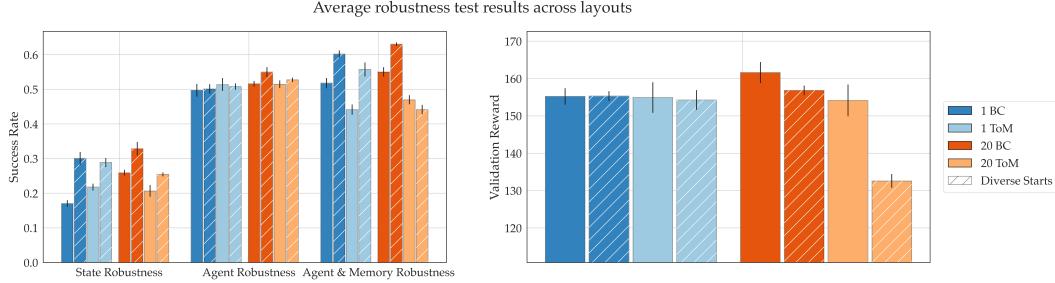


Figure 3: Comparison of robustness scores and validation reward for PPO agents trained with and without diverse starts, with and without a population, and using ToM vs. BC agents. All scores are averaged across the 4 layouts in Figure 2.

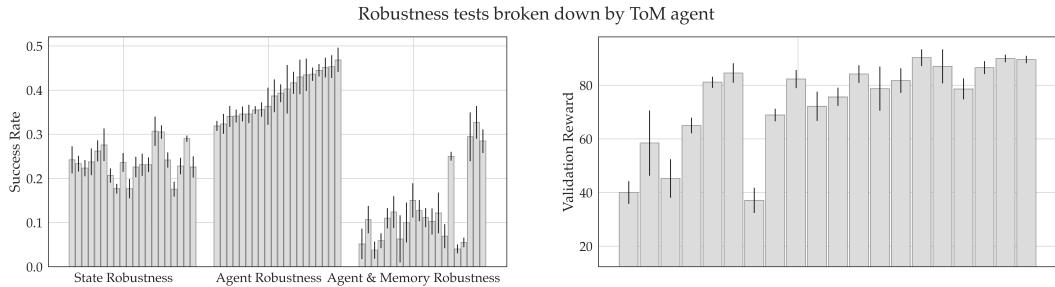


Figure 4: Comparison of robustness scores and validation reward when training with a single ToM agent, for each agent that comprises the ToM population of size 20 (which is used in other experiments). This is performed only on the Counter Circuit layout (see Appendix B for details). The agents are ordered by increasing agent robustness score. The validation reward and the robustness tests often are substantially different from one another, supporting **H1**.

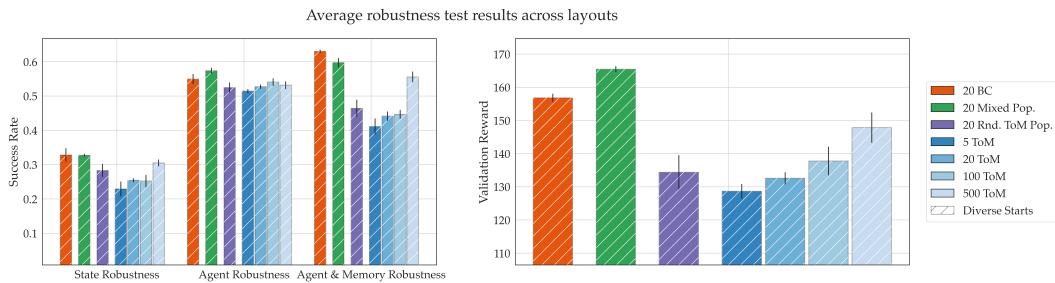


Figure 5: Comparison of robustness scores and validation reward for PPO agents trained with populations of 20 BCs, a mixed population of 10 BCs and 10 ToM agents, a population of 20 random ToM agents, and populations of various sizes of manually selected ToMs. All experiments were performed with diverse starts, and all scores are averaged across the 4 layouts in Figure 2.

H3 (ToM)), but using diverse starts effectively nullifies this improvement. We speculate that this is because the additional robustness conferred by training with the ToM agent is a subset of that conferred by diverse starts, and so once diverse starts is used ToM no longer provides any benefit.

On all other metrics, including validation reward, we see that a single ToM performs comparably to or worse than the corresponding BC agent. This suggests that by using a ToM agent, we are increasing the number of states on which the agent can perform reasonably, but decreasing the agent’s “average” capability. We would not be able to make such inferences from just the validation reward, where BC and ToM are nearly identical, again supporting **H1** (robustness-reward difference).

Looking across all of the settings (instead of just the single BC and single ToM setting), we find that the agents trained with ToM partners tend to perform worse across the board relative to agents trained with BC partners. As before, we speculate that this is because the ToMs add too much diversity to the training, such that the learning problem becomes too challenging.

Mixed population. Figure 5 illustrates the robustness and reward across different methods of constructing the population of agents. We see that according to the unit tests, using a mixed BC and ToM population is approximately on par with the population of BC agents (contradicting **H5** (mixed-population)). However, the mixed population leads to a significant increase in validation reward, most likely because the validation population is itself a mixture of BC and ToM agents. Once again we see that our two evaluation metrics provide different insight into the method, in accordance with **H1** (robustness-reward difference).

The unit tests also suggest that the mixed population has better agent robustness but worse memory robustness than the population of BCs. However, there is no clear reason why this would be the case, and the differences are fairly small.

Random ToM population and Effect of population size. Interestingly, the randomly chosen ToM population actually outperforms choosing parameters manually to maximise ToM diversity. However, any population of ToM agents is significantly outperformed by using a BC or mixed population. Figure 5 shows that all metrics increase (albeit relatively slowly) by increasing the population size, up to the maximum size we tested (500).

7 Limitations and future work

Summary. In this work, we propose the use of testing to evaluate the robustness of collaborative agents. These unit tests search for potential edge cases in possible partner behavior and possible states encountered, in order to reveal when the trained agent will be robust to novel situations during deployment. Using these unit tests, we evaluated three natural proposals for improving robustness in human-AI collaboration via deep RL: improving human model quality through a parameterized Theory of Mind (ToM) agent, training with a diverse population of collaborative agents, and initializing from states visited in human-human gameplay. The unit tests revealed information about the method that was relatively uncorrelated with the average reward metric: sometimes unit test robustness increased at the cost of average reward (as with initialization from states in human-human gameplay), sometimes different types of robustness were affected while average reward stayed the same (as with the use of a single ToM agent as the partner), sometimes unit test robustness remained the same while average reward was improved (as with the use of a mixture of BC and ToM agents), and sometimes unit test robustness and average reward were in sync (as with the effects of using a population). While our best results used a population of 10 BC and 10 ToM agents, we emphasize that our primary finding is that our unit test suite provides information that may not be available by simply considering validation reward, and our conclusions for specific techniques are more preliminary.

Future work on evaluating robustness. One challenge we encountered was how to evaluate robustness in cases where the correct behavior is ambiguous. As an example in Overcooked, what would be the correct behaviour for the blue player in Figure 1a, if the green player was holding nothing (instead of holding a dish)? Fetching either a dish or an onion can be correct, depending on the gamaplay style and preferences of the other player. Future work could address how to create reliable unit tests to measure robustness in these ambiguous scenarios: for example, perhaps a few “reasonable” behaviors could be identified, and we could check whether the agent executes one of these “reasonable” behaviors. Beyond this, a natural extension of our work is to expand the use of unit tests to other domains besides human-AI collaboration.

Future work on *improving* robustness. As mentioned above, we would like to see more work further evaluating our proposals, especially in the case of populations where we found a positive effect for BC but a negative one for ToM. There are also several additional avenues for improving robustness. While in this work we improved the quality and diversity of the partner agent, all of our agents were still trained for a specific layout. Arguably, for true robustness (especially robustness to states), we need diversity in *layouts* as well. An alternative direction for future work is to explore meta learning, in order to train the agent to *adapt* online to the specific human partner it is playing with. This could lead to significant gains, especially on agent robustness with memory.

Acknowledgments

This work was partially supported by Open Philanthropy, Microsoft and NSF CAREER. PK acknowledges support from the Royal Commission for the Exhibition of 1851, and the Foundational Questions Institute (FQXi) under the Intelligence in the Physical World Programme (Grant No. FQXiRFP-IPW-1907). We thank researchers at the Center for Human-Compatible AI and the InterACT lab for helpful discussion and feedback.

References

- [1] Daniel Adiwardana, Minh-Thang Luong, David R So, Jamie Hall, Noah Fiedel, Romal Thoppilan, Zi Yang, Apoorv Kulshreshtha, Gaurav Nemadé, Yifeng Lu, et al. Towards a human-like open-domain chatbot. *arXiv preprint arXiv:2001.09977*, 2020.
- [2] Ilge Akkaya, Marcin Andrychowicz, Maciek Chociej, Mateusz Litwin, Bob McGrew, Arthur Petron, Alex Paino, Matthias Plappert, Glenn Powell, Raphael Ribas, Jonas Schneider, Nikolas Tezak, Jerry Tworek, Peter Welinder, Lilian Weng, Qiming Yuan, Wojciech Zaremba, and Lei Zhang. Solving rubik’s cube with a robot hand. *arXiv preprint*, 2019.
- [3] Michael Bain and Claude Sammut. A framework for behavioural cloning. In *Machine Intelligence 15*, pages 103–129, 1995.
- [4] Christopher Berner, Greg Brockman, Brooke Chan, Vicki Cheung, Przemysław Dębiak, Christy Dennison, David Farhi, Quirin Fischer, Shariq Hashme, Chris Hesse, et al. Dota 2 with large scale deep reinforcement learning. *arXiv preprint arXiv:1912.06680*, 2019.
- [5] Micah Carroll, Rohin Shah, Mark K Ho, Tom Griffiths, Sanjit Seshia, Pieter Abbeel, and Anca Dragan. On the utility of learning about humans for human-AI coordination. In *Advances in Neural Information Processing Systems*, pages 5175–5186, 2019.
- [6] Behdad Chalaki, Logan Beaver, Ben Remer, Kathy Jang, Eugene Vinitsky, Alexandre Bayen, and Andreas A Malikopoulos. Zero-shot autonomous vehicle policy transfer: From simulation to real-world via adversarial learning. *arXiv preprint arXiv:1903.05252*, 2019.
- [7] Rohan Choudhury, Gokul Swamy, Dylan Hadfield-Menell, and Anca D Dragan. On the utility of model learning in hri. In *2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*, pages 317–325. IEEE, 2019.
- [8] A Gasparik, C Gamble, and J Gao. Safety-first ai for autonomous data centre cooling and industrial control. *DeepMind Blog*, 2018.
- [9] Ghost Town Games. Overcooked, 2016. <https://store.steampowered.com/app/448510/Overcooked/>.
- [10] Adam Gleave, Michael Dennis, Cody Wild, Neel Kant, Sergey Levine, and Stuart Russell. Adversarial policies: Attacking deep reinforcement learning. *arXiv preprint arXiv:1905.10615*, 2019.
- [11] Hu, Hengyuan and Lerer, Adam and Peysakhovich, Alex and Foerster, Jakob. "Other-Play" for Zero-Shot Coordination. *arXiv preprint arXiv:2003.02979*, 2020.

- [12] Max Jaderberg, Wojciech M Czarnecki, Iain Dunning, Luke Marris, Guy Lever, Antonio Garcia Castaneda, Charles Beattie, Neil C Rabinowitz, Ari S Morcos, Avraham Ruderman, et al. Human-level performance in 3d multiplayer games with population-based reinforcement learning. *Science*, 364(6443):859–865, 2019.
- [13] Adam Lerer and Alexander Peysakhovich. Learning existing social conventions via observationally augmented self-play. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, pages 107–114, 2019.
- [14] Nancy G Leveson. *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.
- [15] Andrew J Lohn. Estimating the brittleness of ai: Safety integrity levels and the need for testing out-of-distribution performance. *arXiv preprint arXiv:2009.00802*, 2020.
- [16] Anay Pattanaik, Zhenyi Tang, Shuijing Liu, Gautham Bommannan, and Girish Chowdhary. Robust deep reinforcement learning with adversarial attacks. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, pages 2040–2042. International Foundation for Autonomous Agents and Multiagent Systems, 2018.
- [17] Xue Bin Peng, Marcin Andrychowicz, Wojciech Zaremba, and Pieter Abbeel. Sim-to-real transfer of robotic control with dynamics randomization. In *2018 IEEE international conference on robotics and automation (ICRA)*, pages 1–8. IEEE, 2018.
- [18] Lerrel Pinto, James Davidson, Rahul Sukthankar, and Abhinav Gupta. Robust adversarial reinforcement learning. In *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pages 2817–2826. JMLR. org, 2017.
- [19] Stéphane Ross, Geoffrey Gordon, and Drew Bagnell. A reduction of imitation learning and structured prediction to no-regret online learning. In *Proceedings of the fourteenth international conference on artificial intelligence and statistics*, pages 627–635, 2011.
- [20] Roland W. Scholz and Claudia R. Binder. The paradigm of human-environment systems. 2003. doi: 10.3929/ETHZ-A-004520890. URL <http://hdl.handle.net/20.500.11850/147357>.
- [21] John Schulman, Filip Wolski, Prafulla Dhariwal, Alec Radford, and Oleg Klimov. Proximal policy optimization algorithms. *arXiv preprint arXiv:1707.06347*, 2017.
- [22] S. Shamshiri, R. Just, J. M. Rojas, G. Fraser, P. McMinn, and A. Arcuri. Do automatically generated unit tests find real faults? an empirical study of effectiveness and challenges (t). In *2015 30th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pages 201–211, 2015.
- [23] Macheng Shen and Jonathan P How. Robust opponent modeling via adversarial ensemble reinforcement learning in asymmetric imperfect-information games. *arXiv preprint arXiv:1909.08735*, 2019.
- [24] David Silver, Julian Schrittwieser, Karen Simonyan, Ioannis Antonoglou, Aja Huang, Arthur Guez, Thomas Hubert, Lucas Baker, Matthew Lai, Adrian Bolton, et al. Mastering the game of go without human knowledge. *Nature*, 550(7676):354–359, 2017.
- [25] Nisan Stiennon, Long Ouyang, Jeff Wu, Daniel M Ziegler, Ryan Lowe, Chelsea Voss, Alec Radford, Dario Amodei, and Paul Christiano. Learning to summarize from human feedback. *arXiv preprint arXiv:2009.01325*, 2020.
- [26] Dong Su, Huan Zhang, Hongge Chen, Jinfeng Yi, Pin-Yu Chen, and Yupeng Gao. Is robustness the cost of accuracy?—a comprehensive study on the robustness of 18 deep image classification models. In *Proceedings of the European Conference on Computer Vision (ECCV)*, pages 631–648, 2018.
- [27] Jie Tan, Tingnan Zhang, Erwin Coumans, Atil Iscen, Yunfei Bai, Danijar Hafner, Steven Bohez, and Vincent Vanhoucke. Sim-to-real: Learning agile locomotion for quadruped robots. *arXiv preprint arXiv:1804.10332*, 2018.

- [28] Mycal Tucker, Yilun Zhou, and Julie Shah. Adversarially guided self-play for adopting social conventions. *arXiv preprint arXiv:2001.05994*, 2020.
- [29] Jonathan Uesato, Ananya Kumar, Csaba Szepesvari, Tom Erez, Avraham Ruderman, Keith Anderson, Nicolas Heess, Pushmeet Kohli, et al. Rigorous agent evaluation: An adversarial approach to uncover catastrophic failures. *arXiv preprint arXiv:1812.01647*, 2018.
- [30] Oriol Vinyals, Igor Babuschkin, Junyoung Chung, Michael Mathieu, Max Jaderberg, Wojciek Czarnecki, Andrew Dudzik, Aja Huang, Petko Georgiev, Richard Powell, Timo Ewalds, Dan Horgan, Manuel Kroiss, Ivo Danihelka, John Agapiou, Junhyuk Oh, Valentin Dalibard, David Choi, Laurent Sifre, Yury Sulsky, Sasha Vezhnevets, James Molloy, Trevor Cai, David Budden, Tom Paine, Caglar Gulcehre, Ziyu Wang, Tobias Pfaff, Toby Pohlen, Dani Yogatama, Julia Cohen, Katrina McKinney, Oliver Smith, Tom Schaul, Timothy Lillicrap, Chris Apps, Koray Kavukcuoglu, Demis Hassabis, and David Silver. AlphaStar: Mastering the Real-Time Strategy Game StarCraft II. <https://deepmind.com/blog/alphastar-mastering-real-time-strategy-game-starcraft-ii/>, 2019.
- [31] Rose E Wang, Sarah A Wu, James A Evans, Joshua B Tenenbaum, David C Parkes, and Max Kleiman-Weiner. Too many cooks: Coordinating multi-agent collaboration through inverse planning. *arXiv preprint arXiv:2003.11778*, 2020.
- [32] Wenhao Yu, Jie Tan, C Karen Liu, and Greg Turk. Preparing for the unknown: Learning a universal policy with online system identification. *arXiv preprint arXiv:1702.02453*, 2017.
- [33] Sharon Zhou, Mitchell Gordon, Ranjay Krishna, Austin Narcomey, Li F Fei-Fei, and Michael Bernstein. Hype: A benchmark for human eye perceptual evaluation of generative models. In *Advances in Neural Information Processing Systems*, pages 3449–3461, 2019.
- [34] Brian D Ziebart. Modeling purposeful adaptive behavior with the principle of maximum causal entropy. 2010.

A Experimental results split by layout

In Figures 3 and 5 we only reported the experimental results averaged across the four layouts of Figure 2. In Figures 6-9 we report our experimental results broken down by layout.

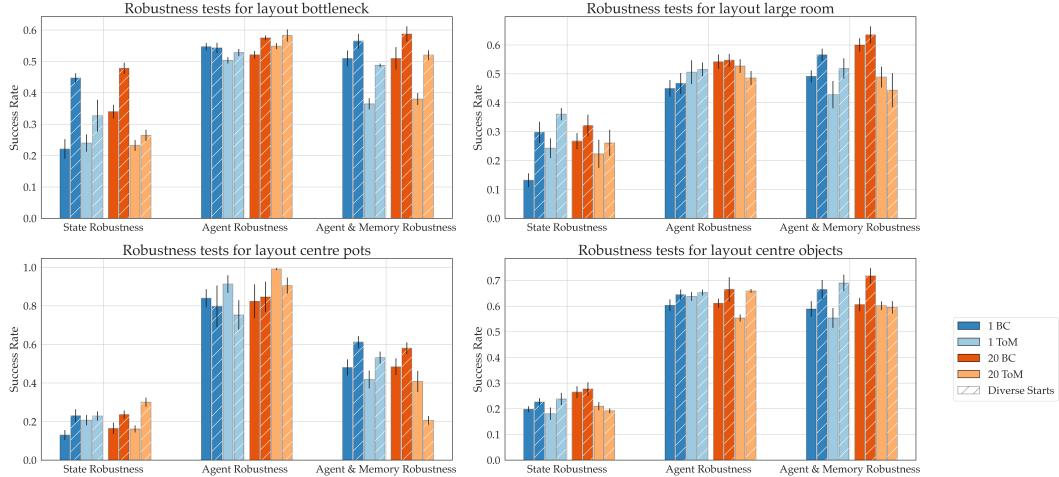


Figure 6: Figure 3 (left sub-graph) broken down by layout.

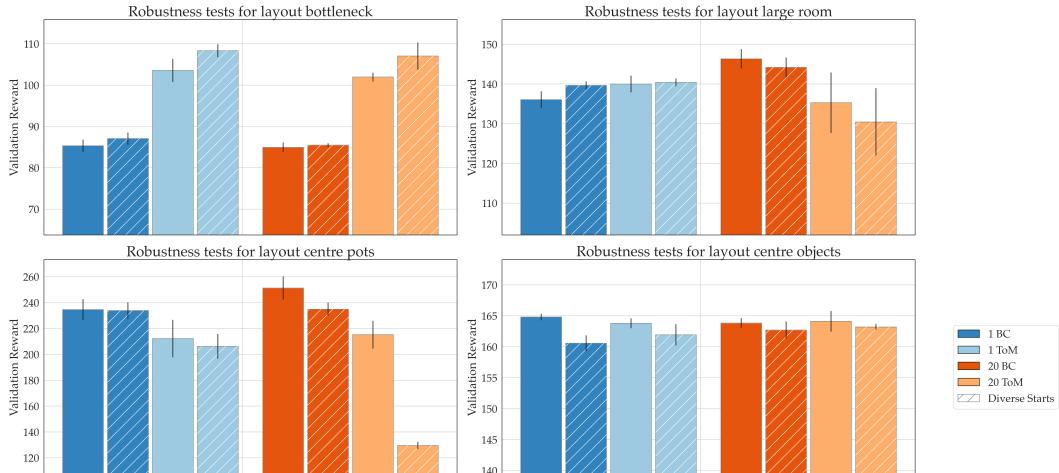


Figure 7: Figure 3 (right sub-graph) broken down by layout.

We will now highlight some notable exceptions to the conclusions drawn from looking only at the results that were averaged across layouts. When averaged over layouts, in Figure 3 we saw an increase in robustness when using diverse starts. One notable exception to this is when playing with the ToM agent on Center Pots for the agent robustness tests: here the diverse starts *decreased* the robustness. For the state robustness tests, when averaged over layouts there was no significant difference between 1 BC and 1 ToM (when both had diverse starts). When this is broken down by layouts in Figures 6 and 7, we see that in Center Objects and Large Room, playing with the ToM was a little more robust than with the BC; whereas for Bottleneck, playing with the ToM was *less* robust. Finally, if we focus just on using ToM populations, we see that, with diverse starts, some noticeable outliers occur for Center Pots. Here, for both the agent robustness with memory tests and the validation reward, the population of 20 ToMs performs significantly worse than the alternatives.

Moving on to Figure 5, we saw that the mixed population receives significantly more validation reward than the BC population. However, we see from Figure 9 that this reward improvement is solely down to the strong performance of the mixed population on Bottleneck. Instead comparing the randomly chosen ToM population with choosing the parameters manually, we saw in Figure 5

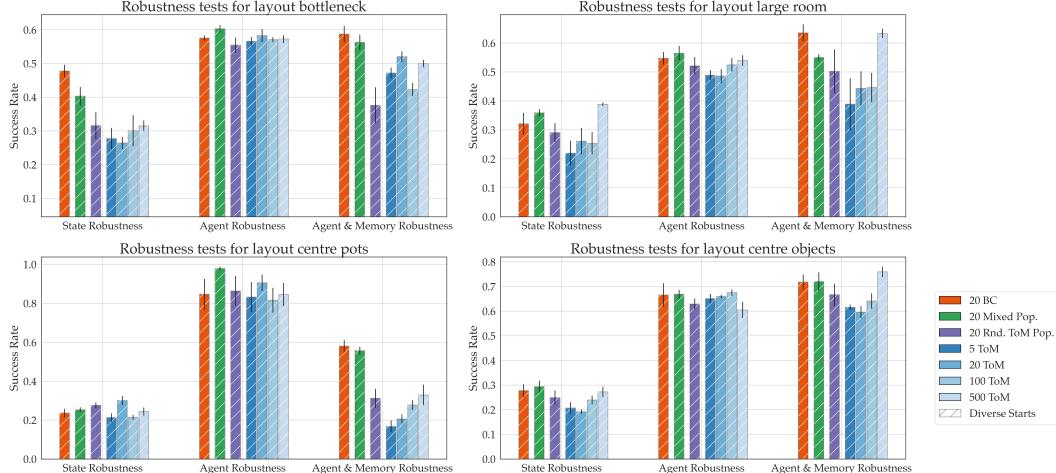


Figure 8: Figure 5 (left sub-graph) broken down by layout.

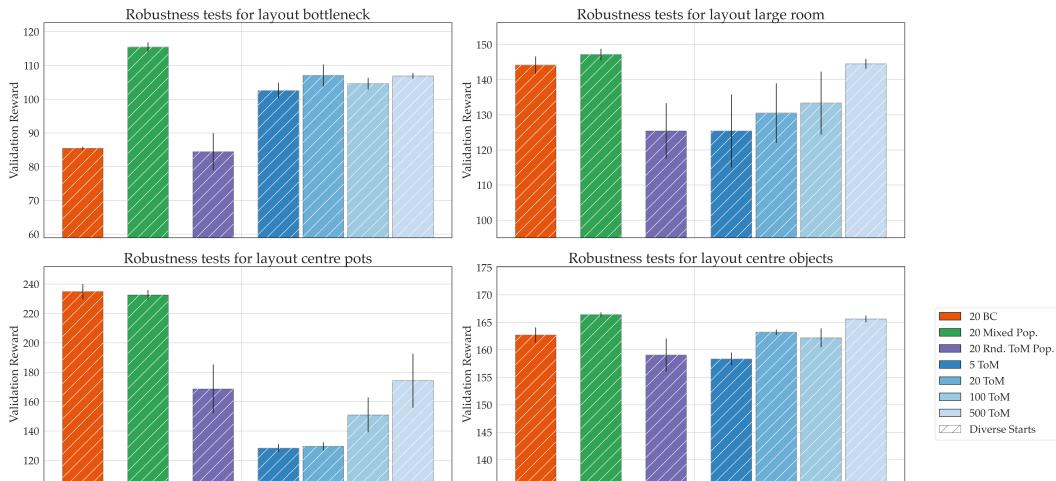


Figure 9: Figure 5 (right sub-graph) broken down by layout.

that randomly-chosen outperforms manually-chosen. There are several minor exceptions to this in Figures 8 and 9, and two strong exceptions, in which manually-chosen does significantly better. The latter both occur on Bottleneck, for both the validation reward and the agent robustness with memory tests. Our final comparison in the main text was between the different sizes of ToM populations. In Figure 5 we saw that all metrics increased gradually when we increase the population size. Broken down by layout in Figures 8 and 9, again there are several minor exceptions to this, in particular on Center Pots.

Future work will analyse these anomalies seen in Figures 6-9, and their implications.

B Preliminary experimental results for original Overcooked layouts

Before running the whole suite of experiments described in Section 6.1 for the 4 layouts of Figure 2, we did a preliminary experimental investigation on two of the original layouts from Carroll et al. [5]. The results of the experiments we conducted – which are just a subset of the final ones – are in Figures 10 and 11.

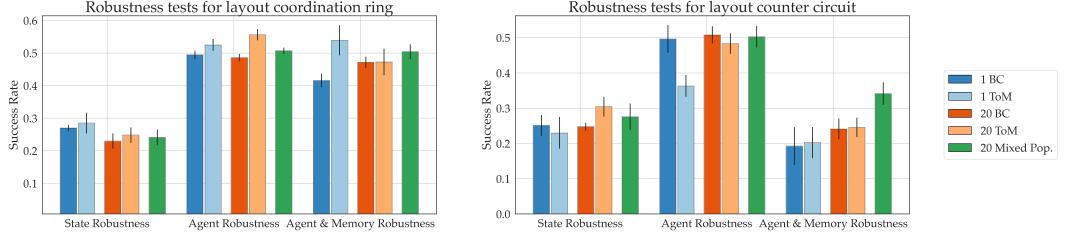


Figure 10: Robustness tests evaluation for two of the original Overcooked layouts.

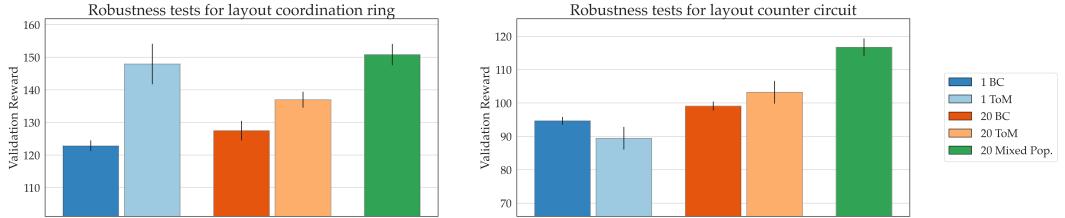


Figure 11: Validation Reward evaluation for two of the original Overcooked layouts.

| Behavior cloning hyperparameters | | | | |
|----------------------------------|------------|------|-------------|-------------|
| Parameter | Bottleneck | Room | Center Obj. | Center Pots |
| Learning Rate | 1e-3 | 1e-3 | 1e-3 | 8e-4 |
| # Epochs | 130 | 90 | 80 | 180 |
| Adam ϵ | 1e-8 | 1e-8 | 1e-8 | 1e-8 |

Table 2: Hyperparameters for behavior cloning across the 4 new layouts.

C Behavior cloning unit test scores

We evaluated the best performing BC for each layout on our suite of unit tests (the ‘best performing’ was found by partnering each BC with every other BC, then finding the average reward over partners). Averaged over layouts, these BCs achieved the following success rates: *state robustness tests*: 0.21; *agent robustness tests*: 0.45; and *agent robustness with memory tests*: 0.29. Note that these BCs performed far worse than the ToM agents (the ToM scores are reported in Appendix D). The average validation score across layouts was 71.8.

D ToM agents

As introduced in the main text, at every timestep our Theory of Mind agent enumerates a list of tasks to be completed (such as “put an onion in the pot” or “deliver the soup”), and decides which task it will pursue. It then chooses a low-level action in pursuit of the goal. We call the former the strategic choice and the latter the motion choice.

Strategic choice

Probability of being greedy: If this is set to 1, then the agent will always do the highest-priority task on the list (or the lowest cost task if there are two equal-priority tasks). In the other extreme, if this is 0 then the agent will always jointly plan the best team strategy in order to complete the first N tasks on the list (the value of N is a separate parameter, “lookahead horizon”, discussed below). For example, if N=2 then the agent will determine the lowest-cost strategy for both agents executing all tasks on the list up to priority 2.

Lookahead horizon: This is the value of N discussed above: i.e. how far to look ahead down the task list when jointly planning.

Probability of factoring in the other agent’s current perceived actions: We determine the other agent’s current perceived action by asking 1) are they already carrying an object that can be used, and if not

then 2) is there a (useful) object in their 180 degree field of view that they could pick up. If either of these is true, then we assume that the other agent will complete the associated task, then we cross this task off the task list. We then plan either greedily or jointly, using the revised task list, according to the value of the *probability of being greedy* parameter.

Retain-goals: At each timestep the agent will keep its current goal with this probability. Here “goal” refers to the sub-task level, i.e. dropping an object; picking up an object; using an object. Each time a sub-task is completed then the agent always re-plans. If retain-goals is zero then at every timestep the agent re-plans.

| PPO hyperparameters | | | | |
|---------------------|------------|-----------|-------------|-------------|
| Parameter | Bottleneck | Room | Center Obj. | Center Pots |
| Learning rate | 5e-4 | 5e-4 | 1e-3 | 1e-3 |
| SP anneal. horizon | [3e6,1e7] | [3e6,7e6] | [3e6,1e7] | [3e6,1.3e7] |

Table 3: Hyperparameters for PPO across the 4 new layouts.

Motion choice

Prob-pausing: This is the probability of pausing in a given timestep. This is needed because human players often “pause” quite a lot simply because they can’t press the keys / think fast enough to make a move on every single timestep.

Thinking-prob: After achieving a sub-task (e.g. picking up an onion) the agent waits to “think”. This simulates the fact that humans will often spend more time pausing to think after they have achieved a sub-task.

Compliance: In games with limited space to move, players will often bump into each other. When this happens, compliance is the probability that the agent will take an avoiding action (e.g. step backwards).

Path-teamwork: Once the agent has a goal, it can choose different paths to reach the goal. Here, path-teamwork is the probability of factoring in the other player when finding the best path (i.e. they use a joint motion planner).

Rationality coefficient: Humans will not always take an action along the shortest path to a goal. The ToM takes a sub-optimal action with a Boltzmann rational probability. Setting to 0 means they always take random actions; setting to ∞ means they always take the lowest cost path (in practice setting to 20 is large enough for the latter).

Prob random action: At each timestep the agent will take one of the 6 random actions with this probability.

Choosing the ToM parameters manually: Our intention here was to make ToM agents that behave like human players, whilst ensuring as much diversity as possible when creating populations of ToM agents. We first made a population of ToMs by fitting all parameters to human-human data, using a metropolis sampling algorithm. For population size 1, we used the maximum likelihood set of parameters for the ToM agent. However, for larger populations, this sampling procedure resulted in a quite uniform population. So, to increase the diversity, we instead decided to manually selected ToM parameters for the population, building from the fitted parameters. Throughout this process, we played several games with different ToM agents to ensure they still had human-like gameplay and skill levels. The values of *prob-pausing* were selected in the range of ± 0.2 from the values from the metropolis sampling (which varied across layout, but were 0.6 on average across layouts). *Lookahead horizon* ranged between 1 and 4; *Rationality coefficient* ranged from 1 and 20; *Thinking-prob* ranged from 0 to 0.4; and *Prob random action* was set to 0. For all other parameters, the full allowed range of $[0, 1]$ was used, and as all such values lead to human-like behavior.

ToM agents’ unit test scores: We evaluated the maximum likelihood ToM agent for each layout on our suite of unit tests. Averaged over layouts, these ToM agents achieved the following success rates: *state robustness tests*: 0.81; *agent robustness tests*: 0.74; and *agent robustness with memory tests*: 0.53. The average validation score across layouts was 77.7.

E PPO agent training

For PPO we built off of the open-source implementation by Carroll et al. [5], following their same procedure unless explicitly stated otherwise. One difference we would like to highlight is that we use recurrent neural networks throughout our experiments. We started with their hyperparameter choices as initial values, then tuned each parameter, focusing largely on total batch size, learning rate, reward shaping horizon (as in [5], we augment the reward with a denser reward signal to facilitate convergence), and SP annealing horizon, varying only 1 or 2 hyperparameters together each time, until we converged on the hyperparameters reported below.

We parameterize the policy with a convolutional neural network with 3 convolutional layers, each of which has 25 filters, followed by 3 fully-connected layers with hidden size 64. Hyperparameters common to all layouts are: entropy coefficient (= 0.1), gamma (= 0.99), lambda (= 0.98), clipping (= 0.05), maximum gradient norm (= 0.1), gradient steps per minibatch per PPO step (= 8), # minibatches (= 15), learning rate annealing (= 1.5), reward shaping horizon (= 2e7), total batch size (= 48000). Layout-specific hyperparameters are reported in Table 3. We ran the PPO training until the training reward failed to improve for 5e6 timesteps.

All PPO agents are trained on 5 seeds. Each seed is then evaluated with our suite of unit tests and with the validation population. All graphs report results with mean and standard errors across seeds.

Our PPO agents were trained, 8 runs in parallel, on an Azure cloud instance with 4x NVIDIA Tesla K80 cards and 24x Intel Xeon E5-2690 v3 processors. Each run took 16-48 hours, with the large variability due to the fact that we trained until convergence of the reward.