Robust Anytime Learning of Markov Decision Processes *

Marnix Suilen
Department of Software Science
Radboud University
Nijmegen, The Netherlands

Thiago D. Simão
Department of Software Science
Radboud University
Nijmegen, The Netherlands

David Parker
Department of Computer Science
University of Oxford
Oxford, United Kingdom

Nils Jansen
Department of Software Science
Radboud University
Nijmegen, The Netherlands

Abstract

Markov decision processes (MDPs) are formal models commonly used in sequential decision-making. MDPs capture the stochasticity that may arise, for instance, from imprecise actuators via probabilities in the transition function. However, in data-driven applications, deriving precise probabilities from (limited) data introduces statistical errors that may lead to unexpected or undesirable outcomes. Uncertain MDPs (uMDPs) do not require precise probabilities but instead use so-called uncertainty sets in the transitions, accounting for such limited data. Tools from the formal verification community efficiently compute robust policies that provably adhere to formal specifications, like safety constraints, under the worst-case instance in the uncertainty set. We continuously learn the transition probabilities of an MDP in a robust anytime-learning approach that combines a dedicated Bayesian inference scheme with the computation of robust policies. In particular, our method (1) approximates probabilities as intervals, (2) adapts to new data that may be inconsistent with an intermediate model, and (3) may be stopped at any time to compute a robust policy on the uMDP that faithfully captures the data so far. Furthermore, our method is capable of adapting to changes in the environment. We show the effectiveness of our approach and compare it to robust policies computed on uMDPs learned by the UCRL2 reinforcement learning algorithm in an experimental evaluation on several benchmarks.

1 Introduction

Sequential decision-making in realistic scenarios is inherently subject to uncertainty, commonly captured via probabilities. *Markov decision processes* (MDPs) are the standard model to reason about such decision-making problems [Puterman, 1994, Bertsekas, 2005]. Safety-critical scenarios require assessments of correctness which can, for instance, be described by temporal logic [Pnueli, 1977] or expected reward specifications. A fundamental requirement for providing such correctness guarantees on MDPs is that probabilities are precisely given. Methods such as variants of model-based reinforcement learning [Moerland et al., 2020] or PAC-learning [Strehl et al., 2009] can learn MDPs by deriving *point estimates* of probabilities from data to satisfy this requirement. This

*Supported by NWO OCENW.KLEIN.187: "Provably Correct Policies for Uncertain Partially Observable Markov Decision Processes", NWA.1160.18.238 (PrimaVera) and by the ERC under the European Union's Horizon 2020 research and innovation programme (FUN2MODEL, grant agreement No. 834115).

36th Conference on Neural Information Processing Systems (NeurIPS 2022).

derivation naturally carries the risk of statistical errors. Optimal policies are highly sensitive to small perturbations in transition probabilities, leading to sub-optimal outcomes such as a deterioration in performance [Mannor et al., 2007, Goyal and Grand-Clement, 2020].

Uncertain MDPs (uMDPs; also known as *interval* or *robust* MDPs) extend MDPs to incorporate such statistical errors by introducing an additional layer of uncertainty via *uncertainty sets* on the transition function [Nilim and Ghaoui, 2005, Wiesemann et al., 2013, Goyal and Grand-Clement, 2020, Rigter et al., 2021]. The solution of a uMDP is a *robust policy* that allows an adversarial selection (i.e., the worst-case scenario) of probabilities within the uncertainty set, and induces a *worst-case performance* (a conservative bound on, e.g., the reachability probability or expected reward). The problem of computing such robust policies, also called *robust verification*, is solved using value iteration or convex optimization, where the uncertainty sets are convex [Wolff et al., 2012, Puggelli et al., 2013].

Our approach. We study the problem of learning an MDP from data. We propose an iterative learning method which uses uMDPs as intermediate models and is able to *adapt to new data* which may be inconsistent with prior assumptions. Furthermore, the method is *task-aware* in the sense that the learning procedure respects temporal logic specifications. In particular, our method learns intervals of probabilities for individual transitions. This Bayesian *anytime-learning approach* employs intervals with linearly updating conjugate priors [Walter and Augustin, 2009], and can iteratively improve upon a uMDP that approximates the true MDP we wish to learn. This method not only decreases the size of each interval, but may also increase it again in case of a so-called *prior-data conflict* where new data suggests the actual probability lies outside the current interval. Consequently, a newly learned interval does not need to be a subset of its prior interval. This property makes our method especially suitable to learn MDPs where the transition probabilities change. Alternatively, we also include *probably approximately correct* (PAC) intervals via Hoeffding's inequality [Hoeffding, 1963], which introduces a correctness guarantee for each transition.

We summarize the key features of our learning method, and what sets it apart from other methods.

- *An anytime approach.* The ability to iteratively update intervals that are not necessarily subsets of each other allows us to design an *anytime-learning approach*. At any time, we may stop the learning and compute a robust policy for the uMDP that the process has yielded thus far, together with the worst-case performance of this policy against a given specification. This performance may not be satisfactory, e.g., the worst-case probability to reach a set of critical states may be below a certain threshold. We continue learning towards a new uMDP that more faithfully captures the true MDP due to the inclusion of further data. Thereby, we ensure that the robust policy gradually gets closer to the optimal policy for the true MDP.
- *Specification-driven.* Our method features the possibility to learn in a task-aware fashion, that is, to learn transitions that matter for a given specification. In particular, for reachability or expected reward (temporal logic) specifications which require a certain set of target states to be reached, we only learn and update transitions along paths towards these states. Transitions outside those paths do not affect the satisfaction of the specification.
- *Adaptive to changing environment dynamics.* When using linearly updating intervals, our approach is adaptive to changing environment dynamics. That is, if during the learning process the probability distributions of the underlying MDP change, our method can easily adapt and learns these new distributions.

2 Related Work

Uncertain MDPs have (often implicitly) been used by *reinforcement learning* (RL) algorithms, for instance, to optimize the *exploration/exploitation* trade-off by guiding the RL agent towards unexplored parts of the environment, following the *optimism in the face of uncertainty* principle [Jaksch et al., 2010, Fruit et al., 2017]. We use the same principle in the exploration phase of our procedure, but compute robust policies as output to account for the uncertainty in an adversarial (or pessimistic) way. Similarly, uncertain MDPs are used to compute robust policies when the data available is limited [Nilim and Ghaoui, 2005, Wiesemann et al., 2013, Russel and Petrik, 2019]. Such robustness is connected to a *pessimistic* principle that has been effective in offline RL settings [Lange et al., 2012], where the agent only has access to a fixed dataset of past trajectories, meaning it needs to base

decisions on limited data [Rashidinejad et al., 2021, Buckman et al., 2021, Jin et al., 2021]. Likewise, our method may be stopped early and return a policy before the problem is fully explored.

Robust RL concerns the standard RL problem, but explicitly accounts for input disturbances and model errors [Morimoto and Doya, 2005]. Often there is a focus on ensuring that a reasonable performance is achieved during data collection. To that end, Lim et al. [2013] and Derman et al. [2019] sample trajectories using a robust policy, which can slow down the process to find an optimal policy. We assume sampling access to the underlying MDP, which allows us to use more efficient exploration. It should be noted that we only use uMDPs as an intermediate model towards learning a standard MDP, whereas in robust RL the model itself may also be an (adversarial) uncertain MDP. As a result, our method converges to an MDP, while robust RL attempts to learn and possibly converge to an uncertain MDP.

Learning MDPs from data is also related to *model learning*, which typically assumes no knowledge about the states and thus iteratively increases the set of states [Vaandrager, 2017]. In [Tappler et al., 2019, 2021] the L^* algorithm for learning finite automata is adapted for MDPs. These methods only yield point estimates of probabilities, and make strong assumptions on the structure of the MDP that is being learned. Ashok et al. [2019] use PAC-learning to estimate the transition functions of MDPs and stochastic games in order to perform *statistical model checking* with a PAC guarantee on the resulting value. In [Bacci et al., 2021] the Baum-Welch algorithm for learning hidden Markov models is adapted to learn MDPs.

Finally, the literature distinguishes two types of uncertainty: *aleatoric* and *epistemic* uncertainty [Hüllermeier and Waegeman, 2021]. Aleatoric uncertainty refers to the uncertainty generated by a probability distribution, like the transition function of an MDP, and is also known as *irreducible uncertainty*. In contrast, epistemic uncertainty is *reducible* by collecting and accounting for (new) data. Our work can be seen as adding an additional layer of epistemic uncertainty on the probability distributions of the transition function that is then, by gathering and including more data, reduced.

3 Preliminaries

A *discrete probability distribution* over a finite set X is a function $\mu\colon X \to [0,1] \subset \mathbb{R}$ with $\sum_{x \in X} \mu(x) = 1$. We write $\mathcal{D}(X)$ for the set of all discrete probability distributions over X, and by $|X|$ we denote the number of elements in X. For any closed interval $I \subseteq \mathbb{R}$ we write $\underline{I}$ and $\overline{I}$ for the lower and upper bounds of the interval, that is, $I = [\underline{I}, \overline{I}]$.

Definition 1 (Markov decision process)**.** *A* Markov decision process *(MDP) is a tuple* (S, s_I, A, P, R) *with* S *a finite set of states,* $s_I \in S$ *the initial state,* A *a finite set of actions,* $P\colon S \times A \times S \to [0,1]$ *with* $\forall s, a \in S \times A, \sum_{s'} P(s,a,s') = 1$ *(such that* $P(s,a) \in \mathcal{D}(S)$*) the probabilistic transition function, and* $R\colon S \times A \to \mathbb{R}_{\geq 0}$ *the reward (or cost) function.*

A *trajectory* in an MDP is a finite sequence $(s_0, a_0, s_1, a_1, \ldots, s_n) \in (S \times A)^* \times S$ where $s_0 = s_I$ and $P(s_i, a_i, s_{i+1}) > 0$ for $0 \leq i < n$. A *memoryless* policy is a function $\pi\colon S \to \mathcal{D}(A)$. If π maps to Dirac distributions, then it is a memoryless *deterministic* (or pure) policy. Applying a policy to an MDP M resolves all the non-deterministic choices and yields an (induced) *discrete-time Markov chain* (DTMC); see, e.g., Puterman [1994] for details.

Definition 2 (Uncertain MDP)**.** *An* uncertain MDP (uMDP) *is a tuple* $(S, s_I, A, \mathbb{I}, \mathcal{P}, R)$ *where* S, s_I, A, R *are as for MDPs,* $\mathbb{I}$ *is a set of probability intervals* $\mathbb{I} = \{[a,b] \mid 0 < a \leq b \leq 1\}$*, and* $\mathcal{P}\colon S \times A \times S \to (\mathbb{I} \cup \{0\})$ *is the* uncertain transition function*, assigning either a probability interval, or the exact probability* 0 *to any transition.*

Uncertain MDPs can be seen as an uncountable set of MDPs that only differ in their transition functions. For a transition function P, we write $P \in \mathcal{P}$ if for every transition the probability of P lies within the interval of $\mathcal{P}$, i.e., $P(s,a,s') \in \mathcal{P}(s,a,s')$ for all $(s,a,s') \in S \times A \times S$. We only allow intervals with a lower bound greater than zero, to ensure a transition cannot vanish under certain distributions generated by the uncertainty. This assumption is standard in uMDPs [Wiesemann et al., 2013, Puggelli et al., 2013]. Applying a policy to a uMDP yields an induced interval Markov chain [Jonsson and Larsen, 1991].

Specifications. We consider *reachability* or *expected reward (cost)* specifications. The value $\mathbb{P}_\pi^M(\Diamond T)$ is the probability to reach a set of *target* states $T \subseteq S$ in the MDP M under the policy π,

also referred to as the *performance of* π.[2] Likewise, $\mathrm{R}_{\pi}^{M}(\Diamond T)$ describes the expected accumulated reward to reach T under π. Note that for probabilistic specifications, we can replace the formula $\Diamond T$ by more general reach-avoid specifications using the until operator from temporal logic.

Formally, the specification $\mathbb{P}_{\text{Max}}(\Diamond T) = \max_{\pi} \mathbb{P}_{\pi}(\Diamond T)$ expresses that the probability of eventually reaching the target set $T \subseteq S$ should be maximized. Likewise, the specification $\mathrm{R}_{\text{Max}}(\Diamond T)$ requires the expected reward for reaching T to be maximized. For minimization, we write $\mathbb{P}_{\text{Min}}(\Diamond T)$ and $\mathrm{R}_{\text{Min}}(\Diamond T)$, respectively. Besides optimizing a probability or reward, a specification may also express an explicit user-provided threshold to compare the performance of a policy to.

For uMDPs, we define *optimistic* and *pessimistic* specifications. In optimistic specifications, we assume the best-case scenario of the uncertainty to satisfy the specification by also minimizing (or maximizing) over the uncertainty set, written as $\mathbb{P}_{\text{MinMin}}(\Diamond T) = \min_{\pi} \min_{P \in \mathcal{P}} \mathbb{P}_{\pi}^{\mathcal{M}[P]}(\Diamond T)$ (or $\mathbb{P}_{\text{MaxMax}}(\Diamond T)$), where the first Min (Max) signals what the decision-maker is trying to achieve, and the second what the uncertainty does. In pessimistic specifications, the uncertainty does the opposite of the goal: $\mathbb{P}_{\text{MaxMin}}(\Diamond T)$ or $\mathbb{P}_{\text{MinMax}}(\Diamond T)$. The notation is similar for reward specifications. A (standard) specification φ can be extended to be optimistic or pessimistic by adding a second Min or Max. We write φ_O for its optimistic extension, and φ_P for its pessimistic extension.

For an MDP M, the aim is to compute a policy π that either optimizes a given specification φ, or whose performance respects a given threshold that, e.g., provides an upper bound on the probability of reaching a set of critical states. Common methods are value iteration or linear programming [Puterman, 1994, Baier and Katoen, 2008]. For uncertain MDPs $\mathcal{M}$, the goal is to compute a policy π that satisfies an optimistic or pessimistic specification φ_O or φ_P. In the latter case, we call π a *robust policy*. Optimal policies in uMDPs can be computed via robust dynamic programming or convex optimization [Wolff et al., 2012, Puggelli et al., 2013].

4 Problem Statement and Outline of the Procedure

We have an unknown but fixed MDP $M = (S, s_I, A, P, R)$, which we will refer to as the *true MDP*, an *initial prior uMDP* $\mathcal{M} = (S, s_I, A, \mathbb{I}, \mathcal{P}, R)$, and a specification φ which we want to satisfy. A discussion of prior (and other parameter) choices follows in Section 6.

Assumption 1 (Underlying graph)**.** *We assume that the underlying graph of the true MDP is known. In particular: transitions that do not exist in the true MDP (transitions of probability* 0*) do also not exist in the uMDP, transitions of probability* 1 *in the true MDP are assigned the point interval* $[1, 1]$ *in the uMDP, and any other transition of non-zero probability* p *has an interval* $I \in \mathbb{I}$ *in the uMDP.*

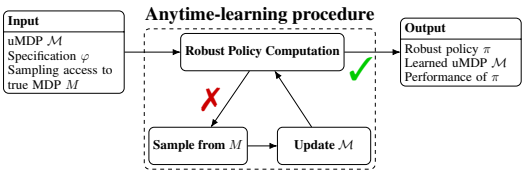


Figure 1: Procedure outline.

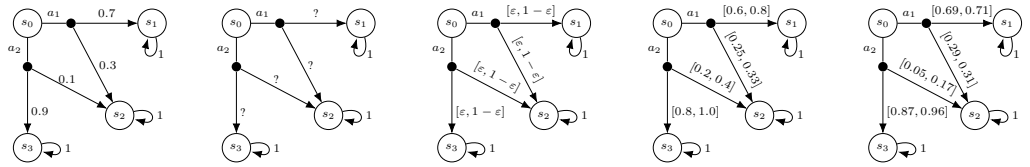
Under Assumption 1 and Definition 2, we construct the initial prior uMDP $\mathcal{M}$ to have transitions of probability 0 and 1 exactly where the true MDP M has these too, and interval transitions $[\varepsilon, 1 - \varepsilon]$ for all other transitions, with $\varepsilon > 0$ free to choose. In particular, our approach does not require ε to be smaller than the smallest probability $p > 0$ occurring in M, which we also do not assume to be known. Alternatively, in case further knowledge is available, one may use any other prior uMDP as long as it satisfies Assumption 1. Our learning problem is expressed as follows:

> The problem is to learn the transition probabilities of a true MDP M, driven by a specification φ, via intermediate uncertain MDPs $\mathcal{M}$ that are iteratively updated to account for newly collected data, such that at any time a robust policy can be computed.

In the following we outline our anytime-learning procedure as illustrated in Figure 1.

1. **Input.** We start with an initial prior uMDP $\mathcal{M}$ and a specification φ we wish to verify. We assume (black box) access to the unknown *true MDP* M to sample trajectories from, or alternatively, assume a (constant) stream of observations from the true MDP.

[2] We will omit the policy π and the MDP M whenever they are clear from the context.



(a) The true MDP. (b) Assumption 1. (c) Initial prior. (d) Intermediate uMDP. (e) Converging towards the true MDP.

Figure 2: Process flow on an example MDP.

2. **Robust policy computation.** We compute a robust policy π for the pessimistic extension of φ, i.e. φ_P, in the uncertain MDP $\mathcal{M}$, together with the worst-case performance of the specification in the current uMDP. If the specification contains an explicit threshold, the value can be compared against the threshold for automatic termination. In case of specifications that optimize a probability or reward, termination needs to be done manually, as it is impossible to tell if the maximum (minimum) was achieved.
3. **Anytime learning.** If the result from step 2 is unsatisfactory, we start learning:
   (a) **Exploration.** We sample one or more trajectories from the true MDP M, using the *optimism in the face of uncertainty* principle.
   (b) **Update.** We update the intervals of the uMDP $\mathcal{M}$ in accordance with the newly collected data. This update yields a new uMDP that more faithfully captures all collected data up to this point than the previous uMDP.
   (c) **Repeat.** We start again at step 2 with this new uMDP until (manual) termination.
4. **Output.** The process may be stopped at any moment and yields the latest uMDP $\mathcal{M}$ together with robust policy π and the performance of π on $\mathcal{M}$.

The effects of this procedure are illustrated in Figure 2. In 2a, we see an example MDP M to learn, and 2b shows the assumed knowledge about M. 2c shows the initial uMDP $\mathcal{M}$ constructed from 2b, using a (symbolic or explicit) lower bound $\varepsilon > 0$ to ensure that all lower bounds of $\mathcal{M}$ are strictly greater than zero. In 2d, we see an intermediate learned uMDP. Some intervals may already have successfully converged towards the probability of that transition in the true MDP, while others may be very inaccurate due to a low sample size and thus a bad estimate. Finally, 2e depicts the learned uMDP converging towards the true MDP.

5 Bayesian Learning

We assume access to trajectories through the true MDP. Due to the Markov property of the MDP, i.e., the fact that the transition probabilities only depend on the current state and not on any further history, we may split each trajectory τ into separate sets of independent experiments where a state-action pair (s, a) is sampled and a successor state s_i is observed; see also Appendix A of [Strehl and Littman, 2008]. We count the number of occurrences of the transition (s, a, s_i) in each trajectory τ, and the number of occurrences of the state-action pair (s, a) in each trajectory τ, denoted by $\#(s, a, s_i)$ and $\#(s, a)$, respectively. In the following, we introduce the two approaches of learning intervals: the standard approach of PAC learning via Hoeffding's inequality which provides a PAC guarantee on the value of the learned model, and a new approach using *linearly updating intervals* (LUI), which is more flexible due to the inclusion of *prior-data conflicts* and its closure properties. Finally, we introduce a minor modification to the LUI approach, making it also applicable to situations where the underlying MDP changes over time. Such a modification is not possible in PAC learning as Hoeffding's inequality assumes independent samples from a fixed distribution.

5.1 Learning PAC Intervals

We use the standard method of maximum a-posteriori probability (MAP) estimation to infer point estimates of probabilities; see Appendix A for details. These point estimates can then easily be turned into *probably approximately correct* (PAC) intervals via Hoeffding's inequality. Given $N = \#(s, a)$ samples and a fixed *error rate* γ, we use Hoeffding's inequality [Hoeffding, 1963] to compute the

interval size $\delta = \sqrt{\log(2/\gamma)/2N}$. This δ may then be used to construct intervals that are PAC with respect to the true transition probability. To lift the PAC guarantee to the entire learned MDP, and consequently also the optimal value for some specification, we need to distribute δ over all transitions, i.e., $\delta_P = \delta / \sum_{(s,a)\in S\times A} |\mathbf{Succ}(s,a)|$, where $\mathbf{Succ}(s,a)$ is the set of successor states of (s,a). Using this δ_P, we then construct the intervals

$$\mathcal{P}(s,a,s_i) = [\max(\varepsilon, \tilde{P}(s,a,s_i) - \delta_P), \min(\tilde{P}(s,a,s_i) + \delta_P, 1)], \tag{1}$$

where $\tilde{P}$ is the (MAP) point estimate, and ε is again a small value to ensure that the interval lower bounds are non-zero. As a result, we have the following Proposition, whose proof is a direct application of Hoeffding's inequality.

Proposition 1. *The true MDP M^* lies within the learned uMDP $\mathcal{M}$ with probability greater or equal to $1-\gamma$.*

This is a standard result and also used in, e.g., PAC statistical model checking [Ashok et al., 2019].

5.2 Learning Linearly Updating Probability Intervals

We use the Bayesian approach of *intervals with linearly updating conjugate priors* [Walter and Augustin, 2009] to learn intervals of probabilities. Each uncertain transition $\mathcal{P}(s,a,s_i)$ is assigned a *prior interval* $\mathcal{P}_i = [\underline{\mathcal{P}}_i, \overline{\mathcal{P}}_i]$, and a *prior strength interval* $[\underline{n}_i, \overline{n}_i]$ that represents a minimum and maximum number of samples on which the prior interval is based. The greater the values of the strength interval, the more emphasis is placed on the prior, and the more data is needed to significantly change the prior when computing the posterior. The greater the difference between the $\underline{n}_i$ and $\overline{n}_i$, the greater the difference between a *prior-data conflict* and a *prior-data agreement*.

Definition 3 (Posterior interval computation)**.** *The interval $[\underline{\mathcal{P}}_i, \overline{\mathcal{P}}_i]$ can be updated to $[\underline{\mathcal{P}}'_i, \overline{\mathcal{P}}'_i]$, using $N = \#(s,a)$ and $k_i = \#(s,a,s_i)$, as follows:*

$$\underline{\mathcal{P}}'_i = \begin{cases} \frac{\overline{n}_i \underline{\mathcal{P}}_i + k_i}{\overline{n}_i + N} & \text{if } \forall j. \frac{k_j}{N} \geq \underline{\mathcal{P}}_j \text{ (prior-data agreement),} \\ \frac{\underline{n}_i \underline{\mathcal{P}}_i + k_i}{\underline{n}_i + N} & \text{if } \exists j. \frac{k_j}{N} < \underline{\mathcal{P}}_j \text{ (prior-data conflict).} \end{cases} \tag{2}$$

$$\overline{\mathcal{P}}'_i = \begin{cases} \frac{\overline{n}_i \overline{\mathcal{P}}_i + k_i}{\overline{n}_i + N} & \text{if } \forall j. \frac{k_j}{N} \leq \overline{\mathcal{P}}_j \text{ (prior-data agreement),} \\ \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\underline{n}_i + N} & \text{if } \exists j. \frac{k_j}{N} > \overline{\mathcal{P}}_j \text{ (prior-data conflict).} \end{cases} \tag{3}$$

The strength interval is updated by adding the number of samples N to it: $[\underline{n}'_i, \overline{n}'_i] = [\underline{n}_i + N, \overline{n}_i + N]$.

The initial values for the priors of each state-action pair can be chosen freely subject to the constraints $0 < \underline{\mathcal{P}}_i \leq \overline{\mathcal{P}}_i \leq 1$, and $\overline{n}_i \geq \underline{n}_i \geq 1$.

Key properties of linearly updating probability intervals.

- *Convergence in the infinite run.* Under the assumption that the true MDP does not change, each interval will converge to the exact transition probability when the total number of samples processed tends to infinity, regardless of how many samples are processed *per iteration* [Walter and Augustin, 2009]. This assumption is, however, not required for our work. If the true MDP changes over time, or is *adversarial* (i.e., a uMDP), our method is still applicable, but will not converge to a fixed MDP.
- *Prior-data conflict.* When the estimated probability k_i/N lies outside the current interval, a so-called *prior data conflict* occurs. Consequently, if at some point we derive an interval that does not contain the true transition probability, the method will correct itself later on.
- *Closure properties under updating.* Finally, updating is closed in two specific ways. First, any interval of probabilities is updated again to a valid interval of probabilities, and second, any set of intervals at a state-action pair that contains a valid distribution over the successor states will again contain a distribution over successor states after updating.

A key requirement for computing robust policies on uMDPs is that the lower bound of every interval is strictly greater than zero (see Definition 2). This closure property is formalized as follows.

Theorem 1 (Closure of intervals under learning)**.** *For any valid prior interval* $[\underline{\mathcal{P}}, \overline{\mathcal{P}}]$ *with* $0 < \underline{\mathcal{P}} \leq \overline{\mathcal{P}} \leq 1$*, we have that the posterior* $[\underline{\mathcal{P}}', \overline{\mathcal{P}}']$ *computed via Definition 3 also satisfies* $0 < \underline{\mathcal{P}}' \leq \overline{\mathcal{P}}' \leq 1$.

Furthermore, we also have closure properties at each state-action pair. In particular, if we choose our prior intervals such that there is at least one valid probability distribution at the state-action pair, then the posterior intervals will again contain a valid probability distribution. We formalize this notion by examining the sum of the lower and upper bounds of the intervals in the following Theorem:

Theorem 2 (Closure of distributions under learning)**.** *We have the following bounds on the set of posterior distributions. In case of a prior data agreement, we have that the sum of the posterior bounds is bounded by the sum of the prior bounds, and the value* 1*. That is,*

$$\sum_i \underline{\mathcal{P}}_i \leq \sum_i \underline{\mathcal{P}}'_i \leq 1, \qquad 1 \leq \sum_i \overline{\mathcal{P}}'_i \leq \sum_i \overline{\mathcal{P}}_i. \tag{4}$$

In case of a prior-data conflict, the sum of posterior bounds is no longer necessarily bounded by the prior, and we only have

$$\sum_i \underline{\mathcal{P}}'_i \leq 1 \leq \sum_i \overline{\mathcal{P}}'_i. \tag{5}$$

Note, however, that this last constraint (5) *is already sufficient to ensure that there is a valid probability distribution at the state-action pair.*

The proofs for both Theorem 1 and 2 can be found in Appendix B.

5.3 Efficient exploration

Above, we assumed that a set of trajectories was given. To actually obtain the trajectories, we use the well-established *optimism in the face of uncertainty* principle [Munos, 2014]. We compute the optimal policy for the optimistic extension (see Section 3) of the specification φ, i.e. φ_O, in the current uMDP and use this policy for exploration. To make exploration specification-driven, we only sample transitions along trajectories towards the target state(s) of the specification. When the last seen state has probability zero or one to reach the target for reachability, or reward zero or infinity, we restart. States satisfying these conditions can be found by analyzing the graph of the true MDP [Baier and Katoen, 2008].

Trajectories and iterations. As explained in Section 4, our method is iterative in terms of updating the uMDP $\mathcal{M}$ and computing a robust policy. After updating the uMDP, we also compute a new exploration policy, based on the new uMDP. Each iteration consists of processing at least one, but possibly more trajectories. To determine how many trajectories to collect, we use a doubling-counting scheme, where we keep track of how often every state-action pair and transition is visited during exploration [Jin et al., 2020]. An iteration is completed when any of the counters is doubled with respect to the previous iteration. A detailed description of this schedule is given in Appendix C.

5.4 Learning under changing environments

Previously, we assumed a fixed unknown true MDP M^* to learn. But what if the transition probabilities of M^* suddenly change? More precisely, we assume two unknown true MDPs, M_1^* and M_2^* with the same underlying graph but (possibly) different transition probabilities. After an unknown number of interactions with the true environment M_1^*, we suddenly continue interacting with M_2^*. We modify our LUI approach by introducing a bound on the strength of the prior, $n_{\text{Max}} = [\underline{n}_{\text{Max}}, \overline{n}_{\text{Max}}]$, and update the strength intervals by the following rule

$$[\underline{n}'_i, \overline{n}'_i] = [\min(\underline{n}_i + N, \underline{n}_{\text{Max}}), \min(\overline{n}_i + N, \overline{n}_{\text{Max}})].$$

The probability intervals themselves are updated in the same way as before in Definition 3. By limiting the prior strength in this way, we trade some rate of convergence for adaptability. The weaker the prior, the greater the effect of a prior-data conflict, and hence adaptability to new data. When suddenly changing environments, new data will likely lead to prior-data conflicts, and thus a higher adaptability of the overall learning method.

We add randomization to the pure optimistic exploration policy. We introduce a hyperparameter $\xi \in [0, 1]$, and follow with probability ξ the action of the optimistic policy, and distribute the remaining $1 - \xi$ uniformly over the other actions, yielding a memoryless randomized policy.

6 Experimental Evaluation

We implement our approach, with both linearly updating intervals (LUI) and PAC intervals (PAC), in Java on top of the verification tool PRISM [Kwiatkowska et al., 2011], together with a variant of value iteration to compute robust policies for uMDPs with convex uncertainties [Wolff et al., 2012].[3] We compare our method to point estimates derived via MAP-estimation (MAP) and with uMDPs learned by the UCRL2 reinforcement learning algorithm [Jaksch et al., 2010] (UCRL2). We modify UCRL2 to make it more comparable to our setting. In particular, we use optimistic policies for exploration, but robust policies to compute the performance, in contrast to the standard UCRL2 setting which only uses optimistic policies, see Appendix E for further details.

Without knowledge about the true MDP apart from Assumption 1, we have to define an appropriate prior interval for every transition. We set $\varepsilon = \texttt{1e-4}$ as constant and define the prior uMDP with intervals $\mathcal{P}_i = [\varepsilon, 1-\varepsilon]$ and strength intervals $[\underline{n}_i, \overline{n}_i] = [5, 10]$ at every transition $\mathcal{P}(s, a, s_i)$, as in Figure 2c. For MAP, we use a prior of $\alpha_i = 10$ for all i. The same prior is used for the point estimates of both PAC and UCRL2, together with an error rate of $\gamma = 0.01$.

Evaluation metrics. We consider two metrics to evaluate the four learning methods.

- *Performance.* How does the robust policy computed on the learned model perform on the true MDP? We evaluate the probability of satisfying the given specification $\mathbb{P}_{\pi}^{M}(\Diamond T)$ or expected reward $\mathrm{R}_{\pi}^{M}(\Diamond T)$ of the robust policy π computed after each update of the model.
- *Performance estimation error.* How well do we *expect* a robust policy to perform on the true MDP based on the performance on the intermediate learned uMDP? We compute the difference between the performance of the robust policy on the learned uMDP (the worst-case performance) and the performance on the true MDP. While values closer to zero are preferable, we do not accept methods with positive estimation errors, since this indicates their estimated performance is not a lower (conservative) bound on the actual performance of the policy. In particular, an estimation error above zero shows the policy is misleading in terms of predicting its performance.

We benchmark our method using several well-known environments: the Chain Problem [Araya-López et al., 2011], Aircraft Collision Avoidance [Kochenderfer, 2015], a slippery Grid World [Derman et al., 2019], a 99-armed Bandit [Lattimore and Szepesvári, 2020], and two version of a Betting Game [Bäuerle and Ott, 2011]. For details on all these environments we refer to Appendix D. We highlight the Betting Game and Chain Problem environments here, as they will be used to explain some of the key observations we make from our experimental results.

- *Betting Game.* The agent starts with 10 coins and attempts to maximize the number of coins after 6 bets. When a bet is won, the number of coins placed is doubled; when lost, the number of coins placed is removed. The agent may bet 0, 1, 2, 5, or 10 coins. We consider two versions of the game, one which is favourable to the player, with a win probability of 0.8, and one that is unfavourable with win probability 0.2. After 6 bets the player receives a reward equal to the number of coins left. The specification is to maximize the reward.
- *Chain Problem.* We consider a chain of 30 states. There are three actions, one progresses with probability 0.95 to the next state, and resets the model to the initial state with probability 0.05. The second action does the same, but with reversed probabilities. The third action has probability 0.5 for both cases. Every action gets a reward of 1. As specification, we minimize the reward to reach the last state of the chain.

Results

We present an excerpt of our experimental results here, and refer the reader to Appendix F for the full set of results, which in particular also includes the estimation error for all environments, an additional model error metric, and further experiments regarding different priors and changing environments. All experiments were performed on a machine with a 4GHz Intel Core i9 CPU, using a single core. Each experiment is repeated 100 times, and reported with a 95% confidence interval.

[3] The implementation is available at `https://github.com/LAVA-LAB/luiaard`.

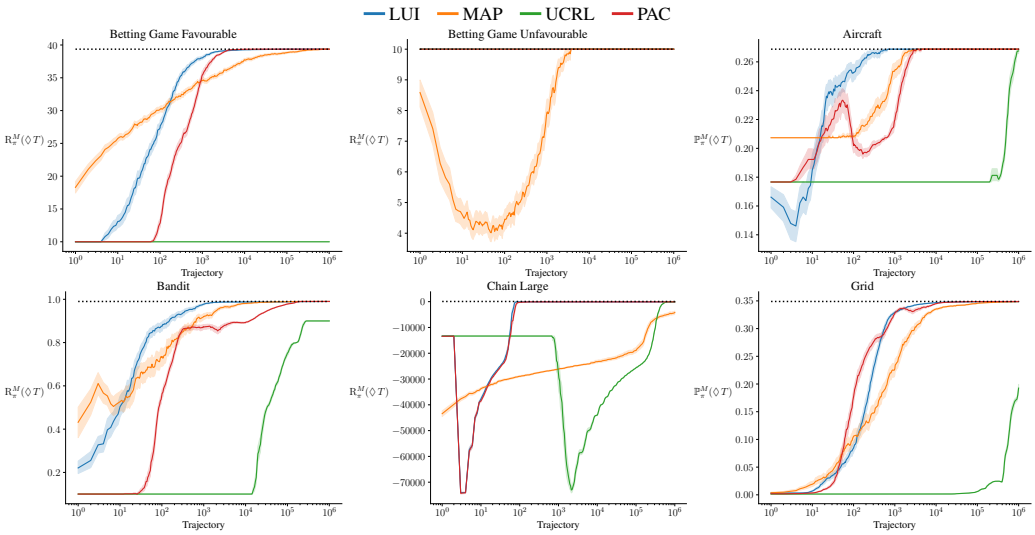


Figure 3: Comparison of the performance of robust policies on different environments against the number of trajectories processed (on log-scale). The dashed line indicates the optimal performance.

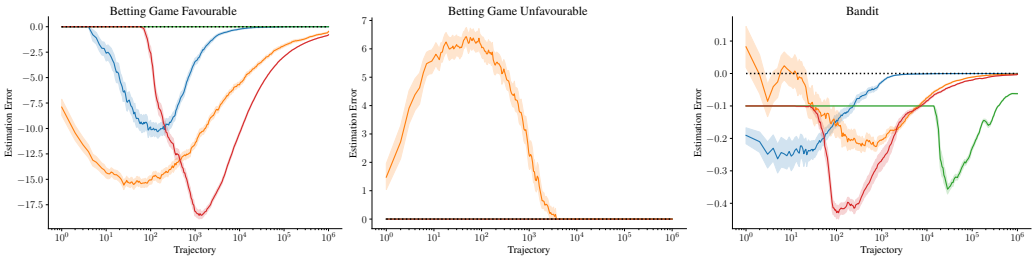


Figure 4: Estimation error on the two Betting Game environments and the Bandit, against the number of trajectories processed (on log-scale).

Figure 3 shows the performance of the robust policies computed via each learning method against the number of trajectories processed on the different environments. We first note that in all environments, our LUI method is the first to find an optimal policy. Depending on the environment, the performance of LUI and PAC may be roughly equivalent (Chain, Grid). When also taking the estimation error into account (Figure 4), we see LUI outperforming other methods on that metric. UCRL2 is the slowest to converge to an optimal policy. This due to UCRL2 being a reinforcement learning algorithm, and thus it is slower in reducing the intervals in favour of a broader exploration.

Recovering from bad estimates. On the Chain environment, we see LUI and PAC (around trajectory 5), and UCRL2 (around trajectory 10^3) choose the wrong action(s), with an decrease in performance as a result. This is most likely due to getting a bad estimate on some of the transitions later on in the chain, leading to many resets to the initial state, and thus decreasing the performance significantly. While all three methods manage to recover and then find the optimal policy, UCRL2 takes significantly longer: only after trajectory 10^5, where LUI and PAC only need about 100 trajectories. MAP-estimation typically sits between LUI and PAC in terms of performance. It is less sensitive to mistakes like the one discussed above, but is less reliable in providing a conservative bound on its performance, as will be discussed below. Furthermore, we see that in the unfavourable Betting Game, only MAP-estimation gives sub-optimal performance, due to bad estimates. It is able to recover from this, but needs almost 10^4 trajectories to do so. Due to the low win probability in this Betting Game, a robust policy on the uMDPs is by default an optimal policy for the true MDP, and we see that LUI, PAC, and UCRL2 do not change to a sub-optimal policy.

Robust policies are conservative. Consider Figure 4. We note the undesirable behaviour of having an Estimation Error above zero, which means the performance of the policy on the learned model

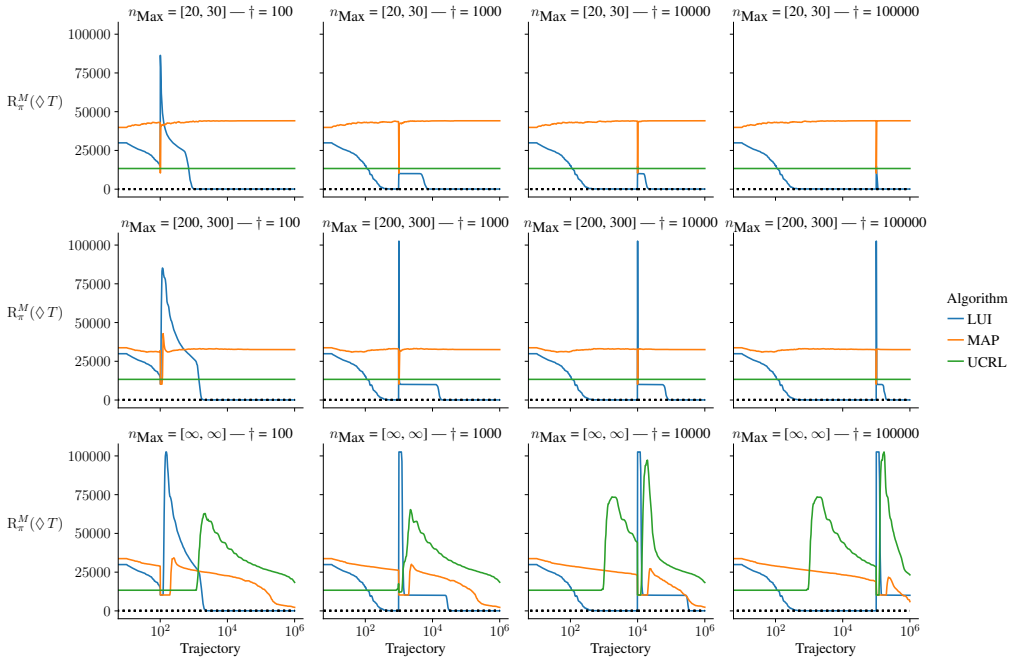


Figure 5: Environment change on the Chain Problem at different points $\dagger \in \{10^2, \ldots, 10^5\}$ using randomization parameter $\xi = 0.8$ in the exploration.

was higher than the performance of that policy on the true MDP. MAP-estimation is particularly susceptible to this, while all three uMDP methods yield policies that are conservative in general, though some exceptions exist as shown in the full results in Appendix F.

LUI is adaptive to changing environments. Finally, we investigate the behaviour of the learning methods when after a fixed number of trajectories the probabilities of the true MDP change, as introduced in Section 5.4. Figure 5 shows the performance of the robust policy for each learning method on the Chain environment, results for the same experiment on the Betting Game can be found in Appendix F. After $\dagger \in \{10^2, \ldots, 10^5\}$ trajectories, we change the environment by swapping the transition probabilities, for three different bounds on the strength intervals. We similarly bound the MAP-estimation priors for MAP and UCRL. PAC is omitted from this experiment as PAC guarantees lose all meaning when changing the underlying distribution. After the change in environment, the new optimal policy has to use the opposite action from the previously optimal policy. We see that LUI is the only method capable of converging to optimal policies both before and after the change in environment. Furthermore, the lower the bounds on the prior strength, the faster it adapts to the change. We conclude that LUI is an effective approach to deal with learning an MDP under potential adversarial sampling conditions.

7 Conclusion and Future Work

We presented a new Bayesian method that learns uMDPs to approximate an MDP, either via linearly updating intervals, or PAC-intervals. Robust policies computed on learned uMDPs are shown to be conservative and reliable in predicting their performance when applied on the MDP that is being learned. The approach of linearly updating intervals is also effective at continuously learning a potentially changing environment. For future work, we aim to extend our method to uncertain POMDPs [Suilen et al., 2020, Cubuktepe et al., 2021]. While we do not see any immediate negative societal impacts of our work, we acknowledge that potential misuse of our work cannot be ruled out due to the generality of MDPs.

References

Mauricio Araya-López, Olivier Buffet, Vincent Thomas, and François Charpillet. Active Learning of MDP Models. In *EWRL*, volume 7188 of *LNCS*, pages 42–53. Springer, 2011.

Pranav Ashok, Jan Kretínský, and Maximilian Weininger. PAC Statistical Model Checking for Markov Decision Processes and Stochastic Games. In *CAV (1)*, volume 11561 of *LNCS*, pages 497–519. Springer, 2019.

Giovanni Bacci, Anna Ingólfsdóttir, Kim G. Larsen, and Raphaël Reynouard. Active Learning of Markov Decision Processes using Baum-Welch algorithm. In *ICMLA*, pages 1203–1208. IEEE, 2021.

Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. MIT Press, 2008.

Nicole Bäuerle and Jonathan Ott. Markov Decision Processes with Average-Value-at-Risk criteria. *Math. Methods Oper. Res.*, 74(3):361–379, 2011.

Dimitri P. Bertsekas. *Dynamic programming and optimal control, 3rd Edition*. Athena Scientific, 2005.

Christopher M. Bishop. *Pattern recognition and machine learning, 5th Edition*. Information science and statistics. Springer, 2007.

Jacob Buckman, Carles Gelada, and Marc G Bellemare. The Importance of Pessimism in Fixed-Dataset Policy Optimization. In *ICLR*, pages 1–11. OpenReview.net, 2021.

Murat Cubuktepe, Nils Jansen, Sebastian Junges, Ahmadreza Marandi, Marnix Suilen, and Ufuk Topcu. Robust Finite-State Controllers for Uncertain POMDPs. In *AAAI*, pages 11792–11800. AAAI Press, 2021.

Esther Derman, Daniel J. Mankowitz, Timothy A. Mann, and Shie Mannor. A Bayesian Approach to Robust Reinforcement Learning. In *UAI*, volume 115 of *Proceedings of Machine Learning Research*, pages 648–658. AUAI Press, 2019.

Ronan Fruit, Matteo Pirotta, Alessandro Lazaric, and Emma Brunskill. Regret Minimization in MDPs with Options without Prior Knowledge. In *NIPS*, pages 3166–3176, 2017.

Vineet Goyal and Julien Grand-Clement. Robust Markov Decision Process: Beyond Rectangularity, 2020.

Wassily Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

Eyke Hüllermeier and Willem Waegeman. Aleatoric and epistemic uncertainty in machine learning: an introduction to concepts and methods. *Mach. Learn.*, 110(3):457–506, 2021.

Bart Jacobs. A channel-based perspective on conjugate priors. *Math. Struct. Comput. Sci.*, 30(1): 44–61, 2020.

Thomas Jaksch, Ronald Ortner, and Peter Auer. Near-optimal Regret Bounds for Reinforcement Learning. *J. Mach. Learn. Res.*, 11:1563–1600, 2010.

Chi Jin, Tiancheng Jin, Haipeng Luo, Suvrit Sra, and Tiancheng Yu. Learning Adversarial Markov Decision Processes with Bandit Feedback and Unknown Transition. In *ICML*, pages 4860–4869. PMLR, 2020.

Ying Jin, Zhuoran Yang, and Zhaoran Wang. Is Pessimism Provably Efficient for Offline RL? In *ICML*, pages 5084–5096. PMLR, 2021.

Bengt Jonsson and Kim Guldstrand Larsen. Specification and refinement of probabilistic processes. In *LICS*, pages 266–277. IEEE Computer Society, 1991.

Mykel J Kochenderfer. *Decision making under uncertainty: theory and application*. MIT press, 2015.

Marta Z. Kwiatkowska, Gethin Norman, and David Parker. PRISM 4.0: Verification of Probabilistic Real-Time Systems. In *CAV*, volume 6806 of *LNCS*, pages 585–591. Springer, 2011.

Sascha Lange, Thomas Gabel, and Martin Riedmiller. Batch Reinforcement Learning. In Marco A Wiering and Martijn van Otterlo, editors, *Reinforcement Learning: State-of-the-Art*, pages 45–73. Springer Berlin Heidelberg, Berlin, Germany, 2012.

Tor Lattimore and Csaba Szepesvári. *Bandit Algorithms*. Cambridge University Press, 2020.

Shiau Hong Lim, Huan Xu, and Shie Mannor. Reinforcement Learning in Robust Markov Decision Processes. In *NIPS*, pages 701–709, 2013.

Shie Mannor, Duncan Simester, Peng Sun, and John N. Tsitsiklis. Bias and Variance Approximation in Value Function Estimates. *Manag. Sci.*, 53(2):308–322, 2007.

Thomas M. Moerland, Joost Broekens, and Catholijn M. Jonker. Model-based Reinforcement Learning: A Survey. *CoRR*, abs/2006.16712, 2020.

Jun Morimoto and Kenji Doya. Robust reinforcement learning. *Neural Comput.*, 17(2):335–359, 2005.

Rémi Munos. From Bandits to Monte-Carlo Tree Search: The Optimistic Principle Applied to Optimization and Planning. *Found. Trends Mach. Learn.*, 7(1):1–129, 2014.

Arnab Nilim and Laurent El Ghaoui. Robust Control of Markov Decision Processes with Uncertain Transition Matrices. *Oper. Res.*, 53(5):780–798, 2005.

Amir Pnueli. The Temporal Logic of Programs. In *FOCS*, pages 46–57. IEEE Computer Society, 1977. doi: 10.1109/SFCS.1977.32.

Alberto Puggelli, Wenchao Li, Alberto L. Sangiovanni-Vincentelli, and Sanjit A. Seshia. Polynomial-Time Verification of PCTL Properties of MDPs with Convex Uncertainties. In *CAV*, volume 8044 of *LNCS*, pages 527–542. Springer, 2013.

Martin L. Puterman. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. Wiley Series in Probability and Statistics. Wiley, 1994.

Paria Rashidinejad, Banghua Zhu, Cong Ma, Jiantao Jiao, and Stuart Russell. Bridging Offline Reinforcement Learning and Imitation Learning: A Tale of Pessimism. In *NeurIPS*. Curran Associates, Inc., 2021.

Marc Rigter, Bruno Lacerda, and Nick Hawes. Minimax Regret Optimisation for Robust Planning in Uncertain Markov Decision Processes. In *AAAI*, pages 11930–11938. AAAI Press, 2021.

Reazul Hasan Russel and Marek Petrik. Beyond Confidence Regions: Tight Bayesian Ambiguity Sets for Robust MDPs. In *NeurIPS*, pages 7047–7056, 2019.

Alexander L. Strehl and Michael L. Littman. An analysis of model-based Interval Estimation for Markov Decision Processes. *J. Comput. Syst. Sci.*, 74(8):1309–1331, 2008.

Alexander L. Strehl, Lihong Li, and Michael L. Littman. Reinforcement Learning in Finite MDPs: PAC Analysis. *J. Mach. Learn. Res.*, 10:2413–2444, 2009.

Marnix Suilen, Nils Jansen, Murat Cubuktepe, and Ufuk Topcu. Robust Policy Synthesis for Uncertain POMDPs via Convex Optimization. In *IJCAI*, pages 4113–4120. ijcai.org, 2020.

Martin Tappler, Bernhard K. Aichernig, Giovanni Bacci, Maria Eichlseder, and Kim G. Larsen. L^*-Based Learning of Markov Decision Processes. In *FM*, volume 11800 of *LNCS*, pages 651–669. Springer, 2019.

Martin Tappler, Edi Muskardin, Bernhard K. Aichernig, and Ingo Pill. Active model learning of stochastic reactive systems. In *SEFM*, volume 13085 of *Lecture Notes in Computer Science*, pages 481–500. Springer, 2021.

Frits W. Vaandrager. Model learning. *Commun. ACM*, 60(2):86–95, 2017.

Gero Walter and Thomas Augustin. Imprecision and prior-data conflict in generalized Bayesian inference. *Journal of Statistical Theory and Practice*, 3(1):255–271, 2009.

Wolfram Wiesemann, Daniel Kuhn, and Berç Rustem. Robust Markov Decision Processes. *Math. Oper. Res.*, 38(1):153–183, 2013.

Eric M. Wolff, Ufuk Topcu, and Richard M. Murray. Robust control of uncertain Markov Decision Processes with temporal logic specifications. In *CDC*, pages 3372–3379. IEEE, 2012.

Checklist

1. For all authors...
   (a) Do the main claims made in the abstract and introduction accurately reflect the paper's contributions and scope? [Yes]
   (b) Did you describe the limitations of your work? [Yes]
   (c) Did you discuss any potential negative societal impacts of your work? [Yes] We briefly reflect on this in the conclusion.
   (d) Have you read the ethics review guidelines and ensured that your paper conforms to them? [Yes] All experiments were ran on a standard desktop PC, see Section 6.
2. If you are including theoretical results...
   (a) Did you state the full set of assumptions of all theoretical results? [Yes] See Assumption 1in particular.
   (b) Did you include complete proofs of all theoretical results? [Yes] See Appendix B in particular.
3. If you ran experiments...
   (a) Did you include the code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL)? [Yes] See supplementary material for the code and instructions on how to reproduce the results in the paper.
   (b) Did you specify all the training details (e.g., data splits, hyperparameters, how they were chosen)? [Yes] All priors and other parameters are mentioned where relevant.
   (c) Did you report error bars (e.g., with respect to the random seed after running experiments multiple times)? [Yes] All experiments are repeated 100 times and reported with 95% confidence intervals, as also mentioned in Section 6.
   (d) Did you include the total amount of compute and the type of resources used (e.g., type of GPUs, internal cluster, or cloud provider)? [Yes] See Section 6.
4. If you are using existing assets (e.g., code, data, models) or curating/releasing new assets...
   (a) If your work uses existing assets, did you cite the creators? [Yes] See Appendix D for descriptions
   (b) Did you mention the license of the assets? [Yes] License is included in the supplementary material (GNU general public license).
   (c) Did you include any new assets either in the supplemental material or as a URL? [Yes] See the `models` folder in the supplementary material. In particular, we translated the existing models from the literature into the Prism language.
   (d) Did you discuss whether and how consent was obtained from people whose data you're using/curating? [N/A]
   (e) Did you discuss whether the data you are using/curating contains personally identifiable information or offensive content? [N/A]
5. If you used crowdsourcing or conducted research with human subjects...
   (a) Did you include the full text of instructions given to participants and screenshots, if applicable? [N/A]
   (b) Did you describe any potential participant risks, with links to Institutional Review Board (IRB) approvals, if applicable? [N/A]
   (c) Did you include the estimated hourly wage paid to participants and the total amount spent on participant compensation? [N/A]

A MAP-estimation

We describe a general setup for learning point estimates of probabilities via *maximum a-posteriori estimation* (MAP-estimation). For a fixed state-action pair (s, a) with m different successor states $s_1, \ldots, s_m$ that is sampled $N = \#(s, a)$ times, and where each successor state is observed $k_i = \#(s, a, s_i)$ times for $i = 1, \ldots, m$, we have the *multinomial likelihood*

$$Mn(k_1, \ldots, k_n \mid P(s, a, \cdot)) = \frac{N!}{k_1! \cdot \ldots \cdot k_m!} \cdot \prod_{i=1}^{m} P(s, a, s_i)^{k_i}, \tag{6}$$

where the transition probabilities $P(s, a, s_i)$ are unknown and given by a Dirichlet distribution with parameters $\alpha_1, \ldots, \alpha_m$ [Bishop, 2007]:

$$Dir(P(s, a, \cdot) \mid \alpha_1, \ldots, \alpha_m) \propto \prod_{i=1}^{m} P(s, a, s_i)^{\alpha_i - 1}. \tag{7}$$

The Dirichlet distribution is a *conjugate prior* to the multinomial likelihood, meaning that we do not need to compute the posterior distribution explicitly, but instead we just update the parameters of the prior Dirichlet distribution. Formally, conjugacy is a closure property, see [Jacobs, 2020].

Given a prior Dirichlet distribution with parameters $\alpha_1, \ldots, \alpha_m$, and observing the i-th successor state k_i times, the posterior Dirichlet distribution is given by simply adding k_i to parameter α_i:

$$Dir(P(s, a, \cdot) \mid \alpha_1 + k_1, \ldots, \alpha_m + k_m). \tag{8}$$

Having computed the posterior Dirichlet distribution, MAP-estimation can be used to infer the probabilities. These estimates are given by the *mode* of each parameter of the posterior distribution:

$$\tilde{P}(s, a, s_i) = \frac{\alpha_i - 1}{(\sum_{j=1}^{m} \alpha_j) - m}. \tag{9}$$

When all parameters α_i are equal, MAP-estimation yields uniform distributions.

B Proofs

The proof of Theorem 1 is straightforward and relies on the observation that for any amount of finite data, a single update can only grow closer to zero but not become zero, and that iterated updates converge to the true probability which is assumed to be non-zero.

Proof Theorem 1. For any transition (s, a, s_i) the following holds. We assume a valid prior, that is, $0 < \underline{\mathcal{P}}_i \leq \overline{\mathcal{P}}_i \leq 1$. We have an empirical estimate of k_i/N. Then we also have $0 < \underline{\mathcal{P}}'_i \leq \overline{\mathcal{P}}'_i \leq 1$, where the first inequality $0 < \underline{\mathcal{P}}'_i$ follows from the fact that Equation 2 can only be 0 when their nominator is zero, which is not possible when $\underline{n}_i \geq 1$ (or $\overline{n}_i \geq 1$) and $\underline{\mathcal{P}}_i > 0$. The second inequality, $\underline{\mathcal{P}}'_i \leq \overline{\mathcal{P}}'_i$ follows directly from Equations 2 and 3 together with $\underline{\mathcal{P}}_i \leq \overline{\mathcal{P}}_i$. The third inequality $\overline{\mathcal{P}}'_i \leq 1$ follows again from Equation 3 when $\overline{\mathcal{P}}_i <\leq 1$ and $k_i \leq N$. All reasoning above is independent of prior-data agreement or conflict and thus applies to both cases in each of the equations. □

The proof of Theorem 2 uses the following Lemma:

Lemma 1. *At a state-action pair with m successor states, there can be at most $m - 1$ prior-data conflicts on the upper (or lower) bound.*

Proof. We prove the lemma for the upper bound, a proof for the lower bound follows by symmetry. Assume a valid prior, that is, $\sum_i \overline{\mathcal{P}}_i \geq 1$. Suppose there is a prior-data conflict for every interval, i.e., $\forall i. \frac{k_i}{N} > \overline{\mathcal{P}}_i$. Then we also have

$$1 = \sum_i \frac{k_i}{N} > \sum_i \overline{\mathcal{P}}_i \geq 1,$$

which is clearly not possible. The possibility for $m - 1$ prior-data conflicts is witnessed in the following example. Take a state-action pair with two successor states, s_1 and s_2. Then $m = 2$. Take

one sample, i.e., $N = 1$, and suppose we observe s_1, such that $k_1 = 1$ and $k_2 = 0$. Then for any valid prior intervals $I_1 = [\underline{\mathcal{P}}_1, \overline{\mathcal{P}}_1]$ and $I_2 = [\underline{\mathcal{P}}_2, \overline{\mathcal{P}}_2]$ we have ${}^{k_1}/_N = 1 > \overline{\mathcal{P}}_1$ and ${}^{k_2}/_N = 0 < \overline{\mathcal{P}}_2$. Hence, a prior-data conflict at I_1 but not at I_2, thus $m-1$ conflicts at the state-action pair in total. □

We additionally have the following Lemma:

Lemma 2. *A prior-data conflict at the upper bound implies a prior-data agreement at the lower bound, and vice versa.*

Proof. Assume a conflict at the upper bound $\overline{\mathcal{P}}_i$. Then $\frac{k_i}{N} > \overline{\mathcal{P}}_i \geq \underline{\mathcal{P}}_i$, which is a prior-data agreement with $\underline{\mathcal{P}}_i$ by definition. The other way around follows by symmetry. □

Now we prove Theorem 2.

Proof Theorem 2. We start with the constraints in Equation 4.

First, $1 \leq \sum_i \overline{\mathcal{P}}'_i$. We use that there is a prior-data agreement, that is, $\forall i. \frac{k_i}{N} \leq \overline{\mathcal{P}}_i$. Then we derive

$$\sum_i \overline{\mathcal{P}}'_i = \sum_i \frac{\overline{n}_i \overline{\mathcal{P}}_i + k_i}{\overline{n}_i + N} \quad \geq \quad \sum_i \frac{\overline{n}_i \frac{k_i}{N} + k_i}{\overline{n}_i + N} = \sum_i \frac{\frac{\overline{n}_i k_i + k_i N}{N}}{\overline{n}_i + N}$$
$$= \sum_i \frac{\frac{k_i(\overline{n}_i + N)}{N}}{\overline{n}_i + N} = \sum_i \frac{k_i}{N} = \frac{1}{N} \sum_i k_i = \frac{N}{N} = 1.$$

The bound $\sum_i \overline{\mathcal{P}}'_i \leq \sum_i \overline{\mathcal{P}}_i$ is derived using that

$$\forall i. \frac{k_i}{N} \leq \overline{\mathcal{P}}_i \iff \forall i. k_i \leq \overline{\mathcal{P}}_i N.$$

Then, it follows that

$$\sum_i \overline{\mathcal{P}}'_i = \sum_i \frac{\overline{n}_i \overline{\mathcal{P}}_i + k_i}{\overline{n}_i + N} \quad \leq \quad \sum_i \frac{\overline{n}_i \overline{\mathcal{P}}_i + \overline{\mathcal{P}}_i N}{\overline{n}_i + N} = \sum_i \frac{\overline{\mathcal{P}}_i(\overline{n}_i + N)}{\overline{n}_i + N} = \sum_i \overline{\mathcal{P}}_i.$$

The proof for the bounds

$$\sum_i \underline{\mathcal{P}}_i \leq \sum_i \underline{\mathcal{P}}'_i \leq 1$$

is symmetrical to the one above.

Next, we consider the case for a prior-data conflict, that is, the bounds from Equation 5. The existential condition $\exists j. \frac{k_j}{N} \geq \overline{\mathcal{P}}_j$ does not have to be unique, hence we make a case distinction on the indexes for which the existential quantification holds and for which it does not. Let $I = \{1, \ldots, m\}$ be the set of indices that enumerates the m successor states at the state-action pair we consider. By Lemma 1 we know that there are at most $m-1$ prior-data conflicts. Hence, we can partition I into two non-empty subsets, I_A containing all indices where the point estimate agrees with the prior interval, and I_C the set of indices where there is a prior-data conflict. That is,

$$I_A = \{i \in I \mid \frac{k_i}{N} \leq \overline{\mathcal{P}}_i\}, \qquad I_C = \{i \in I \mid \frac{k_i}{N} > \overline{\mathcal{P}}_i\}.$$

We use this partition to split the sum over all indices in two:

$$\sum_i \overline{\mathcal{P}}'_i = \sum_{i \in I} \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\underline{n}_i + N} = \sum_{i \in I_A} \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\underline{n}_i + N} + \sum_{i \in I_C} \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\underline{n}_i + N}$$

We now reason on each part separately.

For $i \in I_A$ we have $\frac{k_i}{N} \leq \overline{\mathcal{P}}_i$, which also means $N \leq \frac{k_i}{\overline{\mathcal{P}}_i}$.

$$\sum_{i \in I_A} \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\underline{n}_i + N} \quad \geq \quad \sum_{i \in I_A} \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\left(\underline{n}_i + \frac{k_i}{\overline{\mathcal{P}}_i}\right)} = \sum_{i \in I_A} \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\left(\frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\overline{\mathcal{P}}_i}\right)} = \sum_{i \in I_A} \overline{\mathcal{P}}_i \left(\frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\underline{n}_i \overline{\mathcal{P}}_i + k_i}\right) = \sum_{i \in I_A} \overline{\mathcal{P}}_i.$$

Next, for $i \in I_C$ we have $\frac{k_i}{N} > \overline{\mathcal{P}}_i$, and thus also $k_i > \overline{\mathcal{P}}_i N$. Then we have the following:

$$\sum_{i \in I_C} \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\underline{n}_i + N} \quad > \quad \sum_{i \in I_C} \frac{\underline{n}_i \overline{\mathcal{P}}_i + \overline{\mathcal{P}}_i N}{\underline{n}_i + N} = \sum_{i \in I_C} \overline{\mathcal{P}}_i \frac{\underline{n}_i + N}{\underline{n}_i + N} = \sum_{i \in I_C} \overline{\mathcal{P}}_i.$$

Finally, we put the two partitions back together using the inequalities derived on both, and conclude by using the assumption that the prior is valid, i.e., $\sum_i \overline{\mathcal{P}}_i \geq 1$:

$$\sum_i \overline{\mathcal{P}}'_i = \sum_{i \in I_A} \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\underline{n}_i + N} + \sum_{i \in I_C} \frac{\underline{n}_i \overline{\mathcal{P}}_i + k_i}{\underline{n}_i + N} \quad > \quad \sum_{i \in I_A} \overline{\mathcal{P}}_i + \sum_{i \in I_C} \overline{\mathcal{P}}_i = \sum_{i \in I} \overline{\mathcal{P}}_i \geq 1.$$

The proof for the lower bounds, that $\sum_i \underline{\mathcal{P}}'_i \leq 1$, follows the same reasoning by symmetry.

□

C Exploration Scheme

We detail the exploration scheme in Algorithm 1 below.

Algorithm 1 Exploration scheme.

Input: K : number of trajectories.
Input: H : max trajectory length.
Input: $M(S, s_I, A, P, R)$: underlying MDP.
Input: φ : specification.
Input: $\mathcal{A}$: algorithm for exploration and robust verification.

```
for s, a ∈ S × A do
    ▷ Initialize counters
    #(s, a) = 0
    #(s, a, s') = 0 : ∀s' ∈ S
    #_i(s, a) = 0
    #_i(s, a, s') = 0 : ∀s' ∈ S
end for
for k ∈ [1, ··· , K] do
    if ∃s, a ∈ S × A : #_i(s, a) >= #(s, a) then
        ▷ Compute new policies.
        Give iteration counters #_i(s, a) and #_i(s, a, s') to A
        Get sampling policy from A : π_sampling
        Get robust policy from A : π_robust
        Evaluate π_robust on M according to φ
        ▷ Update global counters
        #(s, a) += #_i(s, a) : ∀s, a ∈ S × A
        #(s, a, s') += #_i(s, a, s') : ∀s, a ∈ S × A × S
        ▷ Reset iteration counters
        #_i(s, a) = 0 : ∀s, a ∈ S × A
        #_i(s, a, s') = 0 : ∀s, a ∈ S × A × S
    end if
    Sample τ from M following π_sampling with max size H
    Increment #_i(s, a) and #_i(s, a, s') according to τ.
end for
```

D Detailed Problem Domain Descriptions

We give a detailed description of each model we use in the experimental evaluation below, together with the specification and (if applicable) its source.

Chain problem. We consider a larger version of the chain problem Araya-López et al. [2011] with 30-states. There are three actions, one progresses with probability 0.95 to the next state, and resets the model to the initial state with probability 0.05. The second action does the same, but with

reversed probabilities. The third action has probability 0.5 for both progressing and resetting. Every action gets a reward of 1. As specification, we minimize the reward to reach the last state of the chain: $\mathrm{R}_{\text{Min}}(\Diamond\, T)$. This can be seen as an instance of the stochastic shortest path problem [Bertsekas, 2005].

Aircraft collision avoidance. We model a small, simplified instance of the aircraft collision avoidance problem Kochenderfer [2015]. Two aircraft, one controlled, one adversarial, approach each other. The controlled aircraft can increase, decrease, or stay at the current altitude with a success probability of 0.8. The adversarial aircraft can do the same, but does so with probabilities 0.3, 0.3, 0.4 respectively. To goal is to maximize the probability of the two aircraft passing each other without a collision, expressed by the temporal logic specification $\mathbb{P}_{\text{Max}}(\neg\text{collision}\,\mathsf{U}\,\text{passed})$.

Grid world. We consider a slippery 10×10 grid world as in Derman et al. [2019], where a robot starts in the north-west corner and has to navigate towards a target position. The robot can move in each of the four cardinal directions with a success probability of 0.55, and a probability of 0.15 to move in each of the other directions. Throughout the grid, the robot has to avoid traps. The model has 100 states and 1450 transitions. We consider *safety* specifications that maximize the probability for reaching the north-east (NE) corner without getting trapped, i.e. $\mathbb{P}_{\text{Max}}(\neg\text{trapped}\,\mathsf{U}\,\text{NE})$.

Bandit. We consider a 99-armed bandit Lattimore and Szepesvári [2020], where each arm (action) has an increased probability of success, $0.01, 0.02, \ldots, 0.99$ respectively. The goal is to find the action that has the highest probability of success: $\mathbb{P}_{\text{Max}}(\Diamond\,\text{success})$.

Betting game. We consider a betting game from [Bäuerle and Ott, 2011], in which an agent starts with 10 coins and attempts to maximize the number of coins after 6 bets. When a bet is won, the amount of coins placed is doubled, when lost the amount of coins placed is removed. The agent may place bets of 0, 1, 2, 5, and 10 coins. We consider two versions of the game, one which is FAVOURABLE to the player, with a win probability of 0.8, and one that is unFAVOURABLE to the player, with a win probability of 0.2. After six bets the player receives a state-based reward that equals the number of coins left. This yields an MDP of 300 states and 1502 transitions. The specification is to maximize the reward after for reaching a terminal state after these six bets.

E Comparison with UCRL2.

UCRL2 [Jaksch et al., 2010] is a reinforcement learning algorithm, meaning it is designed to collect reward while exploring, in contrast to our setting where we have a clear separation between exploration and policy computation (i.e. computing the reward). We use UCRL2 to learn a uMDP, but then compute a robust policy on that learned model, instead of an optimistic policy as is standard for UCRL2. Furthermore, we make the following changes to the UCRL2 algorithm to make it more comparable to our setting:

1. Just as with the PAC intervals, we use MAP-estimation instead of the frequentist approach to estimate the point estimates.
2. UCRL2 does not compute individual intervals, but a set of distributions around the distribution of point estimates. In particular, it takes the set of distributions for which the ℓ^1 norm to the estimated distribution is less than or equal to

$$\sqrt{\frac{14|S|\log(2|A|t_k \cdot {}^1\!/\!_\gamma)}{\max(1, N)}}, \tag{10}$$

   see [Jaksch et al., 2010] for details on this bound. We use this bound for the individual intervals (bounded by ε to ensure lower bounds greater than zero). As the robust value iteration for uMDPs restricts to valid distributions with the product of these intervals, we do not use the ℓ^1 norm, but put in the intervals derived from MAP-estimation with this bound.
3. Finally, the UCRL2 algorithm assumes that the reward function is also unknown, and attempts to learn that as well. We assume the reward function to be known in our setting.

F Complete Experimental Evaluation

In this Section we present the full experimental evaluation of our method. For our main conclusions, we refer back to Section 6, and only comment here on additional experiments not found in the main text.

In Figure 7 we show the Performance, and Estimation Error for all six environments and all four learning methods. Additionally, we also define a *model error*: For each transition, we compute the maximum distance between the true probability and the lower and upper bounds of the interval in the uMDP (or the point estimate for MAP-estimation), and then take the average over all these distances.

Figure 6 shows the performance of LUI on the Grid environment with different prior strength choices. We note little difference, and thus conclude that our LUI approach is not very sensitive to small changes in prior choices.

Figures 8 and 9 shows the results for switching the probabilities on the Chain environment, for two different randomization parameters in the exploration: $\xi = 0.8$ and $\xi = 1.0$ (no randomization). Figures 10 and 11 show the same experiment on the Betting Game, switching from a favourable game to an unfavourable one, again with randomization parameters $\xi = 0.8$ and $\xi = 1.0$. We note the need for randomization during exploration, especially in the Chain environment.

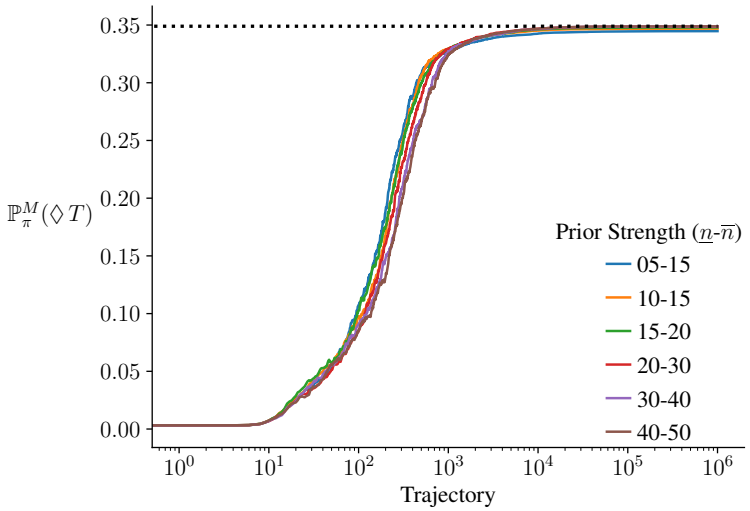


Figure 6: Prior strength evaluation on the Grid environment.

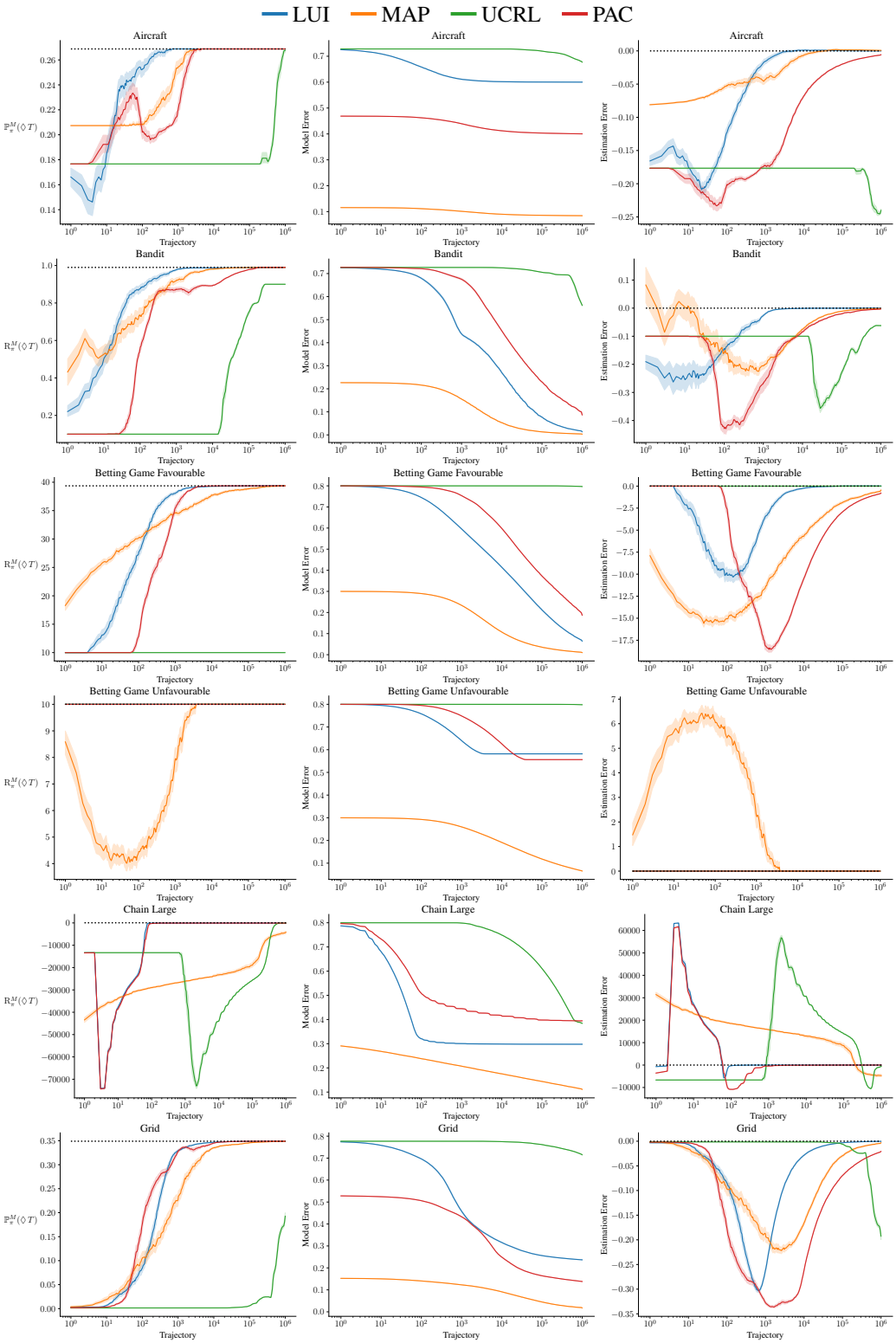


Figure 7: Performance, model error, and estimation error for all four learning methods on all six environments.

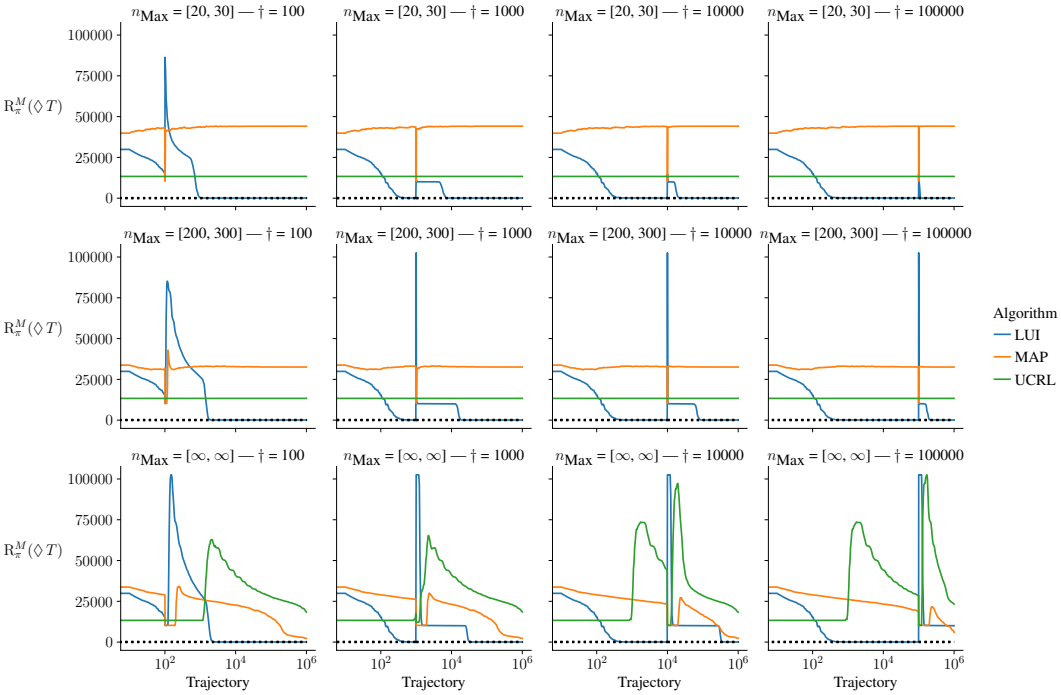


Figure 8: Environment change on the Chain environment at different points $\dagger \in \{10^2, \ldots, 10^5\}$ using randomization parameter $\xi = 0.8$ in the exploration.

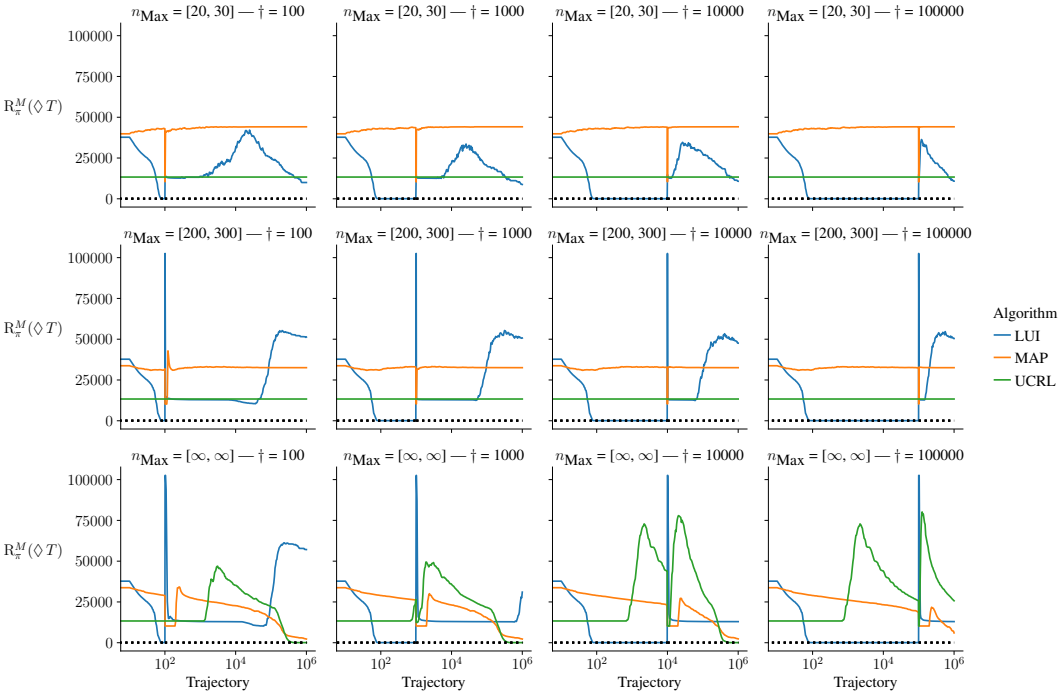


Figure 9: Environment change on the Chain environment at different points $\dagger \in \{10^2, \ldots, 10^5\}$ using randomization parameter $\xi = 1.0$ in the exploration.

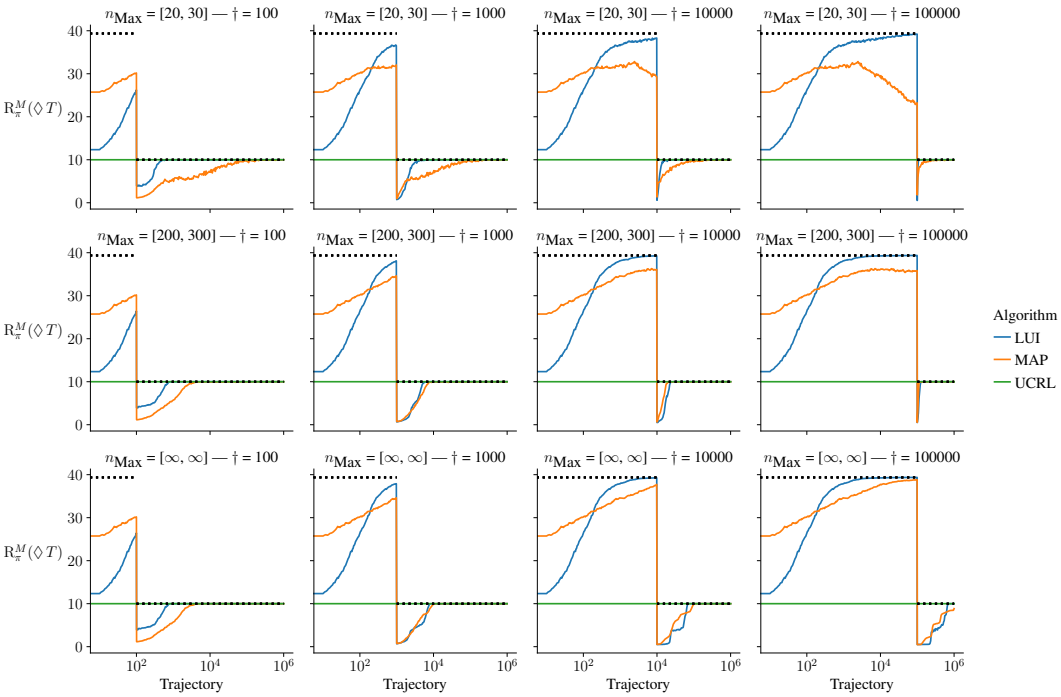


Figure 10: Environment change on the Betting Game environment at different points $\dagger \in \{10^2, \ldots, 10^5\}$ using randomization parameter $\xi = 0.8$ in the exploration.

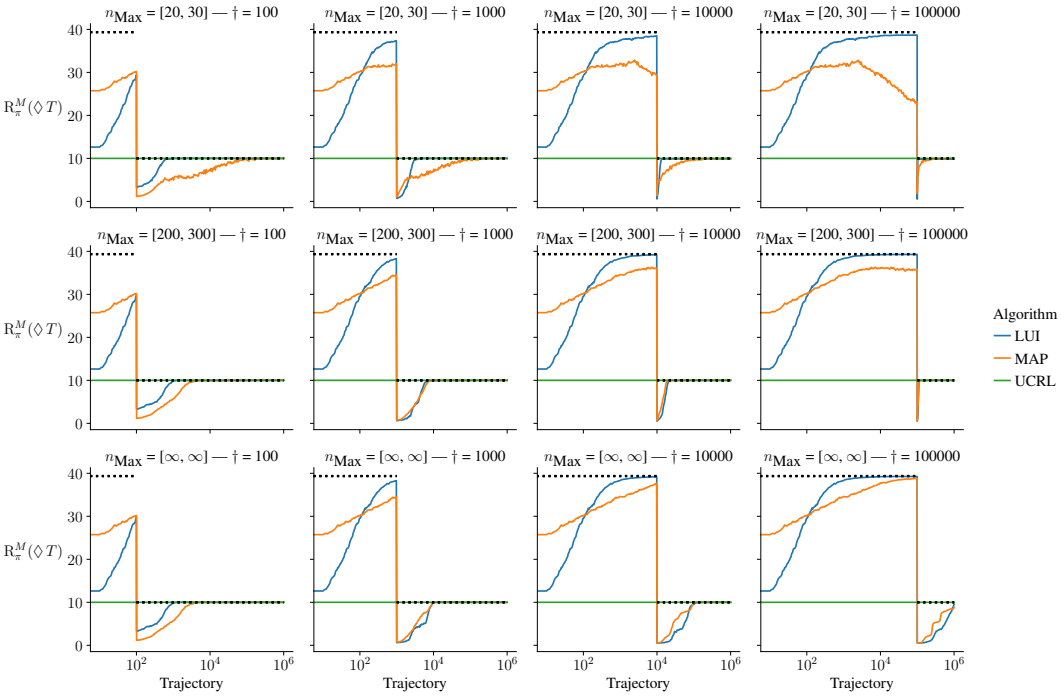


Figure 11: Environment change on the Betting Game environment at different points $\dagger \in \{10^2, \ldots, 10^5\}$ using randomization parameter $\xi = 1.0$ in the exploration.