Abstract

While learning in an unknown Markov Decision Process (MDP), an agent should trade off exploration to discover new information about the MDP, and exploitation of the current knowledge to maximize the reward. Although the agent will eventually learn a good or optimal policy, there is no guarantee on the quality of the intermediate policies. This lack of control is undesired in real-world applications where a minimum requirement is that the executed policies are guaranteed to perform at least as well as an existing baseline. In this paper, we introduce the notion of conservative exploration for average reward and finite horizon problems. We present two optimistic algorithms that guarantee (w.h.p.) that the conservative constraint is never violated during learning. We derive regret bounds showing that being conservative does not hinder the learning ability of these algorithms.

1 Introduction

While Reinforcement Learning (RL) has achieved tremendous successes in simulated domains, its use in real system is still rare. A major obstacle is the lack of guarantees on the learning process, that makes difficult its application in domains where hard constraints (e.g., on safety or performance) are present. Examples of such domains are digital marketing, healthcare, finance, and robotics. For a vast number of domains, it is common to have a known and reliable baseline policy that is potentially suboptimal but satisfactory. Therefore, for applications of RL algorithms, it is important that are guaranteed to perform at least as well as the existing baseline.

In the offline setting, this problem has been studied under the name of safety w.r.t. a baseline (Bottou et al., 2013; Thomas et al., 2015a,b; Swaminathan and Joachims, 2015; Petrik et al., 2016; Laroche et al., 2019; Simão and Spaan, 2019). Given a set of trajectories collected with the baseline policy, these approaches aim to learn a policy –without knowing or interacting with the MDP– that is guaranteed (e.g., w.h.p.) to perform at least as good as the baseline. This requires that the set of trajectories is sufficiently reach in order to allow to perform counterfactual reasoning with it. This often implies strong requirements on the ability of exploration of the baseline policy. These approaches can be extended to a semi-batch settings where phases of offline learning are alternated with the executing of the improved policy. This is the idea behind conservative policy iteration (e.g., Kakade and Langford, 2002; Pirotta et al., 2013b) where the goal is to guarantee a monotonic policy improvement in order to overcome the policy oscillation phenomena (Bertsekas, 2011). These approaches has been successively extended to function approximation preserving theoretical guarantees (e.g., Pirotta et al., 2013a; Achiam et al., 2017). A related problem studied in RL is the one of safety, where the algorithm is forced to satisfy a set of constraints, potentially not directly connected with the performance of a policy (e.g., Altman, 1999; Berkenkamp et al., 2017; Chow et al., 2018).
Conservative Exploration in Reinforcement Learning

armored bandits (Wu et al., 2016), contextual linear bandits (Kazerouni et al., 2017), and stochastic combinatorial semi-bandits (Ketabi et al., 2019). These papers formulate the problem using a constraint defined based on the performance of the baseline policy (mean of the baseline arm in the multi-armed bandit case), and modify the corresponding UCB-type algorithm (Auer et al., 2002) to satisfy this constraint. Another algorithm in the online setting is by Mansour et al. (2015) that balances exploration and exploitation such that the actions taken are compatible with the agent’s (customer’s) incentive formulated as a Bayesian prior.

While the conservative exploration problem is well-understood in bandits, little is known about this setting in RL, where the actions taken by the learning agent affect the system state. This dynamic component makes the definition of the conservative condition much less obvious in RL. While in the bandit case it is sufficient to look at (an estimate of) the immediate reward to perform a conservative decision, in MDPs acting greedily may not be sufficient since an action can be “safe” in a single step but lead to a potentially dangerous state space where it will not be possible to satisfy the conservative constraint. Moreover, after $t$ steps, the action followed by the learning agent may lead to a state that is possibly different from the one observed by following the baseline. This dynamical aspect is not captured by the bandit problem and should be explicitly taken into account by the learning agent in order to perform a meaningful decision. This, together with the problem of counterfactual reasoning in an unknown MDP, make the conservative exploration problem much more difficult (and interesting) in RL than in bandits.

This paper aims to provide the first analysis of conservative exploration in RL. In Sec. 3 we explain the design choices that lead to the definition of the conservative condition for RL (both in average reward and finite horizon settings), and discuss all the issues introduced by the dynamical nature of the problem. Then, we provide the first algorithm for efficient conservative exploration in average reward and analyze its regret guarantees. The variant for finite-horizon problems is postponed to the appendix. We conclude the paper with synthetic experiments.

2 Preliminaries

We consider a Markov Decision Process (Puterman, 1994, Sec. 8.3) $M = (S, A, p, r)$ with state space $S$ and action space $A$. Every state-action pair $(s, a)$ is characterized by a reward distribution with mean $r(s, a)$ and support in $[0, r_{\max}]$, and a transition distribution $p(\cdot | s, a)$ over next states. We denote by $S = |S|$ and $A = |A|$ the number of states and action A stationary Markov randomized policy $\pi : S \rightarrow P(A)$ maps states to distributions over actions. The set of stationary randomized (resp. deterministic) policies is denoted by $\Pi^R$ (resp. $\Pi^{SD}$). Any policy $\pi \in \Pi^R$ has an associated long-term average reward (or gain) and a bias function defined as

$$g^\pi(s) = \lim_{T \to +\infty} \frac{1}{T} \sum_{t=1}^{T} r(s_t, a_t)$$

and

$$h^\pi(s) = C^* \lim_{T \to +\infty} \mathbb{E}_s^\pi \left[ \sum_{t=1}^{T} (r(s_t, a_t) - g^\pi(s_t)) \right],$$

where $\mathbb{E}_s^\pi$ denotes the expectation over trajectories generated starting from $s_1 = s$ with $a_t \sim \pi(s_t)$. The bias $h^\pi(s)$ measures the expected total difference between the reward and the stationary reward in Cesaro-limit (denoted by $C^*$-lim). We denote by $sp(h^\pi) = \max_s h^\pi(s) - \min_s h^\pi(s)$ the span (or range) of the bias function.

Assumption 1. The MDP $M$ is ergodic.

In ergodic MDPs, any policy $\pi \in \Pi^R$ has constant gain, i.e., $g^\pi(s) = g^\pi$ for all $s \in S$. There exists a policy $\pi^* \in \arg \max_{\pi \in \Pi^R} g^\pi$ for which $(g^*, h^*) = (g^\pi^*, h^\pi^*)$ satisfy the optimality equations,

$$h^\pi(s) + g^* = L h^\pi(s) := \max_{a \in A} \{ r(s, a) + p(\cdot | s, a)^T h^* \},$$

where $L$ is the optimal Bellman operator. We use $D = \max_{s, s' \in S} \min_{\pi \in \Pi^D} \mathbb{E}[\tau_{\pi}(s'|s)]$ to denote the diameter of $M$, where $\tau_{\pi}(s'|s)$ is the hitting time of $s'$ starting from $s$. We introduce the “worst-case” diameter

$$\Upsilon = \max_{s \neq s'} \max_{\pi \in \Pi^D} \mathbb{E}[\tau_{\pi}(s'|s)],$$

which defines the worst-case time it takes for any policy $\pi$ to move from any state $s$ to $s'$. Assum. guarantees that $D \leq \Upsilon < \infty$.

Exploration in RL. Let $M^*$ be the true unknown MDP. We consider the learning problem where $S, A$ and $r_{\max}$ are known, while rewards $r$ and transition probabilities $p$ are unknown and need to be estimated online. We evaluate the performance of a learning algorithm $\mathfrak{A}$ after $T$ time steps by its cumulative regret

$$R(\mathfrak{A}, T) = T g^* - \sum_{t=1}^{T} r_t(s_t, a_t).$$

The exploration-exploitation dilemma is a well-known problem in RL and (nearly optimal) solutions have been proposed in the literature both base on optimism-in-the-face-of-uncertainty (OFU, e.g., Jaksch et al., 2010; Bartlett and Tewari, 2009; Fruit et al., 2018a) and Thompson sampling (TS, e.g., Gopalan and Mannor, 2015; Osband and Roy, 2010). Refer to Lazari et al. (2019) for more details.
3 Conservative Exploration in RL

In conservative exploration, a learning agent is expected to perform as well as the optimal policy over time (i.e., regret minimization) under the constraint that at no point in time its performance is significantly worse than a known baseline policy \( \pi_b \in \Pi^{SR} \). This problem has been studied in the bandit literature \cite{wu2016, kazerouni2017}, where the conservative constraint compares the cumulative expected reward obtained by the actions \( a_1, a_2, \ldots, a_t \) selected by the algorithm to the one of the baseline action \( a_b \),

\[
\forall t > 0, \quad \sum_{i=1}^{t} r(a_i) \geq (1 - \alpha) t \cdot r(a_b), \quad (3)
\]

where \( r(a) \) is the expected reward of action \( a \). At any time \( t \), conservative exploration algorithms first query a standard regret minimization algorithm (e.g., UCB) and decide whether to play the proposed action \( \tilde{a}_t \) or the baseline \( a_b \) based on the accumulated budget (i.e., past rewards) and whether the estimated performance of \( \tilde{a}_t \) is sufficient to guarantee that the conservative constraint is satisfied at \( t + 1 \) after \( \tilde{a}_t \) is executed. While \cite{evrardo} effectively formalizes the objective of constraining an algorithm to never perform much worse than the baseline, in RL it is less obvious how to define such constraint. In the following we review three possible directions, we point out their limitations, and we finally propose a conservative condition for RL for which we derive an algorithm in the next section.

**Gain-based condition.** Instead of actions, RL exploration algorithms (e.g., UCRL2), first select a policy and then execute the corresponding actions. As a result, a direct way to obtain a conservative condition is to translate the reward of each action in \( \tilde{a}_t \) to the \textit{gain} associated to the policies selected over time, i.e.,

\[
\forall t > 0, \quad \sum_{i=1}^{t} g^{\pi_i} \geq (1 - \alpha) t \cdot g^{\pi_b}. \quad (4)
\]

The main drawback of this formulation is that the gain \( g^{\pi_i} \) is the expected \textit{asymptotic} average reward of a policy and it may be very far from the \textit{actual} reward accumulated while executing \( \pi_i \) in the specific state \( s_i \) achieved at time \( i \). The same reasoning applies to the baseline policy, whose cumulative reward up to time \( t \) may significantly differ from \( t \) times its gain. As a result, an algorithm that is conservative in the sense of \cite{evrardo} may still perform quite poorly in practice depending on \( t \), the initial state, and the actual trajectories observed over time.

**Reward-based condition.** In order to address the concerns about the gain-based condition, we could define the stronger condition

\[
\forall t > 0, \quad \sum_{i=1}^{t} r_i \geq (1 - \alpha) \sum_{i=1}^{t} r_i^b, \quad (5)
\]

where \( r_i \) is the sequence of rewards obtained while executing the algorithm and \( r_i^b \) is the reward obtained by the baseline. While this condition may be desirable in principle (the learning algorithm never performs worse than baseline), it is impossible to achieve. In fact, even if the optimal policy \( \pi^* \) is executed for all \( t \) steps, the condition may still be violated because of an unlucky realization of transitions and rewards. If we wanted to accounting for the effect of randomness, we would need to introduce an additional slack of order \( O(\sqrt{t}) \) (i.e., the cumulative deviation due to the randomness in the environment), which would make the condition looser and looser over time.

**Condition in expectation.** The previous remarks could be solved by taking the expectation of both sides

\[
\forall t > 0, \quad \mathbb{E}_\mathfrak{A} \left[ \sum_{i=1}^{t} r_i(s_i, a_i) \bigg| s_1 = s \right] \geq (1 - \alpha) \mathbb{E}_\mathfrak{A} \left[ \sum_{i=1}^{t} r_i(s_i, a_i) \bigg| s_1 = s, \pi_b \right], \quad (6)
\]

where \( \mathbb{E}_\mathfrak{A} \) denotes the expectation w.r.t. the trajectory of states and actions generated by the learning algorithm \( \mathfrak{A} \), while the RHS is simply the expected reward obtain by running the baseline for \( t \) steps. Condition \cite{evrardo} effectively captures the nature of the RL problem w.r.t. the bandit case. In fact, after \( t \) steps, the actions followed by the learning algorithm may lead to a state that is possibly very different from the one we would have reached by playing only the baseline policy from the beginning. This deviation in the state dynamics needs to be taken into account when deciding if an exploratory policy is safe to play in the future. In the bandit case, selecting the baseline action contributes to \textit{build a conservative budget} that can be \textit{spent} to play explorative actions later on (i.e., by selecting \( a_b \), the LHS of \cite{evrardo} is increased by \( r(a_b) \), while only a fraction \( 1 - \alpha \) is added to the RHS, thus increasing the margin that may allow playing alternative actions later). In the RL case, selecting policy \( \pi_b \) at time \( t \) may not immediately contribute to increasing the conservative budget. In fact, the state \( s_t \) where \( \pi_b \) is applied may significantly differ from the state that \( \pi_b \) \textit{would have achieved} had we selected it from the beginning. As a result, a conservative RL algorithm should be extra-cautious when selecting policies different from \( \pi_b \), since their execution may lead to unfavorable states, where it is difficult to recover good performance, even when selecting the baseline policy.
While this may seem a reasonable requirement, unfortunately it is impossible to build an empirical estimate of \( \epsilon_t \) that a conservative exploration algorithm could use to guide the choice of policies to execute. In fact, the LHS averages the performance of the algorithm over multiple executions, while in practice we have only access to a single realization of the algorithm’s process. This prevents from constructing accurate estimates of such expectation directly from the data observed up to time \( t \). A possible approach would be to construct an estimate of the MDP and use it to replay the algorithm itself for \( t \) steps. Besides prohibitive computational complexity, the resulting estimate of the expected cumulative reward of \( \mathfrak{A} \) would suffer from an error that increases with \( t \), thus making it a poor proxy for \( \mathfrak{A} \).

**Condition with conditional expectation.** Let \( t \) be a generic time and \( \mu_t = (\pi_1, \pi_2, \ldots, \pi_t) \), the non-stationary policy executed up to \( t \). We require the algorithm to satisfy the following *conditional conservative condition*

\[
\forall t > 0, \quad \mathbb{E} \left[ \sum_{i=1}^{t} r_i(s_i, a_i) | s_1 = s, \mu_t \right] 
\geq (1 - \alpha) \mathbb{E} \left[ \sum_{i=1}^{t} r_i(s_i, a_i) | s_1 = s, \pi_b \right].
\]

(7)

where the expectations are taken w.r.t. the trajectories generated by a fixed non-stationary policy \( \mu_t \) (i.e., we ignore how rewards affect \( \mu_t \)). Notice that this condition is now stochastic, as \( \mu_t \) itself is a random variable and thus we require to satisfy \( \mathfrak{C} \) with *high probability*. This formulation can be seen as resembling a *pseudo-performance evaluation* of the algorithm instead of the actual expectation as in \( \mathfrak{A} \) and it is similar to \( \mathfrak{C} \), which takes the expected performance of each of the (random) actions, thus ignoring their correlation with the rewards. This formulation has several advantages w.r.t. the conditions proposed above: 1) it considers the sum of rewards rather than the gain as \( \mathfrak{C} \), thus capturing the dynamical nature of RL. 2) it contains expected values, so as to avoid penalizing the algorithm by unlucky noisy realizations as \( \mathfrak{C} \). As shown in the next section, it can be verified using the samples observed by the algorithm unlike \( \mathfrak{A} \).

The finite-horizon case. We conclude the section, by reformulating \( \mathfrak{C} \) in the finite-horizon case. In this setting, the learning agent interacts with the environment in episodes of fixed length \( H \). Let \( \pi \) be the initial state, \( \pi_t \) be the policy proposed at episode \( j \) and let \( t = (k - 1)H + 1 \) be beginning of the \( k \)-th episode. Then \( \mu_k \) is a sequence of policies \( \pi_j \), each executed for \( H \) steps. In this case, condition \( \mathfrak{C} \) can be conveniently written as

\[
(1 - \alpha) k \mathbb{V}_1^\pi_b(\pi) \leq \mathbb{E} \left[ \sum_{i=1}^{t} r_i(s_i, a_i) | s_1 = s, \mu_t \right] 
= \sum_{j=1}^{k} \mathbb{E} \left[ \sum_{i=1}^{H} r_i^j(s_i^j, a_i^j) | s_1 = s, \pi_j \right] 
= \sum_{j=1}^{k} \mathbb{V}_1^\pi_j(\pi) 
\]

(8)

where \( \mathbb{V}_1^\pi \) is the \( H \) step value function of \( \pi \) at the first stage. In this formulation, the conservative condition has a direct interpretation, as it directly mimics the bandit case \( \mathfrak{C} \). In fact, the performance of the algorithm up to episode \( k \) is simply measured by the sum of the value functions of the policies executed over time (each for \( H \) steps) and it is compared to the value function of the baseline itself. Note that this definition is compatible with the regret: \( R_H(\mathfrak{A}, K) = \sum_{k=1}^{H} \mathbb{V}^*(\pi) - \mathbb{V}^{\pi_b}(\pi) \). Indeed, the regret defined in expectation w.r.t. the stochasticity of the model but not w.r.t. the algorithm, there is no expectation w.r.t. the possible sequence of policies generated by \( \mathfrak{A} \).

4 Conservative UCRL

In this section, we introduce conservative upper-confidence bound for reinforcement learning (CUCRL2), an efficient algorithm for exploration-exploitation in average reward that both minimize the regret \( \mathfrak{C} \) and satisfy condition \( \mathfrak{C} \).

CUCRL2 builds on UCRL2 in order to perform efficient conservative exploration. At each episode \( k \), CUCRL2 builds a bounded parameter MDP \( \mathcal{M}_k = (\mathcal{S}, \mathcal{A}, r, p) \), \( r(s, a) \in B^k_r(s, a), p(\cdot | s, a) \in B^k_p(s, a) \), where \( B^k_r(s, a) \in [0, r_{\text{max}}] \) and \( B^k_p(s, a) \in \Delta_S \) are high-probability confidence intervals on the rewards and transition probabilities such that \( M^* \in \mathcal{M}_k \) w.h.p. and \( \Delta_S \) is the \( S \)-dimensional simplex. This confidence intervals can be built using Hoefding or empirical Bernstein inequalities by using the samples available at episode \( k \) (e.g., Jaksch et al. 2010 [10]; Agrawal et al. 2018 [18]). CUCRL2 computes an optimistic policy \( \bar{\pi}_k \) in the same way as UCRL2: \( \bar{\pi}_k = \text{arg max}_{\pi \in \mathcal{P}_d} \left\{ \mathbb{E}^\pi(M) \right\} \). This problem can be solved using EVI (see Fig. [3] in appendix) on the optimistic optimal Bellman operator \( \mathcal{L}^+_k \) of \( \mathcal{M}_k \) (Jaksch et al. 2010 [10]). Then, it needs to decide whether policy

\[
\mathcal{L}^+_k v(s) = \max_{a} \left\{ \max_{r \in B^k_r(s,a)} \{ r \} + \max_{p \in B^k_p(s,a)} p^Tv \right\}.
\]
We now derive a checkable conservative condition from data. In order to evaluate \( CUCRL2 \) from data, one may be tempted to first replace the sum of rewards obtained by each policy \( \pi_j \) in \( \mu_1 \) on the lhs side by its gain \( g^{\pi_j} \), similar to the gain-based condition in \( \text{Eq. 4} \). Indeed, under Asm. 1 any stationary policy \( \pi \) receives asymptotically an expected reward \( g^\pi \) at each step. Unfortunately, in our case \( \sum_{i=1}^t r_i / \mu_j \neq \sum_{j=1}^k T_j g^{\pi_j} \). In fact, when evaluating a policy for a finite number of steps, we need to account for the time required to reach the steady regime (i.e., mixing time) and, as such, the influence of the state at which the policy is started. The notion of reward collected during the transient regime is captured by the bias function \( h^\pi \). In particular, for any stationary (unichain) policy \( \pi \in \Pi^{SR} \) with gain \( g^\pi \) and gain function \( h^\pi \) executed for \( t \) steps, we have that:

\[
E \left[ \sum_{i=1}^t r_i \mid s_1 = s, \pi \right] = t g^\pi + h^\pi(s) - P^\pi_1(\cdot\mid s)^T h^\pi. \tag{9}
\]

\[\text{Eq. 9}\]

Puterman (1994) Sec. 8.2.1) refers to the gain as “stationary” reward while to the bias as “transient” reward.

---

**Input:** \( \pi_0 \in \Pi^{SR}, \delta \in (0, 1), r_{max}, S, A, \alpha \in (0, 1) \)

**For episodes** \( k = 1, 2, ... \) **do**

1. **Set** \( t_k = t \) and episode counts \( \nu_k(s, a) = 0 \).
2. **Compute estimates** \( \hat{\rho}_k(s' \mid s, a), \hat{\gamma}_k(s, a) \) and a confidence set \( \mathcal{M}_k \).
3. **Compute an** \( r_{max}/\sqrt{k} \)-approximation \( \tilde{\pi}_k \) of the optimistic planning problem \( \max_{M \in \mathcal{M}_k, \pi \in \Pi^{RS}} g^\pi(M) \).
4. **Compute** \( (g_k^*, h_k^*) = \text{EVI}(\tilde{\pi}_k, r_{max}/\sqrt{k}) \), see Eq. 11.
5. **If** Eq. 15 **is true then** \( \pi_k = \tilde{\pi}_k \) **else** \( \pi_k = \pi_0 \).
6. **Sample action** \( a_t \sim \pi_k(\cdot\mid s_t) \).
7. **While** \( \nu_k(s, a_t) \leq N_k^+(s, a_t) \wedge t \leq t_k + T_{k-1} \) **do**
   - (a) **Execute** \( a_t \), **obtain reward** \( r_t \), and **observe** \( s_{t+1} \).
   - (b) **Set** \( \nu_k(s_t, a_t) = \nu_k(s_t, a_t) + 1 \).
   - (c) **Sample action** \( a_{t+1} \sim \pi_k(\cdot\mid s_{t+1}) \) and **set** \( t = t + 1 \).
8. **Set** \( N_{k+1}(s, a) = N_k(s, a) + \nu_k(s, a), \Lambda_k = \Lambda_k - 1 \cup \{k\} \cdot 1_{\{\nu_k\geq\alpha\}} \) and \( \Lambda_k = \Lambda_k - 1 \cup \{k\} \cdot 1_{\{\nu_k<\alpha\}} \).

Figure 1: CUCRL2 algorithm.

\( \pi_k \) is “safe” to play by checking a conservative condition \( f_c(H_k) \) (see Sec. 4.1) where \( H_k \) contains all the information (samples and chosen policies) available at the beginning of episode \( k \), including the optimistic policy \( \pi_k \). If \( f_c(H_k) \geq 0 \), the UCRL2 policy \( \tilde{\pi}_k \) is “safe” to play and CUCRL2 plays \( \pi_k = \tilde{\pi}_k \) until the end of the episode. Otherwise, CUCRL2 executes the baseline policy \( \pi_b \), i.e., \( \pi_k = \pi_b \). We denote by \( \Lambda_k \) the set of episodes (\( k \) included) where UCRL2 executed an optimistic policy and by \( \Lambda_k = \{1, \ldots, k\} \setminus \Lambda_k \) its complement. Formally, if \( f_c(H_k) \geq 0 \) we set \( \Lambda_k = \Lambda_k - 1 \cup \{k\} \) else \( \Lambda_k = \Lambda_k - 1 \). The pseudocode of CUCRL2 is reported in Fig. 1.

Note that, contrary to what happens in conservative (linear) bandits, the statistics of the algorithm are updated continuously, i.e., using also the samples collected by running the baseline policy. This is possible since UCRL2 is a model-based algorithm and any off-policy sample can be used to update the estimates of the model. To have a better estimate of the conservative condition, it is possible to use the model available at episode \( k \) to re-evaluate the policies \( \pi_l, l < k \) at previous episodes (change line 3 in Fig. 1). This will improve the empirical performance of CUCRL2 but breaks the regret analysis.

**4.1 Algorithmic Conservative Condition**

We now derive a checkable conservative condition that can be incorporated in the UCRL2 structure illustrated in the previous section. In the bandit setting, it is relatively straightforward to turn \( \text{Eq. 4} \) into a condition that can be checked at any time \( t \) using estimates and confidence intervals built from the data collected so far. On the other hand, while condition \( \text{Eq. 7} \) effectively formalizes the requirement that the learning algorithm should constantly perform almost as well as the baseline policy, we need to consider the specific RL structure to obtain a condition that can be verified during the execution of the algorithm itself. In order to simplify the derivation, we rely on the following assumption.

**Assumption 2.** The gain and bias function \( (g^\pi, h^\pi) \) of the baseline policy are known.

As explained in Kazerouni et al., 2017, this is a reasonable assumption since the baseline policy is assumed to be the policy currently executed by the company and for which historical data are available. We will mention how to relax this assumption in Sec. 4.1.

We follow two main steps in deriving a checkable condition:

1. **We need to estimate the cumulative reward obtained by each of the policies played by the learning algorithm directly from the samples observed so far. We do this by relating the cumulative reward to the gain and bias of each policy and then building their estimates.**
2. It is necessary to evaluate whether the policy proposed by UCRL2 is safe to play w.r.t. the conservative condition, before actually executing it. While this is simple in bandit, as each action is executed for only one step. In RL, policies cannot be switched at each step and need to be played for a whole episode. Nonetheless, the length of a UCRL2 episode is not known in advance and this requires predicting for how long the explorative policy could be executed in order to check its performance.

**Step 1: Estimating the conditional conservative condition from data.** In order to evaluate \( \text{Eq. 7} \) from data, one may be tempted to first replace the sum of rewards obtained by each policy \( \pi_j \) in \( \mu_1 \) on the lhs side by its gain \( g^{\pi_j} \), similar to the gain-based condition in \( \text{Eq. 4} \). Indeed, under Asm. 1 any stationary policy \( \pi \) receives asymptotically an expected reward \( g^{\pi} \) at each step. Unfortunately, in our case \( \sum_{i=1}^t r_i / \mu_j \neq \sum_{j=1}^k T_j g^{\pi_j} \). In fact, when evaluating a policy for a finite number of steps, we need to account for the time required to reach the steady regime (i.e., mixing time) and, as such, the influence of the state at which the policy is started. The notion of reward collected during the transient regime is captured by the bias function \( h^\pi \). In particular, for any stationary (unichain) policy \( \pi \in \Pi^{SR} \) with gain \( g^\pi \) and gain function \( h^\pi \) executed for \( t \) steps, we have that:

\[
E \left[ \sum_{i=1}^t r_i \mid s_1 = s, \pi \right] = t g^\pi + h^\pi(s) - P^\pi_1(\cdot\mid s)^T h^\pi. \tag{9}
\]

---

Evra Garcelon, Mohammad Ghavamzadeh, Alessandro Lazaric, Matteo Pirotta
As a result, we have the bounds
\[ t \ g^\pi - sp(h^\pi) \leq \mathbb{E} \left[ \sum_{i=1}^{t} r_i | s_1 = s, \pi \right] \leq t \ g^\pi + sp(h^\pi). \]

Leveraging prior knowledge of the gain and bias of the baseline, we can use the second inequality to directly upper bound the baseline performance as
\[ \mathbb{E} \left[ \sum_{i=1}^{t} r_i | s_1 = s, \pi_b \right] \leq sp(h^{\pi_b}) + t \ g^{\pi_b}. \] (10)

On the other hand, for a generic policy \( \pi \), the gain and bias cannot be directly computed since \( M^* \) is unknown. To estimate the cumulative reward of the algorithm we resort to the estimate of the true MDP build by UCRL2 to construct a pessimistic estimate of the cumulative reward for any policy \( \pi \) (i.e., to perform counterfactual reasoning).

Given a policy \( \pi \) and the bounded-parameter MDP \( \mathcal{M}_k \), we are interested in finding \( g^\pi \) such that: \( g^\pi := \min_{M \in \mathcal{M}_k} \{ \lambda_\pi(M) \} \). Define the Bellman operator \( \mathcal{L}_k^\pi \) associated to \( \mathcal{M}_k \) as: \( \forall v \in \mathbb{R}^n, \forall s \in \mathcal{S} \)
\[ \mathcal{L}_k^\pi v(s) := \min_{r \in B^s_{\mathcal{L}_k} \cap \mathcal{G}_k} r + \min_{p \in B^s_{\mathcal{L}_k} \cap \mathcal{G}_k} \{ p^T v \} \] (11)

Then, there exists \( (g^\pi, h^\pi) \) such that, \( \forall s \in \mathcal{S}, g^\pi e + h^\pi = \mathcal{L}_k^\pi(h^\pi) \) where \( e = (1, \ldots, 1) \) (see Lem. 5 in App. A). Similarly to what is done by UCRL2, we can use EVI with \( \mathcal{L}_k^\pi \) to build an \( \epsilon_k \)-approximate solution of the Bellman equations. Let \( (g_n, v_n) = \mathrm{EVI}(\mathcal{L}_k^\pi, \epsilon_k) \), then \( g_n - \epsilon_k \leq g^\pi \leq g^\pi + \epsilon_k \). The values computed by the pessimistic policy evaluation can be then used to bound the cumulative reward of any stationary policy.

**Lemma 1.** Consider a bounded parameter MDP \( \mathcal{M} \) such that \( M^* \in \mathcal{M} \) w.h.p., a policy \( \pi \) and let \( (g_n, v_n) = \mathrm{EVI}(\mathcal{L}_k^\pi, \epsilon_k) \). Then, under Asm. \( \mathcal{I} \) for any state \( s \in \mathcal{S} \):
\[ \mathbb{E} \left[ \sum_{i=1}^{t} r_i | s_1 = s, \pi \right] \geq t(g_n - \epsilon_k) - sp(v_n). \]

**Step 2: Test safety of optimistic policy.** Let \( t_k \) be the time when episode \( k \) starts. Policies \( \pi_1, \ldots, \pi_{k-1} \) have been executed until \( t_{k-1} \) and UCRL2 computed an optimistic policy \( \bar{\pi}_k \). In order to guarantee that \( \bar{\pi}_k \) is verified the algorithm needs to anticipate how well \( \bar{\pi}_k \) may perform if executed for the next episode. For any policy \( (\pi_j)_{j < k} \cup \{ \bar{\pi}_k \} \), we first compute \( (g_j, h_j) = \mathrm{EVI}(\mathcal{L}_j^\pi_j, \epsilon_j) \) \(^6\) If \( \pi_j = \pi_b \) (i.e., the baseline was executed at episode \( j \)), we let \( (g_j, h_j) = (g_{\pi_b}, h_{\pi_b}) \) and \( \epsilon_j = 0 \). Then
\[ \mathbb{E} \left[ \sum_{i=1}^{t} r_i | s_1 = s, \mu \right] \]
\[ = \sum_{j=1}^{k} \sum_{y \in \mathcal{S}} \mathbb{P} (s_j = y | s, \mu) \cdot \mathbb{E} \left[ \sum_{i=1}^{t_j} r_i | y, \pi_j \right] \] (12)
\[ \geq \sum_{j=1}^{k} T_j (g_j - \epsilon_j) - sp(h_j) \]
\[ + T_k (g_k - \epsilon_k - (1 - \alpha)g_{\pi_b}) \geq 0 \] (13)

where \( t_j \) is time at which episode \( j \) started, \( \mathbb{P} (s_j = y | s, \mu) \) is the probability of reaching state \( y \) after \( t_j \) steps starting from state \( s \) following policy \( \mu \). The inequality follows from Lem. \( \mathcal{I} \). By lower bounding the LHS of (7) by (12) and upper bounding the RHS by (10), the conservative condition becomes:
\[ \sum_{j=1}^{k-1} (T_j (g_j - \epsilon_j - g_{\pi_b}) - sp(h_j)) - sp(h_{\pi_b}) \]
\[ + T_k (g_k - \epsilon_k - (1 - \alpha)g_{\pi_b}) \geq 0 \]

Note that the algorithm should check this condition at the beginning of episode \( k \) in order to understand if the policy \( \bar{\pi}_k \) is safe or if it should resort to playing policy \( \pi_b \). In many OFU algorithms, including UCRL2, the length of episode \( k \) (i.e., \( T_k \) ) is not known at the beginning of the episode. As a consequence, condition (13) is not directly computable. To overcome this limitation, we consider the dynamic episode condition introduced by (Ouyang et al., 2017). This stopping condition provides an upper-bound on the length of each episode as \( T_k \leq T_{k-1} + 1 \), without affecting the regret bound of UCRL2 (up to constants). This condition can be used to further lower-bound the last term in (13) by
\[ T_k (g_k - \epsilon_k - (1 - \alpha)g_{\pi_b}) \]
\[ \geq (T_{k-1} + 1)(g_k - \epsilon_k - (1 - \alpha)g_{\pi_b}) \cdot \mathbb{1}_{(1 - \alpha)g_{\pi_b} \geq g_k - \epsilon_k),} \]

Plugging this lower bound into (13) gives the final conservative condition
\[ \sum_{j=1}^{k-1} (T_j (g_j - \epsilon_j - g_{\pi_b}) - sp(h_j)) - sp(h_{\pi_b}) + (T_{k-1} + 1)(g_k - \epsilon_k - (1 - \alpha)g_{\pi_b}) \cdot \mathbb{1}_{(1 - \alpha)g_{\pi_b} \geq g_k - \epsilon_k)} \]
\[ \geq 0, \] (15)

tested by CUCRL2 at the beginning of each episode. **Unknown** \( g_{\pi_b}, h_{\pi_b} \). If the gain and bias of the baseline are unknown, we can use EVI on \( \mathcal{L}_j^{\pi_b} \) (Eq. 11 with max instead of min) to compute an optimistic
estimate of the cumulative reward of the baseline up to time \( t_l + T_{l-1} + 1 \). While this account for the RHS of Eq. \( 2 \), we simply define \((g^-_l, h^-_l) = \text{EVI}(\mathcal{L}^*_l, \epsilon_l)\) for every episode \( l \in \Lambda^-_{l-1} \) to compute a lower bound to the cumulative reward obtained by the algorithm by playing the baseline in episode before \( k \). Clearly, this approach is very pessimistic and it may be possible to design better strategies for this case.

The finite-horizon case. We conclude this section with a remark on the finite horizon case. This case is much simpler and resemble the bandit setting. We can directly build a lower bound \( 2g^* \) to the value function \( V^*_1 \) by using the model estimate and its uncertainty at episode \( 1 \). This estimate can be computed via extended backward induction –see Azar et al. 2017, Alg. 2– simply subtracting the exploration bonus, see Lem. 10 in App. C. The same approach can be used to construct and optimistic and pessimistic estimate of \( V^*_1 \) when it is unknown. This values can be directly plug in Eq. \( 5 \) to define a checkable condition for the algorithm.

4.2 Regret Guarantees

We start providing an upper-bound to the regret of CUCRL2 showing the dependence on UCRL2 and on the baseline \( \pi_b \). Since the set \( \Lambda_k \) is updated at the end of the episode, we denote by \( \Lambda_T = \Lambda_{k_T} \cup \{k_T\} \cdot 1_{(l \neq k_T)} \) the set containing all the episodes where CUCRL2 played an optimistic policy. The set \( \Lambda_T \) is its complement.

**Lemma 2.** Under Asm. 7 and 3, for any \( T \) and any conservative level \( \alpha \), there exists a numerical constant \( \beta > 0 \) such that the regret of CUCRL2 is upper-bounded as

\[
R(\text{CUCRL2}, T) \leq \beta \left( R_{\text{UCRL2}}(T|\Lambda_T) + (g^* - g^\pi_T) \sum_{l \in \Lambda_T} T_l + sp(h^\pi_T) \sqrt{SAT \ln(T/\delta)} \right),
\]

and the conservative condition \( \text{Eq.} 7 \) is met at every step \( t = 1, \ldots, T \) with probability at least \( 1 - \frac{2\delta}{e} \).

\( R_{\text{UCRL2}}(T|\Lambda_T) \) denotes the regret of UCRL2 over an horizon \( T \) conditioned on the fact that the UCRL2 policy is executed only at episodes \( i \in \Lambda_T \). During the other episodes, the internal statistics of UCRL2 are updated using the samples collected by the baseline policy \( \pi_b \). This does not pose any major technical challenge and, as shown in App. B, the UCRL2 regret can be bounded as follows.

**Lemma 3** (Jaksch et al. 2010). Let \( L_T = \ln \left( \frac{16T}{\delta} \right) \), for any \( T \), there exists a numerical constant \( \beta > 0 \) such that, with probability at least \( 1 - \frac{2\delta}{e} \),

\[
R_{\text{UCRL2}}(T|\Lambda_T) \leq \beta DS \sqrt{ATL_T} + \beta DS^2 AL_T
\]

The second term in Lem. 2 represents the regret incurred by the algorithm when playing the baseline policy \( \pi_b \). The following lemma shows that the total time spent executing conservative actions is sublinear in time (see Lem. 8 in App. B for details).

**Lemma 4.** For any \( T > 0 \) and any conservative level \( \alpha \), with probability at least \( 1 - \frac{2\delta}{e} \), the total number of play of conservative actions is bounded by:

\[
\sum_{l \in \Lambda_T} T_l \leq 2\sqrt{SAT \ln(T)} + \frac{112SATL_T}{(\alpha g^\pi_T)^2} (1 + S(D + Y)^2)
\]

\[
+ \frac{16\sqrt{TL_T}}{\alpha g^\pi_T} \left[(D + Y)\sqrt{SA} + r_{max} + \sqrt{SA}sp(h^\pi_T)\right]
\]

where \( L_T = \ln \left( \frac{5SAT}{\delta} \right) \) and \( Y < \infty \) as in Eq. 7.

**Proof.** Let \( \tau \) be the last episode played conservatively: \( \tau = \sup\{k > 0 : k \in \Lambda_T\} \). This means that at the beginning of episode \( \tau \) the conservative condition was not verified. By rearranging the terms in Eq. 16 and using simple bounds, we can write that:

\[
\Delta_t + 4k_T \left(sp(g^\pi_T) + Y + (1 - \alpha)r_{max}\right) \geq \alpha \sum_{l=1}^{\tau-1} T_l g^\pi_l
\]

where \( \Delta_t := \sum_{l \in \Lambda_t} T_l (\tilde{g}_l - g_l) \) and \((\tilde{g}_l, g_l)\) are optimistic and pessimistic gain of policy \( \pi_t = \pi_{\tau} \). Note that both satisfies the Bellman equation: \( \tilde{g}_l + \tilde{h}_l = \mathcal{L}^+_l \tilde{h}_l \) (see footnote 3) and \( g_l + h_l = \mathcal{L}^*_l h_l \) (see Eq. 17). At this point, the important terms in upper-bounding \( \Delta_t \) are similar to the one analysed in UCRL2. In particular, we have a term depending on the confidence intervals \( \Delta^t_{\text{cl}} := 2\beta_{l}(s_l, a_l) + \beta^l_p(s_l, a_l) \left(sp(\tilde{h}_l) + sp(h^\pi_l)\right) \) and one depending on the transitions \( \Delta^t_{\text{cl}} := p^t(\cdot|s_l, a_l) \left(\tilde{h}_l + h^\pi_l\right) - (\tilde{h}_l(s_{l+1}) - h^\pi_l(s_{l+1})\right) \). Let \( X = \sum_{l=1}^{\tau-1} T_l \). By using the definition of the confidence intervals, it is easy to show that \( \sum_{l \in \Lambda_{\tau-1}} \sum_{t=t_l}^{t_{l+1}-1} \Delta^t_{\text{cl}} \lesssim \sqrt{SATX + (D + Y)v^2AX} \). Define the \( \sigma \)-algebra based on past history at \( t \): \( F_l = \sigma(s_l, a_1, r_1, \ldots, s_l, a_{l}, r_l, s_{l+1}) \). The sequence \( \langle \Delta^t_{\text{cl}}, F_{t_l} \rangle_t \) is an MDS. Thus, using Azuma inequality we have that \( \sum_{l \in \Lambda_{\tau-1}} \sum_{t=t_l}^{t_{l+1}-1} \Delta^t_{\text{cl}} \lesssim (D + Y)\sqrt{T} \). Putting everything together we have a quadratic form in \( X \) and solving it we can write that \( \alpha g^\pi_T X \lesssim b_T + S^2 AL_T (D + Y)^2 / (\alpha g^\pi_T) \) where \( b_T = O(D + Y)\sqrt{SAT} \) (see App. B). The result follows noticing that \( \sum_{l \in \Lambda_{\tau-}} T_l \leq \sum_{l=1}^{\tau-1} T_l + T_{\tau} \).
Conservative Exploration in Reinforcement Learning

Combining the results of Lem. 3 and Lem. 4 into Lem. 2 leads to an overall regret of order $\tilde{O}(\sqrt{T})$, which matches the regret of UCRL2. This shows that CUCRL2 is able to satisfy the conservative condition without compromising the learning performance. Nonetheless, the bound in Lem. 3 shows how conservative exploration is more challenging in RL compared to the bandit setting. While the dependency on the conservative level $\alpha$ is the same, the number of steps the baseline policy is executed can be as large as $\tilde{O}(\sqrt{T})$ instead of constant as in CUCB (Wu et al., 2016). Furthermore, Lem. 2 relies on an ergodicity assumption instead of the more milder communicating assumption needed by UCRL2 to satisfy Lem. 3. Asm. 1 translates into the bound through the “worst-case” diameter $\Upsilon$, which in general is much larger than the diameter $D$. This dependency is due to the need of computing a lower bound to the reward accumulated by policies $\pi_2$ in the past (see Lem. 3). In fact, UCRL2 only needs to compute upper bounds on the gain and the value function returned by EV1 by applying the optimistic Bellman operator $\mathcal{L}^\pi_1$ has span bounded by the diameter $D$. This is no longer the case for computing pessimistic estimates of the value of a policy. Whether Asm. 1 and the worst-case diameter $\Upsilon$ are the unavoidable price to pay for conservative exploration in infinite horizon RL remains as an open question.

The finite-horizon case. App. C shows how to modify UCB-VI (Azar et al., 2017) to satisfy the conservative condition in Eq. 6. In this setting, it is possible to show (see Prop. 1 in appendix) that the number of conservative episodes is simply logarithmic in $T = KH$. Formally, $|A^*_T| = O(H^2 C^2 A \ln(T/\delta)/(\alpha r_b (\Delta_0 + \alpha r_l))$ where $0 < r_b \leq r(s,a)$, for all $(s,a)$, and $\Delta_0 = \min\{V^*_T(s) - V^*_1(s)\}$ is the optimality gap. This problem dependent terms resemble the one in the bandit analysis. The regret of conservative UCB-VI is thus dominated by the UCB-VI term $\tilde{O}(H \sqrt{SAT})$.

5 Experiments

In this section, we report results in the inventory control problem to illustrate the performance of CUCRL2 compared to unconstrained UCRL2 and how it varies with the conservative level. See App. D for additional experiments for both average reward and finite horizon. In order to have a better estimate of the budget, we re-evaluate past policies at each episode. We start considering the stochastic inventory control problem (Puterman, 1994, Sec. 3.2.1) with capacity $M = 6$ and uniform demand. At the beginning of a month $t$, the manager has to decide the number of items to order in order to satisfy the random demand, taking into account the cost of ordering and maintenance of the inventory (see App. D). Since the optimal policy is a threshold policy, as baseline we consider a $(\sigma, \Sigma)$ policy (Puterman, 1994, Sec. 3.2.1) with target stock $\Sigma = 4$ and capacity threshold $\sigma = 4$. Note that $g^* = 0.603$ and $(g^{10}, sp(h^{10})) = (0.565, 0.651)$. We use this domain to perform an ablation study w.r.t. the conservative level $\alpha$. We have taken $T = 70000$ and the results are averaged over 100 realizations.

Fig. 2(left) shows that the regret of CUCRL2 grows at the same speed as the one of the baseline policy $\pi_0$ at the beginning (the conservative phase), because during this phase CUCRL2 is constrained to follow $\pi_0$ to make sure that constraint (7) is satisfied. Clearly, the duration of this conservative phase is proportional to the conservative level $\alpha$. As soon as CUCRL2 has built margin, it starts interleaving exploratory (optimistic) policies with the baseline. After this phase, CUCRL2 has learn enough about the system and has a sufficient margin to behave as UCRL2. As expected, Fig. 2(left) confirms that the convergence to the UCRL2 behavior happens more quickly for larger values of $\alpha$, i.e., when the conservative condition is relaxed and CUCRL2 can explore more freely. On the other hand, UCRL2 converges faster since it is agnostic to the safety constraint and may explore very poor policies in the initial phase. To better understand this condition, Fig. 2(right) shows the percentage of time the constraint was violated in the first 15000 steps (about 20% of the overall time $T$). CUCRL2 always satisfies the constraint for all values of $\alpha$ while UCRL2 fails a significant number of times, especially when the conditions is tight (small values of $\alpha$).

6 Conclusion

We presented algorithms for conservative exploration for both finite horizon and average reward problems with $O(\sqrt{T})$ regret. We have shown that the non-episodic nature of average reward problems makes the definition of the conservative condition much harder than in finite horizon problems. In both cases, we used a model-based approach to perform counterfactual reasoning required by the conservative condition. Recent papers have focused on model-free exploration in tabular settings or linear function approximation (Jin et al., 2018, Yang and Wang, 2019, Jin et al., 2019), thus a question is if it is possible for model-free algorithms to be conservative and still achieve $O(\sqrt{T})$ regret.
References


