On Overfitting and Asymptotic Bias in Batch Reinforcement Learning with Partial Observability (Extended Abstract)*

Vincent François-Lavet 1,3 , Guillaume Rabusseau 2,3 , Joelle Pineau 1,3 , Damien Ernst 4 and Raphael Fonteneau 4

1 McGill University
2 Université de Montréal
3 Mila
4 Université de Liège

Abstract

When an agent has limited information on its environment, the suboptimality of an RL algorithm can be decomposed into the sum of two terms: a term related to an asymptotic bias (suboptimality with unlimited data) and a term due to overfitting (additional suboptimality due to limited data). In the context of reinforcement learning with partial observability, this paper provides an analysis of the tradeoff between these two sources of error. In particular, our theoretical analysis formally characterizes how a smaller state representation increases the asymptotic bias while decreasing the risk of overfitting.

1 Formalization

When acquisition of new observations is possible (the “online” case), data scarcity is gradually phased out using strategies balancing the exploration / exploitation (E/E) tradeoff. The scientific literature related to this topic is vast; in particular, Bayesian RL techniques [Ross et al., 2011; Ghavamzadeh et al., 2015] offer an elegant way of formalizing the E/E tradeoff.

However, such E/E strategies are not applicable when the acquisition of new observations is not possible anymore. In the pure “batch” setting (also called the “offline” setting), the task is to learn the best possible policy from a fixed set of transition samples [Farahmand, 2011; Lange et al., 2012].

We consider a discrete-time POMDP [Sondik, 1978] model $M$ described by the tuple $(\mathcal{S}, \mathcal{A}, T, R, \Omega, \mathcal{H})$, where

- $\mathcal{S}$ is a finite set of states $\{1, \ldots, N_s\}$,
- $\mathcal{A}$ is a finite set of actions $\{1, \ldots, N_a\}$,
- $T : \mathcal{S} \times \mathcal{A} \times \mathcal{S} \to [0, 1]$ is the transition function,
- $R : \mathcal{S} \times \mathcal{A} \times \mathcal{S} \to \mathcal{R}$ is the reward function, where $\mathcal{R}$ is a continuous set of possible rewards in a range $R_{max} \in \mathbb{R}^+$,
- $\Omega$ is a finite set of observations $\{1, \ldots, N_\Omega\}$,
- $\mathcal{H}$ is a finite set of conditional observation probabilities, and
- $\gamma \in [0, 1)$ is the discount factor.

The initial state is drawn from an initial distribution $b(s_0)$. In this paper, the conditional transition probabilities $T$, the reward function $R$ and the conditional observation probabilities $O$ are unknown. The only information available to the agent is the past experience it gathered while interacting with the POMDP.

1.1 Processing a History of Data

A history of previously observed features can be used to estimate the hidden state dynamics [McCallum, 1996; Littman and Sutton, 2002; Singh et al., 2004]. We denote by $\mathcal{H}_t = \Omega \times (\mathcal{A} \times \mathcal{R} \times \Omega)^t$ the set of histories observed up to time $t$ for $t \in \mathbb{N}_o$, and by $\mathcal{H} = \bigcup_{t=0}^{\infty} \mathcal{H}_t$ the space of all possible observable histories.

In this paper, we consider a mapping $\phi : \mathcal{H} \to \phi(\mathcal{H})$, where $\phi(\mathcal{H}) = \{\phi(H) | H \in \mathcal{H}\}$ is of finite cardinality $|\phi(\mathcal{H})|$. On the one hand, we will show that when $\phi$ discards information from the whole history, the state representation $\phi(H)$ that the agent uses to make decision might depart from sufficient statistics, which can hurt performance. On the other hand, we will show that it is beneficial to use a mapping $\phi$ that has a low cardinality $|\phi(\mathcal{H})|$ to avoid overfitting.

Let us first introduce a notion of information on the latent hidden state $s$ through the notion of belief state [Cassandra et al., 1994].

Definition 1.1. The belief state $b(s|H)$ is defined as the vector of probabilities where the $i^{th}$ component $i \in \{1, \ldots, N_S\}$ is given by $P(s = i | H)$, for any history $H \in \mathcal{H}$.

Definition 1.2. The belief state $b_\phi(s|\phi(H))$ is defined as the vector of probabilities where the $i^{th}$ component $i \in \{1, \ldots, N_S\}$ is given by $P(s = i | \phi(H))$, for any history $H \in \mathcal{H}$.

\footnote{Note that $s$ and $H$ are random variables and their exact distribution will depend on the context that is considered. For any given probability distribution $\mathcal{D}_H$ over histories: $H \sim \mathcal{D}_H$, the probability $P(s|\phi(H))$ is the expectation of the state when $\phi(H)$ is observed: $b_\phi(s | \phi) = E_{H \sim \mathcal{D}_H, \phi(H)} b(s | H)$.

* This paper is an extended abstract of an article in the Journal of AI Research [François-Lavet et al., 2019].
Among all possible mappings \( \phi \), the notion of sufficient statistics [Kaelbling et al., 1998; Aberdeen et al., 2007] corresponds to the ones that extract enough information from the history to accurately capture the corresponding belief state.

**Definition 1.3.** In a POMDP \( M \), a statistic \( \phi(H) \) is a sufficient statistic at the condition that \( \forall s \in S: \)
\[
P(s \mid H) = P(s \mid \phi(H)),
\]
for \( H \in \mathcal{H} \). A mapping \( \phi \) which provides sufficient statistics for all histories \( H \in \mathcal{H} \) is called a sufficient mapping and is denoted as \( \phi_0 \).

One of the key notions on which our analysis relies is the one of “approximately sufficient mappings”, i.e. mappings whose corresponding belief state lies in an \( L_1 \)-ball of radius \( \epsilon \) centered on \( b(\cdot | H) \):

**Definition 1.4.** In a POMDP \( M \), a statistic \( \phi(H) \) is an \( \epsilon \)-sufficient statistic at the condition that it meets the following condition with \( \epsilon \geq 0 \) and with the \( L_1 \) norm:
\[
\| b_\phi (\cdot | \phi(H)) - b(\cdot | H) \|_1 \leq \epsilon,
\]
for \( H \in \mathcal{H} \). A mapping \( \phi \) that provides \( \epsilon \)-sufficient statistics for all histories \( H \in \mathcal{H} \) is called an \( \epsilon \)-sufficient mapping and is denoted as \( \phi(\epsilon(H)) \).

### 1.2 Working with a Limited Dataset

Let \( M(S, A, \Omega, \gamma) \) be a set of POMDPs with fixed \( S, A, \Omega \), and \( \gamma \). For any POMDP \( M(T, R, O) \in \mathcal{M} \), we denote by \( D_{M, \pi, N_t, N_0} \) a random dataset generated according to a probability distribution \( D_{M, \pi, N_t, N_0} \) over the set of \( N_t \) trajectories of length \( N_0 \). One such trajectory is defined as the observable history \( H_{N_t} \in \mathcal{H}_{N_0} \) obtained in \( M \) when starting from \( s_0 \) and following a stochastic sampling policy \( \pi_s \) that ensures a non-zero probability of taking any action given an observable history \( H \in \mathcal{H} \). For simplicity we denote \( D_{M, \pi, N_t, N_0} \), simply as \( D \sim D_{M} \). For the purpose of the analysis, we also introduce the asymptotic dataset \( D_\infty = D_{M, \pi, N_t, \infty} \) that would be theoretically obtained in the case where one could generate an infinite number of observations (\( N_t \rightarrow \infty \) and \( N_0 \rightarrow \infty \)).

### 1.3 Assessing the Performance of a Policy

Let us consider stationary and deterministic control policies \( \pi : \phi(\mathcal{H}) \rightarrow A \) with \( \pi \in \Pi \). Any particular choice of \( \pi \) induces a particular definition of the policy space \( \Pi \). We introduce \( V_{\pi M}^\gamma(\phi(H)) \) with \( H \in \mathcal{H} \) as the expected return obtained over an infinite time horizon when the system is controlled using policy \( \pi \) in the POMDP \( M \). For any given distribution \( \mathcal{D}_H \) over histories, this is defined as:
\[
V_{\pi M}^\gamma(\phi(H)) = \mathbb{E}_{H \sim \mathcal{D}_H} V_{M}^\gamma(H' \mid \phi),
\]
with \( V_{\pi M}(H \mid \phi) \) given by
\[
V_{\pi M}(H \mid \phi) = \mathbb{E}_{s_0 \sim b(\cdot | H)} \left[ \sum_{t=0}^{\infty} \gamma^t r_t | s_0 \sim b(\cdot | H), \pi \right],
\]
where we have \( \mathbb{P}(\omega_t \mid s_t) = O(s_t, \omega_t), a_t = \pi(\phi(H_t)), \mathbb{P}(s_{t+1} \mid s_t, a_t) = T(s_t, a_t, s_{t+1}) \) and \( r_t = R(s_t, a_t, s_{t+1}) \).

We also define \( \pi^* \) as an optimal policy in \( M \):
\[
\pi^* \in \arg\max_{\pi : \phi(\mathcal{H}) \rightarrow A} V_{M}^\gamma(\phi_0(H_0)),
\]
where \( H_0 \) is taken out of the distribution of initial observations (compatible with the distribution \( b(s_0) \) of initial states through the conditional observation probabilities).

### 2 Bias-overfitting in RL with Partial Observability

In this section, we study the performance gap between the expected return that can be obtained following the policy built from limited data and the highest possible expected return that we would obtain if the algorithm had access to the POMDP parameters.

To study the importance of the feature space, let us assume that the policies built from limited data are optimal according to frequentist statistics, which allows removing from the analysis how the RL algorithm converges. In order to define the optimal policy according to frequentist statistics, let us first introduce a frequentist-based (augmented) MDP from the dataset \( D \):

**Definition 2.1.** With \( M \) defined by \( (S, A, T, R, \Omega, O, \gamma) \) and the dataset \( D \) built from interactions with \( M \), the frequentist-based augmented MDP \( \tilde{M}_{D, \phi} \), also denoted for simplicity \( \tilde{M}_D = (\Sigma, A, \tilde{T}, \tilde{R}, \Gamma) \), is defined with
- the state space: \( \Sigma = \phi(H) \),
- the action space: \( A = \mathcal{A} \),
- the estimated transition function: for \( \sigma, \sigma' \in \Sigma \) and \( a \in \mathcal{A} \), \( \tilde{T}(\sigma, a, \sigma') \) is the number of times we observe the transition \( (\sigma, a) \rightarrow \sigma' \) divided by the number of times we observe \( (\sigma, a) \)
- the estimated reward function: for \( \sigma, \sigma' \in \Sigma \) and \( a \in \mathcal{A} \), \( \tilde{R}(\sigma, a, \sigma') \) is the mean of the rewards observed for the tuple \( (\sigma, a, \sigma') \)
- the discount factor \( \Gamma \leq \gamma \).

We introduce \( V_{\tilde{M}_D}^\gamma(\sigma) \) with \( \sigma \in \Sigma \) as the expected return obtained over an infinite time horizon when the system is controlled using a policy \( \pi : \Sigma \rightarrow A \) in the augmented decision process \( \tilde{M}_D \):

\[
V_{\tilde{M}_D}^\gamma(\sigma) = \mathbb{E}_{s_0 \sim b(\cdot | H)} \left[ \sum_{t=0}^{\infty} \Gamma^t r_t | s_0 = \sigma, \pi \right],
\]
where \( \hat{r}_t \) is the reward s.t. \( \hat{r}_t = \tilde{R}(\sigma_t, a_t, \sigma_{t+1}) \) and the transition is defined by \( \tilde{P}(\sigma_{t+1} | \sigma_t, a_t) = \tilde{T}(\sigma_t, a_t, \sigma_{t+1}) \).

A policy \( \pi \) is defined to be better than or equal to a policy \( \pi' \) if its expected return is greater than or equal to that of \( \pi' \) for all states. In an MDP, there is always at least one policy

---

2if any \( (\sigma, a) \) has never been encountered in a dataset, we arbitrarily set \( \tilde{T}(\sigma, a, \sigma') = 1/|\Sigma| \forall \sigma' \).

3if any \( (\sigma, a, \sigma') \) has never been encountered in a dataset, we arbitrarily set \( \tilde{R}(\sigma, a, \sigma') \) to the average of rewards observed over the whole dataset \( D \).
that is better than or equal to all other policies and this is an optimal policy [Sutton and Barto, 1998]. In the augmented MDP \( \tilde{M}_D \), we denote the optimal policy as \( \pi_{D,\phi} \) and we also call it the frequentist-based policy. Let us now decompose the error of using a frequentist-based policy \( \pi_{D,\phi} \) in the actual POMDP:

\[
E_{D \sim \tilde{D}_M} \left[ V_{\pi}^*(\phi_0(H)) - V_{\tilde{D}_M}^{\pi_{D,\phi}}(\phi(H)) \right] = \left( V_{\pi}^*(\phi_0(H)) - V_{\tilde{D}_M}^{\pi_{D,\phi}}(\phi(H)) \right) + E_{D \sim \tilde{D}_M} \left[ V_{\pi}^* - V_{\tilde{D}_M}^{\pi_{D,\phi}}(\phi(H)) \right].
\]

The term bias actually refers to an asymptotic bias when the size of the dataset tends to infinity, while the term overfitting refers to the expected suboptimality due to the finite size of the dataset (and thus due to the variance in the estimated transition function and reward function).

We start by providing a bound on the bias, which is an original result based on the belief states via the \( \epsilon \)-sufficient statistic.

**Theorem 1. "Bound on the bias":** Let \( M \) be a POMDP described by the 7-tuple \((S, \mathcal{A}, T, R, O, \Omega, \gamma)\). Let \( M_D \) be an augmented MDP \( (\Sigma, \mathcal{A}, \tilde{T}, \tilde{R}, \Gamma = \gamma) \) estimated, according to Definition 2.1, from a dataset \( D \). Then, for any \( \epsilon \)-sufficient mapping \( \phi = \phi_\epsilon \), the asymptotic bias can be bounded as follows:

\[
\max_{H \in \mathcal{H}} \left( V_{\pi}^*(\phi_0(H)) - V_{\tilde{D}_M}^{\pi_{D,\phi}}(\phi(H)) \right) \leq \frac{2\epsilon R_{max}}{(1-\gamma)^3}. \quad (2)
\]

**Proof.** We consider the frequentist-based MDP \( \tilde{M}_{D_{\infty},\phi_0} = (\Sigma_0, A, T, \tilde{R}, \Gamma = \gamma) \), for \( H \in \mathcal{H} \) and \( a \in \mathcal{A} \), let us define

\[
Q_{\tilde{M}_{D_{\infty},\phi_0}}^0(\phi_0(H), a) = \tilde{R}'(\phi_0(H), a) + \gamma \sum_{\varphi \in \Phi(H)} \tilde{T}(\phi_0(H), a, \varphi) V_{\tilde{D}_{M_{\infty},\phi_0}}^0(\varphi),
\]

where the reward

\[
\tilde{R}'(\phi_0(H), a) = \sum_{\varphi \in \Phi(H)} \tilde{T}(\phi_0(H), a, \varphi) \tilde{R}(\phi_0(H), a, \varphi).
\]

Then the main part of the proof is to demonstrate Proposition 2 below. From there, by applying Lemma 1 by Abel et al. 2016, we have:

\[
\left\| V_{\tilde{M}_{D_{\infty},\phi_0}}^0(\phi(H)) - V_{\tilde{D}_M}^{\pi_{D,\phi}}(\phi(H)) \right\|_\infty \leq \frac{2\epsilon R_{max}}{(1-\gamma)^2} = \frac{2 \epsilon R_{max}}{(1-\gamma)^3}.
\]

By further noticing that, when starting in \( s_0 \), \( M_{D_{\infty},\phi_0} \) and \( M \) provide an identical value function for a given policy \( \pi_{D,\phi} \) and that \( \pi_{D,\phi_0} \sim \pi^* \), i.e. \( V_M = V_{\tilde{D}_M}^{\pi_{D,\phi_0}} \), the theorem follows.

**Remark.** As compared to Hutter 2014 and Abel et al. 2016, this bound relates directly to the capacity of the mapping \( \phi(H) \) to retrieve sufficient information on the latent hidden state. As compared to PBVI [Pineau et al., 2003] and similar approaches, we do not make the assumption that \( T, R \) and \( O \) are known and, as such, they need to be estimated from data.

We now provide Proposition 2, which is the key result required in the proof of Theorem 1.

**Proposition 2.** Let \( \phi_\epsilon \) be an \( \epsilon \)-sufficient mapping, and let \( \phi_0 \) be a sufficient mapping. Then, for any \( H^{(1)}, H^{(2)} \) such that \( \phi_\epsilon(H^{(1)}) = \phi_\epsilon(H^{(2)}) \), we have

\[
\max_{a} \left| Q_{\tilde{M}_{D_{\infty},\phi_0}}^0(\phi_0(H^{(1)}), a) - Q_{\tilde{M}_{D_{\infty},\phi_0}}^0(\phi_0(H^{(2)}), a) \right| \leq \epsilon R_{max} \left( 1 - \frac{1}{\gamma} \right).
\]

**Proof.** For this proposition, we rely on the fact that since \( \phi_{\epsilon}(H^{(1)}) = \phi_{\epsilon}(H^{(2)}) \), we are able to bound the L1 error terms of the associated belief states of \( H^{(1)} \) and \( H^{(2)} \). From that bound, we then present two different ways of independent interest to prove Proposition 2. The first proof makes use of a tree of possible future observations, rewards and corresponding actions given a policy \( \pi \), and we show that when starting from \( H^{(1)} \), \( H^{(2)} \) such that \( \phi_{\epsilon}(H^{(1)}) = \phi_{\epsilon}(H^{(2)}) \), the bound holds. We also provide an alternative proof that makes use of the formalism of the bisimulation metric [Ferns et al., 2004] along with the data processing inequality. The details of the proofs are given in the full paper.

We now provide a bound on the overfitting error that monotonically grows with \( |\phi(H)| \). Theorem 3 shows that using a large set of features potentially leads to a stronger drop in performance when the available dataset \( D \) is limited (the bound decreases proportionally to \( \frac{1}{\sqrt{\ln D}} \)). A theoretical analysis in the context of MDPs with a finite dataset was performed by Jiang et al. 2015.

**Theorem 3. "Bound on the overfitting":** Let \( M \) be a POMDP described by the 7-tuple \((S, \mathcal{A}, T, R, O, \Omega, \gamma)\). Let \( M_D \) be an augmented MDP \( (\Sigma, \mathcal{A}, \tilde{T}, \tilde{R}, \Gamma = \gamma) \) estimated, according to Definition 2.1, from a dataset \( D \) with the assumption that \( D \) has \( n \) transitions from any possible pair \( (\phi(H), a) \in \phi(H) \times A \) (sampled i.i.d according to \( D_M \)). Then the overfitting due to using the frequentist-based policy \( \pi_{D,\phi} \) instead of \( \pi_{D_{\infty},\phi} \) in the POMDP \( M \) can be bounded as follows:

\[
\max_{H \in \mathcal{H}} \left( V_{\pi}^*(\phi(H)) - V_{\tilde{D}_M}^{\pi_{D,\phi}}(\phi(H)) \right) \leq \frac{2 \epsilon R_{max}}{(1-\gamma)^3} \left( \frac{1}{2n \ln(\frac{2|\phi(H)||A|^{1+|\phi(H)|}}{\delta})} \right),
\]

with probability at least \( 1 - \delta \).

**Proof.** The proof of Theorem 3 is deferred to the full paper.
Overall, Theorems 1 and 3 can help choose a good state representation for POMDPs as they provide bounds on the two terms that appear in the bias-overfitting decomposition of Equation 1. An additional feature in the mapping $\phi$ has an overall positive effect only if the increase of information on the belief state prevails over the additional risk of overfitting.

3 Experiments

This section provides empirical illustrations of the theoretical results on a distribution of synthetic POMDPs. Experiments on a POMDP with real-world data are available in the full paper.

3.1 Protocol

We randomly sample $N_P$ POMDPs such that $N_S = 5$, $N_A = 2$ and $N_Q = 5$ (except when stated otherwise) from a distribution $\mathcal{P}$ that we refer to as Random POMDP. Random transition functions $T(\cdot, \cdot)$ are drawn by assigning, for each entry $(s, a, s')$, a zero value with probability 3/4, and, with probability 1/4, a non-zero entry with a value drawn uniformly in $[0, 1]$. For all $(s, a)$, if all $T(s, a, s')$ are zeros, we enforce one non-zero value for a random $s' \in \mathcal{S}$. Values are normalized. Random reward functions are generated by associating to all possible $(s, a, s')$ a reward sampled uniformly and independently from $[-1, 1]$. Random conditional observation probabilities $O(\cdot, \cdot)$ are generated in the following way: the probability of observing $\phi^{(i)}$ when in state $s^{(i)}$ is equal to 0.5, while all other values are chosen uniformly randomly so that it is normalized for any $s$. For all POMDPs, we have $\gamma = 1$ and $\Gamma = 0.95$ if not stated otherwise and we truncate the trajectories to a length of $N_T = 100$ time steps.

For each generated POMDP $D \sim \mathcal{P}$, we generate 20 datasets $D \in D_P$ where $D_P$ is a probability distribution over all possible sets of $n$ trajectories ($n \in [2, 5000]$); where each trajectory is made up of a history $H_{100}$ of 100 time steps, when starting from an initial state $s_0 \in \mathcal{S}$ and taking uniform random decisions. Each dataset $D$ induces a policy $\pi_{D, \phi}$, and we want to evaluate the expected return of this policy while discarding the variance related to the stochasticity of the transitions, observations and rewards. To do so, policies are tested with 1000 rollouts of the policy. For each POMDP $D$, we are then able to get an estimate of the average score $\mu_D$ which is defined as:

$$\mu_D = \mathbb{E}_{D \sim D_P} \left[ \sum_{t=0}^{N_t} \gamma^t r_t | s_0, \pi_{D, \phi} \right].$$

We are also able to get an estimate of a parametric variance $\sigma^2_D$ defined as:

$$\sigma^2_D = \text{Var}_{D \sim D_P} \left[ \sum_{t=0}^{N_t} \gamma^t r_t | s_0, \pi_{D, \phi} \right].$$

3.2 History Processing

We show experimentally that any additional feature from the history $H_\ell$ is likely to reduce the asymptotic bias, but may also increase the overfitting. For any history length $h$, we consider the mapping $\phi_h$ that extracts the current observation and the last $h-1$ (observation, action) tuples. In the experiments, we compare the policies $\pi_{D, \phi_h}$ for $h = 1, 2, 3$.

The values $\mathbb{E}_{D \sim P} \mu_D$ and $\mathbb{E}_{D \sim P} \sigma_D$ are displayed in Figure 1. One can observe that a small set of features (small history) appears to be a better choice when the dataset is small (only a few trajectories). With an increasing number of trajectories, the optimal number of features increases.

In addition, one can also observe that the expected variance of the score decreases as the number of samples increases. As the variance decreases, the risk of overfitting also decreases, and it becomes possible to target a larger policy class (using a larger feature set).

4 Conclusion and Future Works

In the context of POMDPs, this paper discusses the bias-overfitting tradeoff of RL algorithms with limited available data (batch RL). We show that it may be preferable to concede an asymptotic bias in order to reduce overfitting. The main theoretical results of this extended abstract relate to the state representation, for which we introduce the notion of the $\epsilon$-sufficient statistics and showed that it enables the formalization of the bias-overfitting trade-off.

Acknowledgments

We thank the anonymous reviewers for many helpful comments. The authors thank the Walloon Region (Belgium) that funded this research in the context of the BATWAL project. We also acknowledge financial support by the Natural Science and Engineering Research Council Canada (NSERC) and Samsung Electronics Co Ltd. Guillaume Rabusseau acknowledges support of an IVADO postdoctoral fellowship.
References


