Robust Predictable Control

Benjamin Eysenbach\textsuperscript{1 2} Ruslan Salakhutdinov\textsuperscript{1} Sergey Levine\textsuperscript{2 3}
\textsuperscript{1}Carnegie Mellon University, \textsuperscript{2}Google Brain, \textsuperscript{3}UC Berkeley
beysenba@cs.cmu.edu

Abstract

Many of the challenges facing today’s reinforcement learning (RL) algorithms, such as robustness, generalization, transfer, and computational efficiency are closely related to compression. Prior work has convincingly argued why minimizing information is useful in the supervised learning setting, but standard RL algorithms lack an explicit mechanism for compression. The RL setting is unique because (1) its sequential nature allows an agent to use past information to avoid looking at future observations and (2) the agent can optimize its behavior to prefer states where decision making requires few bits. We take advantage of these properties to propose a method (RPC) for learning simple policies. This method brings together ideas from information bottlenecks, model-based RL, and bits-back coding into a simple and theoretically-justified algorithm. Our method jointly optimizes a latent-space model and policy to be self-consistent, such that the policy avoids states where the model is inaccurate. We demonstrate that our method achieves much tighter compression than prior methods, achieving up to 5× higher reward than a standard information bottleneck. We also demonstrate that our method learns policies that are more robust and generalize better to new tasks.

1 Introduction

Many areas of reinforcement learning (RL) research focus on specialized problems, such as learning invariant representations, improving robustness to adversarial attacks, improving generalization, or building better world models. These problems are often symptoms of a deeper underlying problem: autonomous agents use too many bits from their environment. For the purpose of decision making, most information about the world is irrelevant. For example, a lane keeping feature on a car may take as input high-resolution camera input (millions of bits), but only needs to extract a few bits of information about the relative orientation of the car in the lane. Agents that rely on more bits of information run the risk of overfitting to the training task.

Agents that use few bits of information gain a number of appealing properties. These agents can better cope with high-dimensional sensory inputs (e.g., dozens of cameras on a self-driving car) and will be forced to learn representations that are more broadly applicable. Agents that throw away most information will be agnostic to idiosyncrasies in observations, providing robustness to missing or corrupted observations and better transfer to different scenarios. For example, if an agent ignores 99.9% of bits, then corrupting a random bit is unlikely to change the agent’s behavior. Moreover, an agent that minimizes bits will prefer states where the dynamics are easy to predict, meaning that the agent’s resulting behavior will be easier to model. Thus, compression not only changes an agent’s representation, but also changes its behavior: an agent that can only use a limited number of bits will avoid risky behaviors that require more bits to execute (see Fig. 3a).

The generalization and robustness of a machine learning model is directly related to the complexity of that model. Indeed, standard techniques for reducing complexity, such as the information bottleneck [11, 37], can be directly applied to the RL setting [11, 18, 26]. While these approaches make the

\textsuperscript{1}Project site with videos and code: https://ben-eysenbach.github.io/rpc
policy’s action a simple function of the state, they ignore the temporal dimension of decision making. Instead, we will focus on learning policies whose temporally-extended behavior is simple. Our key observation is that a policy’s behavior is simple if it is predictable. Throughout this paper, we will use compression as a measure of model complexity.

Our method improves upon prior methods that apply an information bottleneck to RL [11, 18, 26] by recognizing two important properties of the decision making setting. First, because agents make a sequence of decisions, they can use salient information at one time step to predict salient information at the next time step. These predictions can decrease the amount of information that the agent needs to sense from the environment. We will show that learning a predictive model is not an ad-hoc heuristic, but rather a direct consequence of minimizing information using bits-back coding [9, 16]. Second, unlike supervised learning, the agent can change the distribution over states, choosing behaviors that visit states that are easier to compress. For example, imagine driving on a crowded road. Aggressively passing and tailgating other cars may result in reaching the destination faster, but requires careful attention to other vehicles and fast reactions. In contrast, a policy optimized for using few bits would not pass other cars and would leave a larger following distance (see Fig. 3b). Combined, these two capabilities result in a method that jointly trains a latent space model and a control policy, with the policy being rewarded for visiting states where that model is accurate. Unlike typical model-based methods, our method explicitly optimizes for the accuracy of open-loop planning and results in a model and policy that are self-consistent.

The main contribution of this paper is an RL algorithm, robust predictable control (RPC), for learning policies that use few bits of information. We will refer to such policies as compressed policies. RPC brings together ideas from information bottlenecks, model-based RL, and bits-back coding into a simple and theoretically-justified algorithm. RPC achieves much higher compression than prior methods; for example, RPC achieves $\sim 5 \times$ higher return than a standard information bottleneck compared at the same bitrate. Experiments demonstrate practical benefits from the compressed policies learned by RPC: they are more robust than those learned by alternative approaches, generalize well to new tasks, and learn behaviors that can be composed for hierarchical RL.

2 Related Work

The problem of learning simple models has a long history in the machine learning community [16, 22]. Simplicity is often measured by the mutual information between its inputs and outputs [4, 37], a metric that has been used to study the generalization properties [37] and representations learned by [1] neural networks. Our work extends these results to the RL setting by observing that the agent can change its behavior (i.e., the data distribution) to be more easily compressed. In the RL community, prior work has used the variational information bottleneck (VIB) [2] to minimize communication between agents in a multi-agent setting [38] and to improve exploration in a goal-reaching setting [11]. The most related RL methods are those that use an information bottleneck in RL to improve generalization [18, 26]. Whereas these prior methods compress observations individually, we will compress sequences of observations. This difference, which corresponds to learning a latent-space model, improves compression and increases robustness on downstream tasks.

In the RL setting, compression offers a tool for studying problems such as representation learning, robustness and generalization. Prior RL methods have used mutual information to learn representations that are good for control [10, 21, 23, 31]. Our method learns a representation of observations that, like contrastive learning methods [21, 29, 31], avoids the need to reconstruct the observation. While these contrastive methods maximize the mutual information between representations across time, our method will minimize the mutual information between observations and representations. Moreover, we will jointly optimize the policy and representation using a single, unified objective. Our method is also related to robust RL, which studies the problem of learning RL policies that are resilient against perturbations to the environment [17, 19, 28, 36]. While prior robust RL methods typically involve solving a two-player game, we show that compression is a simpler mechanism for achieving some robustness benefits. Finally, the problem of learning RL policies that generalize has been studied by many prior papers [7, 8]. We will show that compression also yields RL policies that generalize well.

3 Reinforcement Learning with Fewer Bits

This section introduces the idea that predicting the future allows RL policies to operate with fewer bits. We derive this idea from first principles, develop it into a complete RL method, then discuss connections with model-based RL, bits-back coding, and other related topics.
3.1 Notation and Preliminaries

An agent interacts in an MDP defined by states $s_t$ and actions $a_t$. The agent samples actions from a policy $\pi_0(a_t \mid s_t, s_{t-1}, s_{t-2}, \cdots)$\(^2\). We will construct this policy by learning an encoder $\phi(z_t \mid s_t)$ (which produces a representation $z_t$ of the current state $s_t$), and a high-level policy $\pi_0^m(a_t \mid z_t)$ which decodes a representation $z_t$ into an action $a_t$. The environment dynamics are defined by an initial state $s_1 \sim p_1(s_1)$ and a transition function $p(s_{t+1} \mid s_t, a_t)$. The standard RL objective is to maximize the expected $\gamma$-discounted sum of rewards $r(s_t, a_t): \max_{\pi} E_{\pi} \left[ \sum_{t=1}^\infty \gamma^tr(s_t, a_t) \right]$. The discount factor can be interpreted as saying that the episode terminates at every time step with probability $(1 - \gamma)$, an interpretation we will use in Sec. 3.2.

A model is simpler if it expresses a simpler input-output relationship \[^4\,\[^5\]. We will measure the complexity of a function using an information bottleneck, which is the mutual information $I(x; y)$ between an input $x$ and an output $y$ \[^6\,\[^7\]. Mutual information is closely tied to the energy required to implement that function on an ideal physical system \[^8\,\[^9\]. The variational information bottleneck provides a tractable upper bound on mutual information \[^10\,\[^11\]:

$$I(x; y) \leq \mathbb{E}_{p(x,y)} \left[ \log \left( \frac{p(y \mid x)}{m(y)} \right) \right],$$

where $m(y)$ is an arbitrary prior distribution. Applying the information bottleneck to an intermediate layer $z = \phi(x)$ is sufficient for bounding the mutual information between input $x$ and output $y$.

Following prior work on compression in RL \[^12\,\[^13\], we aim to maximize rewards while minimizing the number of bits. While there are many ways to apply compression to RL (e.g., compressing actions, goals, or individual observations), we will focus on compressing sequences of states. The input is a sequence of states, $s_{1:}\infty \triangleq (s_1, s_2, \cdots)$; the output is a sequence of actions, $a_{1:}\infty \triangleq (a_1, a_2, \cdots)$. The objective is to learn a representation $\phi_0(z_1 \mid s_1)$ and policy $\pi_0(a_t \mid z_t)$ that maximize reward, subject to the constraint that the policy makes average $C > 0$ bits of information per episode:

$$\max_{\theta} \mathbb{E}_{\pi, \phi} \left[ \sum_{t=1}^\infty \gamma^t r(s_t, a_t) \right] \quad \text{s.t.} \quad \mathbb{E}_\pi[I(s_{1:}\infty; z_{1:}\infty)] \leq C, \quad (1)$$

While prior work on compression in RL \[^12\,\[^13\] has applied the VIB to states independently, we will aim to compress entire sequences of observations. Applying the VIB to sequences allows us to use more expressive choices of the prior $m(z_{1:}\infty)$. Our prior will use previous representations to predict the prior for the next representation, allowing us to obtain a tighter bound on mutual information.

3.2 Using Fewer Bits by Predicting the Future

The main idea of our method is that if the agent can accurately predict the future, then the agent will not need to observe as many bits from future observations. Precisely, the agent will learn a latent dynamics model that predicts the next representation using the current representation and action. In addition to predicting the future, the agent can also decrease the number of bits by changing its behavior. States where the dynamics are hard to predict will require more bits, so the agent will prefer visiting states where its learned model can accurately predict the next state.

This intuition corresponds exactly to solving the optimization problem in Eq. (1) with a prior that is factored autoregressively: $m_{1:}\infty(z_{1:}\infty \mid a_{1:}\infty) = m(z_1) \prod_t m_0(z_{t+1} \mid z_t, a_t)$. Note that the prior has learnable parameters $\theta$. We apply the VIB to obtain an upper bound on the constraint in Eq. (1):

$$\mathbb{E}_x[I(s_{1:}\infty; z_{1:}\infty)] \leq \mathbb{E}_x \left[ \log \left( \frac{p(z_{1:}\infty \mid s_{1:}\infty)}{m(z_{1:}\infty)} \right) \right] = \mathbb{E}_x \left[ \sum_{t=1}^\infty \gamma^t (\log \phi_0(z_t \mid s_t) - \log m_0(z_{t+1} \mid z_t, a_t)) \right]. \quad (2)$$

This objective is different from prior work that applies the VIB to RL \[^11\,\[^12\,\[^26\] because the prior $m_0(z_t)$ is predicted, rather than fixed to be a unit Normal distribution. The discount factor $\gamma$ reflects the assumption from Sec. 3.1 that the episode terminates with probability $(1 - \gamma)$ at each time step;

\[^2\]We use the terms “states” and “observations” interchangeably.

\[^4\]We introduce the policy as being conditioned on states because, even if the task is Markovian, the agent’s choice to omit certain bits from the representation can turn an otherwise fully-observed task into a partially-observed task.
of course, no bits are used after the episode terminates. Our final objective optimizes the policy $\pi$, the encoder $\phi$, and the prior $m$ to maximize reward and minimizing information:

$$
\max_{\theta} \mathbb{E}_{t, s, a, m} \left[ \sum_{t=1}^{\infty} \gamma^t r(s_t, a_t) \right] \quad \text{s.t.} \quad \mathbb{E}_{t, s, a, m} \left[ \sum_{t} \gamma^t \left( \log \phi(z_t | s_t) - \log m(z_{t+1} | z_t, a_t) \right) \right] \leq C. 
$$

(3)

For the encoder, this objective looks like a modification of the information bottleneck where the prior is predicted from the previous representation and action. Our compression objective modifies the MDP by imposing an information cost associated with gathering information. This new MDP has a reward function

$$
\hat{r}(s_t, a_t, s_{t+1}) = r(s_t, a_t) + \lambda \left( \log m(z_{t+1} | z_t, a_t) - \log \phi(z_{t+1} | s_{t+1}) \right),
$$

(4)

(negative of the) information cost

where $\lambda$ is the cost per bit. The term $\log \phi(z_t | s_t)$ corresponds to the number of bits required to represent the representation $z_t$. The term $\log m(z_{t+1} | z_t, a_t)$ reflects how well the agent can predict the next representation. In effect, the agent has to “pay” for bits of the observation, but it gets a “refund” on bits that it predicted from the previous time step, analogous to bits-back coding \cite{9, 16}. Said in other words, we want to minimize the excess bits required to infer $z_t$ from the current state, relative to the number of bits required to predict $z_t$ from the previous $(z_{t-1}, a_{t-1})$. Note that the standard VIB approaches to RL \cite{11, 18, 26} do not receive this refund because they compress observations independently, rather than compressing sequences of observations. Importantly, the agent optimizes not only its representation but also its behavior to minimize this information cost: the agent learns a representation that is easily predictable and learns to visit states where that representation is easily predictable. We therefore call our method robust predictable control (RPC).

4 A Practical Algorithm

Our method for optimizing (Eq. 3) is an actor-critic method applied to the information-augmented reward function in Eq. 4. We introduce a Q function $Q_{\psi}(s_t, a_t) = \mathbb{E} \left[ \sum_t \gamma^t \hat{r}(s_t, a_t, s_{t+1}) \right]$ for estimating the expected future returns of information-regularized reward function $\hat{r}$. We optimize this Q function using standard temporal difference learning:

$$
\mathcal{L}(\psi) = \frac{1}{2} (Q_{\psi}(s_t, a_t) - y_t)^2
$$

where $y_t = \hat{r}_t + \gamma Q_{\psi}(s_{t+1}, a_{t+1})$. In practice, we use a separate target Q function and do not backpropagate gradients through the target Q function. Since our overall objective (Eq. 1) only entails compressing the policy, not the Q function, we can condition the Q function directly on the state. In effect, we provide the Q-function with “side” information that is not available to the policy, similarly to prior work \cite{25, 32, 34}.

To optimize the encoder, prior, and policy, we note that our overall objective (Eq. 1) can be expressed in terms of the immediate reward plus the Q function (see derivation in Appendix A.1):

$$
\mathcal{L}(\theta; s_t) = \mathbb{E}_{z_{t-1} \sim \phi(s_{t-1}), s_t \sim \rho(s_t | z_{t-1}, a_{t-1})} \left[ Q_{\psi}(s_t, a_t) + \lambda \left( \log m(z_t | z_{t-1}, a_{t-1}) - \log \phi(z_t | s_t) \right) \right].
$$

(6)

Since the encoder is stochastic, we compute gradients through it using the reparameterization trick. The fact that all three components are optimized with respect to the same objective makes implementation of RPC surprisingly simple. Note that RPC does not require sampling from $m(z_{t+1} | z_t, a_t)$ and does not require backpropagation through time. In our implementation, we instantiate the encoder $\phi(s_t)$, the prior $m(z_{t+1} | z_t, a_t)$, and the high-level policy $\pi_{\phi}(a_t | z_t)$ as neural networks with parameters $\theta$. The Q function $Q_{\psi}(s_t, a_t)$ is likewise represented as a neural network with parameters $\phi$. We update the dual parameter $\lambda \geq 0$ using dual gradient descent. We use standard tricks such as target networks and taking the minimum over two Q values. We refer the reader to Appendix B and the open-sourced code for details.
5 Connections and Analysis

In this section we discuss the connections between robust predictable control and other areas of RL. We then prove that RPC enjoys certain robustness guarantees.

5.1 Connections

RPC is closely related to a number of ideas in the RL literature. This section explains these connections, with the aim of building intuition into how RPC works and providing an explanation for why RPC should learn robust policies and useful representations. We include a further discussion of the relationship to MaxEnt RL, the expression for the optimal encoder, and the value of information in Appendix A.3.

Model-Based RL. The prior $m_{\theta}(z_t \mid z_{t-1}, a_{t-1})$ learned by RPC can be viewed as a dynamics model. Rather than predicting what the next state will be, this model predicts what the representation of the next state will be. While the model is trained to make accurate predictions, the policy is also trained to visit states and actions where the model will be more accurate.

Representation learning. What precisely does the representation $z_t$ represent? Given a prior $m(z_{t+1} \mid z_t, a_t)$ and latent-conditioned policy $\pi^z(a_t \mid z_t)$, we can use the current representation $z_t$ to predict good actions at both the current time step and (by unrolling the prior) at future time steps. Thus, the representation $z_t$ can be thought of as a compact representation of open-loop action sequences. Our experiments demonstrate that this compact representation of action sequences, once learned on one task, can be used to quickly learn a range of downstream tasks.

We can view RPC as learning a new action space for the MDP. Precisely, define a new MDP where the actions are $z_t$, and the reward function is $\tilde{r}$ (Eq. 4). What we previously called the encoder, $\phi(z_t \mid s_t)$, is now the policy for selecting the actions $z_t$ in this new MDP. The $-\log \phi(z_t \mid s_t)$ term in $\tilde{r}$ is the entropy of this encoder, so the encoder is performing MaxEnt RL on this new MDP. This new MDP encodes a strong prior for open-loop policies: simply sampling actions from the prior yields high reward.

Open-loop control. RPC learns a model $m(z_t \mid z_{t-1}, a_{t-1})$ that predicts the state representation at the next time step. Thus, we can unroll our policy in an open-loop manner, without observing transitions from the true system dynamics. Because the model and policy are trained to be self-consistent, we expect that the highly compressed policies learned by RPC will perform well in this open-loop setting, as compared to uncompressed policies (see experiments in Sec. 6).

5.2 Theoretical Guarantees

We conclude this section by formally relating model compression to open-loop performance and generalization error. We do not intend this section to be a comprehensive analysis of all benefits deriving from model compression (see, e.g., [3, 4]). All proofs are in Appendix C.

Intuitively, we know that a policy that uses zero bits of information will perform identically in the open-loop setting, as compared to uncompressed policies (see experiments in Sec. 6).

**Lemma 5.1.** Let encoder $\phi(z_t \mid s_t)$, policy $\pi^z(a_t \mid z_t)$, prior $m(z_t \mid z_{t-1}, a_{t-1})$, and reward function $r(s_t, a_t) > 0$ be given. Then our model compression objective (Eq. 3) with reward function $(1 - \gamma) \log r(s_t, a_t)$ is a lower bound on the expected return of the open-loop policy.

\[
\mathbb{E}_{\text{open}(r)} \left[ \sum_{t=1}^{\infty} \gamma^t r(s_t, a_t) \right] \geq f \left( \mathbb{E}_{\text{open,m}(r)} \left[ \sum_{t=1}^{\infty} \gamma^t \left( (1 - \gamma) \log r(s_t, a_t) + \log m(z_t \mid z_{t-1}, a_{t-1}) - \log \phi(z_t \mid s_t) \right) \right] \right),
\]

where $f(x) = \frac{x^e}{1 - \gamma e^x}$ is a monotone increasing function of $x$.

Our next result shows that, not only does RPC optimize for open loop performance, but the difference between the performance of the open-loop policy and the reactive policy can be bounded by the policy’s bitrate. This result could be useful for quantifying the regret incurred when using the learned representation $z_t$ as an action space of temporally-extended behaviors.
Let $\pi^{\text{open}}$ be the open-loop policy corresponding to the composition of the prior $m(z_{t+1} \mid z_t, a_t)$ and the high-level policy $\pi^z(a_t \mid z_t)$. Let $\pi^{\text{reactive}}$ be the reactive policy corresponding to the composition of the encoder $\phi(z_t \mid s_t)$ and the high-level policy $\pi^z(a_t \mid z_t)$. To simplify notation, we further define the sum of discounted rewards of a trajectory as $\hat{R}(\tau) \triangleq \sum_t \gamma^t r(s_t, a_t)$ and let $R_{\text{max}} = \max_{\tau} R(\tau)$ be the maximum return of any trajectory.

**Lemma 5.2.** The expected return of the open-loop policy $\pi^{\text{open}}$ is at most $R_{\text{max}} \sqrt{C/2}$ worse than the expected return of the reactive policy $\pi^{\text{reactive}}$:

$$\mathbb{E}_{\pi^{\text{open}}}[\sum_t \gamma^t r(s_t, a_t)] \geq \mathbb{E}_{\pi^{\text{reactive}}}[\sum_t \gamma^t r(s_t, a_t)] - R_{\text{max}} \sqrt{C/2}.$$ 

One oft-cited benefit of compression is that the resulting models generalize better from the training set to the testing set. Our final result applies this same reasoning to RL. We assume that the policy has been trained on an empirical distribution of MDPs, and will be evaluated on a new MDP sampled from that sample distribution. For the following result, we assume that the given stochastic MDP is a mixture of deterministic MDPs, each described by a $b$-bit random string (see Ng and Jordan [30]).

**Lemma 5.3.** Let stochastic MDP $\mathcal{M}$ and reactive policy $\pi^{\text{reactive}}$ be given. Define $R^n(\mathcal{M})$ to be the expected reward of policy $\pi$ on MDP $\mathcal{M}$. Then the probability that the policy’s expected return on an observed (deterministic) MDP $\hat{\mathcal{M}}$ is much different than the policy’s expected return on the stochastic MDP is bounded by the policy’s bitrate:

$$P_{\mathcal{M}}[\|R^n(\hat{\mathcal{M}}) - R^n(\mathcal{M})\| > \epsilon] \leq \frac{C + 1}{2b\epsilon^2 - 1}.$$ 

The proof is a direct application of Bassily et al. [4] Theorem 8]. This result may be of interest in the offline RL setting, where observed trajectories effectively constitute a deterministic MDP. The intuition is that policies that use fewer bits will be less likely to overfit to the offline dataset.

In summary, our theoretical results suggest that compressed policies learn representations that can be used for planning and that may generalize better. We emphasize that the theoretical benefits of model compression have been well studied in the supervised learning literature. As our method is likewise performing model compression, we expect that it will inherit a wide range of additional guarantees, such as guarantees about sample complexity.

### 6 Experiments

Our experiments have two aims. First, we will demonstrate that RPC achieves better compression than alternative approaches, obtaining a higher reward for the same number of bits. Second, we will study the empirical properties of compressed policies learned by our method, such as their robustness and ability to learn representations suitable for hierarchical RL. We do not intend this section to exhaustively demonstrate every possible benefit from compression; we acknowledge that there are many purported benefits of compression, such as exploration and sample efficiency, which we do not attempt to study here. We include additional experiments in Appendix B.

#### 6.1 Evaluating Compression

Our first experiment studies whether RPC out-performs alternative approaches to compression, which we summarize in the inline table. We compare against a standard VIB [18] and an extension that adds the information cost to the reward, “VIB+reward” [26]. This baseline can be viewed as a special case of RPC where the blue arrows in Fig. 1 are removed. Finally, since the predictive prior in RPC is similar to a recurrent network, we compare against an extension of the VIB [18] that uses an LSTM (“RNN + VIB”). Unlike RPC, this baseline requires training on entire trajectories (rather than individual transitions) and requires backpropagating gradients through time. We evaluate all methods on four tasks from OpenAI-Gym [5] and two image-based tasks from dm-control [35]. Because of computational constraints, we omit the RNN+VIB baseline on the image-based tasks.
Learning Compressed Policies. We measure the return achieved by policies constrained to have a fixed bit rate. Especially at low bit rates, RPC achieves higher return than alternative methods.

Figure 2

(a) Driving with Traffic
(b) Active Cruise Control

Behavior of compressed policies. On two driving tasks, we observe that highly compressed policies (Left) avoid passing other cars and (Right) leave a larger following distance between cars. The passing and tailgating that our method forgoes would require more bits of information about the precise locations of the other cars.

Figure 3

Behavior of compressed policies: On two driving tasks, we observe that highly compressed policies (Left) avoid passing other cars and (Right) leave a larger following distance between cars. The passing and tailgating that our method forgoes would require more bits of information about the precise locations of the other cars.

Figure 4: Representations: (Top) Compressed policies observe more bits from observations that have a large value of information. (Bottom) Compressed policies learn sparse representations.

Representations of compressed policies. A policy learned by compression must trade off between maximizing reward and paying to receive bits of information. Using the HalfCheetah task, we plot

We plot results in Fig. 2. To make the rewards comparable across tasks, we normalize the total return by the median return of the best method. On almost all tasks, RPC achieves higher return than prior methods for the same bitrate. For example, when learning the Walker task using 0.3 bits per observation, RPC achieves a return of 3,562, the VIB+RNN baseline achieves a return of 1,978 (-44%), and the other VIB baselines achieve a return of around 530 (-85%). We include full results on a wider range of bitrates in Appendix Fig. 10. While, in theory, the VIB+RNN baseline could implement RPC internally, in practice it achieved lower returns, perhaps because of optimization challenges associated with training LSTMs [6]. Even if the VIB+RNN baseline could implement the strategy learned by RPC, RPC is simpler (it does not require training on trajectories) and trains about 25% times faster (it does not require backpropagation through time).

6.2 Visualizing Compressed Policies

Behavior of compressed policies. To visualize how compression changes behavior, we applied RPC to two simulated driving tasks shown in Fig. 3a (top left), which are based on prior work [24]. In the first task, the agent can pass cars by driving into the lane for oncoming traffic; the second task uses the same simulated environment but restricts the agent to remain in its own lane. The rewards for these tasks corresponds to driving to the right as quickly as possible, without colliding with any other vehicles. In the first task, we observe that compressed policies passed fewer cars than uncompressed policies. Intuitively, a passing maneuver requires many bits of information about the relative positions of other cars, so we expect that compressed policies to engage in fewer passing maneuvers. Fig. 3a (bottom) shows that the bitrate of RPC is directly correlated with the number of cars passed. In the second task, we observe that compressed policies leave a larger following distance from the leading car (Fig. 3b (top)). Fig. 3b (bottom) shows that the number of bits used per observation increases when the car is within 15m of another car. Thus, by maintaining a following distance of more than 30m, the compressed policy can avoid these situations where it would have to use more bits. See the project website for videos.

4Project site with videos and code: https://ben-eysenbach.github.io/rpc
Figure 5: Hierarchical RL: We apply RPC to the pushing task shown in the top-left. We then use the learned representation of action sequences as the action space for solving three new tasks. On all tasks, the representations learned by RPC accelerate learning. All episodes have a fixed length.

The value of information versus cost of information for many sampled states. See Appendices A.4 and B.5 for details. As shown in Fig. 4 (top), the RPC uses more bits from observations that are more valuable for maximizing future returns. Then, to visualize the learned representation $z_t$, we sample the representation from randomly sampled states, and plot the numbers of bits used for each coordinate. Fig. 4 (bottom) shows that RPC learns sparse representations. Whereas the uncompressed policy uses all coordinates, a policy compressed with bitrate 10 uses only $10/50$ coordinates and a policy compressed with bitrate 0.3 uses only $2/50$ coordinates.

6.3 Hierarchical RL using the Learned Representation

RPC learns a representation of temporally-extended action sequences (see Sec. 5.1). We hypothesize that these representations can accelerate the learning of new tasks in a hierarchical setting. Our goal is not to propose a complete hierarchical RL system, but rather evaluate whether these action representations are suitable for high-level control. During training, we apply RPC to a goal-conditioned object pushing task, shown in Fig. 5 (top-left). The initial position of the object and the goal position are randomized, so we expect that different representations $z_t$ will correspond to high-level behaviors of moving the end effector and object to different positions. At test-time, the agent is presented with a new task. The agent will attempt to solve the task by commanding one or two behaviors $z_t$. See Appendix B for details and pseudocode.

We compare the action representations learned by RPC to three baselines. To test whether RPC has learned a prior over useful action sequences, we use a variant of RPC (“RPC (randomly initialized)” ) where the policy and model are randomly initialized. “Action Repeat” constantly outputs the same action. Finally, “RL from scratch” applies a state-of-the-art off-policy RL algorithm (SAC [14]) to the task. We apply all methods to four tasks and present results in Fig. 5. First, as a sanity check, we apply all methods to the training task, finding that RPC quickly finds a single $z_t$ that solves the task. On the remaining three tasks, we likewise observe that the representations learned by RPC allow for much faster learning than the baselines. The final task, “pusher wall” requires chaining together multiple representations $z_t$ to solve. While the “RL from scratch” baseline eventually matches and then surpasses the performance of RPC, RPC accelerates learning in the low-data regime.

6.4 Robustness

The connection between compression and robustness has been well established in the literature (e.g., [13, 40]). Our next set of experiments test the robustness of compressed policies to different types of disturbances: missing observations (i.e., open-loop control), adversarial perturbations to the observations, and perturbations to the dynamics (i.e., robust RL). We emphasize that since these experiments focus on robustness, the policy is trained and tested in different environments.

Robustness to missing observations and open-loop control. Since compressed policies rely on fewer bits of input from the observations, we expect that they not only will be less sensitive to missing observations, but will actively modify their behavior to adopt strategies that require fewer bits from the observation. In this experiment, we drop each observation in-
dependently with probability \( p \in [0, 1] \), where \( p = 1 \) corresponds to using a fully open-loop policy. For RPC, we handle missing observations by predicting the representation from the previous time step. Our two main baselines take a policy used by standard RL and learn either a latent-space model or a state-space model. When the observation is missing, these baselines make predictions using the learned model. We also compare against RNN+VIB, the strongest baseline from Fig. 2. When observations are missing, the LSTM’s input for that time step is sampled from the prior. Fig. 6 shows that all methods perform similarly when no observations are dropped, but RPC achieves a higher reward than baselines when a larger fraction of observations are dropped. This experiment shows that more effective compression, as done by RPC, yields more robust policies. This robustness may prove useful in real-world environments where sensor measurements are missing or corrupted.

**Adversarial Robustness.** Compressed policies extract fewer bits from each observation, so we expect that compressed policies will be more robust to adversarial perturbations to the observation. While prior work has proposed purpose-designed methods for achieving robustness [28, 36], here we investigate whether compression is simple yet effective means for achieving a modicum of robustness. We do not claim that compression is the best method for learning robust policies.

We first study adversarial perturbations to the dynamics on the Ant-v2 environment. Given a policy \( \pi(a_t \mid s_t) \) and the current state \( s_t \), the adversary aims to apply a small perturbation to that state to make the policy perform as poorly as possible. We implement the adversary using projected gradient descent [27]; see Appendix B for details. Fig. 7 (left) shows the expected return as we increase the magnitude of the attack. The compressed policy is more resilient to larger attacks than the uncompressed policy. Our next experiment looks at perturbations to the observation. Unlike the previous experiment, we let the adversary perturb every step in an episode; see Appendix B for full details. Fig. 7 (right) shows that policies that use fewer bits achieve higher returns in this adversarial setting. When the Ant-v2 agent uses too many bits (3 or more), the adversarial perturbations to the dynamics flip the agent over, whereas agents that use fewer bits remain upright.

**Robust RL.** Our final set of experiments look at higher-level perturbations to the dynamics, as are typically studied in the robust RL community [28, 36]. Using the same Ant-v2 environment as before, we (1) increase the mass of each body element by a fixed multiplier, or (2) decrease the friction of each body geometry by a fixed multiplier. These experiments test whether the learned policies are robust to more massive robots or more “slippery” settings. Fig. 8 shows that compressed policies generalize to larger masses and smaller frictions more effectively than an uncompressed policy. Comparing the policies learned by RPC with a bit rate of 0.3 bits versus 3.0 bits, we observe that the bit rate effectively balances performance versus robustness. See Appendix Fig. 11 for a larger version of this plot with error bars.

### 7 Conclusion

In this paper, we presented a method for learning robust and predictable policies. Our objective differs from prior work by compressing sequences of observations, resulting in a method that jointly trains a policy and a model to be self-consistent. Not only does our approach achieve better compression than prior methods, it also learns policies that are more robust (Fig. 7). We also demonstrate that our method learns representations that are suitable for use in hierarchical RL.

**Limitations.** The main limitation of this work is that policies that use few bits will often receive lower reward on the training tasks. Also, for the purpose of exploration, the most informative states may be those that are hardest to compress. While the first limitation is likely irreconcilable, the second might be lifted by maximizing information collected during exploration but minimizing information for policy optimization.
Acknowledgments. We thank Dibya Ghosh and the members of the Salakhutdinov lab for feedback throughout the project. We thank Oscar Ramirez for help setting up the image-based experiments and thank Rico Jonschkowski for introductions to potential collaborators. We thank Ryan Julian and Vincent Vanhoucke for feedback on the paper draft, and thank Abhishek Gupta for discussions during the early stages of this project.

This material is supported by the Fannie and John Hertz Foundation and the NSF GRFP (DGE1745016).

References

[1] Achille, A. and Soatto, S. (2018). Emergence of invariance and disentanglement in deep representations. *The Journal of Machine Learning Research*, 19(1):1947–1980.

[2] Alemi, A., Fischer, I., Dillon, J., and Murphy, K. (2017). Deep variational information bottleneck. In *ICLR*.

[3] Arora, S., Ge, R., Neyshabur, B., and Zhang, Y. (2018). Stronger generalization bounds for deep nets via a compression approach. In *International Conference on Machine Learning*, pages 254–263. PMLR.

[4] Bassily, R., Moran, S., Nachum, I., Shafer, J., and Yehudayoff, A. (2018). Learners that use little information. In *Algorithmic Learning Theory*, pages 25–55. PMLR.

[5] Brockman, G., Cheung, V., Pettersson, L., Schneider, J., Schulman, J., Tang, J., and Zaremba, W. (2016). Openai gym. *arXiv preprint arXiv:1606.01540*.

[6] Cho, K., van Merrienboer, B., Gülçehre, Ç., Bahdanau, D., Bougares, F., Schwenk, H., and Bengio, Y. (2014). Learning phrase representations using RNN encoder-decoder for statistical machine translation. In Moschitti, A., Pang, B., and Daelemans, W., editors, *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing, EMNLP*, pages 1724–1734. ACL.

[7] Cobbe, K., Klimov, O., Hesse, C., Kim, T., and Schulman, J. (2019). Quantifying generalization in reinforcement learning. In *International Conference on Machine Learning*, pages 1282–1289. PMLR.

[8] Farebrother, J., Machado, M. C., and Bowling, M. (2018). Generalization and regularization in dqn. *arXiv preprint arXiv:1810.00123*.

[9] Frey, B. J. and Hinton, G. E. (1997). Efficient stochastic source coding and an application to a bayesian network source model. *The Computer Journal*, 40(2_and_3):157–165.

[10] Gelada, C., Kumar, S., Buckman, J., Nachum, O., and Bellemare, M. G. (2019). Deepmdp: Learning continuous latent space models for representation learning. In *International Conference on Machine Learning*, pages 2170–2179. PMLR.

[11] Goyal, A., Islam, R., Strouse, D., Ahmed, Z., Larochelle, H., Botvinick, M., Levine, S., and Bengio, Y. (2019). Transfer and exploration via the information bottleneck. In *International Conference on Learning Representations*.

[12] Guadarrama, S., Korattikara, A., Ramirez, O., Castro, P., Holly, E., Fishman, S., Wang, K., Gonina, E., Wu, N., Kokioptoulou, E., Sbaiz, L., Smith, J., Bartók, G., Berent, J., Harris, C., Vanhoucke, V., and Brevedo, E. (2018). TF-Agents: A library for reinforcement learning in tensorflow. [https://github.com/tensorflow/agents](https://github.com/tensorflow/agents) [Online; accessed 25-June-2019].

[13] Gui, S., Wang, H. N., Yang, H., Yu, C., Wang, Z., and Liu, J. (2019). Model compression with adversarial robustness: A unified optimization framework. *Advances in Neural Information Processing Systems*, 32:1285–1296.

[14] Haarnoja, T., Zhou, A., Abbeel, P., and Levine, S. (2018). Soft actor-critic: Off-policy maximum entropy deep reinforcement learning with a stochastic actor. In *International Conference on Machine Learning*, pages 1861–1870. PMLR.

[15] Hansen, N. (2006). The cma evolution strategy: a comparing review. *Towards a new evolutionary computation*, pages 75–102.

[16] Hinton, G. E. and Van Camp, D. (1993). Keeping the neural networks simple by minimizing the description length of the weights. In *Proceedings of the sixth annual conference on Computational learning theory*, pages 5–13.

[17] Huang, S. H., Papernot, N., Goodfellow, I. J., Duan, Y., and Abbeel, P. (2017). Adversarial attacks on neural network policies. In *5th International Conference on Learning Representations, ICLR 2017, Toulon, France, April 24-26, 2017, Workshop Track Proceedings*. OpenReview.net.
[18] Igl, M., Ciosek, K., Li, Y., Tschatschek, S., Zhang, C., Devlin, S., and Hofmann, K. (2019). Generalization in reinforcement learning with selective noise injection and information bottleneck. *Advances in Neural Information Processing Systems*, 32:13978–13990.

[19] Kamalaruban, P., Huang, Y., Hsieh, Y., Rolland, P., Shi, C., and Cevher, V. (2020). Robust reinforcement learning via adversarial training with langevin dynamics. In Larochelle, H., Ranzato, M., Hadsell, R., Balcan, M., and Lin, H., editors, *Advances in Neural Information Processing Systems 33: Annual Conference on Neural Information Processing Systems 2020, NeurIPS 2020, December 6-12, 2020*, virtual.

[20] Kingma, D. P. and Ba, J. (2015). Adam: A method for stochastic optimization. In *ICLR* (Poster).

[21] Laskin, M., Srinivas, A., and Abbeel, P. (2020). Curl: Contrastive unsupervised representations for reinforcement learning. In *International Conference on Machine Learning*, pages 5639–5650. PMLR.

[22] LeCun, Y., Denker, J. S., and Solla, S. A. (1990). Optimal brain damage. In *Advances in neural information processing systems*, pages 598–605.

[23] Lee, A., Nagabandi, A., Abbeel, P., and Levine, S. (2020). Stochastic latent actor-critic: Deep reinforcement learning with a latent variable model. *Advances in Neural Information Processing Systems*, 33.

[24] Leurent, E. (2018). An environment for autonomous driving decision-making. [https://github.com/eleurent/highway-env](https://github.com/eleurent/highway-env).

[25] Levine, S., Finn, C., Darrell, T., and Abbeel, P. (2016). End-to-end training of deep visuomotor policies. *The Journal of Machine Learning Research*, 17(1):1334–1373.

[26] Lu, X., Lee, K., Abbeel, P., and Tiomkin, S. (2020). Dynamics generalization via information bottleneck in deep reinforcement learning. *arXiv preprint arXiv:2008.00614*.

[27] Madry, A., Makelov, A., Schmidt, L., Tsipras, D., and Vladu, A. (2018). Towards deep learning models resistant to adversarial attacks. In *6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, April 30 - May 3, 2018, Conference Track Proceedings*. OpenReview.net.

[28] Morimoto, J. and Doya, K. (2005). Robust reinforcement learning. *Neural computation*, 17(2):335–359.

[29] Nachum, O., Gu, S., Lee, H., and Levine, S. (2019). Near-optimal representation learning for hierarchical reinforcement learning. In *7th International Conference on Learning Representations, ICLR 2019, New Orleans, LA, USA, May 6-9, 2019*. OpenReview.net.

[30] Ng, A. Y. and Jordan, M. I. (2000). PEGASUS: A policy search method for large mdps and pomdps. In Boutilier, C. and Goldszmidt, M., editors, *UAI ’00: Proceedings of the 16th Conference in Uncertainty in Artificial Intelligence, Stanford University, Stanford, California, USA, June 30 - July 3, 2000*, pages 406–415. Morgan Kaufmann.

[31] Oord, A. v. d., Li, Y., and Vinyals, O. (2018). Representation learning with contrastive predictive coding. *arXiv preprint arXiv:1807.03748*.

[32] OpenAI, Akkaya, I., Andrychowicz, M., Chociej, M., Litwin, M., McGrew, B., Petron, A., Paino, A., Pappert, M., Powell, G., Ribas, R., Schneider, J., Tezak, N., Tworek, J., Welinder, P., Weng, L., Yuan, Q., Zaremba, W., and Zhang, L. (2019). Solving rubik’s cube with a robot hand. *CoRR*, abs/1910.07113.

[33] Ortega, P. A. and Braun, D. A. (2013). Thermodynamics as a theory of decision-making with information-processing costs. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 469(2153):20120683.

[34] Pinto, L., Andrychowicz, M., Welinder, P., Zaremba, W., and Abbeel, P. (2018). Asymmetric actor critic for image-based robot learning. In Kress-Gazit, H., Srinivasa, S. S., Howard, T., and Atanasov, N., editors, *Robotics: Science and Systems XIV, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA, June 26-30, 2018*.

[35] Tassa, Y., Doron, Y., Muldal, A., Erez, T., Li, Y., Casas, D. d. L., Budden, D., Abdolmaleki, A., Merel, J., Lefrancq, A., et al. (2018). Deepmind control suite. *arXiv preprint arXiv:1801.00690*.

[36] Tessler, C., Efroni, Y., and Mannor, S. (2019). Action robust reinforcement learning and applications in continuous control. In *International Conference on Machine Learning*, pages 6215–6224. PMLR.

[37] Tishby, N. and Zaslavsky, N. (2015). Deep learning and the information bottleneck principle. In *2015 IEEE Information Theory Workshop (ITW)*, pages 1–5. IEEE.
[38] Wang, R., He, X., Yu, R., Qiu, W., An, B., and Rabinovich, Z. (2020). Learning efficient multi-agent communication: An information bottleneck approach. In International Conference on Machine Learning, pages 9908–9918. PMLR.

[39] Yarats, D., Kostrikov, I., and Fergus, R. (2021). Image augmentation is all you need: Regularizing deep reinforcement learning from pixels. In International Conference on Learning Representations.

[40] Ye, S., Xu, K., Liu, S., Cheng, H., Lambrechts, J.-H., Zhang, H., Zhou, A., Ma, K., Wang, Y., and Lin, X. (2019). Adversarial robustness vs. model compression, or both? In Proceedings of the IEEE/CVF International Conference on Computer Vision, pages 111–120.

[41] Yu, T., Quillen, D., He, Z., Julian, R., Hausman, K., Finn, C., and Levine, S. (2020). Meta-world: A benchmark and evaluation for multi-task and meta reinforcement learning. In Conference on Robot Learning, pages 1094–1100. PMLR.
A More Analysis

A.1 Objective for the Encoder, Model, and Policy

This section describes how the objective for the encoder, model, and policy (Eq. 6) is derived from our overall objective (Eq. 1). Our aim is to maximizing the sum of (information-augmented) rewards (Eq. 3), starting at state \( s_t \):

\[
L(\theta; s_t) = E \left[ \sum_{t'=t}^{\infty} \gamma^{t'-t} r(s_{t'}, a_{t'}) \mid s_t \right]
\]

\[
= E \left[ \sum_{t'=t}^{\infty} \gamma^{t'-t} (r(s_{t'}, a_{t'}) + \lambda (\log m_{\theta}(z_{t'+1} \mid z_{t'}, a_{t'}) - \log \phi_{\theta}(z_{t'} \mid s_{t'}))) \mid s_t \right]
\]

\[
= E \left[ r(s_t, a_t) + \lambda (\log m_{\theta}(z_{t+1} \mid z_t, a_t) - \log \phi_{\theta}(z_t \mid s_t)) \right]
\]

\[
+ \sum_{t'=t+1}^{\infty} \gamma^{t'-t} (r(s_{t'}, a_{t'}) + \lambda (\log m_{\theta}(z_{t'+1} \mid z_{t'}, a_{t'}) - \log \phi_{\theta}(z_{t'} \mid s_{t'}))) \mid s_t \right]
\]

\[
= E \left[ r(s_t, a_t) + \lambda (\log m_{\theta}(z_{t+1} \mid z_t, a_t) - \log \phi_{\theta}(z_t \mid s_t)) + \gamma Q(\psi(s_{t+1}, a_{t+1})) \right].
\]

Note that the reward at the current time step, \( r(s_t, a_t) \), is not influenced by the parameters \( \theta \), so we can drop this term:

\[
L(\theta; s_t) \overset{\text{const.}}{=} E \left[ \lambda (\log m_{\theta}(z_{t+1} \mid z_t, a_t) - \log \phi_{\theta}(z_t \mid s_t)) + \gamma Q(\psi(s_{t+1}, a_{t+1})) \right].
\]

The remaining difference between this objective and Eq. 5 is that the Q value term is scaled by \( \gamma \). However, this difference has no effect on the optimization problem because the parameter \( \lambda \) is automatically tuned. If we scale the second term, \( Q \), by some value (say, \( \gamma \)), then tuning \( \lambda \) to satisfy the bitrate constraint will result in a different value for \( \lambda \) (one which is \( \gamma \) times smaller). For optimizing this objective, we sample states \( s_t \) from the replay buffer.

A.2 Prior on the Initial Representation

For simplicity, we have omitted the prior \( m(z_1) \) on the representation of the first observation. This prior cannot be predicted from prior observations. Instead, we fix \( m(z_1) \) to be a zero-mean, unit-variance Gaussian. The information-augmented reward at the first time step is therefore

\[
\tilde{r}_\lambda(s_0, a_0, s_1) \triangleq r(s_0, a_0) + \lambda (\log m_{\theta}(z_1) - \log \phi_{\theta}(z_1 \mid s_1)).
\]

A.3 MaxEnt RL and the Optimal Encoder

Maximum entropy (MaxEnt) RL is a special case of our compression objective. If the high-level policy is the identity function \( (\pi^\ast(a_t \mid z_t) = \delta(a_t = z_t)) \) and the prior is the uniform distribution over \( Z \) (i.e., \( m(z_{t+1} \mid z_t, a_t) = \text{Unif}(z_{t+1})) \), then we recover standard MaxEnt RL. Another way of describing this connection is that MaxEnt RL is equivalent to imposing an information bottleneck on the final (i.e., action) output of the policy. This connection suggests that some of the empirically-oberved benefits of MaxEnt RL might be derived from the fact that it implicitly is performing model compression. For example, the objective from MaxEnt RL can be interpreted as optimizing for behavior under which random actions (sampled from the prior) do not significantly decrease the expected reward. Nonetheless, directly optimizing for the model compression objective yields a prior that depends on time. As shown in our experiments, such a prior yields a policy that not only is more compressed, but is also more robust to sensor failure (i.e., the open-loop setting).

In MaxEnt RL, the optimal policy can be expressed in terms of the soft value function: \( \pi(a_t \mid s_t) \propto e^{Q(s_t, a_t)} \), where \( Q(s_t, a_t) \) is the expected, entropy-regularized return. We can express the optimal encoder learned by RPC in similar terms. First, we reparametrize the Q function in terms of \( z_t \) instead of \( a_t \): \( Q^\ast(s_t, z_t) = E_{\pi^\ast(a_t \mid s_t)}[Q(s_t, a_t)] \). The optimization problem for the encoder is

\[
\max_{\phi(z_t \mid s_t)} E_{\phi(z_t \mid s_t)} \left[ \sum_t \gamma^t \tilde{r}(s_t, a_t, s_{t+1}) \right]
\]

\[
= E_{\phi(z_t \mid s_t)} [r(s_t, a_t) + \log m(z_t \mid z_{t-1}, a_{t-1}) - \log \phi(z_t \mid s_t) + \gamma Q(s_{t+1}, a_{t+1})].
\]
We used the following function for squashing:

\[
\text{def squash_to_range}(t, low=-\infty, high=\infty):
\]

Thus, the optimal encoder is trained to \( \tilde{t} \) the predictions from the prior by the Q function.

### A.4 Value of Information

An optimal agent must balance these information costs against the value of information gained from these observations. Precisely, the value of information is how much more reward an optimal agent could receive if it observes the representation \( z_t \) instead of predicting \( z_t \) from the previous representation and action. We expect that the optimal policy will only look at representations where the value of information is greater than the cost of information. We confirm this prediction experimentally in Fig. 4. In practice, the policy learned by RPC looks at every observation, but may only look at a few bits from that observation.

### B Experimental Details

#### B.1 Implementation Details

We implemented RPC on top of the SAC \([14]\) implementation in TF-Agents \([12]\). Unless otherwise noted, we used the default hyperparameters from that implementation and trained all agents for 3e6 steps. We provide pseudocode in Alg. 1.

**State-based RPC.** We parameterized the model \( m_\theta(z_{t+1} \mid z_t, a_t) \) by predicting the difference between the \( z_t \) and \( z_{t+1} \). That is, we trained a 2-layer neural network (both layers have 256 units with ReLU activations) to model \( p(z_{t+1} \mid z_t, a_t) \). We parameterized the encoder \( \phi_\theta(z_t \mid s_t) \) as a 2-layer neural network (both layers have 256 units with ReLU activations). Both the model and encoder output the mean and (diagonal) standard deviation of a multivariate Normal distribution. We squashed the mean to be within \([-30, 30] \) and squashed the standard deviation to be within \([0.1, 10.0] \). We used the following function for squashing:

```python
def squash_to_range(t, low=-np.inf, high=np.inf):
    if low == -np.inf:
        t_low = t
    else:
        t_low = low * tf.nn.tanh(t / (-low))
    if high == np.inf:
        t_high = t
    else:
        t_high = high * tf.nn.tanh(t / high)
    return tf.where(t < 0, t_low, t_high)
```

### Algorithm 1 Robust Predictable Control

The updates below are written using a learning rate of \( \eta \). In practice we perform gradient steps using the Adam \([20]\) optimizer.

| Line | Description |
|------|-------------|
| 1:   | Initialize prior \( m_\theta(z_{t+1} \mid z_t, a_t) \), encoder \( \phi_\theta(z_{t+1} \mid s_t) \), Q function \( Q_\psi(s_t, a_t) \), and high-level policy \( \pi_\theta(z_{t+1} \mid z_t) \) |
| 2:   | Initialize replay buffer \( D \leftarrow \emptyset \) |
| 3:   | Initialize dual variable \( \log \lambda \leftarrow \log(1e - 6) \) |
| 4:   | while not converged do |
| 5:   | Sample a batch of transitions: \( \{ (s_t, a_t, r_t, s_{t+1}) \sim D \} \) |
| 6:   | Compute information cost: \( c_t \leftarrow E[|\log \phi_\theta(z_t \mid s_t) - \log m_\theta(z_{t+1} \mid z_t, a_t)|] \) \( \triangleright \text{Eq. 4} \) |
| 7:   | Compute information-regularized reward \( \tilde{r}_t \leftarrow r_t - \lambda c_t \) |
| 8:   | Update Q function: \( \psi \leftarrow \psi - \eta \nabla_\psi \mathcal{L}(\psi) \) \( \triangleright \text{Eq. 5} \) |
| 9:   | Update prior, encoder, and high-level policy: \( \theta \leftarrow \theta + \eta \nabla_\theta \mathcal{L}(s_t) \) \( \triangleright \text{Eq. 6} \) |
| 10:  | Update dual variable: \( \log \lambda \leftarrow \log \lambda - \eta(C - E[c_t]) \) |
| 11:  | return \( \pi_\theta(z_t \mid z_t), \phi_\theta(z_t \mid s_t), m_\theta(z_{t+1} \mid z_t, a_t) \) |
Unless otherwise noted, we set the dimension of \( z_t \) to 50, though found this parameter has little effect.

We parameterized the high-level policy \( \pi_{\theta}(a_t \mid s_t) \) as a 2-layer neural network (both layers have 256 units with ReLU activations). Following the TF-Agents implementation of SAC, this network first predicts a Normal distribution, which is then squashed by \( \text{tf.tanh} \) to only output actions within the action space.

**Image-based RPC.** Our image-based version of RPC was based on DrQ \cite{39}. Unless otherwise specified, we used the same hyperparameters and architecture as that paper. For example, we used the same action repeat (4 actions) and frame stack (3 frames) as that paper. The only architectural difference was the policy network. We parameterized the encoder \( \phi_{\theta}(z_t \mid s_t) \) as follows:

```python
tf.keras.Sequential([
  tf.keras.layers.Lambda(lambda t: tf.cast(t, tf.float32) / 255.0),  # Normalize image
  tf.keras.layers.Conv2D(filters=32, kernel_size=(3, 3), strides=(2, 2), activation='relu'),
  tf.keras.layers.Conv2D(filters=32, kernel_size=(3, 3), strides=(1, 1), activation='relu'),
  tf.keras.layers.Conv2D(filters=32, kernel_size=(3, 3), strides=(1, 1), activation='relu'),
  tf.keras.layers.Conv2D(filters=32, kernel_size=(3, 3), strides=(1, 1), activation='relu'),
  tf.keras.layers.Flatten(),
  tfp.layers.IndependentNormal(params_size(latent_dim), activation=_activation),
  tfp.layers.IndependentNormal(latent_dim),
])
```

We used the same model and high-level policy as in the state-based experiments. Following DrQ

**Dual parameter \( \lambda \).** We updated the dual parameter \( \lambda \) via dual gradient ascent to satisfy the bitrate constraint. We parametrized this variable as \( \log \lambda \) to ensure that it remains positive. We initialized \( \lambda = 1e-6 \approx 0 \), and performed updates using \( \text{tf.keras.optimizers.Adam(learning_rate=3e-4)} \). We confirmed via visual inspection that the bitrate constraint was satisfied.

**RNN baseline.** We based the RNN baseline experiments on SAC-RNN implementation in TF-Agents \cite{12}. We trained the agent on sequences of length 20. For fair comparison, we used the same number of transitions per batch as other agents that trained on individual transitions. The default batch size in TF-Agent’s implementation of SAC is 256, so we trained the RNN on batches with 256 // 20 = 13 sequences.

**Model-based baselines.** The state-space model and latent-space models used the same model architecture as RPC. This model was trained using standard maximum likelihood with the same optimizer that RPC used for optimizing \( m(z_{t+1} \mid z_t, a_t) \).

### B.2 Learning Compressed Policies (Fig. 2)

We ran this experiment with 5 random seeds, with error bars depicting the [25%, 75%] quantiles across random seeds. To compute the return of each policy, we took the average of the last 50 evaluations, corresponding to the last 5e5 training steps (out of a total of 3e6 training steps). For each task, we normalized the return by the median return of the best performing baseline. Fig. 10 plots returns without normalization.

### B.3 Behavior of Compressed Policies (Fig. 3a (bottom))

We used the two-way task from Leurent \cite{24}. We initially observed that the agent often crashed into other cars, so we modified the reward function by adding a penalty of -50 when the agent crashes. The original environment has discrete actions, so we added a wrapper around the environment that allows RPC to command continuous actions, which would then be discretized. We trained RPC for 1e5 steps on this environment.

### B.4 Behavior of Compressed Policies (Fig. 3b)

For this experiment, we used a modified version of the two-way task from Leurent \cite{24}. We modified the environment to disable passing, so the car was forced to remain in the same lane. To encourage

[https://github.com/tensorflow/agents/blob/master/tf_agents/agents/sac/examples/v2/train_eval_rnn.py](https://github.com/tensorflow/agents/blob/master/tf_agents/agents/sac/examples/v2/train_eval_rnn.py)
aggressive driving, we modified the reward function to be \( (x/2000)^{10} \), where \( x \) is the distance traveled. We trained RPC for \( 2 \times 10^5 \) steps. The “Compressed Policy” refers to RPC using a bitrate constraint of 0.1.

B.5 Value of Information (Fig. 4 (top))

The value of observing \( z_t \) is given by

\[
\text{ValueOfInfo}(z_{t+1}) = \mathbb{E} \left[ \sum_t \gamma^t r(s_t, a_t) \mid z_{t+1} \right] - \mathbb{E} \left[ \sum_t \gamma^t r(s_t, a_t) \mid z_t \right],
\]

while the cost of observing \( z_t \) is given by

\[
\text{CostOfInfo}(z_{t+1}) = \mathbb{E} \left[ \log \phi(z_{t+1} \mid s_{t+1}) - \log m(z_{t+1} \mid z_t, a_t) \right].
\]

Intuitively, the optimal policy will only choose to look at representations \( z_t \) when \( \text{ValueOfInfo}(z_{t+1}) > \text{CostOfInfo}(z_{t+1}) \). We compare these two quantities in the experiments (Fig. 4 (top)). Note that both the cost of information and value of information depend on the encoder, \( \phi(s_t) \).

For this experiment, we applied RPC to the \texttt{HalfCheetah-v2} environment using a bitrate constraint of 10.0.

B.6 Sparse Representations (Fig. 4 (bottom))

For this experiment, we applied RPC to the \texttt{HalfCheetah-v2} environment. Since both the encoder \( \phi(z_t \mid s_t) \) and model \( m(z_{t+1} \mid z_t, a_t) \) predict diagonal normal distributions, we can compute the KL divergence between each coordinate. For the plot in Fig. 4 (bottom), we sorted these KLs before plotting.

B.7 Hierarchical RL (Fig. 5)

Pre-training. We learned the representation of actions by applying RPC to the \texttt{push-v2} task in Metaworld \footnote{41}. To make the subsequent optimization easier, we set the dimension of \( z_t \) to 3.

Hierarchical RL. We optimize over the list of \( z_t \)s using CMA-ES \footnote{15}. We provide pseudocode in Fig. 9. The aim of this approach is to test whether compression results in behaviors that can transfer to new tasks. We use CMA-ES as a black-box optimizer because of its simplicity, and emphasize that more sophisticated optimization routines (e.g., actor-critic RL with actions corresponding to \( z_t \)) would likely perform better.

For the pusher task (which was the same as the training task), we used one behavior \( z_t \) for a horizon of 100 steps. For the pusher_wall task, we used two behaviors \( z_t \), each with horizon 100 steps. For the button task, we used one behavior \( z_t \) for a horizon of 100 steps. For the drawer_open task, we used two behaviors \( z_t \), each with a horizon of 75 steps.

Action Repeat. In some tasks, actions correspond to a desired pose. Thus, action repeat would correspond to moving to a desired pose, which seemed like a reasonable baseline in these manipulation tasks. Our experiments highlight that the behaviors learned by RPC do more than move to a particular pose. In addition, the behaviors learned by RPC do obstacle avoidance and objective manipulation.
B.8 Robustness to missing observations (Fig. 6)

For this experiment, we trained RPC using a bitrate of 0.1 for HalfCheetah-v2 and 3.0 for Walker2d-v2. We evaluated all methods by dropping observations independently. Note that none of the methods were trained using observation dropout, so this experiment explicitly tests robustness to new disturbances introduced at test time.

B.9 Adversarial Robustness to Dynamics (Fig. 7 (left))

The adversary aims to apply a small perturbation to that state to make the policy perform as poorly as possible. The adversary’s objective is

$$\min_{s_{\text{adv}} \in B(s)} V^\pi(s_{\text{adv}}) = Q^\pi(s_{\text{adv}}, a \sim \pi(a | s_{\text{adv}})).$$

We instantiate the adversary using projected gradient descent [27] with step size 0.1. For fair comparison, we evaluate each policy on states collected by rolling out that policy. This experiment used the Ant-v2 environment, applying RPC using a bitrate of 0.3. We repeated this attack on 20 states sampled from each policy’s state distribution. The dark line shows the average across these 20 attacks. As expected, the agent is more vulnerable to attacks in some states than in other states.

B.10 Adversarial Robustness to Observations (Fig. 7 (right))

We optimize the adversary to corrupt the state using the following objective:

$$\min_{s_{\text{adv}} \in B(s)} Q^\pi(s, a \sim \pi(a | s_{\text{adv}})).$$

The adversary is optimized using PGD, using three steps of size 0.1 for each state. Note that we only change the observation, not the true state of the environment. This difference from the previous experiment is important, as it allows us to unroll the policy and adversary for an entire trajectory. We used the Ant-v2 environment for this experiment.

B.11 Robust RL (Fig. 8)

We followed prior work in setting up the robust RL experiments [36]. To modify the mass, we scaled the env.model.body_mass attribute of the environment by a fixed constant. To modify friction, we scaled the env.model.geom_friction attribute of the environment by a fixed constant. We used perturbations much larger than prior work [36] because we found that standard RL was already robust to smaller ranges of perturbations.

C Proofs

C.1 Model Compression is a Lower Bound on Open-Loop Control (Lemma 5.1)

In this section we formally define the assumptions for Lemma 5.1 and then provide the proof. First, we define an open loop policy with hidden state $z_t$. This policy updates its hidden state as $m(z_{t+1} | z_t, a_t)$ and produces actions by sampling $p(a_t | z_t)$. Note that the open-loop sequence of actions generated by the policy is evaluated under the true system dynamics, $p(s_{t+1} | s_t, a_t)$. The open loop policy does not observe the transitions from the true system dynamics.

The main idea of the proof will be to apply an evidence lower bound on the expected reward objective. This idea alone almost completes the proof. The main technical challenge is accounting for discount factors: a naive application of an ELBO will result in discounted rewards but an undiscounted information term.

**Proof.** The first step is to recognize that the expected discounted return objective can be written as the expected terminal reward of a mixture of finite-length episodes. Define $p_H(\tau)$ as a distribution over length-$H$ episodes. We can then write the expected discounted return objective as follows:

$$E_{p(\tau)} \left[ \sum_{t=1}^{\infty} \gamma^t r(s_t, a_t) \right] = \sum_{H=1}^{\infty} \gamma^H E_{p_H(\tau)} [r(s_H, a_H)].$$
We can now obtain a lower bound on the \( \log \) of the expected return objective:

\[
\log \mathbb{E}_p(s_{1:\infty}, a_{1:\infty}, z_{1:1}) \left[ \sum_{t=1}^{\infty} \gamma^t r(s_t, a_t) \right] = \log \left( \sum_{H=1}^{\infty} \gamma^H \mathbb{E}_p(s_{1:H}, a_{1:H}, z_{1:H}) \left[ r(s_H, a_H) \right] \right)
\]

\[
= \log \left( \frac{1 - \gamma}{\gamma} \sum_{H=1}^{\infty} \gamma^H \mathbb{E}_p(s_{1:H}, a_{1:H}, z_{1:H}) \left[ r(s_H, a_H) \right] \right) + \log \frac{\gamma}{1 - \gamma} \geq \frac{(1 - \gamma)}{\gamma} \sum_{H=1}^{\infty} \gamma^H \log \left( \mathbb{E}_p(s_{1:H}, a_{1:H}, z_{1:H}) \left[ r(s_H, a_H) \right] \right) + \log \frac{\gamma}{1 - \gamma}. \quad (7)
\]

The inequality is Jensen’s inequality. The constant \( \frac{1 - \gamma}{\gamma} \) was introduced because Jensen’s inequality must be applied to a proper probability distribution.

The second step is to define a variational distribution \( q(s_{1:\infty}, a_{1:\infty}, z_{1:1}) \) as

\[
q(s_{1:\infty}, a_{1:\infty}, z_{1:1}) = \prod_t p(a_t \mid z_t) q(z_t \mid s_t) p(s_{t+1} \mid s_t, a_t).
\]

We can then obtain a lower bound on Eq. [7]

\[
\log \mathbb{E}_p(s_{1:\infty}, a_{1:\infty}, z_{1:1}) \left[ \sum_{t=1}^{\infty} \gamma^t r(s_t, a_t) \right] \geq \frac{1 - \gamma}{\gamma} \sum_{H=1}^{\infty} \gamma^H \mathbb{E}_q(s_{1:H}, a_{1:H}, z_{1:H}) \left[ \log r(s_H, a_H) + \log p(s_1, a_1, z_{1:1}) - \log q(s_1, a_1, z_{1:1}) \right] + \log \frac{\gamma}{1 - \gamma}
\]

\[
= \frac{1 - \gamma}{\gamma} \sum_{H=1}^{\infty} \gamma^H \mathbb{E}_q(s_{1:H}, a_{1:H}, z_{1:H}) \left[ \log r(s_H, a_H) + \sum_{t=1}^{H} \log m(z_{t+1} \mid z_t, a_t) - \log \phi(z_t \mid s_t) \right] + \log \frac{\gamma}{1 - \gamma}. \quad (8)
\]

The final line follows from simplifying the definitions of \( p(s_{1:\infty}, a_{1:\infty}, z_{1:1}) \) and \( q(s_{1:\infty}, a_{1:\infty}, z_{1:1}) \). Note that we have used the assumption that \( r(s_t, a_t) > 0 \) to ensure that \( \log r(s_t, a_t) \) is well defined.

Our third step is to do the opposite of the first step: recognize that expectations over a mixture of finite-horizon episodes are equivalent to expectations over a discounted infinite-length episode. With this, we can rewrite Eq. [8] as follows:

\[
\log \mathbb{E}_p(s_{1:\infty}, a_{1:\infty}, z_{1:1}) \left[ \sum_{t=1}^{\infty} \gamma^t r(s_t, a_t) \right] \geq \frac{1 - \gamma}{\gamma} \mathbb{E}_q(s_{1:\infty}, a_{1:\infty}, z_{1:1}) \left[ \sum_{H=1}^{\infty} \gamma^H \left( \log r(s_H, a_H) + \sum_{t=1}^{H} \log m(z_{t+1} \mid z_t, a_t) - \log \phi(z_t \mid s_t) \right) \right] + \log \frac{\gamma}{1 - \gamma}. \quad (9)
\]

We can simplify the double summation using the following identity, where \( x_t \) is shorthand for \( \log m(z_{t+1} \mid z_t, a_t) - \log \phi(z_t \mid s_t) \):

\[
\sum_{H=1}^{\infty} \gamma^H \sum_{t=1}^{H} x_t = \gamma x_1 + \gamma^2 (x_1 + x_2) + \gamma^3 (x_1 + x_2 + x_3) + \cdots
\]

\[
= x_1 (\gamma + \gamma^2 + \gamma^3 + \cdots) + x_2 (\gamma^2 + \gamma^3 + \cdots) + \cdots
\]

\[
= x_1 \frac{\gamma}{1 - \gamma} + x_2 \frac{\gamma^2}{1 - \gamma} + x_3 \frac{\gamma^3}{1 - \gamma} + \cdots
\]

\[
= \frac{1}{1 - \gamma} \sum_{t=1}^{\infty} \gamma^t x_t.
\]
Applying this identity to Eq. 9, we get
\[
\log \mathbb{E}_{p(s_{1:}\infty, a_{1:}\infty, s_{1:}\infty)} \left[ \sum_{t=1}^{\infty} \gamma^t r(s_t, a_t) \right] \\
\geq \frac{1}{\gamma} \mathbb{E}_{q(s_{1:}\infty, a_{1:}\infty, s_{1:}\infty)} \left[ \sum_{t=1}^{\infty} \gamma^t \left( \log r(s_t, a_t) + \frac{1}{1-\gamma} \log m(z_{t+1} | z_t, a_t) - \frac{1}{1-\gamma} \log \phi(z_t | s_t) \right) \right] + \log \frac{\gamma}{1-\gamma}
\]
\[
\geq \frac{1}{\gamma} \mathbb{E}_{q(s_{1:}\infty, a_{1:}\infty, s_{1:}\infty)} \left[ \sum_{t=1}^{\infty} \gamma^t \left( (1-\gamma) \log r(s_t, a_t) + \log m(z_{t+1} | z_t, a_t) - \log \phi(z_t | s_t) \right) \right] + \log \frac{\gamma}{1-\gamma}.
\]
Exponentiating both sides, we obtain the desired result.

This derivation is useful because it relates model compression to open-loop control. Precisely, it says that a compressed model is one that will perform well under open loop rollouts.

C.2 Proof of Lemma 5.2

**Proof.** To start, we define the distribution over trajectories \(\tau = (s_{1:}\infty, a_{1:}\infty, z_{1:}\infty)\) produced by \(\pi^{\text{open}}\) and \(\pi^{\text{reactive}}\):
\[
p^{\text{open}}(\tau) = p_1(s_1) \prod_{t} p(s_{t+1} | s_t, a_t) \pi^z(a_t | z_t) m(z_{t+1} | z_t, a_t)
\]
\[
p^{\text{reactive}}(\tau) = p_1(s_1) \prod_{t} p(s_{t+1} | s_t, a_t) \pi^z(a_t | z_t) \phi(z_t | s_t).
\]
Note that \(R(\tau) = \sum t \gamma^t r(s_t, a_t)\) is a deterministic function of a random variable, \(\tau\). We can now write the difference in returns as \(\mathbb{E}_{\pi^{\text{reactive}}}[R(\tau)] - \mathbb{E}_{\pi^{\text{open}}}[R(\tau)]\). The main idea of our proof will be to show that this difference is not too large.
\[
\mathbb{E}_{\pi^{\text{reactive}}}[R(\tau)] - \mathbb{E}_{\pi^{\text{open}}}[R(\tau)] = \int R(\tau)(p^{\text{reactive}}(\tau) - p^{\text{open}}(\tau))d\tau \leq (a) R_{\text{max}} \int |(p^{\text{reactive}}(\tau) - p^{\text{open}}(\tau))|d\tau \leq (b) R_{\text{max}} \sqrt{\frac{1}{2} KL(p^{\text{reactive}}(\tau)||p^{\text{open}}(\tau))}.
\]
We used Hőlder’s inequality in (a) and Pinsker’s inequality in (b). Our second step is to relate the KL divergence to the compression objective.
\[
KL(p^{\text{reactive}}(\tau)||p^{\text{open}}(\tau))
\]
\[
= \mathbb{E}_{\pi^{\text{reactive}}} \left[ \log p_1(s_1) + \sum_t p(s_{t+1} | s_t, a_t) \pi^z(a_t | z_t) + \log \phi(z_t | s_t) \right]
\]
\[
- \log p_1(s_1) - \sum_t \left( p(s_{t+1} | s_t, a_t) \pi^z(a_t | z_t) + \log \phi(z_t | s_t) + \log m(z_{t+1} | z_t, a_t) \right)
\]
\[
= \mathbb{E}_{\pi^{\text{reactive}}} \left[ \sum_t \log \phi(z_t | s_t) - \log m(z_{t+1} | z_t, a_t) \right] \leq C.
\]
where \(C\) is the information constraint (Eq. 3). We then substitute this simplified expression for the KL into Eq. 10.
\[
\mathbb{E}_{\pi^{\text{reactive}}}[R(\tau)] - \mathbb{E}_{\pi^{\text{open}}}[R(\tau)] \leq R_{\text{max}} \sqrt{\frac{1}{2} C}.
\]
Rearranging terms, we obtain the desired result:
\[
\mathbb{E}_{\pi^{\text{open}}}[R(\tau)] \geq \mathbb{E}_{\pi^{\text{reactive}}}[R(\tau)] - R_{\text{max}} \sqrt{\frac{1}{2} C}.
\]

\(\square\)
For this result to be non-vacuous, we need that $\sqrt{\frac{1}{2}C} < 1$, so the average per-transition $c$ must satisfy $c = (1 - \gamma)C \leq 2 \cdot (1 - \gamma)$:

$$\mathbb{E}_\pi [\log \phi(z_t | s_t) - \log m(z_{t+1} | z_t, a_t)] \leq 2 \cdot (1 - \gamma).$$

For example, when $\gamma = 0.99$, we would need that the average per-transition KL be less than 0.02.

**D Additional Experiments**

Figure 10: **Learning Compressed Policies.** This plot shows the same experiment as Fig. 2 on a wider range of bitrates, without using normalized returns.

Figure 11: **Robust RL:** This plot shows the same experiment as Fig. 8 with error bars corresponding to the standard deviation across five training random seeds.

Figure 12: **Behavior of compressed walking policies.**

Figure 13: **Adversarial Robustness:** The agent is most vulnerable just before its feet leave the ground.
Visualizing more compressed policies. In Fig. 12 we demonstrate that compressed policies also learn different walking gaits on a locomotion task. The agent requires many more bits each time it touches the ground, so the compressed policy takes bigger steps to minimize the number of footsteps. See the project website for videos comparing the behaviors learned for varying levels of compression.

Behavior of Attacked Policies We visualize the behavior of the adversarial attack on dynamics described in Sec. 6.4. Visualizing the uncompressed policy in Fig. 13 we observe that the policy is most vulnerable to attack the moment the robot launches off the ground for each step. This makes sense, as the actions right before takeoff dictate the path taken when the robot is in the air before the next step.