Back to the Manifold: recovering from Out-of-Distribution States

Alfredo Reichlin\textsuperscript{1}, Giovanni Luca Marchetti\textsuperscript{1}, Hang Yin\textsuperscript{1}, Ali Ghadirzadeh\textsuperscript{2} and Danica Kragic\textsuperscript{1}

Abstract—Learning from previously collected datasets of expert data offers the promise of acquiring robotic policies without unsafe and costly online explorations. However, a major challenge is a distributional shift between the states in the training dataset and the ones visited by the learned policy at the test time. While prior works mainly studied the distribution shift caused by the policy during the offline training, the problem of recovering from out-of-distribution states at the deployment time is not very well studied yet. We alleviate the distributional shift at the deployment time by introducing a recovery policy that brings the agent back to the training manifold whenever it steps out of the in-distribution states, e.g., due to an external perturbation. The recovery policy relies on an approximation of the training data density and a learned equivariant mapping that maps visual observations into a latent space in which translations correspond to the robot actions. We demonstrate the effectiveness of the proposed method through several manipulation experiments on a real robotic platform. Our results show that the recovery policy enables the agent to complete tasks while the behavioral cloning alone fails because of the distributional shift problem.

I. INTRODUCTION

Data-driven methods in robotics, including reinforcement learning (RL), are often challenged by expensive, slow and unsafe data collection on real systems \cite{1}. Offline solutions, such as Offline RL \cite{2} and Behavior Cloning (BC) \cite{3}, learn a control policy from a pre-collected dataset hence avoiding the problems of interacting with a physical robot. However, learning from a fixed offline dataset may compromise the capacity of the learner on dealing with novel situations not contained in the training dataset at the test time. Querying the trained policy on such out-of-distribution (OOD) inputs can exacerbate the compounding of the errors when the policy is subsequently applied to states evolved according to the previous state and action \cite{4}. Offline RL avoids this problem by constraining the learned policy to deviate minimally from the policy that collected the data \cite{5}–\cite{7}. However, there is no mechanism for offline RL to recover from OOD conditions, for example, when starting at a random unseen initial state or being exposed to external perturbations during execution.

One way to improve the performance of the agent in the deployment phase is to optimize an extra objective, e.g., by minimizing the uncertainty-level of the agent in predicting the next state \cite{8}, \cite{9} which implicitly helps the agent to stay in-distribution. However, designing such objectives is challenging and they may require learning probabilistic visual forward dynamic models that output a measure of uncertainty.

\textsuperscript{1}KTH Royal Institute of Technology, \textsuperscript{2}Stanford University

In this work, we propose a method to augment a policy trained by offline behavior cloning with a recovery policy whose actions are computed by a gradient ascent on the estimated density of the training distribution. This is illustrated in Figure 1, in which the robot is guided by the recovery policy providing action directions to stay in-distribution while approaching the task object. We achieve this by training a model that encodes input visual observations into a Euclidean latent space, where translations in this space correspond to robot actions, such as Cartesian displacements of the robot end-effector. The encoding has a property known as translational equivariance that allows for the conversion of the aforementioned gradient of the estimated training data density into an action. Therefore, the recovery design benefits from a latent representation that (1) is low-dimensional, thus amenable to density estimation, and (2) is task-agnostic, i.e., it can be shared among other tasks.

We empirically demonstrate the feasibility of the proposed method on real-robotic visuomotor policy training tasks. Compared to a behavioral cloning policy, we show that the augmented policy improves the success rate on manipulation tasks. Additionally, when the robot is externally pushed OOD, it allows to recover and successfully complete the task. We also demonstrate how the trained latent equivariant representation can be shared among several tasks, making it task-agnostic. Our main contributions are:

- A method to augment policies trained with offline data...
to recover from OOD conditions through the gradient of a conditional density estimator.

- An empirical evaluation of the performances of the proposed method on real-robotic manipulation tasks.

II. RELATED WORK

**Offline policy learning** mainly fall into behavior cloning [10] and offline RL [2]. The classic formulation of BC has a number of limitations when learning on real-world data. The most prominent of which, is called the compounding error [11] and occurs due to the sequential nature of the learning framework. This problem is even more profound when learning from small-sized datasets. There have been a number of works targeting this, however, they generally break the fully offline formulation [4], [12], [13].

Offline RL, on the other hand, formulates the problem of learning a policy using offline data from an RL perspective. A naive application of RL on previously collected data results in either an high variance of the learning process [14] or wrong estimates of the expected return [15]. Possible solutions to this involve either constraining the learned policy to minimize the deviation from the one that collected the data (behavioral policy) [5], [16], [17] or incentivizing the policy to avoid actions on the boundary of the training distribution by changing the reward function [6], [7], [18]. Moreover, in case the agent happens to step OOD, or it is forcefully brought there, there is no explicit way to recover. Which is what we address in this work.

**Safety measures** in the context of a learned controller have been addressed in different forms [19]. One common thread is the identification of safe regions where the agent can operate and the use of a recovery policy. In [20], unknown regions are defined by the uncertainty estimate of a perception module. When the agent steps there, a model-based reset policy is triggered. Differently from our method, they require a model of the objects and they assume the transition function is known in a subset of the state space. Other works instead assume to directly have access to a constraint function from the environment or approximate it from data, which quantifies the safeness of states. A policy can then be learned to actively avoid such states [21], [22] or plan a trajectory that remains in the safe region of the state space [23]–[25]. Having access to the constraint function or data-points in unsafe states can, however, be problematic for robotic applications. A similar work to ours proposes to learn an approximation of the tangent space of the task manifold at any point [26]. This can, in turn, be used to plan the overall trajectory. If some kind of perturbation occurs, the agent can project its current position in the manifold and plan a path to get back in. The projection is learned explicitly using a dataset of perturbed points. On the contrary, the way we learn the encoder allows us to automatically get the projection direction even from high-dimensional states like images.

**State Representation** for control has been widely studied in prior works [27]–[29]. Dividing the optimization of the representation from the policy has the advantage of easing the learning process and enables to constrain the policy formulation [30], [31]. Moreover, the learned representation can be re-used for different tasks assuming the underlying dynamics remain the same. In [32] and [33] an encoder is trained to compress the state representation while retaining all of the information. A transition model is then inferred on top of the representation to predict the dynamics of the environment. This formulation, however, produces a generic representation with no particular properties. To this end, more rigid constraints have been proposed. In [34] the representation is forced to evolve linearly in time, while in [30] the model outputs spatial features representing the observations. Moreover, by imposing a linear dynamic on the representation, the learned controller can be simplified and, under some assumptions, learned optimally [35], [36]. Unlike our method, this dynamic cannot be directly converted into an action. [37] train a variational autoencoder with the additional constraint of making the latent representation evolve according to Newtonian physics. This allows for classical controllers, like a PID, to be applied directly. In [38], they propose to learn an encoder and a transition model at the same time. Both models are learned such that the latent representation is equivariant to the transition model. Differently from all of these methods, we require our representation to be globally translational-equivariant in order to convert the gradient of the density estimator into a viable action.

III. BACKGROUND

We study the problem of learning a policy using a Markov decision process (MDP). We assume the MDP to be fully observable and specified by the tuple \((S, A, T)\). Here \(S\) is the set of observations representing the state of the environment, \(A\) is the set of actions the agent can take, and \(T: S \times A \rightarrow S\) is the transition function governing the change in observations when the agent performs an action. We can then formulate the problem of policy training as learning a map \(\pi: S \rightarrow A\) by minimizing a cost function. Throughout this paper we define the set of states \(S\) to be images and the set of actions \(A \subseteq \mathbb{R}^n\) to be continuous translations of the agent’s end-effector in the Euclidean space. A dataset \(D\) of experts’ demonstrations is a collection of trajectories representing the robot completing a task in different conditions. This dataset can be considered as a collection of tuples \(D = \{(s, a, s')\}\) with \(s' = T(s, a)\).

**A. Behavioral Cloning**

Behavioral Cloning is one of the most widely used imitation learning (IL) approaches due to its ease of implementation. It defines the cost function of the policy \(\pi\) as a supervised learning loss. As such, the policy’s parameters \(\theta\) can be inferred by minimizing the Mean Squared Error (MSE) between its estimated actions and the ones in the dataset \(D\):

\[
\pi = \pi_{\theta^*}, \quad \theta^* = \arg\min_{\theta} \sum_{(s, a) \in D} \|\pi_{\theta}(s) - a\|^2.
\]  

This simple IL strategy offers a number of advantages. First, it is easy to implement and stable to train. Second, it can be
Fig. 2: Commutative diagram illustrating equivariance as a property of the mapping $E$.

learned completely from offline data requiring neither access to the environment nor any knowledge of the transition model or a reward function.

B. Equivariant Mapping

In this section, we explain equivariance as a property of a mapping $E$ that in our case maps an input observation $s$ into a latent representation $z \in Z$, i.e., $z = E(s)$. Here, we consider two transition functions, $T : S \times A \rightarrow S$ and $T' : Z \times A \rightarrow Z$. The map $E : S \rightarrow Z$ is defined to be equivariant with respect to the transitions $T, T'$ if [39], [40]:

$$E(T(s, a)) = T'(E(s), a).$$

(2)

Figure 2 visually illustrates the equivariance property for the mapping $E$ and the transitions $T$ and $T'$. Intuitively, mapping the observation into the latent space followed by the transition $T'$ must result in the same latent value $z$ as applying the transition $T$ followed by mapping the resulting observation into the latent space.

IV. Method

In this section, we introduce our method that augments a policy trained with BC with a recovery strategy which can bring the agent back in-distribution, where the BC policy performs optimally. We achieve this by introducing a recovery policy $\pi_R : S \rightarrow A$ whose actions move the agent to the training manifold, i.e., within the support of the observations in the training dataset. The intuition is that the agent should follow the recovery policy to recover from OOD states, and the BC policy when in-distribution to complete the task. Therefore, we propose to compute the actions given by each policy, and find the weighted sum of the actions to obtain the final policy output. The weights are computed according to a normalized estimation of the density of the training states. However, as we describe in section IV-B, we estimate the density by first mapping the observation into a latent space $z = E(s)$, and then computing the density given the latent variable $z$ as the input $\rho(z)$. To ensure values in $(0, 1)$, the estimated density is normalized using a sigmoid function $\hat{\rho}(z) = 1/(1+\exp(-z^2/\tau))$ with an appropriate offset $\varepsilon$ and temperature $\tau$ parameters, and then used as the following to compute the output of the augmented policy $\bar{\pi}$:

$$\bar{\pi}(s) = \hat{\rho}(z)\pi(s) + (1-\hat{\rho}(z))\pi_R(s).$$

(3)

In the following sections, we first introduce our proposed equivariant mapping which maps raw visual observations into a latent space in which translation corresponds to the robot actions. Then, we introduce our method to estimate the density of the training observations in the latent space. Finally, we describe how the recovery policy is constructed based on the learned equivariant mapping.

A. Learning an Equivariant Mapping

We propose to learn a low-dimensional representation of the input visual observations by explicitly learning an equivariant mapping $E : S \rightarrow Z$. As we describe in section IV-C, we exploit the equivariant property of the mapping to construct the recovery policy. Besides, learning a low-dimensional representation of visual inputs can also help in estimating the density of the training data.

Given the transition of the MDP $T(s, a)$, we consider the following transition in the latent space: $T'(z, a) = z + a$. This is because the robot actions translate the end-effector in the Euclidean space. We refer to Section VI for a discussion on how this can be generalized to actions beyond translations of an end-effector of a manipulator. We want to learn an equivariant mapping with respect to $T, T'$ i.e., $E$ has to satisfy the following version of Equation 2:

$$E(T(s, a)) = E(s) + a.$$  

(4)

As shown in Figure 3 (left), $E$ implements translational equivariance since it converts transitions into translations. Note that Equation 4 assumes that $A$ and $Z$ share the same ambient space $\mathbb{R}^n$. The equivariant model $E$ is trained on states and actions well-distributed within the environment i.e., a dataset $D'$ is pre-collected independently from the specific task. As long as the scene composed of the extrinsic objects in the robot’s environment remains constant, $E$ can be deployed in different tasks. In order to ensure a correct representation, $D'$ needs to be distributed as uniformly as possible. The mapping $E$ is parameterized by a neural network $E = E_{\theta}$ with output space $\mathbb{R}^n$ and optimized by minimizing the following objective function on the dataset $D'$:

$$\theta^* = \text{argmin}_{\theta} \sum_{(s', a') \in D'} \|E_{\theta}(s') - E_{\theta}(s) - a\|^2.$$  

(5)

B. Estimating the Density of the Training States

We estimate the probability density of the agent being within the support of the training data by learning a parametric density estimator. The density estimator needs to be conditioned on the position of the manipulation objects for the task. It is thus conditioned on the image observation for the initial configuration of the manipulation task (Figure 3, right). We use Mixture Density Networks (MDN) [41], which estimate a conditional Gaussian mixture density. The MDN outputs the density in the form of means $\mu_i$, (diagonal) co-variances $\sigma_i$ and weights $w_i$ of a mixture of Gaussians.
The density in the point $z$ can then be computed as follows:

$$
\rho(z) = \sum_{i=1}^{N} w_i \mathcal{N}(z; \mu_i, \sigma_i).
$$

(6)

The MDN is trained by minimizing the average negative log-likelihood of $\rho$ over the observations in the training dataset $\mathcal{D}$.

C. Recovery Policy

The recovery policy is responsible to output actions that bring the agent closer to states within the support of the training data. This is done by finding an action that brings the agent into a state with higher estimated density. This is equivalent to performing gradient ascent on the estimated density function in the latent space. Because of the translational-equivariant property of our mapping, i.e., $z' = E(s') = E(s) + a = z + a$, the gradient $\nabla_z \rho(z)$ is equal to a robot action that moves the agent to higher density states. Therefore, we can simply define the output of the recovery policy for an observation $s$ as:

$$
\pi_R(s) = \eta \nabla_z \rho(E(s))
$$

(7)

where $\eta$ is a scale parameter. Once the density of states has been estimated in the latent space, the recovery policy can be implemented accordingly without any further training phase.

V. Experiments

In order to assess the effectiveness of the recovery of the proposed model, we present the results of a number of experiments. First, the experimental setup is described, then details on each of the experiments are presented.

• The first experiment compares the performances of a BC agent with and without recovery on a robotic manipulation task.

• The second experiment tests the ability of a BC agent learned from noisy data, with and without recovery, in performing the same task.

• The third experiment compares the ability of BC, with and without recovery, in resuming a task if brought forcefully OOD.

• The fourth experiment involves solving a different task. The goal of this experiment is to show that the representation is agnostic to the task.

A. Experimental Setup

All the experiments are performed in the real world using a YuMi-IRB 14000 collaborative robot by ABB. We record all the data through teleoperation of the robot by a human. To implement the teleoperation system we used a virtual reality (VR) system connected to the robot’s controllers. Teleoperation through VR has, in fact, proved to be a viable option for robotics applications thanks mainly to its ease in use and speed of data collection [42]–[45]. In particular, for our experiments, we interface an Oculus Quest 2 device to the robot’s operating system.

To record the data, the human operator stands in front of the robot and operates the VR hand controller to command desired velocities to the end-effector of the robotic arm. Commands are thus mirrored with respect to the human perspective. Velocity commands are sent with a frequency of 10Hz to the robot that then translates them to the equivalent joint velocities. In all of the experiments, the velocities are just translations in space as no angular velocities are considered, meaning that $A \subseteq \mathbb{R}^3$. Images, representing the state of the system by a static camera placed in front of the robot in coordination with the VR commands.

The setup is the same across all experiments and its shown in Figure 4. The robot is placed in front of a table where two objects are placed, a small plastic orange cylinder, the \textit{manipulated object}, and a bigger plastic yellow cylinder, the \textit{target object}. Throughout all the experiments the target object is never moved while the robot needs to interact with the manipulated object.

B. Networks’ Architectures

The equivariant encoder $E$ is parameterized by 5 convolutional layers with 64 channels except the last one with
followed by a hidden fully-connected layer with 64 units, every hidden layer is followed by a ReLU activation function. The network is trained with a learning rate of $10^{-3}$ using the Adam optimizer. Input images are cropped, resized and normalized before being fed to the network.

The policy is parameterized by a neural network with a ResNet18 backbone pre-trained on ImageNet and a randomly initialized fully connected head with 2 hidden layers of 64 units each. The MDN density estimator is parameterized by a CNN model of 4 layers with 64 channels and one with 8 channels followed by 3 output layers for the mean, diagonal variance and weights of the mixture of Gaussians. The MDN is trained, as stated in Section IV-B, to minimize the negative log-likelihood of the latent representation of the equivariant encoder. The MDN is conditioned on the initial image of each trajectory and the gripper state. The reason being that the model needs to be aware of the position of the object to be picked up to output a conditional density but it should not have access to the position of the gripper. There is, in fact, a functional dependency between images where the gripper is shown and the density estimate itself. By conditioning the MDN on the current image during the roll-out, the density would collapse. Conditioning the model on the gripper state is also needed as the position of the gripper should be considered in-distribution or not based on the object being grasped or not, respectively. Training an MDN is notoriously unstable [46] and we found that adding a deconvolution decoder that maps a middle representation of the model into a reconstruction of the original image can stabilize the training. Both the policy and the MDN are trained using the Adam optimizer with a learning rate of $10^{-4}$. The other hyper-parameters used for this experiment are the following: $\eta = 0.05$, $\varepsilon = 2.0$ and $\tau = 0.5$.

C. Equivariant Encoder

The equivariant representation used for the density estimator is agnostic to the task and can be learned a priori.

For the dataset $\mathcal{D'}$, we collect 6 trajectories of the robotic arm moving uniformly in the space and interacting with the manipulated object for a total of 1741 steps. Interaction with the objects is needed in order to make the learned encoder invariant to its position. Equivariance is defined with respect to the robot’s actions only and the learned representation should not be sensitive to the object’s position.

Because the actions are translations in the Euclidean 3D space the equivariant representation will correspond to points in 3D where the gripper of the robot is located (the central point of the actual movement). The representation preserves distances so the scale is one to one with the actions’ magnitude. This can be seen in Figure 4 where the expert’s trajectories have been mapped into the latent space of the encoder and projected in 2D. In fact, the shape of the table and the relative position of the objects are maintained. For interpretability, we force the initial configuration of the robot to be the origin of the representation by including a second term in the loss of Equation 5.

Fig. 4: Experimental setup for the pick-and-drop task. The small bin (manipulated object) has to be dropped inside the larger one (target object). A trajectory recorded by the expert via teleoperation is also displayed.

D. Pick-and-Drop Experiment

1) Experiment description: In the first experiment, the goal is for the robot to pick the manipulated object, move it on top of the target object and drop it inside. Here the actions are the combination of the gripper’s velocity and a binary value representing the state of the gripper (either open or close). The initial position of the manipulated object is initialized randomly in the first half of the table while the target object is kept fixed on the other half of the table. A dataset of 120 trajectories of a human demonstrating the task is used to train the model. The dataset accounts for 5526 steps in total and is used to train both the behavioral cloning policy and the density estimator. The demonstrations are collected using the VR teleoperation system described above. However, these demonstrations cannot be assumed optimal due to the noise in the teleoperation system and the non-Markovianity of the environment. In fact, there are two elements here that break the Markovian assumption. The first is the current velocity and acceleration the robot has before giving it a command. The next state will vary depending on these properties that are not inferable from one single image. The second element is the inverse kinematic module of the robot. The resulting actual displacement of the end effector will also depend on the current state of the joints that is not fully observable from the images.

2) Results: In the first set of experiments, we test the proposed method against the imitation learning policy without the recovery term. The models are evaluated on 20 trials with the manipulated object in different positions. Performances are based on their ability to successfully grasp the manipulated object and their ability to then drop it inside the target bin. Table I shows the results of this experiment. The standard BC model manages to complete the task only one-fourth of the time. On the other hand, coupling the same policy with the proposed recovery lets the agent adjust its position every time it makes a mistake that would bring it OOD. This results in a much higher success rate.
Further, to assess the robustness of the recovery policy, we test it in noisy conditions. We train a second BC policy on the same dataset but with all the actions shifted by one step with respect to the images. We effectively simulate a data gathering scenario where there is a delay between the camera sensor and the actual movement of the robot. Two subsequent states are not connected by the saved action. However, because of the uniformity of the task, the real action does not differ considerably and the overall motion of the agent keeps a similar behavior. Nonetheless, a policy trained on this sub-optimal dataset does not manage to solve the task even once. On the other hand, by coupling the same policy with the proposed recovery module the performances are quite unchanged with respect to the correct dataset case, see Table I.

Lastly, we test the BC policy with and without recovery by applying a random displacement to the robot. At the beginning of the task, we move the gripper in a random direction and let it continue the task from there. The new position could be outside of the training distribution, making the imitation learning policy behave randomly. The recovery policy instead can climb back to the training manifold and continue with the task normally. The object is initialized in a position where the imitation learning agent is able to complete the task. As shown in Table I, the learned policy suffers considerably from this kind of perturbations. On the other hand, when coupled with the proposed recovery it can always get back in and most of the time complete the task.

### E. Pushing Experiment

The second set of experiments involves the same environment with unchanged dynamics. The goal is for the agent to insert the gripper’s tip into the manipulated object and push it all the way towards the target object. In this experiment, the gripper is always closed. Because the robotic arm moves in the same way and only the manipulated object is moved throughout the roll-outs, the encoder can be used without retraining. Both the imitation learning policy and the density estimator have to be retrained on the new demonstrations. For this experiment, a new dataset of 60 demonstrations is collected for a total of 3895 steps. Results in Table II show that the encoder can be used without retraining and that the recovery policy increases the performances of the learned policy.

### VI. Conclusions and Future Work

We proposed to couple an agent learned on experts’ demonstrations with a recovery policy to keep it within the training data. This is achieved by explicitly modeling the training distribution with a density estimator and bypassing the agent’s action whenever the current state is detected to be OOD. By training an encoder to be equivariant to the agent’s actions, the recovery policy can be formulated as a form of gradient ascent on the density estimate.

We applied the proposed methodology to a robotic manipulator whose actions correspond to Euclidean translations. As a possible extension, more complex actions could be considered such as rotations of joins and end-effectors. This would involve Lie groups beyond the Euclidean space such as the group of rotations SO(n), n = 2, 3. A further extension of the framework lies in designing more complex recovery strategies than pure gradient ascent in order to smooth the resulting movement.

### VII. Acknowledgements

This work has been supported by the Swedish Research Council, Knut and Alice Wallenberg Foundation, European Research Council (BIRD-884807) and H2020 CANOPIES.

### References

[1] S. Levine, P. Pastor, A. Krizhevsky, J. Ibarz, and D. Quillen, “Learning hand-eye coordination for robotic grasping with deep learning and large-scale data collection,” The International Journal of Robotics Research, vol. 37, no. 4-5, pp. 421–436, 2018.

[2] S. Levine, A. Kumar, G. Tucker, and J. Fu, “Offline reinforcement learning: Tutorial, review, and perspectives on open problems,” arXiv preprint arXiv:2005.01643, 2020.

[3] A. Hussein, M. M. Gaber, E. Elyan, and C. Jayne, “Imitation learning: A survey of learning methods,” ACM Computing Surveys (CSUR), vol. 50, no. 2, pp. 1–35, 2017.

[4] S. Ross, G. Gordon, and D. Bagnell, “A reduction of imitation learning and structured prediction to no-regret online learning,” in Proceedings of the fourteenth international conference on artificial intelligence and statistics. JMLR Workshop and Conference Proceedings, 2011, pp. 627–635.
