Data Lifecycle Management in Evolving Input Distributions for Learning-based Aerospace Applications

Somrita Banerjee, Apoorva Sharma, Edward Schmerling
Department of Aeronautics and Astronautics
Stanford University
Stanford, CA 94305
{somrita, apoorva, schmrlng}@stanford.edu

Max Spolaor, Michael Nemerouf
The Aerospace Corporation
2310 E. El Segundo Blvd.
El Segundo, CA 90245
{max.spolaor, michael.k.nemerouf}@aero.org

Marco Pavone
Department of Aeronautics and Astronautics
Stanford University
Stanford, CA 94305
pavone@stanford.edu

Abstract—Learning-enabling components are increasingly popular in many aerospace applications, including satellite pose estimation. However, as input distributions evolve over a mission lifetime, it becomes challenging to maintain performance of learned models. In this work, we present an open-source benchmark of a satellite pose estimation model trained on images of a satellite in space and deployed in novel input scenarios (e.g., different backgrounds or misbehaving pixels). We propose a framework to incrementally retrain a model by selecting a subset of test inputs to label, which allows the model to adapt to changing input distributions. Algorithms within this framework are evaluated based on (1) model performance throughout mission lifetime and (2) cumulative costs associated with labeling and model retraining. We also propose a novel algorithm to select a diverse subset of inputs for labeling, by characterizing the information gain from an input using Bayesian uncertainty quantification and choosing a subset that maximizes collective information gain using concepts from batch active learning. We show that our algorithm outperforms others on the benchmark, e.g., achieves comparable performance to an algorithm that labels 100% of inputs, while only labeling 50% of inputs, resulting in low costs and high performance over the mission lifetime.

1. INTRODUCTION

Motivation—Learning-based models are being increasingly used in aerospace applications because of their ability to deal with high-dimensional observations and learn difficult-to-model functions from data. However, the performance of these models depends strongly on the similarity of the test input to the training data. During a mission lifetime, anomalous inputs and changing input distributions are very common. For example, a model that uses camera images to estimate the pose of a satellite could encounter out-of-distribution (OOD) inputs such as different backgrounds, lighting conditions, lens flares, or misbehaving pixels [1], [2]. For rover dynamics models that are adaptive and learning-enabled, the OOD inputs could result from encountering novel terrain or sensor degradation [3]. Without any intervention, these OOD inputs would then lead the model to produce incorrect predictions and potentially unsafe results.

For safety-critical and high consequence applications, such as those in aerospace, it is crucial that the model remains trustworthy throughout the mission lifetime. In order to support long deployment lifetimes, during which the input distribution may evolve, it is critical to design models that are resilient to such changes. This highlights the need for frameworks like Aerospace’s Framework for Trusted AI in High Consequence Environments [4] and methods of retraining the model during the mission lifetime, so that it can adapt to evolving conditions. We refer to this challenge as the problem of “data lifecycle management,” entailing how to detect when a learning-based model may be uncertain or performing poorly, and how to design strategies to mitigate this poor performance, e.g., by referring to a human operator or fallback system, or obtaining labels for new inputs to retrain and adapt the model for continued high performance.

Closing the data lifecycle loop is challenging because it requires storing data, downlinking data, obtaining oracle labels, and uplinking labels for retraining, all of which are expensive operations, and must usually be done in a batched episodic manner to ensure safety and computational feasibility. These challenges are discussed in more detail in Section 2. In order to practically retrain models during their lifetimes, we need onboard real-time decision making about which inputs are most informative to store and label. In this work, we focus on managing the data lifecycle within the context of the framework shown in Figure 1, which consists of the following steps: select a subset of test inputs for labeling, obtain labels for these inputs (either by expert humans or an oracle fallback system), and use these labels to retrain / adapt the model over time, so that the model can adapt to changing distributions.

Related work—The data lifecycle framework, as presented, can be broadly divided into two algorithmic components: (1) selecting a subset of inputs for labeling and (2) retraining the model using these inputs. For the first task, techniques such as uncertainty quantification [5] and OOD detection [6]...
Figure 1: Given a sequence of inputs, a model outputs a prediction and, potentially, an uncertainty. Data lifecycle management for a model requires adapting to changing input distributions, e.g., novel backgrounds, by periodically refining the model with inputs that were flagged, i.e., inputs that the model is uncertain about.

are useful for detecting inputs the model is most uncertain about, has not encountered previously, and is likely to perform poorly on. However, these techniques only provide information about a single test input and do not capture the mutual information correlation between multiple test inputs. A practical solution to selecting inputs requires augmenting these techniques with a notion of group uncertainty and choosing subsets that are collectively maximally informative. Choosing subsets of inputs that maximize information gain has been the focus of active learning [7], especially batch mode active learning [8], [9], [10], [11]. Some approaches for selecting inputs include labeling the inputs that lead to greatest expected error reduction [12], that would change the model the most [13], or that maximize diversity and information gain [11]. However, these works do not address how to quantify the information gain from an input. Our proposed algorithm bridges the gap by using Bayesian uncertainty to express the information gain from an input and techniques from batch active learning to choose a diverse subset.

The literature also lacks a benchmark to evaluate these algorithms in a full data lifecycle context. For example, the WILDS benchmark [15] is useful to evaluate the robustness of models to distribution shifts, but does not close the loop on evaluating the effect of labeling and retraining the model on the lifelong performance of the model. Similarly, the second algorithmic component, i.e., retraining the model, has been the focus of continual learning algorithms [16], for which benchmarks such as CLEAR have been developed [17], [18] but these benchmarks do not consider the impact of judiciously selecting which inputs to label on the downstream retraining task. This paper addresses this gap by presenting a benchmark for the full data lifecycle.

Contributions—As our first contribution, we propose a benchmark that evaluates algorithms for subselecting and retraining along two macro-level metrics (1) model performance throughout mission lifetime and (2) cumulative costs associated with labeling and retraining. While this benchmark is generalizable to any application, we provide open-source interfaces and test sequences from the ExoRomper dataset, developed by The Aerospace Corporation. The ExoRomper simulation dataset was assembled in support of Aerospace’s Slingshot program [19], which recently launched a commercial 12U smallsat bus, Slingshot 1, with 19 “plug and play” payloads, including ExoRomper. The ExoRomper payload is designed with thermal and visible light cameras facing a maneuverable model spacecraft and leverages an AI accelerator payload also on Slingshot 1 to experiment with machine learning-based pose estimation solutions. The ExoRomper dataset contains simulated camera images of the maneuverable model spacecraft as viewed on-orbit, along with ground truth labels of the satellite model’s pose. Test sequences constructed from this dataset include different types of OOD images which can be used to evaluate a pose estimation model and compare different algorithms in the context of a data lifecycle.

In order to balance labeling costs and maintain model performance, we need onboard real-time decision making about which inputs are most informative to store and label. This leads us to our second contribution—a novel algorithm, Diverse Subsampling using Sketching Curvature for OOD Detection (DS-SCOD)—which selects a diverse subset of OOD inputs for labeling and retraining. This algorithm leverages Jacobians from a state-of-the-art OOD detection and uncertainty quantification algorithm, SCOD, [20] and concepts from Bayesian active learning [11] to select a diverse subset of inputs for labeling, which are then used to adapt the model to changing distributions. We show that this algorithm outperforms other algorithms (naive, random, and uncertainty threshold-based) on the benchmark, i.e., results in Section 6, and includes minor edits.

A previous version of this paper was presented at the AI4Space Workshop (part of ECCV 2022) on 23 October 2022. This version adds an illustrative example on the canonical MNIST dataset in Figure 2a, expands the discussion of results in Section 6, and includes minor edits.
in high model performance throughout the mission lifetime, while also incurring low labeling costs.

**Organization**—The paper is organized as follows. Section 2 discusses the challenges associated with data lifecycle management and introduces two tools that are instrumental to our approach: OOD detection algorithms and batch active learning methods. Section 3 describes the problem formulation for data lifecycle management. Section 4 presents our open-source benchmark for evaluating data lifecycle algorithms. Section 5 introduces our novel data subselection algorithm, DS-SCOD. Section 6 presents results of evaluating our algorithm on the benchmark using the ExoRomper dataset where it outperforms other methods, e.g., achieves performance comparable to an algorithm that labels 100% of inputs while only labeling 50% of inputs. Finally, Section 7 provides conclusions and future research directions.

**2. BACKGROUND**

**Challenges for Data Lifecycle Management**

Data lifecycle management, especially for aerospace applications, has a number of challenges. We use the example of pose estimation for CubeSats [21], such as the Slingshot satellite, to contextualize these challenges, which include:

1. Data collection and storage may be limited by onboard storage capacity, especially for large input sizes, constant streams of data, and having to store inputs for future labeling.
2. Data transmission may be limited, e.g., by cost, intermittent connectivity to ground stations, narrow downlink windows, and limited bandwidth [21].
3. Operations associated with labeling are expensive, e.g., obtaining a label from a human expert.
4. Retraining the model is expensive, and doubly so if carried out on space hardware which is limited by onboard computation power [22], [21]. Rather than retraining on each individual flagged input, it is more computationally feasible to retrain on batches of flagged inputs.
5. Lastly, building safe and trusted AI systems often requires model updates to be episodic and versioned in nature, in order to ensure adequate testing. This results in a batched, rather than streaming, source of ground truth labels as well as delays between flagging inputs and receiving labels.

These challenges highlight the need for a judicious, real-time, and onboard decision-making algorithm that selects inputs for storage, downlinking, labeling, and retraining. In this work, we model some of these challenges by designing our algorithms to operate on batches and explicitly optimizing for low labeling cost. Next, we discuss two key tools that enable our algorithmic design.

**Out-of-Distribution Detection**

A key requirement of data lifecycle management is to be able to detect when inputs to the model are no longer similar to those seen during training, i.e., detect when inputs are OOD and the model is likely to perform poorly. Detecting when inputs are OOD is useful in many ways, e.g., as a runtime monitor or anomaly/outlier detector so that the corresponding outputs can be discarded or a fallback system can be used. OOD detection is also useful in deciding which inputs to use to adapt the model, so model performance does not degrade as input distributions evolve. A principled approach to OOD is to quantify the functional uncertainty of the model for each test input, i.e., how well does the training data determine the predictions at a new test input. This work employs the Bayesian approach to uncertainty quantification developed by Sharma et al., Sketching Curvature for Out-of-Distribution Detection (SCOD) [20], which is summarized below.

Consider a pre-trained model \( f \) with weights \( w \in \mathbb{R}^N \) that maps from input \( x \in \mathcal{X} \) to the parameters \( \theta \in \Theta \) of a probability distribution \( p_\theta(y) \) on targets \( y \in \mathcal{Y} \), where \( \theta = f(x, w) \). The model is trained on a dataset of examples \( \mathcal{D} = \{ x_i, y_i \}_{i=1}^M \). The prior over the weights of the model is \( p(w) \) and the posterior distribution on these weights given the dataset is \( p(w | \mathcal{D}) \). Characterizing the posterior and marginalizing over it produces the posterior predictive distribution

\[
p(y | x) = \int p(w | \mathcal{D})p(y | x, w)dw.
\]

**Estimating posterior offline.**—To tractably compute this posterior for Deep Neural Networks, SCOD uses the Laplace second order approximation of the log posterior \( \log p(w | \mathcal{D}) \) about a point estimate \( w^* \). If the prior on the weights is the Gaussian \( p(w) = \mathcal{N}(0, \epsilon^2 I_N) \), the Laplace posterior is also a Gaussian, with mean equal to the point estimate \( w^* \), and covariance given by

\[
\Sigma^* = \left( H_L + \epsilon^{-2}I_N \right)^{-1},
\]

where \( H_L \) is the Hessian with respect to \( w \) of the log likelihood of the training data, namely, \( L(w) = \sum_{i=1}^M \log p_{w^*}(y_i | x_i) \). The Hessian can in turn be well approximated by the dataset Fisher information matrix, i.e.,

\[
H_L = \frac{\partial^2 L}{\partial w^2} \bigg|_{w^*} \approx MF_{w^*}^D.
\]

The dataset Fisher information matrix \( F_{w^*}^D \) describes the impact of perturbing the weights \( w \) on the predicted output distribution for each output in the dataset \( \mathcal{D} \), i.e.,

\[
F_{w^*}^D = \frac{1}{M} \sum_{i=1}^M F_{w^*}^{(i)}
\]

where \( F_{w^*}^{(i)}(x_i, w^*) = J_{f, w}^T \cdot F_{\theta}^{(i)}(\theta)J_{f, w^*} \),

\[
F_{\theta}^{(i)}(\theta) = \Sigma(x^{(i)}, w^*)^{-1}.
\]

SCOD uses a matrix sketching-based approach to efficiently compute a low-rank approximation of the dataset Fisher \( F_{w^*}^D \), which in turn enables the computation of the Laplace posterior \( \Sigma^* \) using Equations 2, 3, and 4. This is done offline.

**Online computation of predictive uncertainty.**—For a test input \( x^{(t)} \), the predictive uncertainty is computed as the expected change in the output distribution (measured by a KL divergence \( \delta_{\text{KL}} \)) when weights are perturbed according to the Laplace posterior \( \Sigma^* \). Sharma et al. show that this
expectation can be related back to the Fisher information matrix for this test input $F_u^{(i)}$, i.e.,

$$\text{Unc}(x^{(i)}) = \mathbb{E}_{u \sim N(0, \Sigma)} \left[ \delta_{KL}(x^{(i)}) \right] \approx \text{Tr} \left( F_u^{(i)} \Sigma^* \right). \quad (7)$$

Therefore, for a test input $x^{(i)}$, SCOD uses a forward pass to calculate the output $p(y) = f(x^{(i)}, w)$, a backward pass to calculate the Jacobian $J_f(w)$ at $x^{(i)}$, and the output covariance $\Sigma(x^{(i)}, w^*)$. Then, using Equations 5, 6, and 7, the predictive uncertainty $\text{Unc}(x^{(i)})$ can be efficiently computed. This predictive uncertainty can be thought of as a measure of epistemic uncertainty: if it is high, then the prediction for input $x^{(i)}$ is not well supported by the training data, while if it is low, then the training data supports a confident prediction. Therefore, this estimate is useful for detecting OOD inputs.

Bayesian Batch Active Learning

Detecting inputs that have high uncertainty allows those inputs to be flagged for labeling and retraining. However, in practice, a limited budget for retraining precludes selecting every uncertain input. While a naive solution might be to select the subset with the highest uncertainties, this can lead to subsets with redundancy: including many similar inputs while leaving out other inputs that are also informative. Instead, it is important that we not select inputs greedily, but rather sets of diverse inputs for which labels would jointly provide more information. To do so, we take inspiration from active learning, where the goal is to select the most informative inputs, and, in particular, batch active learning, which selects a batch of informative inputs instead of a single input, allowing retraining to be done epidiomically rather than sequentially, further lowering labeling costs [8], [9], [10], [11]. This work closely utilizes the Bayesian batch active learning approach developed by Pinsler et al. [11], which is summarized below.

Consider a probabilistic predictive model $p(y \mid x, \theta)$ parameterized by $\theta \in \Theta$ mapping from inputs $x \in X$ to a probabilistic output $y \in Y$. The model is trained on the dataset $D_0 = \{x_i, y_i\}_{i=1}^n$, resulting in the prior parameter distribution $p(\theta \mid D_0)$. During deployment, the model encounters a set of test inputs $X_p = \{x_i\}_{i=1}^m$. It is assumed that an oracle labeling mechanism exists which can provide labels $Y_p = \{y_i\}_{i=1}^m$ for the corresponding inputs. From a Bayesian perspective, it is optimal to label every point and use the full dataset $D_p = (X_p, Y_p)$ to update the model. The resultant data posterior is given by Bayes’ rule

$$p(\theta \mid D_0 \cup (X_p, Y_p)) = \frac{p(\theta \mid D_0) p(Y_p \mid X_p, \theta)}{p(Y_p \mid X_p, D_0)}. \quad (8)$$

In practice, only a subset of points $D' = (X', Y') \subseteq D_p$ can be selected. From an information theoretic perspective, it is desired that the query points $X' = \{x_i\}_{i=1}^k$ (where $k \leq m$) are maximally informative, which is equivalent to minimizing the expected entropy, $\mathbb{E}[H]$, of the posterior, i.e.,

$$X' = \arg \min_{X' \subseteq X_p, |X'| \leq k} \mathbb{E}_{y' \sim p(y' \mid X', D_0)} [H(\theta \mid D_0 \cup (X', Y'))]. \quad (9)$$

Solving equation 9 requires considering all possible subsets of the pool set, making it computationally intractable. Instead, Pinsler et al. choose the batch $D'$ such that the updated log posterior $\log p(\theta \mid D_0 \cup D')$ best approximates the complete data log posterior $\log p(\theta \mid D_0 \cup D_p)$. The log posterior, following equation 8 and taking the expectation over unknown labels $Y_p$, is given by

$$\mathbb{E} \left[ \log p(\theta \mid D_0 \cup (X_p, Y_p)) \right] = \mathbb{E} \left[ \log p(\theta \mid D_0) + \log p(Y_p \mid X_p, \theta) - \log p(Y_p \mid X_p, D_0) \right]$$

$$= \mathbb{E} \left[ \log p(y_i \mid x_i, \theta) \right] + \mathbb{E} \left[ y_i \mid x_i, D_0 \right] \right) \right) \right) \right). \quad (10)$$

where $L_i(\theta)$ is the belief update as a result of choosing input $x_i \in X_p$. The subset $X'$ can now be chosen to best approximate the complete belief update, i.e., by choosing

$$c^* = \text{minimize}_c \left( \sum_i L_i - \sum_i c_i L_i \right)^2$$

subject to $c_i \in \{0, 1\}$ \quad \forall i

$$\sum_i c_i \leq k. \quad (11)$$

Here $c \in \{0, 1\}^m$ is a weight vector indicating which of the $m$ points to include in the subset of maximum size $k$. Pinsler et al. show that a relaxation,

$$c^* = \text{minimize}_c (1 - c)^T K (1 - c)$$

subject to $c_i \geq 0$ \quad \forall i,

$$\sum_i c_i \| L_i \| = \sum_i \| L_i \|, \quad (12)$$

where $K$ is a kernel matrix $K_{mn} = \langle L_m, L_n \rangle$, can be solved efficiently in real-time using Frank-Wolfe optimization, yielding the optimal weights $c^*$ after $k$ iterations. The number of non-zero entries in $c^*$ will be less than or equal to $k$, denoting which inputs (up to a maximum of $k$) are to be selected from the batch of $m$ inputs. Empirically, this property leads to smaller subselections as more data points are acquired. We leverage this Bayesian approach to selecting maximally informative subsets in our algorithm design, which enables maintaining high model performance while reducing labeling costs. In the next section, we discuss the framework and problem formulation guiding our approach.

3. Problem Formulation and Framework

In this paper, we consider the problem of data lifecycle management as applied to model adaptation via retraining using the specific framework shown in Figure 1. This framework assumes that the model receives inputs in a sequence of batches and that the model outputs a prediction for each input. Additionally, the model may also output an estimate of uncertainty for each input, such as the epistemic uncertainty estimate provided by SCOD. Based on the outputs for each batch, a decision must be made about which (if any) inputs to flag for labeling. If flagged, the input is labeled by an oracle and then used to retrain the model.
In the context of this framework, we seek to (1) develop a benchmark that evaluates algorithms not just for their accuracy and sample efficiency on a single batch, but over lifecycle metrics such as average improvement in lifetime model performance and cumulative lifetime labeling cost, and (2) develop an algorithm to select inputs for labeling, that are ideally diverse and informative, in order to minimize costs associated with labeling and retraining. In support of the first goal, we propose an evaluation benchmark that is described in the next section. In support of the second goal, we present a novel algorithm for diverse subset selection in Section 5.

4. Evaluation Benchmark

In this section, we present a benchmark to evaluate algorithms that decide which inputs to flag for labeling. A flagging algorithm is evaluated based on how well it manages the performance of a pre-trained model on a sequence of test input batches. The two metrics used for this evaluation are: the cumulative labeling cost, i.e., how many inputs were flagged for labeling, and the rolling model performance, i.e., the prediction loss of the model during the deployment lifetime. The ideal flagging algorithm keeps model performance high while incurring a low labeling cost. This benchmark procedure is described in Procedure 1.

**Procedure 1: Evaluation benchmark for “flagging” algorithms**

| Input: | model, test_seq, test_labels, flagger |
| Output: | labeling_cost, rolling_performance |
| 1 | Initialize flagged vector and outputs |
| 2 | foreach i, batch ∈ test_seq do |
| | /* store model predictions */ |
| | outputs[i] ← model(batch) |
| | /* flag to request oracle labels */ |
| | flags = flagger(batch) |
| | if any(flags) then |
| | /* store flagged inputs */ |
| | flagged_inputs = batch[flags] |
| | /* get oracle labels */ |
| | true_labels = test_labels[i][flags] |
| | /* refine model */ |
| | model ← refine_model(flagged_inputs, true_labels) |
| | end |
| 3 | /* calculate benchmark metrics */ |
| 4 | labeling_cost = cumsum(flagged) |
| 5 | rolling_performance = [-loss(outputs[i], test_labels[i]) for i, batch ∈ test_seq] |
| 6 | return labeling_cost, rolling_performance |

We provide an open-source benchmark to test flagging algorithms\(^2\). This interface includes a pre-trained pose estimation model and test sequences drawn from the ExoRomper dataset, as well as a categorization of different “types” of out-of-distribution images, such as those with different backgrounds (Earth/space), lens flares, or with added sensor noise. These input sequences can be passed in sequentially to the model, or as batches. Additionally, the benchmark also contains implementations of some simple flagging algorithms to compare against, such as flagging every input (naive_true), flagging none of the inputs (naive_false), and randomly flagging \(k\) inputs from each batch (random_k). The benchmark also contains implementations of two proposed flagging algorithms: (1) scod\(k\)_highest (or scod for short), which wraps the pre-trained model with a SCOD wrapper that provides an estimate of epistemic uncertainty for each input. From each batch, the \(k\) inputs with the highest SCOD uncertainties are flagged for labeling, and (2) diverse, Diverse Subsampling using SCOD (DS-SCOD), which is a novel algorithm that uses the Jacobians from SCOD and Bayesian active learning to select a subset of inputs that are not only out-of-distribution but also diverse. This algorithm is further described in the next section.

5. Diverse Subsampling Using SCOD (DS-SCOD)

To obtain performance improvement without high cost, it is necessary that the inputs chosen for labeling and retraining should provide information to the model that improves downstream performance, e.g., OOD inputs for which the model has high predictive uncertainty. However, an approach that greedily selects the \(k\) most uncertain images from a batch may be suboptimal. Consider a batch of inputs containing multiple “types” of OOD, e.g., images with an Earth background or with a lens flare, where flagging the \(k\) highest uncertainty images could lead to subsets containing only one type, while neglecting the information available from other types of OOD images. Downstream, this would lead to improved model performance for only the OOD type selected. In contrast, DS-SCOD seeks to capture the mutual correlation between multiple inputs, leading to a subset that contains diverse images and is maximally informative for the model. As discussed later in Section 6, empirical testing shows that diverse subselecting leads to higher downstream performance, while allowing for low labeling cost.

DS-SCOD is based on two governing principles: (1) that the inputs selected for labeling should provide information that improves downstream performance, e.g., inputs where the model has high uncertainty or OOD inputs and (2) that the subselected inputs from each batch be chosen to maximize collective information gain. Therefore, the representation of information gain due to an input must lend itself to expressing the total information gain after selecting a subset of multiple inputs. An ideal choice for representing this information gain is the Bayesian posterior for each input that is provided by Bayesian OOD algorithms such as SCOD, as described in Section 2. Specifically, the Jacobian of the output with respect to the weights, \(J_{f(w)}\), encodes the uncertainty for a single input, i.e., the impact of small weight changes on the output, and also encodes a correlation in uncertainty where \(J_{f(w)}\) shows that diverse subselecting leads to higher downstream performance, while allowing for low labeling cost.

The core methodology employed by DS-SCOD is to use batch active learning to select the maximally informative batch, as described in Section 2, where the information value of an input is expressed using a Bayesian belief update that

\(^2\) Code for the benchmark and our experiments is available at https://github.com/StanfordASL/data-lifecycle-management.
we obtain from SCOD, as described in Section 2. In DS-SCOD, we express the belief update, $L_i(\theta)$ as a result of choosing input $x_i$, from Equation 10, as

$$L_i(\theta) = \left(F_{\theta}(i) \theta\right)^{1/2} J_{f,w^*}^{(i)}$$

(13)

where $J_{f,w^*}^{(i)}$ is the Jacobian of the output with respect to the weights evaluated at $x_i$ and $F_{\theta}(i)$ is the Fisher information matrix of the output probability distribution $p_{\theta}(y)$ from Equation 6. Both of these expressions are calculated efficiently online by SCOD. Next, from each batch of size $m$, we select a maximum of $k$ inputs to flag for labeling by solving the optimization problem in Equation 12. Specifically, the optimization takes the form

**DS-SCOD:**

$$c^* = \text{minimize } (1 - c)^T K (1 - c)$$

where

$$K_{ij} = \langle L_i, L_j \rangle$$

$$= \text{Tr} \left( \left(F_{\theta}^{(i)} \right)^{1/2} J_{f,w^*}^{(i)} J_{f,w^*}^{(j)^T} \left(F_{\theta}^{(j)} \right)^{1/2} \right)$$

subject to

$$c_i \geq 0 \quad \forall i,$$

$$\sum_i c_i \|L_i(\theta)\| = \sum_i \|L_i(\theta)\|.$$  

(14)

This optimization is solved using the Frank-Wolfe algorithm in real-time. By minimizing the difference between the belief update after choosing all $m$ points and after choosing inputs according to $c$, the loss of information is minimized. This results in a maximally informative subsample of inputs, without exceeding the given labeling budget $k$.

To further illustrate the effect of the DS-SCOD algorithm, two illustrative examples are presented in Figure 2. For the first example in Figure 2a, a model is trained on the MNIST dataset [23] of handwritten digits and wrapped with a SCOD wrapper. From a random batch of images consisting of both MNIST digits (in-distribution) and Fashion-MNIST images of clothing [24] (out-of-distribution), two images are selected that have the highest SCOD uncertainties and two images are selected using DS-SCOD. This example illustrates the difference between selecting images with the highest SCOD uncertainties (which results in correlated images such as two shirts) versus selecting images using DS-SCOD that are not only uncertain, but also form a diverse set (resulting in diverse clothing).

Similarly, for the second example in Figure 2b, a model is trained on ExoRomper space only images and wrapped with a SCOD wrapper. Again, from a random batch of images, two images are selected that have the highest SCOD uncertainty and two images are selected using DS-SCOD. A similar trend is observed here with SCOD-k highest selecting correlated images.
Figure 3: Comparing performance of the naive, random, scod, and diverse (DS-SCOD) algorithms in terms of average improvement in model performance over the lifecycle and the labeling cost. The latter three algorithms were evaluated with labeling budgets between 5% and 75% at intervals of 5%. The metrics are reported in percentages relative to the naive_false (0%) and naive_true (100%) algorithms.

As shown in Figure 3, the algorithms were evaluated on two metrics: the improvement in model performance as a result of retraining, averaged over the full test sequence, and the labeling cost, which is the number of images flagged for labeling expressed as a percentage of the total number of images. For some algorithms, we set a value k that determines what percentage of inputs the algorithm is allowed to select for labeling, henceforth referred to as the budget. The following algorithms were tested:

- naive_false: This simple algorithm never flags any image. Thus, the labeling cost is zero. The performance of this algorithm is used as a baseline for other algorithms, therefore the percentage improvement in model performance is also zero.
- naive_true: This simple algorithm flags every image. Thus, the labeling cost is 100%. The performance of this algorithm improves due to the retraining. Since no algorithm can do better than having every input labeled (barring stochasticity, as we discuss later), we use the performance of this algorithm as the 100% benchmark.
- random k%: This algorithm randomly selects k% of inputs from each batch for labeling. This budget is varied between 5% and 75%, at intervals of 5%.
- scod k%: This algorithm wraps the pre-trained model with a SCOD wrapper which computes the uncertainty for each input. From each batch, the top k% of inputs with the highest SCOD uncertainties are flagged for labeling.
- diverse k%: This algorithm uses DS-SCOD, as presented in Section 5, to select not only uncertain inputs, but also a diverse subset of inputs. For each batch, the optimization problem from Equation 14 is solved efficiently. This results in flagging up to k% of inputs, in contrast to the previous algorithms that select a fixed, i.e. exactly k%, number of inputs.

We observe from Figure 3 that the random sampling approach leads to an improvement in performance over naive_false, which aligns with our expectations since periodically retraining the model allows it to adapt to distribution shifts. We also observe that higher labeling budgets lead
to better model performance. SCOD-k performs better than random sampling, on average, for a given budget since it selects inputs for which the model is most uncertain, rather than selecting randomly, which results in higher information gain and downstream model performance. Diverse subsampling, DS-SCOD, outperforms random and SCOD-k by achieving better performance for a given budget. We observe that when the labeling budget is low, e.g., 10% to 25%, DS-SCOD expends the full budget, i.e., chooses exactly k% of inputs to label. However, due to the relaxed optimization process, when given a higher budget, e.g., 40% to 75%, DS-SCOD uses only a fraction of the budget, not exceeding 60% in Figure 3. Remarkably, DS-SCOD achieves performance comparable to naive_true while incurring only 50% of the labeling cost. DS-SCOD’s performance sometimes slightly exceeds 100% on our benchmark, i.e., makes slightly better predictions than naive_true, due to the stochastic nature of the stochastic gradient descent we use to retrain the model. Overall, DS-SCOD results in the highest average lifetime model performance, while reducing labeling cost.

Additionally, the algorithms were benchmarked on test sequences drawn only from one of the three categories, as shown in Figure 4. The labeling budgets were set to 50%. For the space-only images, all the algorithms resulted in relatively constant test loss over time. This result is unsurprising because the model was trained on space background images, and likely reached convergence on these “in-distribution” images. For both the Earth background and lens flare images, all of the labeling algorithms (naive_true, random, scod, and diverse) led to a decrease in loss over time, indicating that retraining is effective in increasing model performance when encountering OOD inputs. We observe that naive_true achieves the greatest reduction in loss by labeling every input in each batch. Further, we note that the diverse (DS-SCOD) algorithm achieves a reduction in loss most comparable to naive_true while accruing a labeling cost of less than 50% that of naive_true. Therefore, we show that DS-SCOD offers a cost-effective solution to adapting learning-based models to changing input distributions.

7. CONCLUSION

In this work, we discussed the challenges associated with data lifecycle management for learning-based components. We presented a framework for online adaptation by labeling a subset of test inputs and using the labels to retrain the model. We provided a benchmark for evaluating algorithms, that choose which subset of test inputs should be labeled, in the context of two macro-level metrics: the average model performance over the lifecycle and the cost of labeling. Lastly, we presented a novel subsampling algorithm, Diverse Subsampling using SCOD (DS-SCOD), inspired by ideas from Bayesian uncertainty quantification and Bayesian batch active learning. We showed that this algorithm, when evaluated on the benchmark, achieves performance comparable to labeling every input while incurring 50% of the labeling costs.

Interesting future directions include investigating and exploiting the temporal correlations between inputs, to determine if certain inputs are likely to reoccur in the future and should be retrained on, or if similar temporal structure between inputs allows us to choose a single representative sample. Another direction of work involves adding a delay between flagging inputs for labels and receiving labels for retraining, to better simulate the data lifecycle [26]. Another direction would be to expand the benchmark to other applications beyond satellite pose estimation, as well as different tasks and types of OOD inputs, since algorithm performance may be better suited to some tasks than others. Another promising research direction is to evaluate the effect of retraining algorithms on the improvement in model performance and design a retraining algorithm that makes maximal use of the information gain from diverse labeled inputs while avoiding catastrophic forgetting, e.g., by borrowing concepts from transfer learning and continual learning [27], [16].

ACKNOWLEDGMENTS

Somrita Banerjee was supported in part by the Stanford Graduate Fellowship (SGF). The authors were also supported by The Aerospace Corporation’s University Partnership Pro-
gram and by DARPA under the Assured Autonomy program. The NASA University Leadership initiative (grant #80NSSC20M0163) provided funds to assist the authors with their research, but this article solely reflects the opinions and conclusions of its authors and not any NASA entity. The authors would like to thank Rohan Sinha and the reviewers for their helpful comments. The authors wish to thank Matteo Zallio for help in the design of figures.

REFERENCES

[1] M. Kisantal, S. Sharma, T. H. Park, D. Izzo, M. Märtens, and S. D’Amico, “Satellite pose estimation challenge: Dataset, competition design, and results,” IEEE Transactions on Aerospace and Electronic Systems, vol. 56, no. 5, pp. 4083–4098, 2020.

[2] G. Murray, T. Bourlai, and M. Spolaor, “Mask R-CNN: Detection performance on SPEEED spacecraft with image degradation,” in IEEE Int. Conf. on Big Data, 2021.

[3] L. Wellhausen, R. Ranfil, and M. Hutter, “Safe robot navigation via multi-modal anomaly detection,” IEEE Robotics and Automation Letters, vol. 5, no. 2, pp. 1326–1333, 2020.

[4] P. Slingerland, L. Mandrake, L. Perry, G. Doran, J. Kaufman, A. Goebl, B. Bycroft, M. Feather, E. Linehan, L. Fesq, H. Ono, and R. Amini, “Adapting a trusted AI framework to space mission autonomy,” in IEEE Aerospace Conference, 2022.

[5] M. Abdar, F. Pourpanah, S. Hussain, D. Rezazadegan, L. Liu, M. Ghavamzadeh, P. Fieguth, X. Cao, A. Khosravi, U. R. Acharya, V. Makarenkov, and S. Nahavandi, “A review of uncertainty quantification in deep learning: Techniques, applications and challenges,” Information Fusion, vol. 76, pp. 243–297, 2021.

[6] J. Yang, K. Zhou, Y. Li, and Z. Liu. (2021) Generalized out-of-distribution detection: A survey. Available at https://arxiv.org/abs/2110.11334.

[7] B. Settles, “Active learning,” Synthesis Lectures on Artificial Intelligence and Machine Learning, vol. 6, no. 1, pp. 1–114, 2012.

[8] S. C. Hoi, R. Jin, J. Zhu, and M. R. Lyu, “Batch mode active learning and its application to medical image classification,” in Int. Conf. on Machine Learning, 2006.

[9] Y. Guo and D. Schuurmans, “Discriminative batch mode active learning,” in Conf. on Neural Information Processing Systems, 2007.

[10] O. Sener and S. Savarese, “Active learning for convolutional neural networks: A core-set approach,” in Int. Conf. on Learning Representations, 2018.

[11] R. Pinsler, J. Gordon, E. Nalisnick, and J. M. Hernández-Lobato, “Bayesian batch active learning as sparse subset approximation,” in Conf. on Neural Information Processing Systems, 2019.

[12] N. Roy and A. McCallum, “Toward optimal active learning through sampling estimation of error reduction,” in Int. Conf. on Machine Learning, 2001.

[13] A. Freytag, E. Rodner, and J. Denzler, “Selecting influential examples: Active learning with expected model output changes,” in European Conf. on Computer Vision, 2014.

[14] Y. Yang and M. Loog, “Active learning using uncertainty information,” in IEEE Int. Conf. on Pattern Recognition, 2016.

[15] P. W. Koh, S. Sagawa, H. Marklund, S. M. Xie, M. Zhang, A. Balsubramani, W. Hu, M. Yasunaga, R. L. Phillips, I. Gao, T. Lee, E. David, I. Stavness, W. Guo, B. A. Earnshaw, I. S. Haque, S. Beery, J. Leskovec, A. Kundaje, E. Pierson, S. Levine, C. Finn, and P. Liang, “WILDS: A benchmark of in-the-wild distribution shifts,” in Int. Conf. on Machine Learning, 2021.

[16] G. I. Parisi, R. Kemker, J. L. Part, C. Kanan, and S. Wermter, “Continual lifelong learning with neural networks: A review,” Neural Networks, vol. 113, pp. 54–71, 2019.

[17] Z. Lin, J. Shi, D. Pathak, and D. Ramanan, “The CLEAR benchmark: Continual learning on real-world imagery,” in Conf. on Neural Information Processing Systems - Datasets and Benchmarks Track, 2021.

[18] Y.-C. Hsu, Y.-C. Liu, and Z. Kira, “Re-evaluating continual learning scenarios: A categorization and case for strong baselines,” in Conf. on Neural Information Processing Systems, 2018.

[19] H. Weiher, D. J. Mabry, and A. C. Uitter, “Slingshot: In-space modularity test platform,” in AIAA Aerospace Sciences Meeting, 2022.

[20] A. Sharma, N. Azizan, and M. Pavone, “Sketching curvature for efficient out-of-distribution detection for deep neural networks,” in Proc. Conf. on Uncertainty in Artificial Intelligence, 2021.

[21] A. Poghosyan and A. Golkar, “CubeSat evolution: Analyzing CubeSat capabilities for conducting science missions,” Progress in Aerospace Sciences, vol. 88, pp. 59–83, 2017.

[22] G. Doran, A. Daigavane, and K. Wagstaff, “Resource consumption and radiation tolerance assessment for data analysis algorithms onboard spacecraft,” IEEE Transactions on Aerospace and Electronic Systems, 2022.

[23] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” Proc. of the IEEE, vol. 86, no. 11, pp. 2278–2324, 1998.

[24] H. Xiao, K. Rasul, and R. Vollgraf. (2017) Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms. Available at https://arxiv.org/abs/1708.07747.

[25] B. Chen, J. Cao, A. Parra, and T.-J. Chin, “Satellite pose estimation with deep landmark regression and non-linear pose refinement,” in IEEE Int. Conf. on Computer Vision, 2019.

[26] M. Grzenda, H. M. Gomez, and A. Bifet, “Delayed labelling evaluation for data streams,” Data Mining and Knowledge Discovery, vol. 34, no. 5, pp. 1237–1266, 2020.

[27] K. Weiss, T. M. Khoshgoftaar, and D. Wang, “A survey of transfer learning,” Journal of Big data, vol. 3, no. 1, pp. 1–40, 2016.
Biography

Somrita Banerjee is a Ph.D. candidate in the Autonomous Systems Lab at Stanford University. She received her B.S. in Mechanical and Aerospace Engineering from Cornell University in 2017. Her research interests lie at the intersection of trajectory optimization, machine learning, and control algorithms, specifically towards development of the next generation of space robotics.

Apoorva Sharma is a research scientist at NVIDIA, in the Autonomous Vehicles Group. He obtained his Ph.D. in Aeronautics & Astronautics at Stanford University in the Autonomous Systems Lab in 2022, where his research focused on quantifying, representing and utilizing uncertainty in the learning-enabled autonomy stack. He received a B.S. in Engineering at Harvey Mudd College in 2016. Apoorva's research interests focus on quantifying uncertainty in modern deep learning architectures and using these estimates to ensure the safety and robustness of ML systems.

Edward Schmerling is a research scientist with the Autonomous Systems Laboratory at Stanford University, where he received his Ph.D in 2019 in Computational & Mathematical Engineering. His research interests span the modern robotics stack, with a particular focus on the development of data-driven methodologies for system modeling that may be leveraged to provide quantifiable safety and performance in the face of uncertainty. Prior to returning to Stanford, Ed worked as a research engineer with Waymo Research towards enabling capable and trustworthy autonomous vehicles.

Max Spoloar is a Senior Engineering Specialist in the Vehicle Engineering and Autonomy Department at The Aerospace Corporation. Spoloar’s work focuses on artificial intelligence and advanced autonomy for space systems, verification and validation of cognitive adaptive systems, and machine learning for Cyber applications. Previously, he worked as a Senior Software & Systems Engineer at the NASA IV&V Facility, at the National Radio Astronomy Observatory, and for the NASA Airborne Science Program at UCLA. Spoloar has a background in applied physics with a Ph.D. in Astrophysics.

Michael Nemerouf is a Department Director in the Communications Software Implementation Department at The Aerospace Corporation. Mike’s group focuses on applying artificial intelligence and advanced signal processing for communications and RF data exploitation applications. Mike is also a prominent voice at the Aerospace Corporation in shaping and executing Aerospace’s Corporate AI strategy. Prior to working at The Aerospace Corporation, Mike spent 10 years as an Army Intelligence specialist then went on to get his BS in Mathematics and MS in Computational and Data Science.

Marco Pavone is an Associate Professor of Aeronautics and Astronautics at Stanford University, where he is the Director of the Autonomous Systems Laboratory. Before joining Stanford, he was a Research Technologist within the Robotics Section at the NASA Jet Propulsion Laboratory. He received a Ph.D. degree in Aeronautics and Astronautics from the Massachusetts Institute of Technology in 2010. His main research interests are in the development of methodologies for the analysis, design, and control of autonomous systems, with an emphasis on self-driving cars, autonomous aerospace vehicles, and future mobility systems. He is a recipient of a number of awards, including a Presidential Early Career Award for Scientists and Engineers, an ONR YIP Award, an NSF CAREER Award, and a NASA Early Career Faculty Award. He was identified by the American Society for Engineering Education (ASEE) as one of America’s 20 most highly promising investigators under the age of 40.