

BaCOUn: Bayesian Classifiers with Out-of-Distribution Uncertainty

Théo Guénais^{* 1} Dimitris Vamvourellis^{* 1} Yaniv Yacoby¹ Finale Doshi-Velez¹ Weiwei Pan¹

Abstract

Traditional training of deep classifiers yields overconfident models that are not reliable under dataset shift. We propose a Bayesian framework to obtain reliable uncertainty estimates for deep classifiers. Our approach consists of a plug-in “generator” used to augment the data with an additional class of points that lie on the boundary of the training data, followed by Bayesian inference on top of features that are trained to distinguish these “out-of-distribution” points.

1. Introduction

In high-risk domains, classifiers must provide predictive uncertainty, so that decision making can be deferred to human expertise when the model is in doubt. For humans to make effective decisions under uncertainty, a classifier must furthermore decompose uncertainty into: epistemic uncertainty, uncertainty that can be reduced with more observations; and aleatoric uncertainty, uncertainty that cannot be reduced due to inherent noise in the system (Gal, 2016). For a classifier, epistemic uncertainty can be further decomposed into out-of-distribution (OOD) uncertainty arising in regions far away from the high-mass regions, and model uncertainty referring to uncertainty over the classification boundary in the high-mass regions of the data space (Malinin & Gales, 2018). As such, OOD uncertainty depends on the expressiveness of the functions in the model class. The higher the capacity of the model class, the more the models in this class will extrapolate differently in data-scarce regions resulting in higher OOD uncertainty.

Gaussian Processes (GPs) have long served as standard method for providing both reliable and accurate estimates of predictive uncertainty in classification. However, due to their inability to scale with the number of observations, Bayesian Neural Networks (BNNs) have been proposed as a

^{*}Equal contribution ¹John A. Paulson School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, USA. Correspondence to: Théo Guénais <tguenais@fas.harvard.edu>, Dimitris Vamvourellis <dvamvourellis@g.harvard.edu>.

Presented at the ICML 2020 Workshop on Uncertainty and Robustness in Deep Learning. Copyright 2020 by the author(s).

scalable alternative (Neal, 2012; MacKay, 1992). BNNs provide a way to capture model uncertainty by placing a prior distribution over network weights. Although more scalable than GPs, inference for large BNNs remains challenging. For this reason, Neural Linear Models (NLM) are becoming a popular BNN replacement (Pinsler et al., 2019; Riquelme et al., 2018). In a NLM, we place priors only on the last layer of network weights and we learn point estimates for the remaining weights. Inference for the last weight layer can then be performed analytically.

Unfortunately, both BNNs and NLMs struggle with modeling OOD uncertainty. While BNNs are equivalent to GPs in the limit of infinite width (Neal, 1996), recent work shows that, unlike GPs, the epistemic uncertainty of finite-sized BNN classifiers does not increase in data-poor regions (Vernekar et al., 2019b). In this work, we show that NLM likewise struggles with providing high epistemic uncertainty for OOD data, irrespective of the architecture chosen.

Our contributions in this paper are twofold. We first explain why, using pedagogical examples NLM classifiers are unable to model OOD uncertainty. Specifically, we show that in order to capture OOD uncertainty, the posteriors of these models must include decision boundaries that properly bound the data. However, the training procedure of NLM does not encourage learning such boundaries. Next, we propose a novel scalable framework for training NLM classifiers that provides reliable model uncertainty, OOD uncertainty and aleatoric uncertainty.

On synthetic datasets we show that we attain uncertainty estimates comparable with that of GPs while baseline models underestimate OOD uncertainty. On real datasets, we show that our training framework attains higher AUC on observed data and provides reliable epistemic uncertainty estimates allowing for distinguishing in-distribution and OOD test data.

Related Work Several non-Bayesian methods have been proposed to model OOD uncertainty. They fall into two categories. The first constrains a classifier to output high-entropy predictions on a priori OOD examples (Liang et al., 2017; Lee et al., 2017; Srirangan & Srivastava, 2018), and the second trains a classifier on the original classes, plus an additional class of OOD examples (Vernekar et al., 2019b;a). However, these methods do not provide uncertainty decomposition. In the first approach, points lying on the boundary

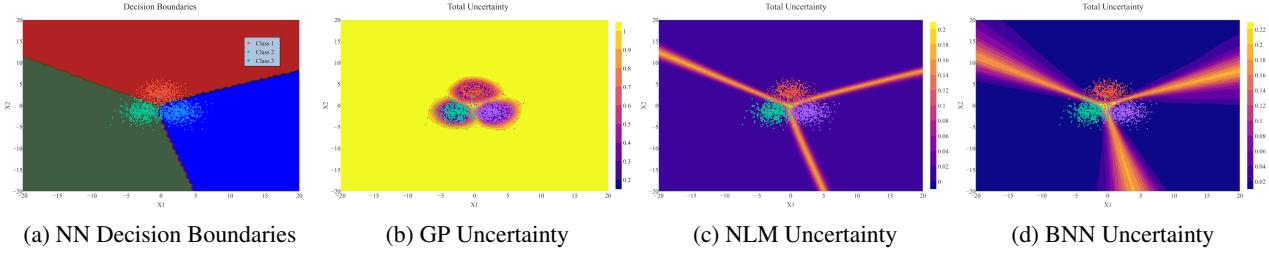


Figure 1. Neural network models cannot capture OOD uncertainty. The above shows the decision boundaries of a Neural Net (a) along with entropy of the categorical distribution predicted by different methods: GP (b), NLM (c), BNN (d). GPs make high-entropy (uncertain) predictions far from the training data while other models significantly underestimate OOD uncertainty.

between classes (which should have high aleatoric uncertainty) and points lying on the boundary of the data (which should have high epistemic uncertainty) both have high predictive entropy, but the different sources of the uncertainty (aleatoric and OOD) cannot be disentangled. Both approaches do not account for uncertainty over model parameters which may lead a classifier to make overconfident predictions for OOD points.

Background Let $\mathcal{D} = \{(x_1, y_1), \dots, (x_N, y_N)\}$ be a dataset of N observations. Each input $x_n \in \mathbb{R}^D$ is a D -dimensional vector and each output y_n is a label corresponding to one of K classes.

A Neural Linear Model classifier assumes the following generative process:

$$y|x \sim \text{Cat}(\text{softmax}(W^\top \phi_\theta(x))), \quad W \sim p(W), \quad (1)$$

where $\phi_\theta(x)$ is the output of a neural network with L number of output nodes and parameter θ , augmented with a 1 for the bias term. We call ϕ_θ the feature map since it extracts meaningful features from the data for the Bayesian linear classifier. First, the feature map ϕ_θ is trained to maximize the observed data log-likelihood:

$$\theta^* = \underset{\theta, W}{\operatorname{argmax}} \log p(y_1, \dots, y_N | x_1, \dots, x_N; \theta, W). \quad (2)$$

Then, fixing ϕ_{θ^*} , we infer the posterior $p(W|\mathcal{D}, \theta^*)$ for the NLM classifier by either Hamiltonian Monte Carlo (Neal et al., 2011) or mean-field Gaussian variational inference (Ranganath et al., 2014). At test time, we make predictions by computing the posterior predictive distribution:

$$p(y^*|x^*, \mathcal{D}) = \int p(y^*|x^*, W)p(W|\mathcal{D}, \theta^*)dW. \quad (3)$$

2. Analysis of the OOD Uncertainty of Neural Linear Model Classifiers

In this section, we show that in order for posterior predictive of NLMs to capture OOD uncertainty, these posteriors

must include decision boundaries that bound high likelihood data regions. However, the training objective for NLM classifiers does not encourage learning these boundaries.

Neural Linear Model Classifiers are unable to model OOD uncertainty.

In Figure 1, we visualize the entropy of the posterior predictive mean of various classifiers over the input space. While the GP classifier makes low-entropy (i.e. confident) predictions for points close to the observed data and high-entropy predictions for points far away, NLM classifiers make overconfident low-entropy predictions far from the observed data. The same failure can be observed in other models that provide predictive uncertainty such as full BNN trained with Black-Box Variational Inference (BBVI) (Ranganath et al., 2014). The OOD uncertainty of the GP classifier comes from the fact that a significant number of decision boundaries in the GP posterior properly bound each class in the data and hence the predicted labels probabilities for points far from the data have high variance. So why doesn't the posterior for NLM classifiers include such decision boundaries?

Neural Linear Model underestimates OOD uncertainty because training does not encourage learning decision boundaries that bound the data. The training objective for the NLM model encourages ϕ_θ to extract features that are predictive of y . But a ϕ_θ that is good for classification (e.g. one that expresses only linear boundaries) is not necessarily capable of expressing a decision boundary $W^\top \phi_\theta(x)$ that bounds the data. Hence, for these ϕ_θ 's, the resulting NLM classifier will underestimate OOD uncertainty.

In a simple experiment, we demonstrate that the features learned by an NLM classifier is good for classification but is not useful for OOD detection. Consider a dataset $\{(x_n, y_n, b_n)\}_{n=1}^N$, where x_n is the input, y_n is the label, and b_n is a binary indicator signaling whether the data-point is OOD. We train an NLM classifier to predict $y|x$ and ensure that the AUC is high. We then train a Naive Bayes classifier to predict b given the features learned by ϕ_{θ^*} .

In Appendix E Figure 5, we see that the features learned by ϕ_θ for classification are unable to predict the label b (i.e. if a point is OOD). Furthermore, the posterior of the NLM model underestimates OOD uncertainty.

In contrast, we train a neural network classifier to jointly predict y, b given x . We then extract the learned features, given by output of the last hidden layer $\phi_{\text{latent}}(x)$, to predict b . In this case, since the features are explicitly trained to predict the OOD points, we can accurately predict b with a Naive Bayes classifier fitted on these features. Appendix E Figure 5 shows that the posterior of this model includes decision boundaries that bound the data and thus the posterior uncertainty is higher for OOD points. The intuition behind this experiment forms the core of our inference framework in Section 3.

We emphasize that we show a problem with the training objective of NLMs and not an issue with the architecture of the model. In fact, we show later that, given identical NLM architectures, our training framework is able to capture OOD uncertainty while traditional training cannot.

3. BaCOUn: Bayesian Classifier with OOD Uncertainty

To ensure that the features of NLMs can be used to build decision boundaries that separate data from OOD points, we propose BaCOUn, a general training framework for NLMs:

1. Generate OOD samples on the boundary of the data.
2. Train a deterministic classifier to distinguish between the original K classes and additionally between the generated OOD samples.
3. Fix the features, $\phi_{\theta^*}(x)$, learned by the deterministic classifier, and fit a Bayesian logistic regression model (in Equation 1) on these features.

By explicitly training a classifier on the boundary samples, we show later that the learned features will be able to express decision boundaries that bound the data, and hence the posteriors of BaCOUn will capture OOD uncertainty.

Our framework is general, one can plug-in any method for each step. Here, we propose one instantiation of this framework that performs well in practice. For the first step – generating OOD samples – we present a novel OOD sampler, described below. For the second step, we train a deep neural network with a softmax output activation, and for the final step, we use Hamiltonian Monte-Carlo (HMC) as well as mean-field BBVI on more taxing experiments.

Novel Method for Generating OOD Boundary Points

We propose a novel method to generate samples from the boundary of a given data distribution based on Normalizing Flows (Rezende & Mohamed, 2015; Dinh et al., 2016b;

Huang et al., 2018). In our method, we train a Real-NVP (Dinh et al., 2016a) to maximize the log likelihood of the data x . We then sample points on the boundary of the latent space of the learned flow, mapping the samples back into the data space. Details in Appendix D.

4. Experiments

Baselines. In our experiments, we compare BaCOUn with NLM, BNN, and MC-Dropout on both synthetic and real datasets. See Appendix B for details on each method.

Evaluation. We evaluate the fit of the learned models using AUC. We quantitatively evaluate epistemic and aleatoric uncertainties using in-distribution and OOD points. On image data we additionally provide a qualitative evaluation. We consider a model successful if it is able to have high AUC while being uncertain about OOD points. We use the uncertainty decomposition used by (Depeweg et al., 2017), shown in Appendix C Equation 4.

Datasets We conduct experiments on two synthetic datasets: the Gaussian Mixture Model dataset and the Moons dataset (Appendix A). We also conducted experiments on two real datasets: *Wine Quality* (Cortez et al., 1998) and MNIST (LeCun & Cortes, 2010). On *Wine Quality*, we train our classifier on only two of the K classes and used the remaining classes as OOD examples at test-time together with artificially created OOD points (details in Appendix A.2). On MNIST, we used examples from other datasets (CIFAR (Krizhevsky et al.), USPS (Hull, 1994), EMNIST (Cohen et al., 2017)), as well as boundary points created from the normalizing flow) as example OOD points for evaluation. See Appendix F and G for details.

5. Results

BaCOUn can capture OOD uncertainty whereas baselines struggle. Figure 2a shows the decision boundaries learned by the $K + 1$ -class classifier trained in Step 2 of BaCOUn. The classifier labels points on the data boundary as OOD and this labeling generalizes to regions far from the data. The final hidden layer of this classifier encodes these decision boundaries. Consequently, NLM trained with BaCOUn expresses higher uncertainty far from the training data, recovering the optimal GP behaviour. Appendix G Figure 10 shows that BaCOUn captures OOD uncertainties even in more complex data settings like the Moons dataset. Appendix G Figure 11 and Figure 12 show that baselines significantly underestimate OOD uncertainty.

BaCOUn provides simple decomposition of total uncertainty. Using BaCOUn, we are able to reliably decompose the total predictive uncertainty into: epistemic uncertainty (Figure 2d), arising due to lack of knowledge in a region of

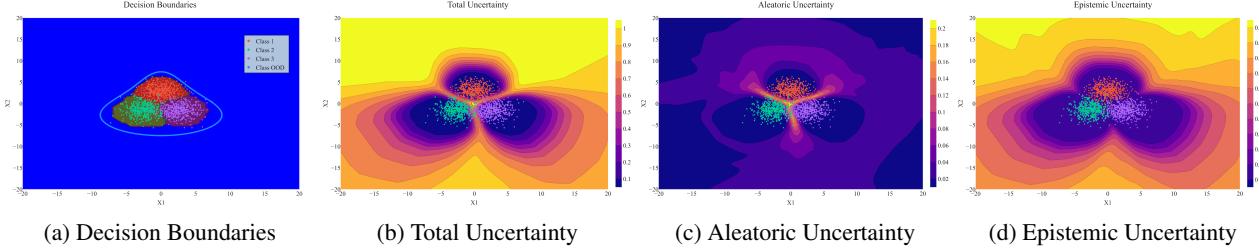


Figure 2. Uncertainty decomposition provided by BaCOUn along with the decision boundaries learned in Step 2 of BaCOUn’s training procedure (a). BaCOUn captures OOD uncertainty and decomposes uncertainty accurately, giving high aleatoric uncertainty in regions of class overlap and high epistemic uncertainty in regions far from the observed data.

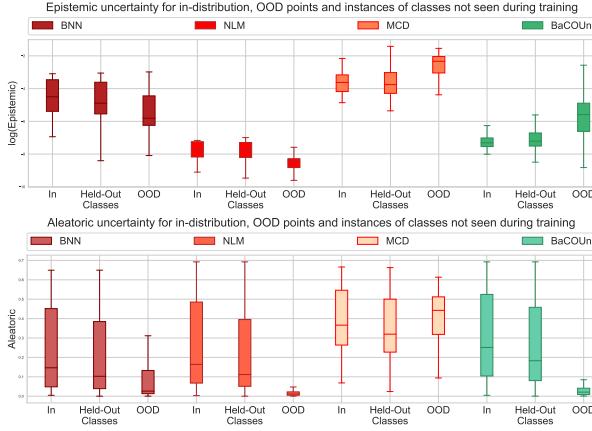


Figure 3. Epistemic and aleatoric uncertainty of BNN, NLM, MC-Dropout and BaCOUn for in-distribution points, instances of held-out classes and OOD points on *Wine Quality* dataset. BaCOUn provides reliable OOD uncertainty while maintaining accurate aleatoric uncertainty. Specifically, epistemic uncertainty is maximized while aleatoric uncertainty is minimized for OOD points.

the feature space, and aleatoric uncertainty (2c), arising due to class overlap. To our knowledge, there is no easy way to decompose GP predictive uncertainty.

BaCOUn provides interpretable uncertainty in real data settings. Using *Wine Quality*, we show that BaCOUn provides uncertainties on real datasets that align with human intuition. Figure 3 shows that BaCOUn returns higher epistemic uncertainty for instances of held-out classes (classes 3,4,8,9) compared to the uncertainty for in-distribution points (class 5 or 7). As expected, BaCOUn gives even higher epistemic uncertainty estimates for OOD points. Only MC-Dropout achieves comparable performance in terms of detecting OOD points using epistemic uncertainty; however it fails to provide interpretable aleatoric uncertainty, since it is maximized for OOD points where classes do not overlap. In contrast, BaCOUn provides aleatoric uncertainty that also aligns with human intuition: points from held-out classes have comparable aleatoric uncertainty to in-distribution samples, however aleatoric uncertainty is much lower for OOD points, since they are sampled from

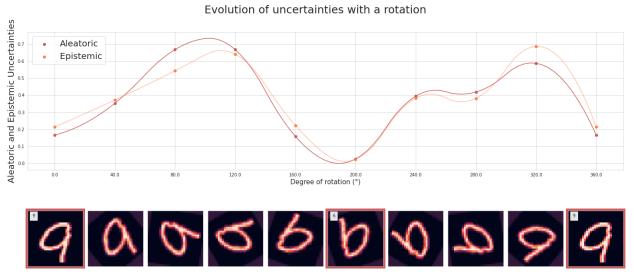


Figure 4. Aleatoric and epistemic uncertainty of rotated MNIST images. When the rotated image looks like a known digit, both types of uncertainties decrease; both uncertainties increase when the rotated image does not look like a digit.

regions far from where the observed data overlap.

In Appendix F, Figure 7, we show that BaCOUn’s uncertainty estimates for OOD data sampled from EMNIST, CIFAR and USPS align well with human intuition: BaCOUn gives high epistemic uncertainty for CIFAR samples (which do not contain digit-like images), whereas EMNIST samples (which has some data overlap with MNIST) are given the highest aleatoric uncertainty. In comparison, baselines either provide epistemic uncertainties that do not align with intuition or aleatoric uncertainties that are hard to interpret.

In a qualitative experiment, we track changes in BaCOUn’s resulting uncertainties as we rotate an image (Figure 4). We see that, as expected, epistemic uncertainty is low when the rotated image looks like a digit and is high when it does not. Aleatoric uncertainty is high when a rotated image can be ambiguously classified and low when it cannot. In Appendix G, we describe additional similar experiments.

6. Conclusion

In this paper, we show that BNNs, NLMs and MC-Dropout underestimate OOD uncertainty in classification tasks. We propose a novel Bayesian classifier, BaCOUn, which explicitly encourages posterior to capture OOD uncertainty. On synthetic and real datasets with complex patterns and

sources of uncertainty, we demonstrate the ability of epistemic uncertainty produced by BaCOUn to distinguish in-distribution and OOD points. We further show that the uncertainty decomposition provided by BaCOUn aligns with human intuition on image datasets.

7. Acknowledgments

DV, TG, and WP are supported by the Harvard Institute of Applied Computational Sciences. YY acknowledges support from NIH 5T32LM012411-04 and from IBM Research.

References

- Bingham, E., Chen, J. P., Jankowiak, M., Obermeyer, F., Pradhan, N., Karaletsos, T., Singh, R., Szerlip, P., Horsfall, P., and Goodman, N. D. Pyro: Deep universal probabilistic programming. *The Journal of Machine Learning Research*, 20(1):973–978, 2019.
- Cohen, G., Afshar, S., Tapson, J., and van Schaik, A. Emnist: an extension of mnist to handwritten letters, 2017.
- Cortez, P., Cerdeira, A., Almeida, F., Matos, T., and Reis, J. Modeling wine preferences by data mining from physicochemical properties. *Decision Support Systems*, 47(4): 547–553, 1998.
- Depeweg, S., Hernández-Lobato, J. M., Doshi-Velez, F., and Udluft, S. Decomposition of uncertainty for active learning and reliable reinforcement learning in stochastic systems. *stat*, 1050:11, 2017.
- Dinh, L., Sohl-Dickstein, J., and Bengio, S. Density estimation using real nvp. *arXiv preprint arXiv:1605.08803*, 2016a.
- Dinh, L., Sohl-Dickstein, J., and Bengio, S. Density estimation using real nvp. *arXiv preprint arXiv:1605.08803*, 2016b.
- Gal, Y. Uncertainty in deep learning. *University of Cambridge*, 1:3, 2016.
- Hoffman, M. D. and Gelman, A. The no-u-turn sampler: adaptively setting path lengths in hamiltonian monte carlo. *J. Mach. Learn. Res.*, 15(1):1593–1623, 2014.
- Huang, C.-W., Krueger, D., Lacoste, A., and Courville, A. Neural autoregressive flows. *arXiv preprint arXiv:1804.00779*, 2018.
- Hull, J. J. A database for handwritten text recognition research. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 16(5):550–554, 1994.
- Ioffe, S. and Szegedy, C. Batch normalization: Accelerating deep network training by reducing internal covariate shift. *arXiv preprint arXiv:1502.03167*, 2015.
- Kingma, D. P. and Ba, J. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.
- Kingma, D. P. and Welling, M. Auto-encoding variational bayes. *arXiv preprint arXiv:1312.6114*, 2013.

- Krizhevsky, A., Nair, V., and Hinton, G. Cifar-10 (canadian institute for advanced research). URL <http://www.cs.toronto.edu/~kriz/cifar.html>.
- LeCun, Y. and Cortes, C. MNIST handwritten digit database. 2010. URL <http://yann.lecun.com/exdb/mnist/>.
- Lee, K., Lee, H., Lee, K., and Shin, J. Training confidence-calibrated classifiers for detecting out-of-distribution samples. *arXiv preprint arXiv:1711.09325*, 2017.
- Liang, S., Li, Y., and Srikant, R. Enhancing the reliability of out-of-distribution image detection in neural networks, 2017.
- MacKay, D. J. A practical bayesian framework for backpropagation networks. *Neural computation*, 4(3):448–472, 1992.
- Malinin, A. and Gales, M. Predictive uncertainty estimation via prior networks. In *Advances in Neural Information Processing Systems*, pp. 7047–7058, 2018.
- Mitra, N. J., Kokkinos, I., Guerrero, P., Thuerey, N., Kim, V., and Guibas, L. Creativeai: Deep learning for graphics. In *SIGGRAPH 2019 Courses*, Siggraph 2019, 2019.
- Neal, R. M. Priors for infinite networks. In *Bayesian Learning for Neural Networks*, pp. 29–53. Springer, 1996.
- Neal, R. M. *Bayesian learning for neural networks*, volume 118. Springer Science & Business Media, 2012.
- Neal, R. M. et al. Mcmc using hamiltonian dynamics. *Handbook of markov chain monte carlo*, 2(11):2, 2011.
- Paszke, A., Gross, S., Massa, F., Lerer, A., Bradbury, J., Chanan, G., Killeen, T., Lin, Z., Gimelshein, N., Antiga, L., Desmaison, A., Kopf, A., Yang, E., DeVito, Z., Raison, M., Tejani, A., Chilamkurthy, S., Steiner, B., Fang, L., Bai, J., and Chintala, S. Pytorch: An imperative style, high-performance deep learning library. In Wallach, H., Larochelle, H., Beygelzimer, A., d Alché-Buc, F., Fox, E., and Garnett, R. (eds.), *Advances in Neural Information Processing Systems 32*, pp. 8024–8035. Curran Associates, Inc., 2019.
- Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., and Duchesnay, E. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12:2825–2830, 2011.
- Pinsler, R., Gordon, J., Nalisnick, E., and Hernández-Lobato, J. M. Bayesian batch active learning as sparse subset approximation. In *Advances in Neural Information Processing Systems 32*, pp. 6359–6370, 2019.
- Ranganath, R., Gerrish, S., and Blei, D. M. Black box variational inference. In *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Statistics*, 2014.
- Rezende, D. J. and Mohamed, S. Variational inference with normalizing flows. *arXiv preprint arXiv:1505.05770*, 2015.
- Riquelme, C., Tucker, G., and Snoek, J. Deep bayesian bandits showdown: An empirical comparison of bayesian deep networks for thompson sampling. In *International Conference on Learning Representations (ICLR)*, 2018.
- Ryzhikov, A., Borisjak, M., Ustyuzhanin, A., and Derkach, D. Normalizing flows for deep anomaly detection. *arXiv preprint arXiv:1912.09323*, 2019.
- Schlegl, T., Seeböck, P., Waldstein, S. M., Schmidt-Erfurth, U., and Langs, G. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. In *International conference on information processing in medical imaging*, pp. 146–157. Springer, 2017.
- Sricharan, K. and Srivastava, A. Building robust classifiers through generation of confident out of distribution examples. *arXiv preprint arXiv:1812.00239*, 2018.
- Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., and Salakhutdinov, R. Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, 15(56):1929–1958, 2014. URL <http://jmlr.org/papers/v15/srivastava14a.html>.
- Vernekar, S., Gaurav, A., Abdelzad, V., Denouden, T., Salay, R., and Czarnecki, K. Out-of-distribution detection in classifiers via generation. *arXiv preprint arXiv:1910.04241*, 2019a.
- Vernekar, S., Gaurav, A., Denouden, T., Phan, B., Abdelzad, V., Salay, R., and Czarnecki, K. Analysis of confident-classifiers for out-of-distribution detection. *arXiv preprint arXiv:1904.12220*, 2019b.

A. Data

A.1. Synthetic Datasets

Gaussian Mixture We generate points from a Gaussian Mixture Model with 3 components corresponding to 3 different classes. The three classes are distributed with means $(0, 2)$, $(-\sqrt{3}, -1)$ and $(\sqrt{3}, -1)$ respectively, and identical isotropic covariance matrices $\sigma \cdot \mathbb{I}_{\mathbb{R}^2}$. We set $\sigma = 3$ in order to obtain class overlap. We generate 500 points per cluster, for a total of 1500 training points.

We generate 2000 OOD points for BaCOUn by sampling from a circle of radius 3 bounding the data distribution in latent space, and then mapping the points into input space using BaCOUn’s Normalizing Flow. See [D](#) for more details about the generation of OOD points.

Uncertainties of BaCOUn and baseline methods are presented in [F](#).

Moon-shaped data We use `sklearn` ([Pedregosa et al., 2011](#)) and its built-in “two-moons” data generator to generate $K = 2$ classes, with 2000 points per class (for a total of 4000 data points), using a noise parameter of 0.05. For this dataset, we generate 3000 OOD points. Uncertainties for various models are presented in [F](#) and [G](#).

A.2. Real Datasets

UCI Wine Quality This dataset ([Cortez et al., 1998](#)) contains instances of wines with ratings ranging from 3 to 9. All features are standardized to have zero mean and unit standard deviation.

We use class 5, 7 during training and we test the model’s predictions and corresponding uncertainties on held-out instances of class 5, 7, as well as on instances of held-out classes 3,4,8,9 and artificially created OOD points.

OOD points are created by inflating the first dimension with Gaussian noise centered at 10 with unit variance (i.e. the first dimension is larger by 10 standard deviations on average compared to in-distribution points). Boundary points used to train BaCOUn were generated by mapping shells of radii 5 and 5.1 in latent space into input space (see [D](#) for details).

Model uncertainties are presented in [F](#).

Images We use instances from MNIST ([LeCun & Cortes, 2010](#)) as in-distribution points and points from USPS ([Hull, 1994](#)), EMNIST ([Cohen et al., 2017](#)), CIFAR ([Krizhevsky et al.](#)) as OOD instances. All datasets are normalized using the training set’s statistics, converted to grayscale and the dimensions reduced to 28×28 when necessary.

USPS consists of digits, similar to MNIST, however the images present patterns different from MNIST. Therefore, we

intuitively expect that epistemic and aleatoric uncertainties should be relatively high for USPS instances compared to in-distribution MNIST digits. EMNIST consists of some digit images which are also part of MNIST, but also includes other categories such as hand-written characters. On instances from EMNIST, we similarly expect both epistemic and aleatoric uncertainties to be relatively high.

CIFAR on the other hand is made of images which are significantly different from the training data. Intuitively, on CIFAR instances, a well-calibrated model would output higher epistemic uncertainty and lower aleatoric uncertainty than for the rest of the image datasets.

Also, a model with well-calibrated uncertainty should assign higher epistemic uncertainty to points on the data boundary than to in-distribution points. The boundaries used to train BaCOUn are generated by training one normalizing flow for each class in the training data (id est 10 normalizing flows) and mapping a shell of radii 3 and 3.1 in the latent space into input space for each flow (see [D](#) for details). In total, we generate 10,000 OOD samples.

Model uncertainties are presented in [F](#) and [G](#).

Selecting the number of OOD points The number of OOD points is selected with a simple heuristic: the OOD class should be (approximately) balanced with the K initial classes in order to avoid issues related to class imbalance. Depending on the number of classes in the data, we may want to generate more OOD samples than the number of samples in each class (small K) in order to properly bound the points in that class. As the number of classes K grows, we ensure that the OOD samples do not over-dominate the dataset. In addition, potentially negative outcomes caused by the inclusion of a new class in the dataset (e.g degraded training accuracy) is mitigated when we fit a Bayesian classifier that accounts for the uncertainty over the position of the generated boundaries.

B. Implementation details

We implement deterministic Neural Networks using PyTorch ([Paszke et al., 2019](#)). Bayesian layers are implemented using Pyro ([Bingham et al., 2019](#)).

GMM, Moons We use similar architectures for experiments on both synthetic datasets. **BaCOUn** and **NLM** are based on a feed-forward network with 4 hidden layers of dimensions 64, 64, 64, 1024. We use a batch size of 256, a L2 penalty term of 1 and a dropout rate ([Srivastava et al., 2014](#)) of 0.1.

The deterministic network is trained for 500 epochs, using Adam optimizer ([Kingma & Ba, 2014](#)) and a learning rate of 10^{-3} .

Inference for the Bayesian logistic regression built on top of the features of the deterministic network is performed using Hamiltonian Monte-Carlo (HMC) (Neal et al., 2011), in particular, we use the No-U-Turn Sampler (NUTS) (Hoffman & Gelman, 2014). We run NUTS for 1000 iterations, with 100 burn-in steps.

MC-Dropout and the **BNN** baselines are based on a network of 4 hidden layers with dimension 512. A dropout rate of 0.2 is used for MC-Dropout, with batch sizes, number of epochs, and learning rates the same as for the deterministic network. Inference for BNN is performed using BBVI (Ranganath et al., 2014), with 10,000 total iterations, and a learning rate of 10^{-2} . LeakyRelu activation was chosen (for all networks). In all cases, 200 samples from the posterior distribution were used.

We run each baseline with the following architectures:

- 2 hidden layers of size 64
- 4 hidden layers of size 64
- 4 hidden layers with sizes 64, 64, 64, 1024
- 4 hidden layers with size 512

The best architecture is selected for testing.

The Real-NVP normalizing flow used to generate data boundaries consists of 5 blocks with 64 hidden neurons each. Batch Normalization (Ioffe & Szegedy, 2015) is used to stabilize the training. We use a batch size of 256, L2 penalty term of 4 (GMM) and 5 (Moons) and 200 (GMM) or 100 (Moons) epochs. The learning rate for training the flows is set to 10^{-3} . Hyperparameters are selected using grid search.

We note that for a fair comparison we allow a larger parameters budgets for **MC-Dropout** and **BNN** trained with BBVI, since the speed of the inference for these models allows for larger architectures. In realistic settings, HMC sampling for BNNs is not efficient. On the other hand, for **BaCOUn** and **NLM**, exact inference is feasible using HMC.

It is worth noting that the expressiveness of BaCOUn framework depends on the width of the last layer of the base neural network. This is expected since the final layer of the neural network forms an information bottleneck making it harder to encode the boundaries of K+1 classes with a small number of nodes.

UCI Wine Quality All models were trained using 1238 points of class 5 and 1238 of class 7. For BaCOUn training, we additionally generated 1400 boundary OOD points.

The base for all models is a neural network with 4 hidden layers of 64 nodes each. The deterministic network is trained

for 500 epochs with Adam optimizer and a learning rate of 10^{-4} and L2 penalty equal to 1. For **MC-Dropout**, we use a dropout rate of 0.4 and calculated posterior predictive mean over 500 samples.

We train **BNN** with BBVI (Ranganath et al., 2014) for 2000 iterations and calculated posterior predictive mean over 500 samples. The inference for Bayesian layer in **NLM** and **BaCOUn** is performed with NUTS for 1000 steps with a burn-in of 100 steps. The posterior predictive mean is computed over 500 samples from the Markov chain.

To generate boundary points for BaCOUn framework, we use one Real-NVP of 5 blocks with 64 neurons per class, trained for 100 epochs, with batch size equal to 256, learning rate equal to 10^{-3} and L2 penalty equal to 1.

Image Datasets All methods except for BNN, use a neural network with 2 Convolutional layers (kernels of size 5), Max Pooling followed by either one or two hidden layers of size 50, 1024 (**BaCOUn**) or 50 (**NLM**, **MC-Dropout**). As a matter of fact, an additional layer does not yield better results for NLM and MC-Dropout.

We use a batch size of 64, L2 penalty term of 1 and a dropout rate of 0.5. The deterministic network is trained for 15 epochs, using Adam and a learning rate of 10^{-3} . Inference for the Bayesian layer in **NLM** and **BaCOUn** is performed using BBVI (for all methods), with a learning rate of 10^{-2} and for 30,000 iterations.

One Normalizing Flow per class in the training data is used to generate boundary points. Each flow had the same architecture, that is 5 blocks with 64 hidden neurons each, trained for 250 epochs, with a batch size of 512, and a L2 penalty of 2.

C. Uncertainty measures

The output probabilities of a K -classes classifier can be considered as the parameters of a Categorical distribution. Thus, entropy of the predicted Categorical distribution is a measure of the total uncertainty in predictions of a traditional non-Bayesian classifier. However, given an ensemble of models (such as the models obtained by sampling from the posterior distribution over the parameters of a BNN), the entropy of the posterior predicted Categorical distribution is a measure of the total predictive uncertainty.

The total uncertainty can be further decomposed into: aleatoric uncertainty, arising due to noise, and epistemic uncertainty, arising due to lack of knowledge when no data are observed on a given region of the feature space. We can calculate the expected entropy at a given point by averaging the entropies of the Categorical distributions predicted by each member of the ensemble. This is a measure of aleatoric

uncertainty in predicting a single point. Finally, the Mutual Information (MI) between the categorical label y and the parameters of the model W (i.e. in deep learning models these are the weights of the network), calculated by subtracting the expected entropy from total entropy, is a measure of the spread of the ensemble, and in turn a measure of epistemic uncertainty (Depeweg et al., 2017):

$$\underbrace{I(y, W|x^*, \mathcal{D})}_{\text{Epistemic Uncertainty}} = \underbrace{\mathbb{H}[\mathbb{E}_{p(W|\mathcal{D})}[p(y|x^*, W)]]}_{\text{Total Uncertainty}} - \underbrace{\mathbb{E}_{p(W|\mathcal{D})}[\mathbb{H}[p(y|x^*, W)]]}_{\text{Expected Aleatoric Uncertainty}} \quad (4)$$

D. Generating boundary points with Normalizing Flows

Normalizing Flows (Rezende & Mohamed, 2015; Dinh et al., 2016b; Huang et al., 2018) are generative models that use the change of variables theorem to transform a simple distribution $p(z)$ into a complex distribution $p(x)$ using a function $f_\phi^{-1}(z)$, composed of a sequence of simple invertible transforms with cheaply computable Jacobians (for tractability). Since directly sampling from the “boundary” of the data manifold in the original data space is a complicated, we propose to train a normalizing flow to maximize the log likelihood of the x ’s, and then use the boundary in the latent space of the flow to generate data lying on the boundary of the data-space. Specifically, since we assume a simple distribution over the latent space, $f(X) \approx \mathcal{N}(0, \sigma)$ in \mathcal{Z} , we propose to sample $\tilde{z} \in \text{Bound}_{\mathcal{Z}}$, the latent boundary and use our flow to map it into the input space, obtaining $\tilde{x} = f^{-1}(\tilde{z})$. In practice, we choose $\text{Bound}_{\mathcal{Z}}$ to be a shell of given inner and outer radii, that is, $\{\tilde{z}|\alpha < d(0, \tilde{z}) < \beta\}$. For example, in the case of a uni-dimensional standard Gaussian distribution, since approximately 99% of the probability mass is in the interval $[-3; 3]$, we may want to invert points that are sampled at the boundary of this interval and we consider $\text{Bound}_{\mathcal{Z}} = [-3 - \eta; -3] \cup [3; 3 + \eta]$, where η is a smoothing term.

E. Pathologies of the Neural Linear Model

In this section we show that in an NLM classifier, one generally does not learn features capable of expressing OOD uncertainty. In NLM training, one learns features ϕ_θ by maximizing the log likelihood of the observed data, as shown in Equation 2. While the learned ϕ^* is good for classification, it is not capable of expressing the boundary of the high-mass region of the data. Specifically, the learned basis can express functions that separate the classes, but not functions that surround the data, and as a result cannot model a distribution over decision boundaries that surround the data (corresponding to OOD uncertainty).

We verify this hypothesis as follows: consider a synthetic dataset $\{(x_n, y_n, b_n)\}_{n=1}^N$, where x_n is the input, y_n is the label, and b_n is a binary indicator signaling whether the data-point is OOD or not. We train a classifier to predict $y|x$ (as in Equation 2). We then fix the features given by the last hidden layer of this classifier, $\phi(x; \theta^*)$, and train a logistic regressor to predict $b|x$. In other words, we train a regressor to map $\phi(x) \rightarrow b$. As demonstrated in Figure 5, this learned classifier is incapable of learning $b|x$ given features useful for predicting $y|x$. Specifically, far from the data, the learned classification boundaries incorrectly generalize along the boundaries between the original K classes, as opposed to between the in-distribution data and the OOD data. As a result, a Bayesian logistic regression model trained using this learned basis functions will not be able to express functions that surround the data, and thus will not model OOD uncertainty. In contrast, we train a classifier to predict $y, b|x$ and then use the learned features to predict $b|x$ (i.e $\phi(x) \rightarrow b$). In this case, since the basis is explicitly trained to predict the OOD points, the resultant classifier predicts $b|x$ accurately.

We emphasize that these findings show a pathology of the training objective. Thus, increasing the dimensionality and expressivity of the basis will not help. In fact, we show later that BaCOUn is able to model OOD uncertainty while remaining predictive of y for the same capacity networks.

Based on this evidence, we further hypothesize that with finite-sized BNNs, the uncertainty over the weights does not add enough diversity of features in order to model OOD uncertainty, in contrast to a GP which has an infinite dimensional basis.

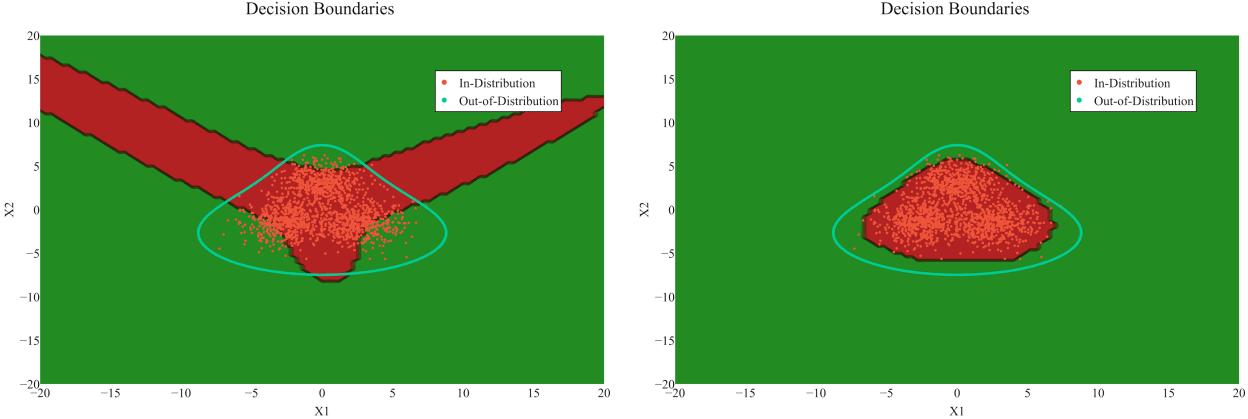


Figure 5. Comparison of features used to classify OOD points vs. non-OOD points. **Left:** We train the features to maximize the log likelihood of the data (i.e. to classify the points into their respective mixture components correctly). We see that a classifier given these features fails to classify points as OOD vs. non-OOD fails. Specifically, far from the data the learned classification boundaries generalize along the boundaries between the original K classes as opposed to between the in-distribution data and the OOD data. **Right:** We train the features using BaCOUn’s basis functions – i.e. we train on the original K classes (corresponding to the mixture components) and additionally a class representing the boundary of the data. We see that using those features, a classifier trained to classify points as OOD or non-OOD performs well.

F. Quantitative Results

F.1. BaCOUn models OOD uncertainty

GMM In Table 1, we present the aleatoric and epistemic uncertainties obtained by BaCOUn on the GMM dataset. We use a grid of the input space $[15, 17.5] \times [15, 17.5]$, “far” from the observed data manifold (and consider it “OOD”). We also take points from high data density with no class overlap (“In”) as well as points from a region with high class overlap (“Middle”).

We take 100 points from each region, and report averages of the uncertainties obtained by the different methods, as well as the classification accuracy for each method. The models used are: the BaCOUn framework, a BNN fitted with BBVI, MC-Dropout (MCD) and a Gaussian Process (GP). All models provide relatively similar accuracies and aleatoric uncertainties in all regions. However, only the Gaussian Process (that we consider more or less as the gold standard) and BaCOUn provides reliable epistemic uncertainty in the OOD region. BNN, NLM and MC-Dropout dramatically fail by providing excessively low epistemic uncertainty for OOD points.

F.2. BaCOUn yields interpretable aleatoric and epistemic uncertainty

In both our experiments on the *Wine Quality* dataset and Images datasets, BaCOUn is the only approach that provides interpretable and accurate epistemic and aleatoric uncertainty. Here, we define interpretable as aligned with human intuition about what is considered OOD. Specifically, on

both datasets we construct OOD examples using either held-out classes or other datasets, which a human would agree are considered OOD with respect to the training data. We then check whether models distinguish the original training data (as in-distribution) from the held-out classes / different datasets (as OOD data). In all cases, baselines systematically fail to decompose uncertainty accuracy, producing over-confident predictions, while BaCOUn is able to correctly distinguish between OOD and in-distribution.

Wine quality dataset In Table 2 and 3, we show the accuracy (as a goodness of fit indicator) and decomposition of uncertainties obtained by BaCOUn and the baselines. In Figure 6, we additionally present boxplots that summarize the entire distribution of the uncertainties.

Image Datasets To check whether BaCOUn’s uncertainty decomposition aligns with human intuition, we used MNIST as the training data (and thus the “in-distribution” data), and other datasets (CIFAR, USPS, EMNIST) as OOD examples, since a human would regard those as qualitatively different from MNIST. In Figure 7 and 8, we present the mean \pm standard deviation of the epistemic and aleatoric uncertainties obtained on different image datasets. As shown in the figures, uncertainties obtained using MC-Dropout or a BNN (with BBVI) do not seem to align with human intuition, with either the epistemic or aleatoric uncertainty being predominant and the other uncertainty being negligible. The Neural Linear Model appears to have uncertainties that align better with human intuition; however, for NLM, the uncertainties on OOD points close to the data manifold (i.e. on the boundary) extremely low, implying overconfident predictions. We

Model	Accuracy		Aleatoric			Epistemic	
	In-Dist	In	Out	Middle	In	Out	Middle
BaCOUn	0.94	0.11	0.15	0.30	0.03	0.74	0.08
BNN	0.93	0.10	8.7e-4	0.32	0.07	0.04	0.11
MCD	0.94	0.123	5.8e-05	0.40	0.01	8.4e-06	0.03
GP	0.95	0.42	1.1	0.54	0.42	1.1	0.54

Table 1. Results on synthetic GMM dataset. The uncertainty estimates are averaged over three types of regions: “In”, which corresponds to in-distribution points in regions $p(x)$ is high and the classes do not overlap, “Out”, which corresponds to OOD points far from the observed data, and “Middle”, which correspond to in-distribution points in regions of high class overlap.

Model	AUC		Epistemic ($\times 10^{-2}$)		Epistemic Pct Change From In	
	In	In	Held-Out Classes	OOD	Held-Out Classes	OOD
BaCOUn	0.862	0.089	0.121	0.667	0.357	6.479
BNN	0.854	1.719	1.492	0.96	-0.132	-0.441
MCD	0.852	3.225	3.622	9.19	0.123	1.85
NLM	0.856	0.049	0.046	0.02	-0.047	-0.581

Table 2. Epistemic uncertainty obtained by BaCOUn, BNN, MCD and NLM on the *Wine Quality* dataset. BaCOUn provides higher epistemic uncertainty for points of held-out classes and much higher epistemic uncertainty for OOD points compared to in-distribution points.

Model	Aleatoric				Aleatoric Pct Change From In		
	In	Held-Out (3,4,8,9)	Held-Out (6)	OOD	Held-Out (3,4,8,9)	Held-Out (6)	OOD
BaCOUn	0.308	0.269	0.392	0.031	-0.127	0.273	-0.899
BNN	0.245	0.212	0.320	0.112	-0.136	0.308	-0.543
MCD	0.392	0.354	0.45	0.413	-0.095	0.149	0.054
NLM	0.266	0.224	0.343	0.023	-0.159	0.291	-0.914

Table 3. Aleatoric uncertainty obtained by BaCOUn, BNN, MCD and NLM on the *Wine Quality* dataset. BaCOUn provides aleatoric uncertainty which is higher for class 6 which contains many instances which are similar to both points of class 5 and class 7, while aleatoric uncertainty is much lower for OOD points far from where classes overlap.

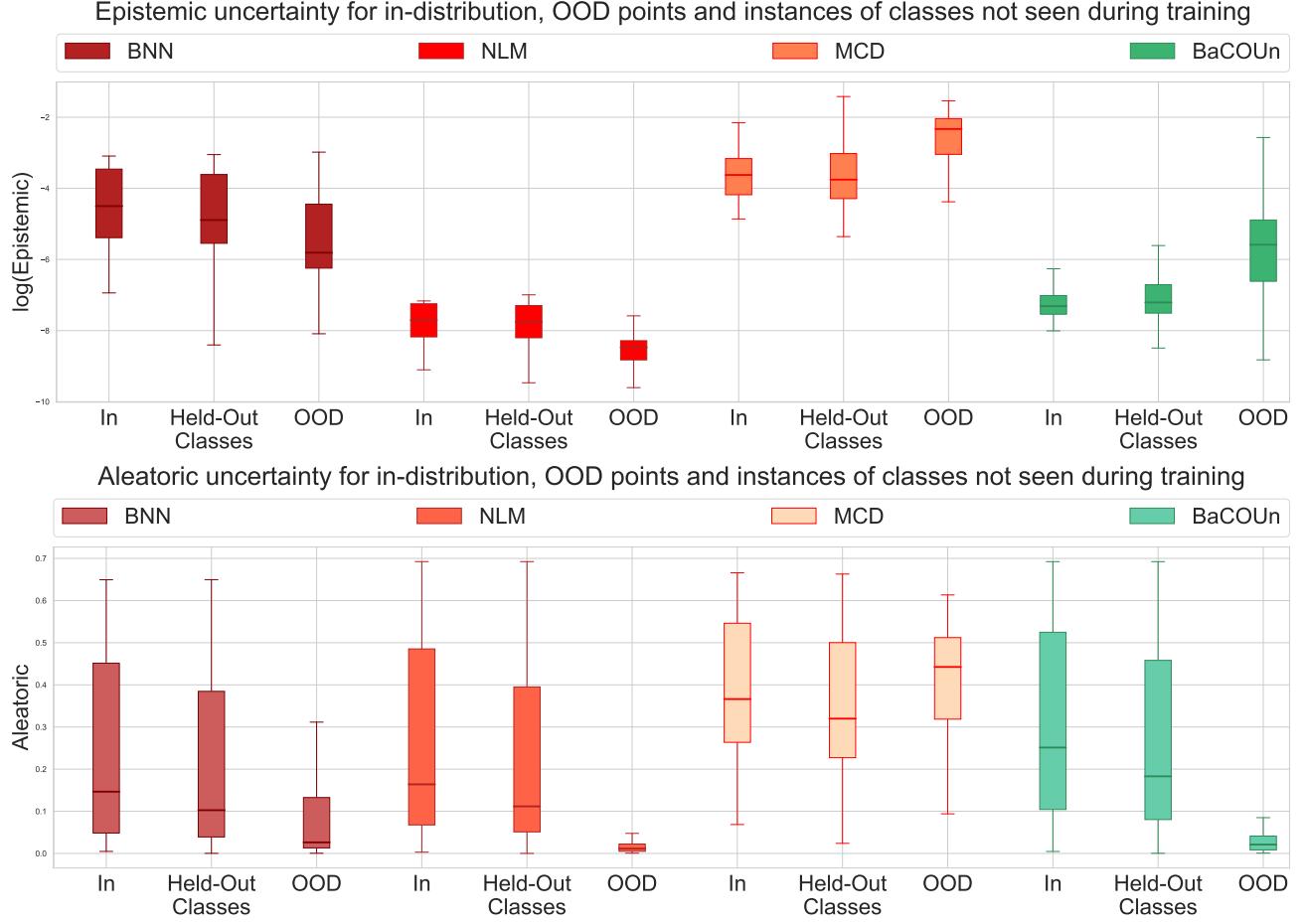


Figure 6. Epistemic and aleatoric uncertainty of BNN, NLM, MC-Dropout and BaCOUn for in-distribution points (i.e. held-out instances of class 5 and 7), instances of held-out classes (i.e. classes 3,4,8,9) and OOD points. BaCOUn provides reliable OOD uncertainty while maintaining accurate aleatoric uncertainty. Specifically, epistemic uncertainty is maximized for OOD points while aleatoric uncertainty is minimized in OOD regions where data have not been observed.

hypothesize that for robustness evaluations and downstream tasks, the Neural Linear Model could be easily attacked with adversarial samples, generated “close enough” to the data manifold. Lastly, as desired, BaCOUn learns models with low epistemic uncertainty on the in-distribution points and high epistemic uncertainty on the OOD points (both close to and far from the data).

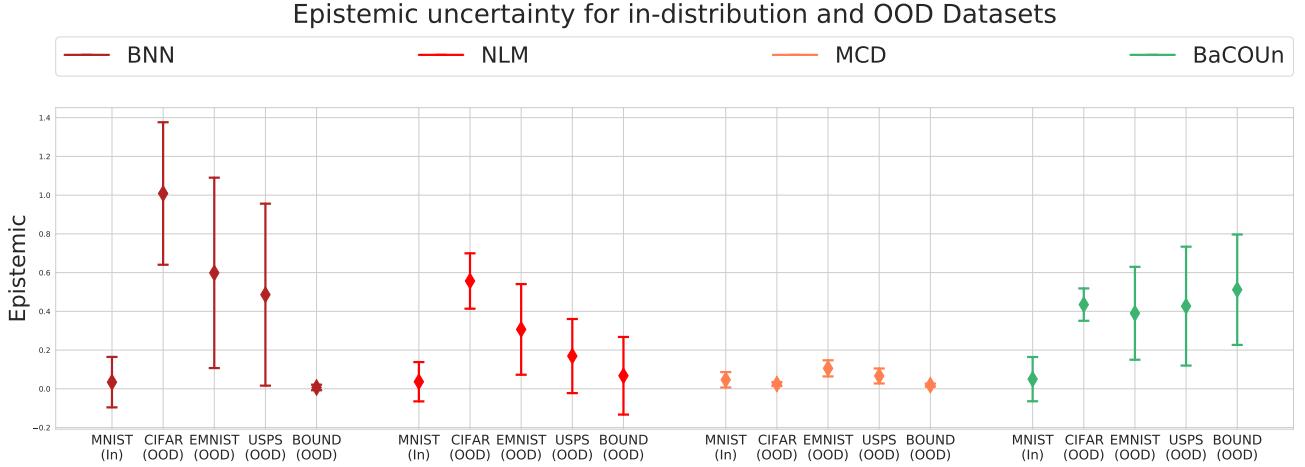


Figure 7. Mean \pm standard deviation of the epistemic uncertainty obtained on the different datasets by BaCOUn and its competitors. Despite the apparent good intuitive results obtained by the NLM and a BNN run with BBVI, those results are to be contrasted with the inaccurate aleatoric uncertainty obtained below.

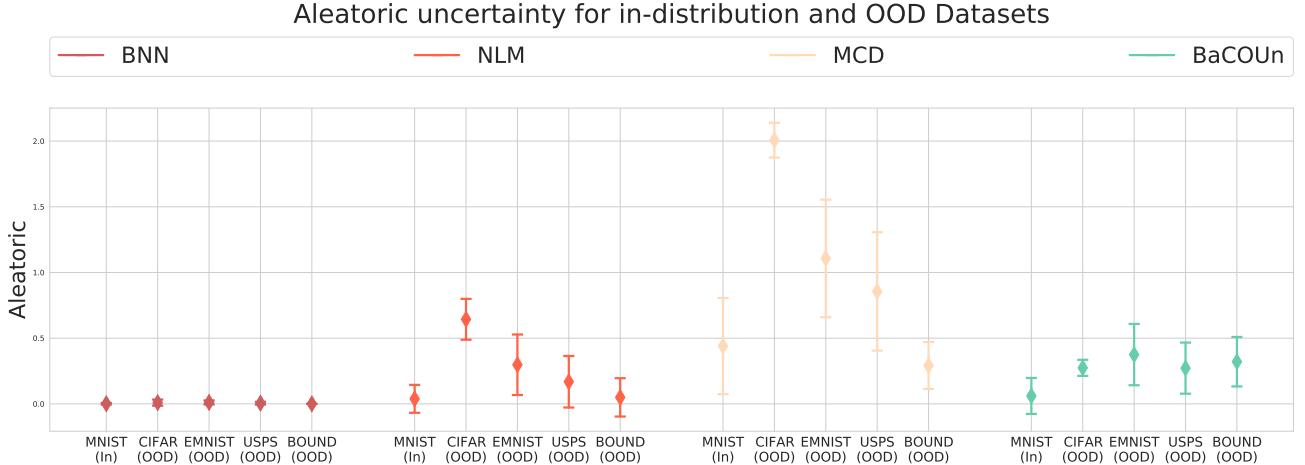


Figure 8. Mean \pm standard deviation of the aleatoric uncertainties obtained by different models on the image datasets.

G. Qualitative Results

G.1. BaCOUn provides GP-like behavior

Figure 9 shows that, on the moon-shaped clusters dataset (see Appendix A), BaCOUn learns GP-like uncertainty whereas MC-Dropout and NLM do not. Figures 10, 11, 12 show the uncertainty decomposition of BaCOUn, MC-Dropout and NLM on the moons dataset, respectively. BaCOUn is the only model that has increasing epistemic uncertainty as distance from the data increases; the remaining models make overconfident predictions nearly everywhere in the data-space. Moreover, MC-Dropout and NLM have high aleatoric uncertainty in data-poor regions where the classifier should only have high epistemic uncertainty. Similarly, we present the uncertainty decomposition obtained by the aforementioned methods on the GMM data (see Ap-

pendix A) in Figures 14, 15, 16, 17 and 18.

G.2. BaCOUn provides interpretable uncertainty

Individual Examples for Models Trained on MNIST

On a set of specific inputs, we demonstrate that in comparison to baselines, BaCOUn is able to obtain uncertainty decomposition that align with human intuition. That is, BaCOUn gives higher epistemic uncertainty on OOD data points that are

- in the MNIST dataset but not in the training data (Figure 19)
- in the USPS dataset (Figure 20 and 21)
- artificially generated to lie on the boundary of the MNIST data (Figure 22)

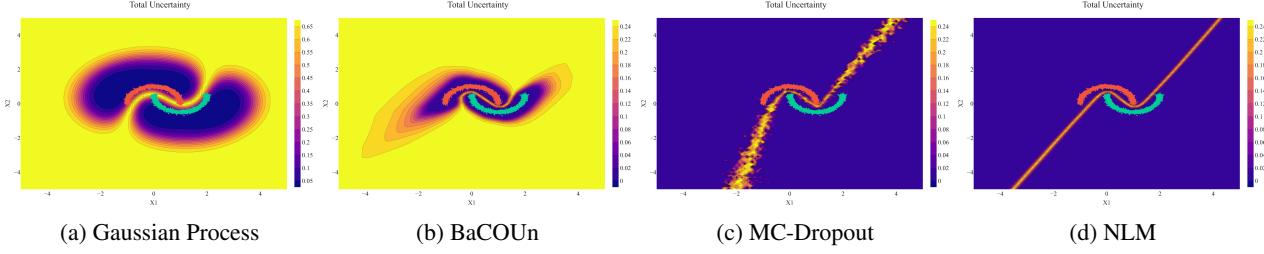


Figure 9. Comparison of Total Uncertainty. BaCOUn is the only model which obtains GP-like uncertainty, with high uncertainty far from the observed data as well as in regions of high class overlap.

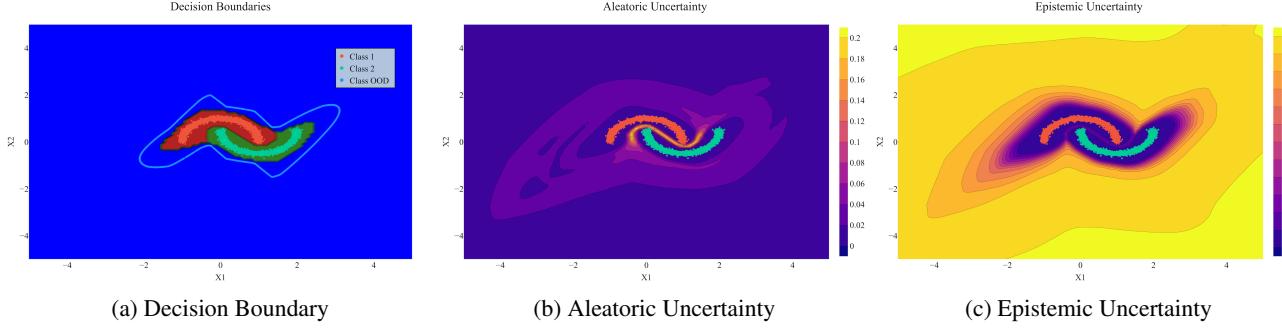


Figure 10. BaCOUn Uncertainty Decomposition. BaCOUn provides reliable OOD uncertainty while maintaining accurate aleatoric uncertainty in regions with high class overlap.

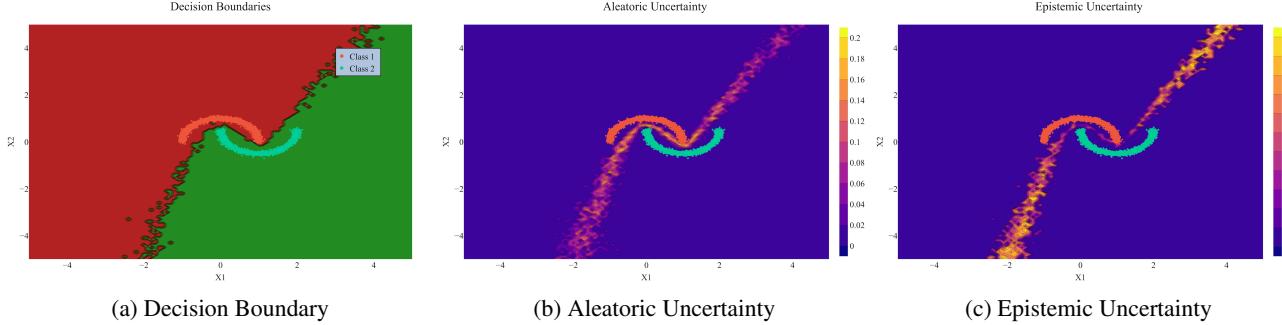


Figure 11. MC-Dropout Uncertainty Decomposition. The model overgeneralizes and produces overconfident predictions in regions of low-data density, failing to provide well-calibrated OOD uncertainty.

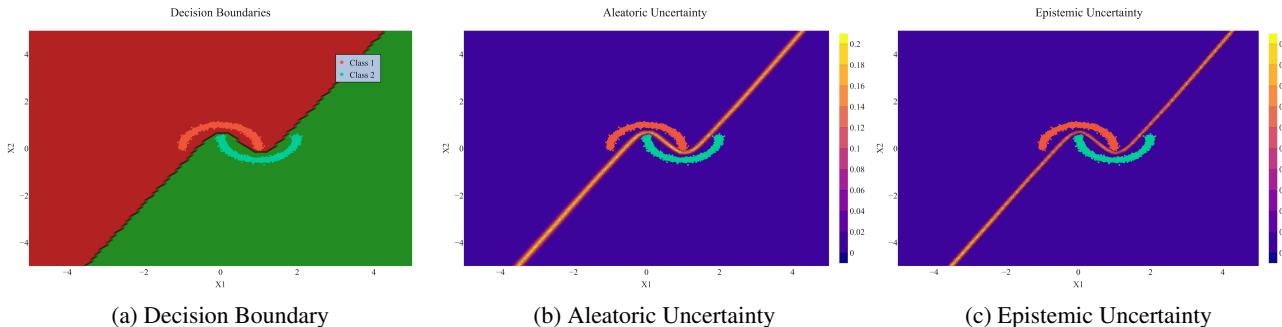


Figure 12. NLM Uncertainty Decomposition. Similarly to MC-Dropout, the model overgeneralizes and produces overconfident predictions in regions of low-data density, failing to provide well-calibrated OOD uncertainty.

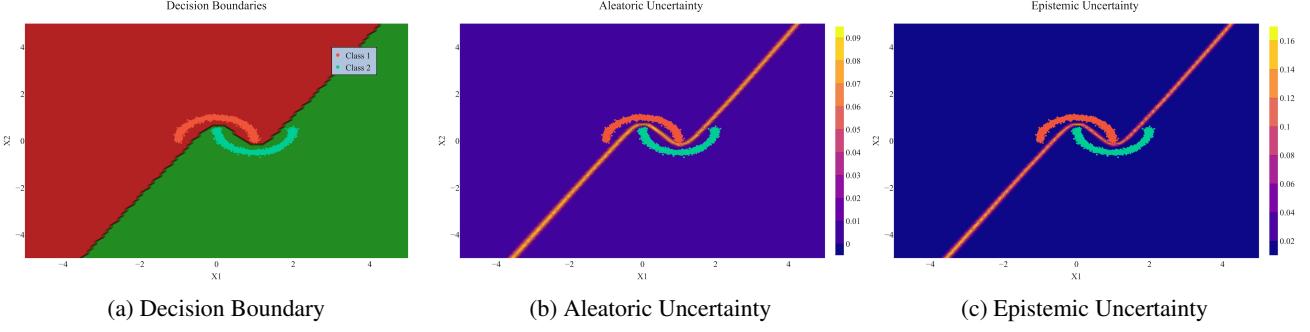


Figure 13. BNN Uncertainty Decomposition. A BNN provides the same pattern, as MC-Dropout and the NLM: the OOD uncertainty is underestimated in some directions.

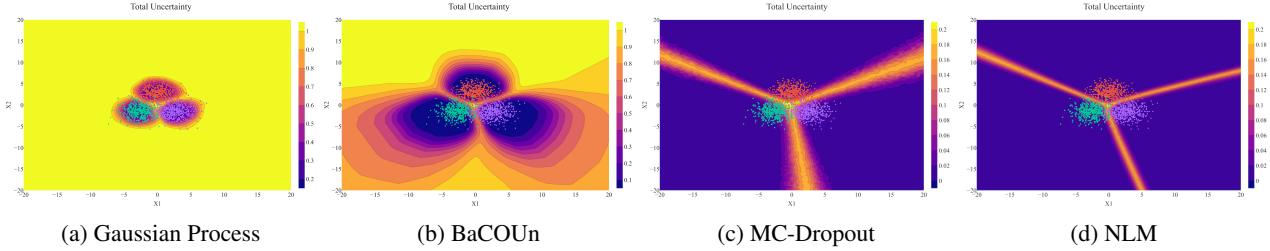


Figure 14. Comparison of Total Uncertainty. BaCOUn is the only model which obtains GP-like uncertainty, with high uncertainty far from the observed data as well as in regions of high class overlap.

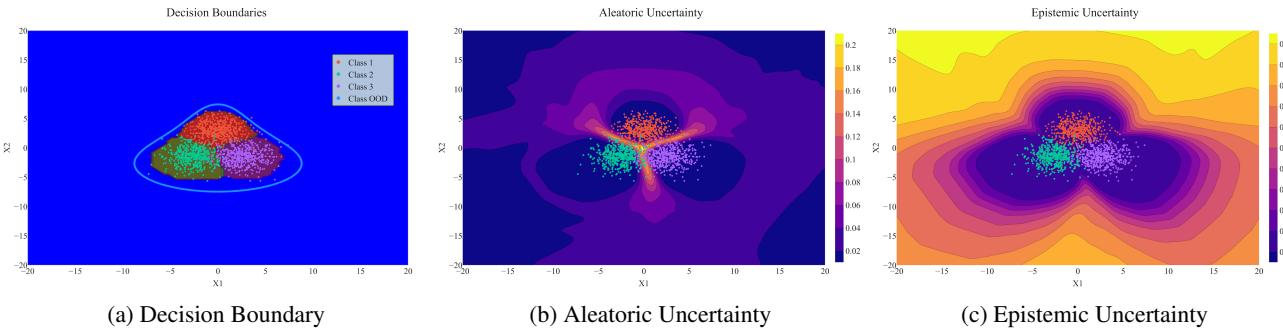


Figure 15. BaCOUn Uncertainty Decomposition. BaCOUn provides reliable OOD uncertainty while maintaining accurate aleatoric uncertainty in regions with high class overlap.

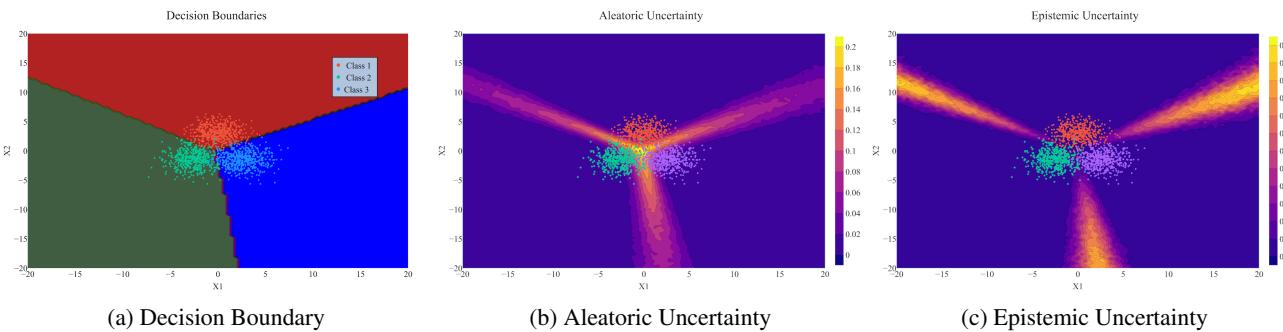


Figure 16. MC-Dropout Uncertainty Decomposition. The model overgeneralizes and produces overconfident predictions in regions of low-data density, failing to provide well-calibrated OOD uncertainty.

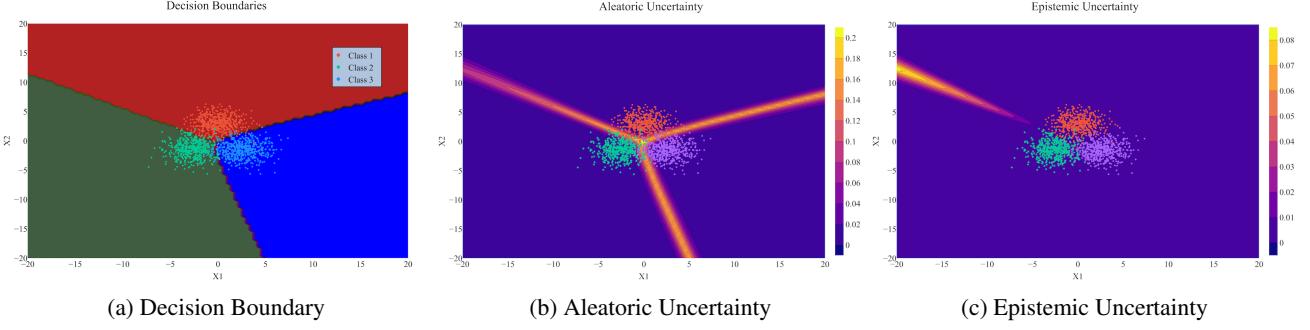


Figure 17. NLM Uncertainty Decomposition. Similarly to MC-Dropout, the model overgeneralizes and produces overconfident predictions in regions of low-data density, failing to provide well-calibrated OOD uncertainty.

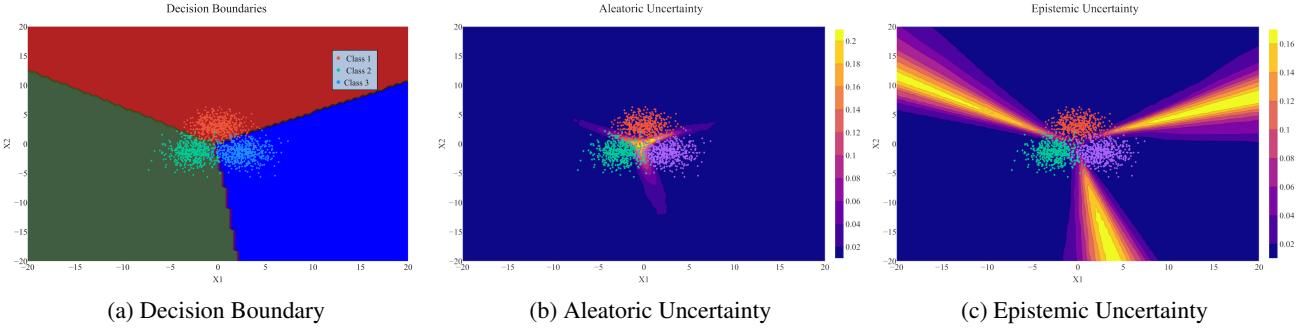


Figure 18. BNN Uncertainty Decomposition. A BNN provides the same pattern, as MC-Dropout and the NLM: the OOD uncertainty is underestimated in some directions.

In all of these case, baselines consistently make overconfident predictions (even when wrong), whereas BaCOUn remains conservatively uncertain. We note that in Figures 19 and 21, baseline models make overconfident and *incorrect* predictions.

Decomposition of uncertainty when crossing class boundaries We use a Variational Autoencoder (VAE) (Kingma & Welling, 2013), pre-trained on MNIST (Mitra et al., 2019)¹ in order to encode digits in a continuous 2D latent space. We then selected two points in the latent space, one in each of two neighboring classes, linearly interpolated between the two points, and decoded the points in the trajectory. Figures 23 and 25 show two latent-space trajectories, as well as the decoded digits and the uncertainty decomposition along these trajectories. At the beginning and end of each trajectory, BaCOUn is certain about the digits (as it should be). In the middle of the trajectories, when the trajectory crosses BaCOUn’s decision boundary, we see both high epistemic uncertainty and aleatoric uncertainty. This is because the classes are not perfectly separable – digits in the middle of the trajectory look like an uncanny

mixture of the two digits – leading to high aleatoric uncertainty, and because between the classes there’s uncertainty over the exact boundary, leading to high epistemic uncertainty. Figures 24 and 26 show the corresponding behavior of the NLM. They show that the NLM is over-confident about digits in the middle of the trajectory, which do not look realistic.

Decomposition of uncertainty when moving away from data-rich regions In Figure 27, we demonstrate how BaCOUn’s aleatoric and epistemic uncertainty change when moving away from the data-rich regions of the space. We do this by taking a digit and adding more and more Gaussian noise to it. We then examine the uncertainty decomposition as the digit gets more noisy, and observe that epistemic uncertainty increases drastically in comparison to aleatoric uncertainty. Figure 28 shows the behavior of the NLM model on the same noisy digits. It shows that NLM is unable to distinguish between data-rich and data-poor regions.

BaCOUn is more certain about digits that look like they should belong to the data In Figure 29, we present different images from MNIST’s test set along with the uncertainty obtained by BaCOUn as the image gets rotated by different degrees. We observe that uncertainties increase as the digit starts looking like an element that is not digit-like and

¹Pre-trained VAE from CreativeAI: Deep Learning for Computer Graphics. See <https://github.com/smartgeometry-ucl/dl4g>.

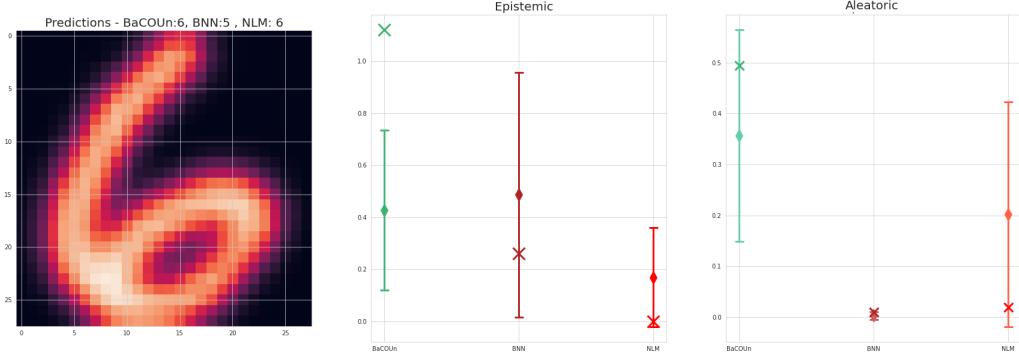


Figure 19. Uncertainty decomposition on MNIST example not in MNIST training set. Given an image not in the training-set, the BNN makes an overconfident and wrong prediction, the NLM correctly predicts the digit but does so with low uncertainty, whereas BaCOUn provides higher epistemic uncertainty.

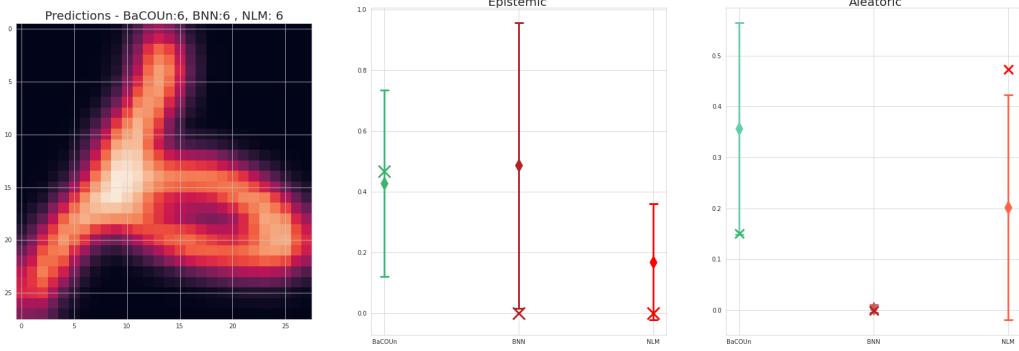


Figure 20. Uncertainty decomposition given USPS example for model trained on MNIST. Consider a digit that, according to a human might or might not be a “6” (i.e. a human would have high uncertainty). On this example, BaCOUn is more uncertain (like a human) whereas baseline methods are overconfident.

decreases back when the image looks like a MNIST digit. These uncertainties reflect a human’s intuition of uncertainties.

NLM fail to provide intuitive uncertainty decomposition In Figures, 28, 24 and 26 we present the uncertainty metrics obtained by a NLM on the same examples as BaCOUn, namely, when we move away from the data-rich regions of the space, or following a latent trajectory between two classes. We observe that the NLM often provides overconfident predictions, even when the digits do not look like digits from the training data (Figures 24 and 26) and fail to provide a useful uncertainty decomposition as we move away from the data manifold (Figure 28).

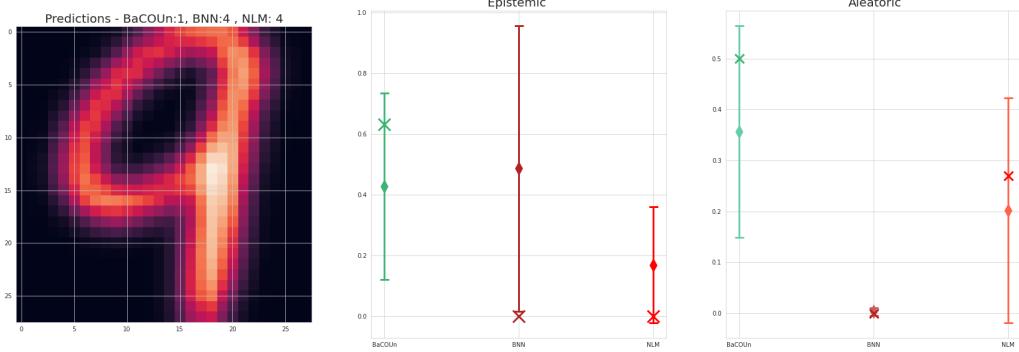


Figure 21. Uncertainty decomposition given USPS example for model trained on MNIST. We present an example from USPS on which all methods predict incorrectly. BaCOUn provides high epistemic uncertainty while BNN and NLM are overconfident in their wrong prediction.

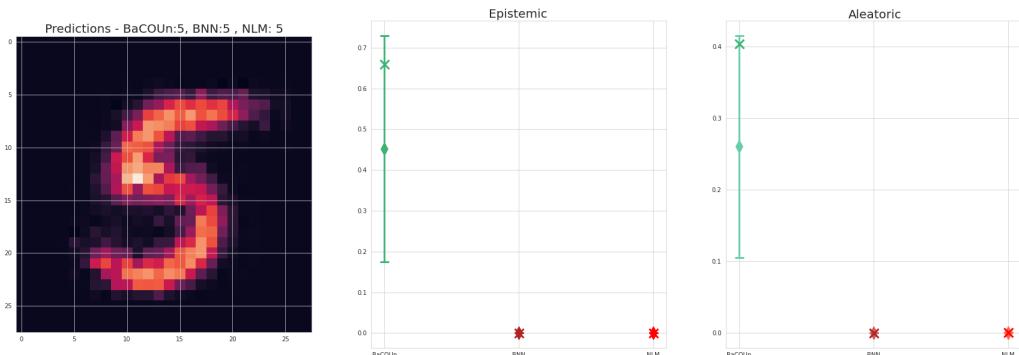
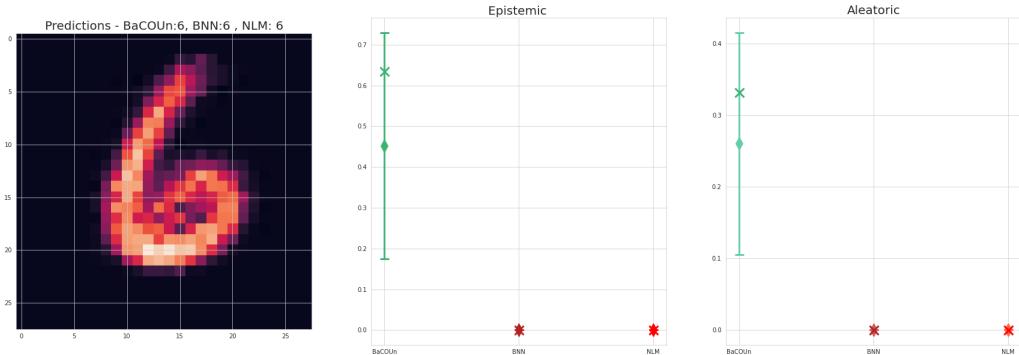
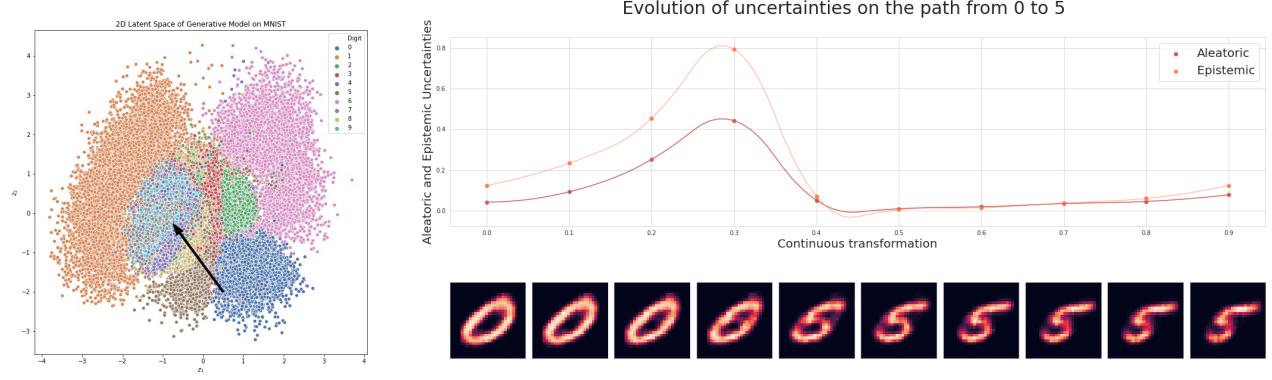


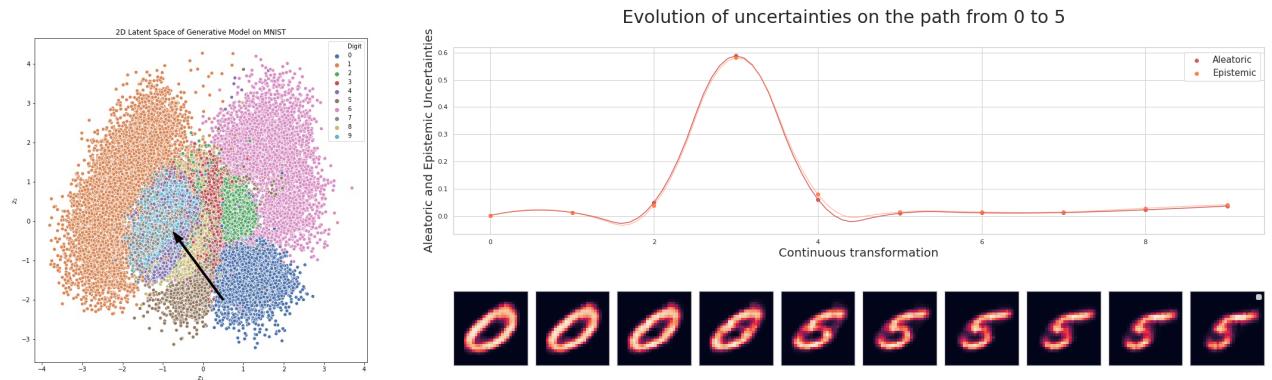
Figure 22. Uncertainty decomposition on artificially generated OOD MNIST images. We present the predictions of our methods on points chosen from the “generated ood” dataset. We observe that the generated examples are very blurry images and thus should be considered OOD. NLM and BNN are excessively confident in their predictions, whereas BaCOUn is appropriately more uncertain.



(a) Linear interpolation in 2D latent space of VAE trained on MNIST

(b) Decomposition of uncertainty for digits along latent space interpolation.

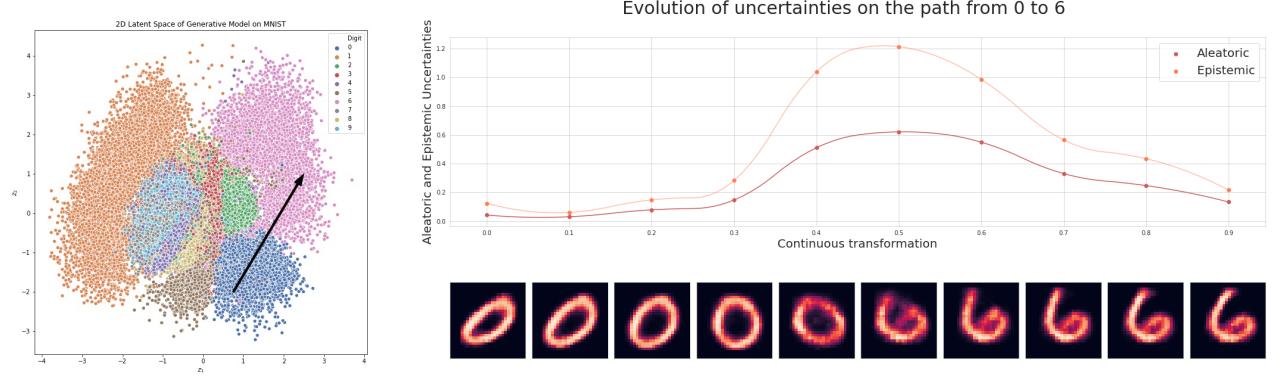
Figure 23. BaCOUn’s decomposition of uncertainty across class boundaries: MNIST’s 0 and 5 classes. (a) We use a VAE to morph a 0 into a 5 by linearly interpolating in the VAE’s latent space, (b) we present the uncertainty for the generated images. At the beginning (and end) of the trajectory, we see that BaCOUn is confident that the digit is a 0 (and a 5). In the middle, when the trajectory crosses BaCOUn’s decision boundary, we see both high epistemic uncertainty and aleatoric uncertainty. This is because the classes are not perfectly separable – some digits look like both a 0 and a 5 – leading to high aleatoric uncertainty, and because between the classes there’s uncertainty over the exact boundary, leading to high epistemic uncertainty.



(a) Linear interpolation in 2D latent space of VAE trained on MNIST

(b) Decomposition of uncertainty for digits along latent space interpolation.

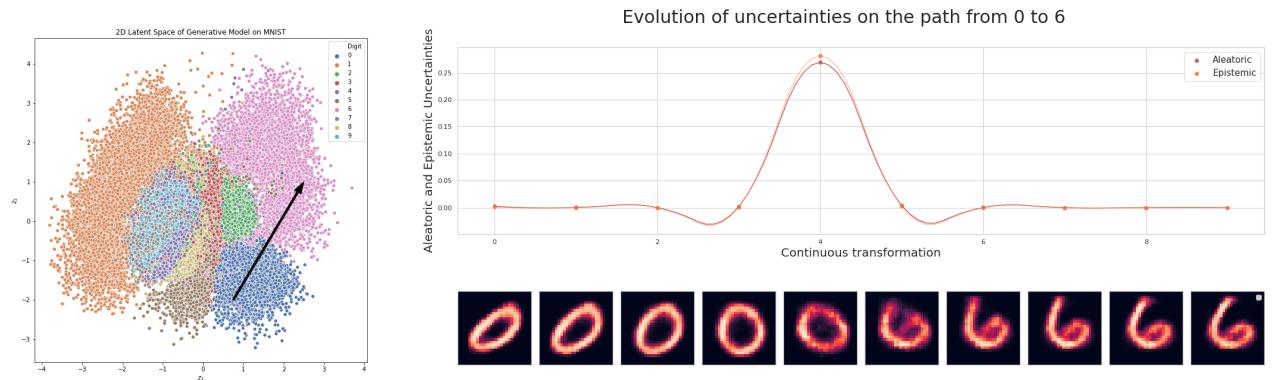
Figure 24. NLM’s decomposition of uncertainty across class boundaries: MNIST’s 0 and 5 classes. We use a VAE to morph a 0 into a 5 by linearly interpolating in the VAE’s latent space. We present the uncertainty for the generated images. NLM is highly uncertain on only one of the morphed digits, while it should be uncertain about several in the “middle” of the trajectory, where the digits look neither like a 0 nor like a 5.



(a) Linear interpolation in 2D latent space of VAE trained on MNIST

(b) Decomposition of uncertainty for digits along latent space interpolation.

Figure 25. BaCOUn’s decomposition of uncertainty across class boundaries: MNIST’s 0 and 6 classes. (a) We use a VAE to morph a 0 into a 6 by linearly interpolating in the VAE’s latent space, (b) we present the uncertainty for the generated images. At the beginning (and end) of the trajectory, we see that BaCOUn is confident that the digit is a 0 (and a 6). In the middle, when the trajectory crosses BaCOUn’s decision boundary, we see both high epistemic uncertainty and aleatoric uncertainty. This is because the classes are not perfectly separable – some digits look like both a 0 and a 6 – leading to high aleatoric uncertainty, and because between the classes there’s uncertainty over the exact boundary, leading to high epistemic uncertainty.



(a) Linear interpolation in 2D latent space of VAE trained on MNIST

(b) Decomposition of uncertainty for digits along latent space interpolation.

Figure 26. NLM’s decomposition of uncertainty across class boundaries: MNIST’s 0 and 6 classes. We use a VAE to morph a 0 into a 6 by linearly interpolating in the VAE’s latent space. We present the uncertainty for the generated images. NLM is highly uncertain on only one of the morphed digits, while it should be uncertain about several in the “middle” of the trajectory, where the digits look neither like a 0 nor like a 6.

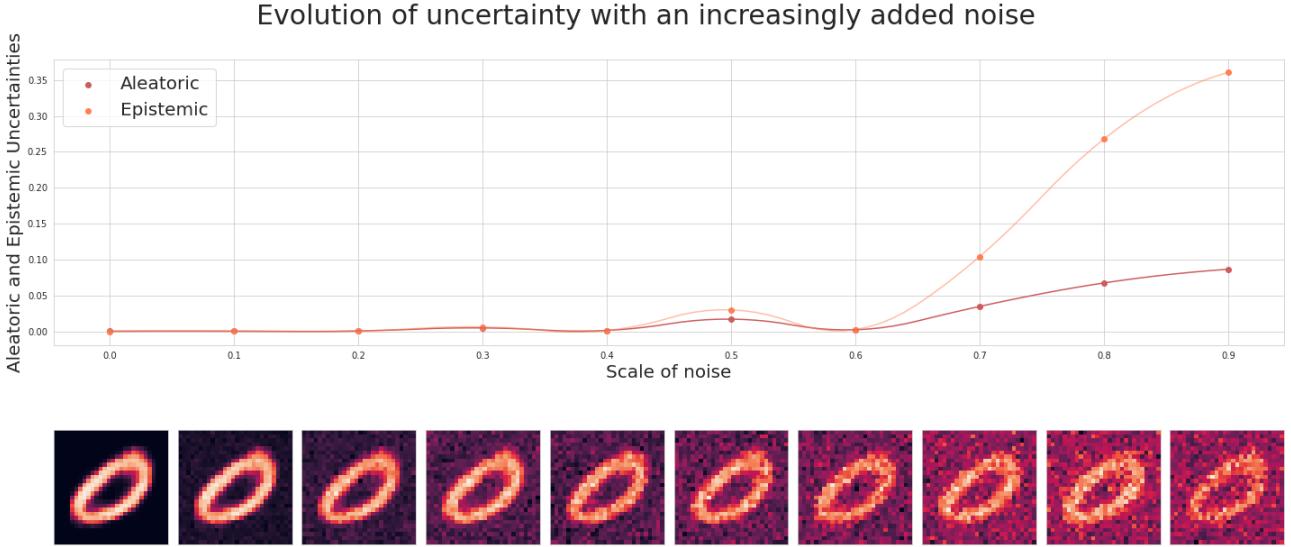


Figure 27. BaCOUn’s decomposition of uncertainty when moving to data-poor regions. We take an MNIST image (left) and progressively add more Gaussian noise to it (right) in order to move it farther and farther away from the high-mass region of the data. We see that as we move farther from the data, epistemic uncertainty increases significantly while aleatoric uncertainty does not.

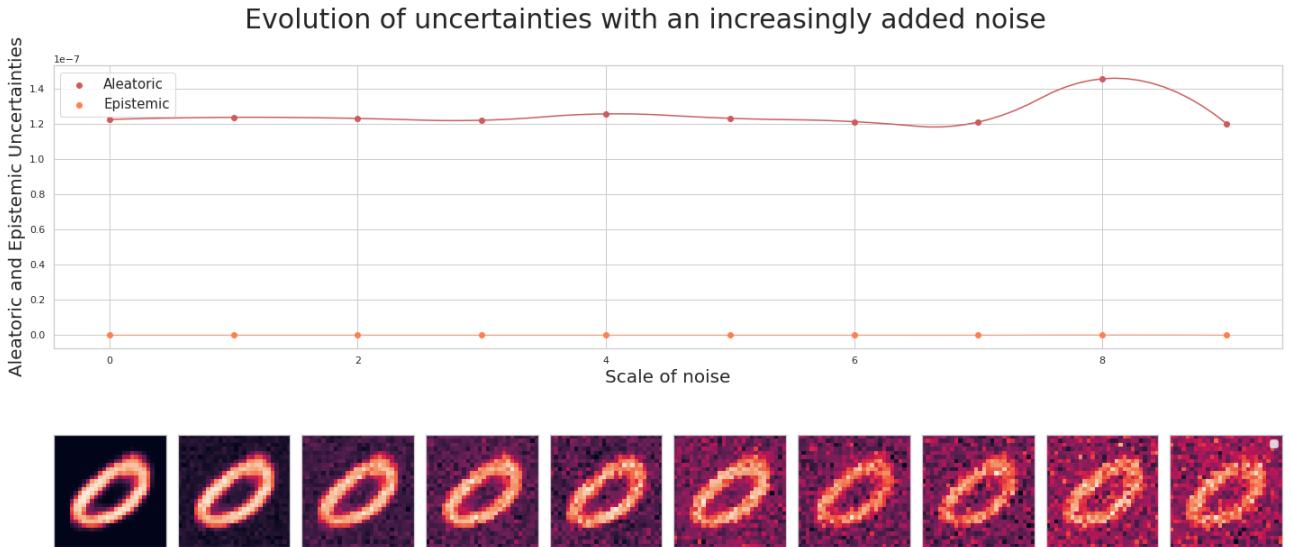


Figure 28. MLM’s decomposition of uncertainty when moving to data-poor regions. We take an MNIST image (left) and progressively add more Gaussian noise to it (right) in order to move it farther and farther away from the high-mass region of the data. We see that as we move farther from the data, epistemic and aleatoric remain constant. As such the learned classifier is unable to distinguish between data-rich and data-poor regions.

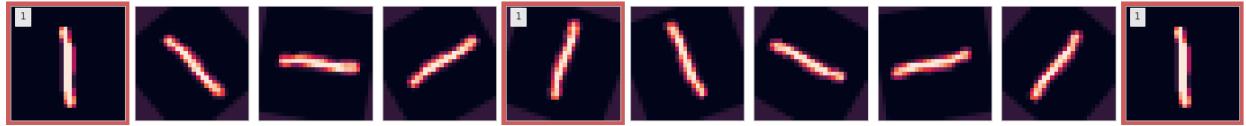
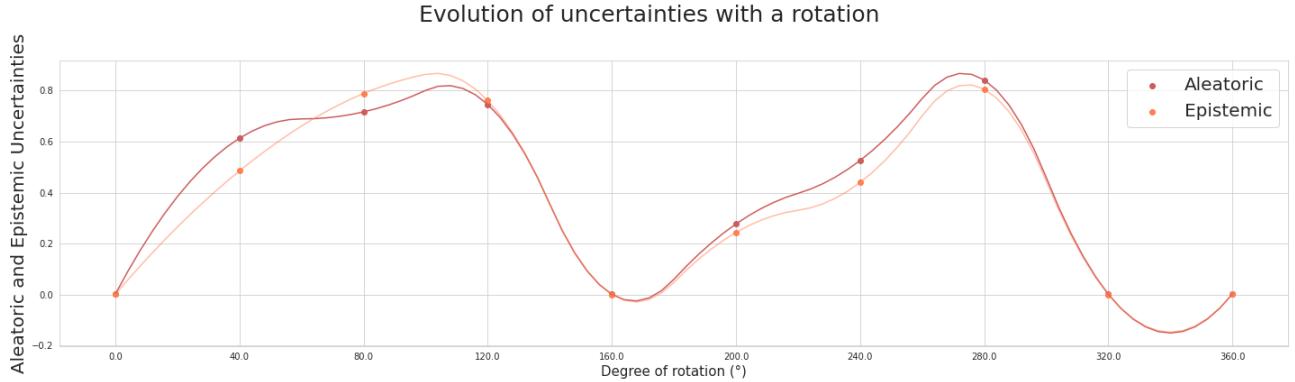
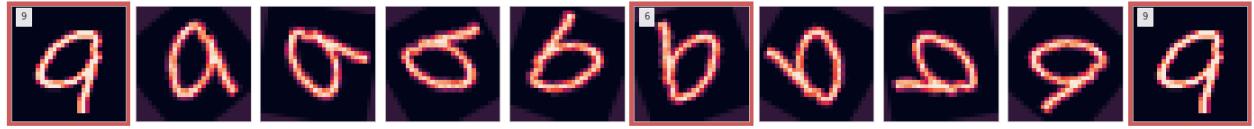
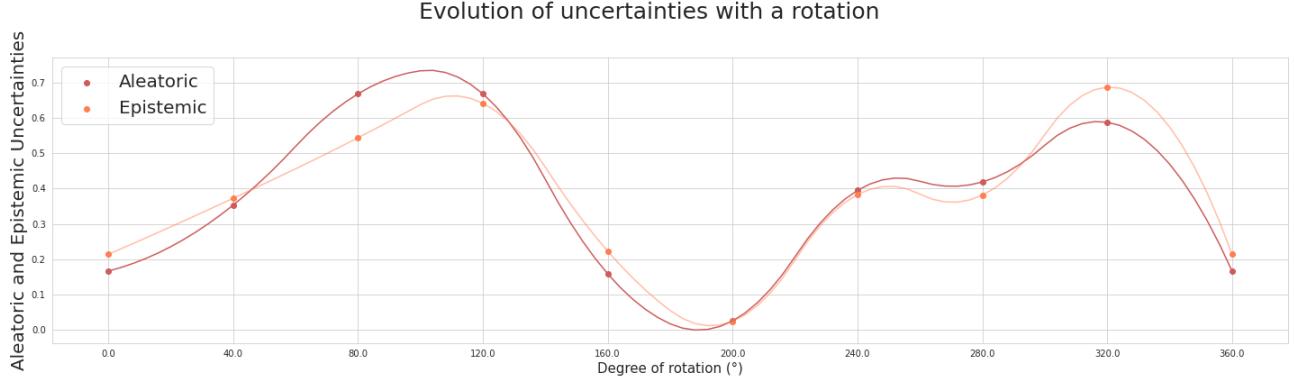


Figure 29. BaCOUn is certain about images that look like they belong in the training set. We take MNIST digits and rotate them. We see that BaCOUn’s uncertainty is low when the rotated digit resembles another digit. **Top:** a “9” can be flipped upside-down to look like a “6”. **Bottom:** a “1” can be flipped upside-down and will still look like a “1”.

H. Robustness to Outliers

When dealing with OOD data and uncertainty, the question of outliers arises and becomes an important one. Outliers are often considered as perturbations or anomalies that one should remove from a dataset as a pre-processing step. Even if the border between OOD points and outliers is porous, we present a simple and scalable approach to deal with outliers in a dataset.

A recent line of work has focused on using Generative models for anomaly detection. For instance, (Schlegl et al., 2017) present AnoGAN and use Generative Adversarial Networks for Marker Discovery, whereas (Ryzhikov et al., 2019) propose to use Normalizing Flows for Bayesian inference and deal with class imbalance. Our approach consists of using the density modelled by BaCOUn’s Normalizing flow in order to rank and remove the data points which are most likely to be outliers. Despite its simplicity, our method provides reliable anomaly detection in relatively simple settings and is composed of the following steps:

- Train the Normalizing flow on the data (including potential outliers).
- Compute the log probabilities of the data points under the Normalizing low.
- Remove k data points with lowest probabilities.

To demonstrate our method, we design an experiment on the Moons data (see Appendix A. Outliers are artificially generated as $\tilde{x} = x + \epsilon$, where $\epsilon \sim \mathcal{N}(0, \sigma)$ (see Figure 30). 4000 data points are originally in the dataset, and 200 outliers are added. One Normalizing Flow is then trained on the entire data. Due to its ability to model the data density and the geometry of the space it assigns high probability scores to points the closest to the data manifold and lower probabilities to most outliers that are “far” from the data manifold. The k points with highest probability are kept, or equivalently, the $\text{card}(X) - k$ are removed. We visualize the remaining data at the end of the procedure, for different values of k in Figure 31.

I. Future Work

In future work, we plan to address some the following themes:

- Searching for adequate basis functions presents both theoretical and practical challenges. As we aim to approximate a Gaussian Process, a better understanding of the need for wider or deeper networks is of interest.
- In addition, our approach is motivated by the need to obtain accurate uncertainty decomposition in real-

world critical applications like medical diagnosis. Using our framework in such context would be an end goal.

- Ideally, a better theoretical understanding of the method and the phenomenon at stake would be performed, maybe in order to understand an implied relationship with Gaussian processes. We leave that aspect to a future work.

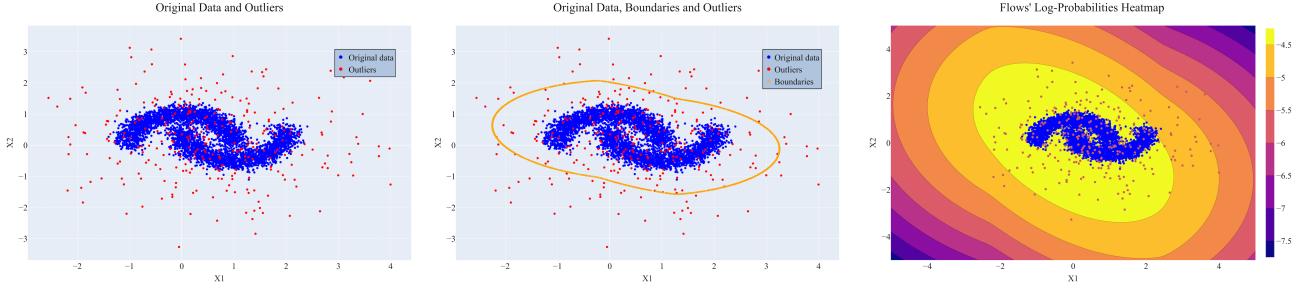


Figure 30. Data with outliers (a), Trained Normalizing flow and generated boundaries (b), (c) HeatMap of the Flow's log probabilities. Normalizing Flows are powerful tools to capture the global geometry of the problem without being overly sensitive to outliers, as shown in (b). The boundary generated doesn't play any role in the selection procedure, but it shows how robust the density estimation is. Furthermore, the heatmap of the Normalizing Flow's probabilities in (c) aligns with our intuition: points far from the training data have lower probability under the flow.

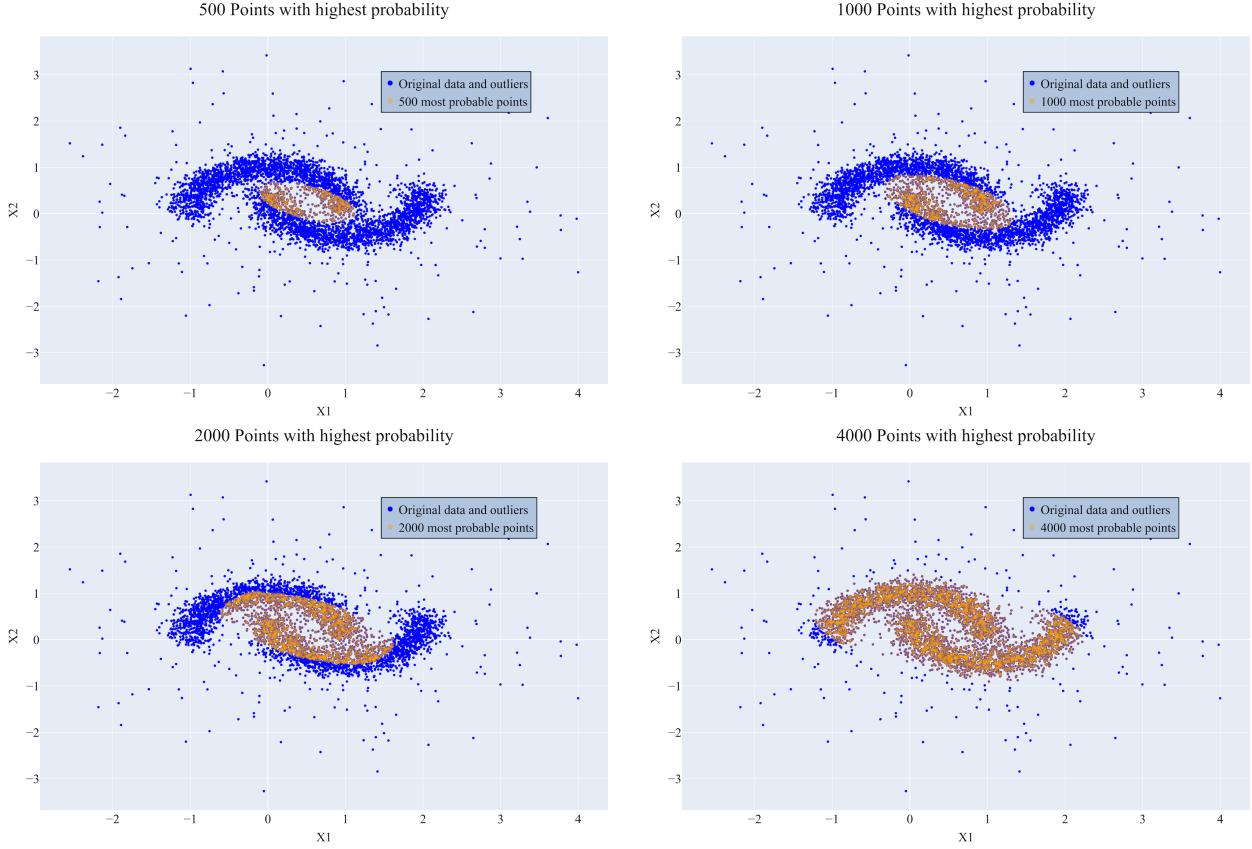


Figure 31. k points with highest probability under the normalizing flow, for $k=500$ (Top left), $k=2000$ (Top right), $k=3000$ (Bottom left) and $k=4000$ (Bottom right). The procedure successfully removes the points farthest away from the real data.