Notes on GVI in FS for Image Data

1. Gaussian Processes for Classification

Notes taken from chapter 4 of Matthews (2017).

For Gaussian process regression (GPR), a class of models is defined:

$$f \sim \mathcal{GP}(0, K(\theta))$$

where $f : X \to \mathbb{R}$, mapping to the set of real numbers $\mathbb{R}$ and K is the covariance function $K : X \times X \to \mathbb{R}$ parameterised by θ.

For binary Gaussian process classification (GPC), a mapping is defined:

$$g : \mathbb{R} \to [0, 1]$$

transforming a value on the real line to the unit interval to represent a probability. A bernoulli random variable $\mathcal{B}$ can be defined such that:

$$f_c \sim \mathcal{B}(g(f))$$

where $f_c : X \to \{0, 1\}$, the desired binary classifier.

For multiclass classification of J different classes, models are defined:

$$f^{(j)} \sim \mathcal{GP}(0, K(\theta^{(j)}))$$

where $j = 1, \ldots, J$, defining J i.i.d. Gaussian processes. Concatenating $\mathbf{f} = [f_1 \cdots f_J]^T$, the classification operation can be defined:

$$\mathbf{f}_c \sim Cat(\mathcal{S}(\mathbf{f}))$$

where $\mathbf{f}_c : X \to \{0, \ldots, J\}$, the desired multiclass classifier. $\mathcal{S} : \mathbb{R}^J \to \Delta(J)$, a mapping from a J dimensional real vector to a J dimensional probability simplex. Cat is the categorical distribution (generalisation of Bernoulli distribution for Categorical Data).

There are different possible choices for $\mathcal{S}$. The multiclass generalisation of the logit likelihood:

$$\mathcal{S}_{softmax}(\mathbf{f})_i = \frac{\exp(f^{(i)})}{\sum_{j=1}^{J} \exp(f^{(j)})}$$

The robust max function:

$$\mathcal{S}^{(\epsilon)}_{robust}(\mathbf{f})_i = \begin{cases} 1 - \epsilon, & \text{if } i = \arg\max(\mathbf{f}) \\ \epsilon, & \text{otherwise} \end{cases}$$

taking class label of the maximum value with probability of $1-\epsilon$ and probability ϵ of picking one of the other classes uniformly at random, where ϵ is chosen. This formulation provides robustness to outliers, as it only considers the ranking of the GPR models for each class.

A benefit of the robust max function is that the variational expectation is analytically tractable with respect to the normal CDF ($q(\mathbf{f}) = \mathcal{N}(\mu, C), \mathbf{f} \in \mathbb{R}^J$) and one dimensional quadrature ($\mathcal{S}^{(\epsilon)}_{robust}(\mathbf{f})_i \in \mathbb{R}$):

$$\int_{\mathbb{R}^J} q(\mathbf{f}) \log(\mathcal{S}^{(\epsilon)}_{robust}(\mathbf{f})_y) d\mathbf{f} = \log(1-\epsilon)S + \log\left(\frac{\epsilon}{J-1}\right)(1-S)$$

where S is the probability that the function value corresponding to observed class y is larger than the other function values at that point:

$$S = \mathbb{E}_{\mathbf{f}^{(y)} \sim \mathcal{N}(\mathbf{f}^{(y)}|\mu^{(y)}, C^{(y)})}\left[\prod_{i \neq y} \phi\left(\frac{\mathbf{f}^{(y)} - \mu^{(i)}}{\sqrt{C^{(i)}}}\right)\right]$$

where ϕ is the standard normal CDF. This one dimensional integral can be evaluated using Gauss-Hermite quadrature.

2. GWI for Multiclass Classification

Notes taken from A.6 of Wild et al. (2022).

2.1 Objective Function

The likelihood:

$$p(y|f_1, \ldots, f_J) = \prod_{n=1}^{N} p(y_n|f_1, \ldots, f_J)$$

where $p(y_n|f_1, \ldots, f_J) \coloneqq h^{\epsilon}_{y_n}(f_1(x_n), \ldots, f_J x_N)$ and $y_n \in \{1, \ldots, J\}$. $h^{\epsilon}_{y_n}$ is the robust max function $\mathcal{S}^{(\epsilon)}_{robust}$ as described in Matthews (2017). Wild et al. (2022) used $\epsilon = 1\%$.

The model consists of J independent Gaussian Random Elements such that:

$$f_j \sim P_j = \mathcal{N}(m_{\mathbb{P},j}, C_{\mathbb{P},j})$$

with the corresponding variational measures:

$$Q_j = \mathcal{N}(m_{\mathbb{Q},j}, C_{\mathbb{Q},j})$$

The objective to minimise:

$$\mathcal{L} = -\mathbb{E}_{\mathbb{Q}}\left[\log p(y_n|F_1, \ldots, F_J)\right] + \sum_{j=1}^{J} W_2^2(P_j, Q_j)$$

The variational (posterior) approximation of the probability of $\{(F_1(x), \ldots, F_J(x)) \in A\}$ will be denoted:

$$\mathbb{Q}\left((F_1(x), \ldots, F_J(x)) \in A\right)$$

where $A \subset \mathbb{R}^J$. We get the expected log-likelihood:

$$\mathbb{E}_{\mathbb{Q}}\left[\log p(y_n|F_1,\ldots,F_J)\right] \approx \sum_{n=1}^{N} \log(1-\epsilon)S(x_n,y_n) + \log\left(\frac{\epsilon}{J-1}\right)(1-S(x_n,y_n))$$

where:

$$S(x,j) \coloneqq \frac{1}{\sqrt{\pi}} \sum_{i=1}^{I} w_i \prod_{l\neq j} \phi\left(\frac{\sqrt{2r_j(x,x)}\xi_i + m_{Q,j}(x) - m_{Q,l}(x)}{\sqrt{r_l(x,x)}}\right)$$

for any $x \in \mathcal{X}$, $j = 1,\ldots,J$ where $(w_i,\xi_i)_{i=1}^I$ are the weights and roots of the Hermite polynomial of order $I \in \mathbb{N}.$, calculated with `scipy.special.roots_hermite`. ϕ is the standard normal cumulative distribution function.

The Wasserstein distance $W_2^2(P_j,Q_j)$ can be estimated in the same way as for regression:

$$\begin{aligned}\hat{W}^2 \coloneqq & \frac{1}{N}\sum_{n=1}^{N}(m_{\mathbb{P}}(x_n) - m_{\mathbb{Q}}(x_n))^2 + \frac{1}{N}\sum_{n=1}^{N} k(x_n,x_n) \\ & + \frac{1}{N}\sum_{n=1}^{N} r(x_n,x_n) - \frac{2}{\sqrt{NN_S}}\sum_{s=1}^{N_S}\sqrt{\lambda_s(r(X_S,X)k(X,X_S))}\end{aligned}$$

where:

- $X_S \coloneqq (x_{S,1},\ldots,x_{S,N_S})$ with $x_{S,1},\ldots,x_{S,N_S} \in \mathbb{R}^D$, a set of N_S points sub-sampled from the input data X
- $r(X_S,X) \coloneqq \left(r(x_{S_s,x_n})\right)_{s,n} \in \mathbb{R}^{N_s\times N}$
- $k(X,X_S) \coloneqq \left(k(x_{x_n,S_s})\right)_{n,s} \in \mathbb{R}^{N\times N_s}$
- $\lambda_s(\cdot)$ calculates the s-th eigenvalue

and $n = 1,\ldots,N$, $s = 1,\ldots,N_S$, k is the kernel for $\mathbb{P}$, r is the kernel for $\mathbb{Q}$

2.2 Prediction

For an unseen point $x^* \in \mathcal{X}$, the probability that it belongs to class $j \in \{1,\ldots,J\}$:

$$\mathbb{Q}(Y^* = j) = (1-\epsilon)S(x^*,j) + \frac{\epsilon}{J-1}(1-S(x^*,j))$$

where the predicted label class is the maximiser of this probability:

$$Cat(\mathbb{Q}(Y^*)) = \underset{j\in\{1,\ldots J\}}{\arg\max}\, \mathbb{Q}(Y^* = j)$$

3. Uncertainty Quantification Review

Notes taken from a review paper by Abdar et al. (2021).

There are two main types of uncertainty: aleatoric and epistemic. Epistemic uncertainty is the model uncertainty (i.e. choosing to fit the data with a quadratic function when the data is sinusoidal) and can be formulated as a probability distribution over the model parameters. Aleatoric uncertainty is the irreducible uncertainty of the data (data uncertainty) and considered an inherent property of the data distribution. Aleatoric uncertainty can be further divided into homoscedastic and heteroscedastic uncertainties.

3.1 Monte Carlo Dropout

Estimate epistemic uncertainty by applying MC dropout with Bernoulli distribution at the output of the neurons of a NN. Different options for dropout-based methods include Bernoulli/Gaussian dropout of either the nodes of a NN or the weights of a NN.

3.2 Markov Chain Monte Carlo

This uses MCMC to estimate intractable posterior distributions. There are issues with the required iterations for sufficient burn-in of the sampler being unknown, an issue with MCMC that extends beyond uncertainty quantification.

3.3 Variational Inference

An approximation method learning the posterior distribution over BNN weights.

3.4 Ensemble Techniques

NNs generally have competitive accuracy but poor predictive uncertainty quantification, usually generating overconfident predictions. Calibration and domain shift are two evaluation measures used to evaluate the quality of predictive uncertainty. Calibration measures the discrepancy between long-run frequencies and subjective forecasts. Domain shift quantifies the generalisation of predictive uncertainty to a domain shift in the data (i.e. trained on cats and dogs but then asked to make a prediction on a bird). Quantifies if the model is aware of what it does/doesn't know.

An ensemble of models enhances predictive performance, but it's not immediately obvious why it would generate good uncertainty estimation. Bayesian model averaging (BMA) holds belief that the true model lies within the hypothesis class of the prior $\mathcal{H}$. Ensembles combine models to discover more powerful models, so they can be expected to be better when true model does not lie in $\mathcal{H}$.

An evaluation approach for measuring uncertainty estimators in vision problems can be found in Gustafsson et al. (2020).

Measures of spread or "disagreement" of ensembles such as mutual information can be used to assess uncertainty in predictions due to knowledge uncertainty:

$$\mathcal{MI}\left[y, \theta | \mathbf{x}^*, \mathcal{D}\right] = H[\mathbb{E}_{p(\theta|\mathcal{D})}[P(y|\mathbf{x}^*, \theta)]] - \mathbb{E}_{p(\theta|\mathcal{D})}[H[y|\mathbf{x}^*, \theta]]$$

where:

- $\mathcal{MI}[y, \theta|\mathbf{x}^*, \mathcal{D}]$ is the knowledge uncertainty
- $H[\mathbb{E}_{p(\theta|\mathcal{D})}[P(y|\mathbf{x}^*, \theta)]]$ is the total uncertainty
- $\mathbb{E}_{p(\theta|\mathcal{D})}[H[y|\mathbf{x}^*, \theta]]$ is the expected data uncertainty (i.e. regions of severe class overlap)

Two situations: all models have similar uncertainty distribution are very uncertain for each label (data uncertainty) or the models in the ensemble have very different predictions (model uncertainty).

3.5 Other Uncertainty Quantification Methods

Neural Architecture Distribution Search (NADS) finds an appropriate distribution of different architectures that perform significantly well on a specified task.

explored the training dynamics of over-parameterised NNs under natural gradient descent. They showed that the discrepancy between NNs trained on non-linearised and linearised natural gradient descent is smaller than that of standard gradient descent. Also, that empirically there was no need to formulate a limit argument about the width of the neural network layers, as the discrepancy was small for over-parameterised NNs.

BNNs have been used as a solution for NN predictions but specifying priors is still an open problem. Independent normal prior in weight space leads to weak constraints on function posterior, allowing it to generalise in unanticipated ways on OOD data. Noise contrastive priors (NCPs) used to estimate consistent uncertainty by Hafner et al. (2020).

Mixup is a DNN training technique where extra samples are produced during training by convexly integrating random pairs of images and their labels. Thulasidasan et al. (2019) showed that this provided much better model calibration and was less likely to yield overconfident predictions using random noise and OoD data.

Adversarial training can eradicate the vulnerability in a single model by forcing it to learn more robust features, but this approach is rigid and suffers from substantial loss on clean data accuracy. Ensemble techniques can be induced to have diverse sub-models robust to a transfer adversarial example.

Gaussian processes do not scale well, but a common technique is to have a variational GP using inducing samples. Deep Gaussian processes represent a multilayer hierarchy of Gaussian processes.

Most weight perturbation-based algorithms suffer from high variance of gradient estimation due to sharing the same perturbations among all samples in a mini-batch. Flipout by Wen et al. (2018) is an approach that samples pseudo-independent weight perturbations for each input to decorrelate the gradients within a minibatch.

DNNs have been successful with complex high-dimensional image data but are not robust to adversarial examples as shown in Szegedy et al. (2013). Bradshaw et al. (2017) proposed a hybrid model of GP and DNNs (GPDNNs) to deal with the uncertainty caused by adversarial examples. Convolutional structures have also been introduced into GPs such as in Van der Wilk et al. (2017).

4. Neural Tangents

Notes taken from Novak et al. (2019).

The infinite-width limit of a large class of Bayesian neural networks become Gaussian Processes with specific, architecture-dependent, compositional kernel, forming a Neural Network Gaussian Process (NNGP) model. Kernels can be defined with recurrence relationships for a wide range of non-linearities (activation functions), convolutional layers, residual connections, and pooling. Neural Tangent Kernels (NTK) relates to the gradient descent training of the infinite-width limit of a Bayesian Neural Network. Infinite-width kernels that cannot be constructed analytically can be approximated by Monte Carlo sampling.

Neural Tangents provide framework for automatic construction of infinite-width kernels that would otherwise need to be derived for each new architecture by hand.

References

Moloud Abdar, Farhad Pourpanah, Sadiq Hussain, Dana Rezazadegan, Li Liu, Mohammad Ghavamzadeh, Paul Fieguth, Xiaochun Cao, Abbas Khosravi, U Rajendra Acharya, et al. A review of uncertainty quantification in deep learning: Techniques, applications and challenges. *Information Fusion*, 76:243–297, 2021.

John Bradshaw, Alexander G de G Matthews, and Zoubin Ghahramani. Adversarial examples, uncertainty, and transfer testing robustness in gaussian process hybrid deep networks. *arXiv preprint arXiv:1707.02476*, 2017.

Fredrik K Gustafsson, Martin Danelljan, and Thomas B Schon. Evaluating scalable bayesian deep learning methods for robust computer vision. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops*, pages 318–319, 2020.

Danijar Hafner, Dustin Tran, Timothy Lillicrap, Alex Irpan, and James Davidson. Noise contrastive priors for functional uncertainty. In *Uncertainty in Artificial Intelligence*, pages 905–914. PMLR, 2020.

Alexander Graeme de Garis Matthews. *Scalable Gaussian process inference using variational methods*. PhD thesis, University of Cambridge, 2017.

Roman Novak, Lechao Xiao, Jiri Hron, Jaehoon Lee, Alexander A Alemi, Jascha Sohl-Dickstein, and Samuel S Schoenholz. Neural tangents: Fast and easy infinite neural networks in python. *arXiv preprint arXiv:1912.02803*, 2019.

Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*, 2013.

Sunil Thulasidasan, Gopinath Chennupati, Jeff A Bilmes, Tanmoy Bhattacharya, and Sarah Michalak. On mixup training: Improved calibration and predictive uncertainty for deep neural networks. *Advances in Neural Information Processing Systems*, 32, 2019.

Mark Van der Wilk, Carl Edward Rasmussen, and James Hensman. Convolutional gaussian processes. *Advances in Neural Information Processing Systems*, 30, 2017.

Yeming Wen, Paul Vicol, Jimmy Ba, Dustin Tran, and Roger Grosse. Flipout: Efficient pseudo-independent weight perturbations on mini-batches. *arXiv preprint arXiv:1803.04386*, 2018.

Veit D Wild, Robert Hu, and Dino Sejdinovic. Generalized variational inference in function spaces: Gaussian measures meet bayesian deep learning. *arXiv preprint arXiv:2205.06342*, 2022.