# Uncertainty in Deep Learning & The case of Bayesian Deep Learning

Presenter: Son Nguyen

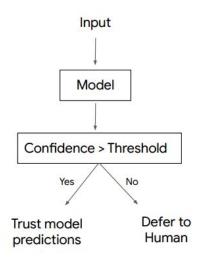
Machine Learning Group, VinAl Research

# Why need uncertainty in Deep Learning

- Uncertainty estimation: critical problem (applicable <-- reliable) in Intelligent Systems</p>
  - provide **confidence** along with prediction: *the model knows what it doesn't know*
  - go beyond **accuracy** regime: toward **model calibration** in Deep Learning (DL)

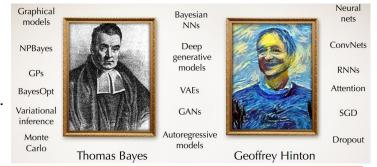
#### ❖ Applications:

- Safety, Trustworthy systems: autonomous driving, medical diagnosis, and meteorological forecasting.
- Active learning, Continual learning, Reinforcement learning, Bayesian optimization, Decision making: trade off exploration-exploitation, stability-plasticity, memorization-adaptation



# What Bayesian Deep Learning

- **Bayesian Deep Learning (BDL)**: general principle, structural probabilistic approach
  - intersection of Bayesian method and deep learning
  - Bayesian neural nets, deep latent variable models, and related learning techniques are particular treatments of BDL.
  - Advances in BDL: <u>Bayesian Deep Learning workshops</u>



In supervised tasks, BDL provide considerable improvements in *accuracy and calibration* compared to standard training, while retaining scalability.

- ❖ A main goal: exploring a renowned class of BDL Bayesian neural nets (BNNs)
  - the core direction promoting the research of uncertainty quantification in DL
  - but, has many controversies in the community

## Content

## A. Uncertainty in Deep Learning

- 1. Background
- 2. Main approaches
- 3. The state-of-the-art and a unified perspective
- 4. Some potential research

## B. Bayesian neural network and its controversies

- 1. Why Bayesian neural nets
- 2. Expressive or simple approximate posterior distribution
- 3. Tempered or original true posterior distribution
- 4. Informative or vague prior distribution

This presentation involves various works of Yarin Gal (OATML), Andrew G. Wilson (NYU), B. Lakshminarayanan (Google), Dustin Tran (Google), Max Welling (UvA) and many others.

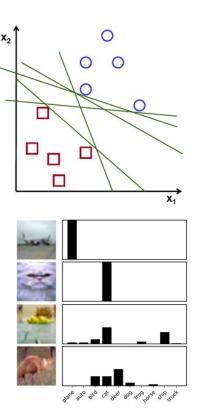
## Content

## A. Uncertainty in Deep Learning

- 1. Background
  - a. Sources of uncertainty
  - b. Disentangle types of uncertainty
  - c. Metrics for uncertainty quantification
  - d. Common criticism of traditional neural nets uncertainty
- 2. Main approaches
- 3. The state-of-the-art and a unified perspective
- 4. Some potential research

# Source of uncertainty: [NeurlPS-17]

Model uncertainty, a.k.a epistemic uncertainty	capture our ignorance about which model generated our collected data
	incurred by lack of training data, imbalanced/sparse data, out-of-distribution data
	reducible with more data (vanish in the limit of infinite data)
Data uncertainty, a.k.a aleatoric uncertainty	capture noise inherent in the data
	caused by inherent noise, ambiguous/missing data, human bias
	irreducible with more data



#### Disentangle types of uncertainty

- Disentangling and reasoning about uncertainty is critical, but **non-trivial**, for applications:
  - active learning [NeurlPS-19]
  - o out-of-distribution detection
  - semantic segmentation [NeurlPS-17]
  - o fraud detection, forecast

#### Disentangle types of uncertainty [UAI-18]

epistemic and aleatoric uncertainty are <u>distinguishable under Bayesian models:</u>

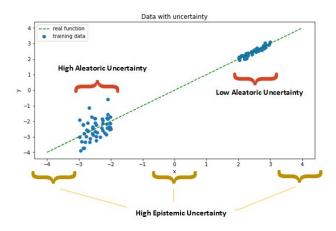
Model parameters W governed by a prior p(W), and  $p(W|\mathcal{D})$  is a posterior given the training data  $\mathcal{D}$ . The **predictive distribution** for a new datapoint (x,y) is:  $p(y|x,\mathcal{D}) = \mathbb{E}_{p(W|\mathcal{D})} p(y|x,W)$ 

- $\circ$  the predictive entropy  $\mathbb{H}[y|x,\mathcal{D}]$  of  $p(y|x,\mathcal{D})$  is defined by predictive uncertainty
- o predictive uncertainty is **total uncertainty** of epistemic and aleatoric uncertainty.

$$\underbrace{\mathbb{H}[Y|x,\mathcal{D}]}_{\text{predictive}} = \underbrace{\mathbb{I}[Y;w|x,\mathcal{D}]}_{\text{epistemic}} + \underbrace{\mathbb{E}_{p(W|\mathcal{D})}[\mathbb{H}[Y|x,w]]}_{\text{aleatoric (for iD }x)}$$

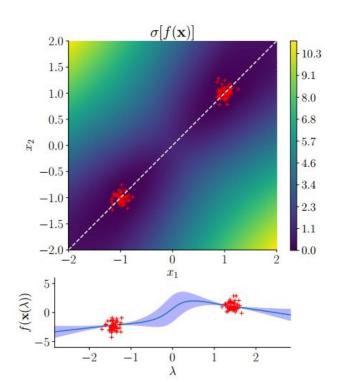
In Bayesian linear regression case:

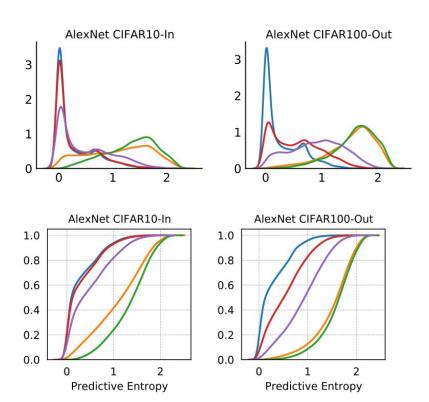
$$\mathbb{V}(y|x,\mathcal{D}) = \phi(x)^T \Sigma \phi(x) + \sigma^2$$



#### **❖** Metrics for uncertainty quantification

How to represent uncertainty: heat map, predictive variance, predictive entropy (PDF, CDF).





#### Metrics for uncertainty quantification

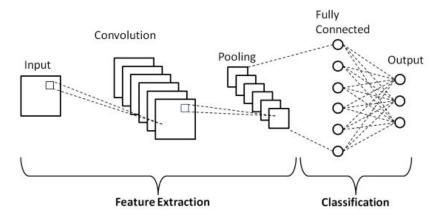
- How to measure the quality of uncertainty:
  - p predictive log-likelihood:  $\mathbb{E}_{x\sim\mathcal{D}}\log[\mathbb{E}_{p(W|\mathcal{D})}p(y|x,W)]$
  - $\circ$  calibration error (CE) [ICML-17]: suppose a model predict a class y with probability  $\hat{p}$

$$\text{CE} = |\text{Prob}(Y = y | \hat{p} = p) - p|$$
 
$$\text{ECE} = \sum_{b=1}^{B} \frac{n_b}{N} |\text{acc}(b) - \text{conf}(b)|$$
 Confidence < Accuracy => Underconfident => Underconfident => Underconfident

SCE = 
$$\frac{1}{K} \sum_{k=1}^{K} \sum_{b=1}^{B} \frac{n_{bk}}{N} |\operatorname{acc}(b, k) - \operatorname{conf}(b, k)|$$

with acc(b, k) and conf(b, k) are the accuracy and confidence of bin b for class label k

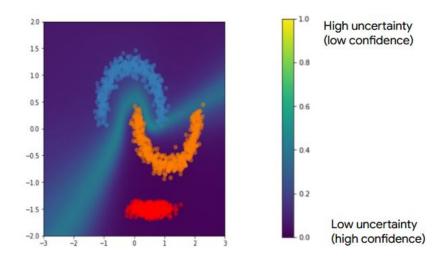
- Common criticism of traditional neural nets uncertainty
- **Trend**: larger and more accurate models produce poorly calibrated predictions.
- **Disentangle** epistemic and aleatoric uncertainty is non-trivial: use **softmax entropy** in general.
- **Softmax** deterministic neural nets can not capture epistemic uncertainty: **feature collapse** (theory and empirical results) --> extractor can map OOD sample to iD regions in feature space (local constant representation). [ICML-20]



When training using empirical risk minimisation, *features not relevant to classification accuracy* can simply be ignored by the feature extractors.

- Common criticism of traditional neural nets uncertainty
- NNs do not generalize well under distribution shift.
   but, NNs do not know when they do not know.
  - Clean Severity = 3 Severity = 4 Severity = 5 0.2 0.1 -0.0 -0.30 0.20 0.10

 Models assign high confidence predictions to OOD data



# **Summary**

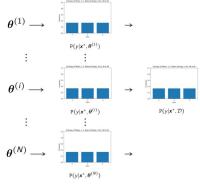
- Source of uncertainty: epistemic (lack of data) and aleatoric (noise inherent)
- Disentangle epistemic and aleatoric is non-trivial, but possible with Bayesian models:

$$\underbrace{\mathbb{H}[Y|x,\mathcal{D}]}_{\text{predictive}} = \underbrace{\mathbb{I}[Y;w|x,\mathcal{D}]}_{\text{epistemic}} + \underbrace{\mathbb{E}_{p(W|\mathcal{D})}[\mathbb{H}[Y|x,w]]}_{\text{aleatoric (for iD }x)}$$

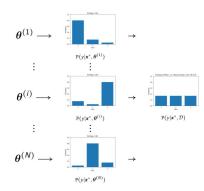
In Bayesian linear regression case:

$$\mathbb{V}(y|x,\mathcal{D}) = \phi(x)^T \Sigma \phi(x) + \sigma^2$$

A connection with bias-variance trade-off:  $y = f(x) + \epsilon$ 



high aleatoric



high epistemic

$$\mathbb{E}_{y}\mathbb{E}_{p(W|\mathcal{D})}\Big[y-\widehat{f}\left(x,W
ight)|\mathcal{D}=\mathcal{D}_{train}\Big]^{2}=\left(f(x)-\mathbb{E}_{p(W|\mathcal{D})}\left[\widehat{f}\left(x,W
ight)
ight]
ight)^{2}+\mathbb{V}_{p(W|\mathcal{D})}\left[\widehat{f}\left(x,W
ight)
ight]+\sigma^{2}$$

- Measure deep network models: predictive accuracy (generalization), likelihood/ECE/SCE (model calibration)
- Criticisms of traditional deep learning uncertainty: poor generalization under distribution shift, uncalibrated and
  overconfident prediction, inability to capture epistemic uncertainty (feature collapse)

# Content

## A. Uncertainty in Deep Learning

- 1. Background
- 2. Main approaches
  - a. Bayesian neural nets
  - b. Ensemble methods
  - c. Deterministic uncertainty estimation
- 3. The state-of-the-art and a unified perspective
- 4. Some potential research

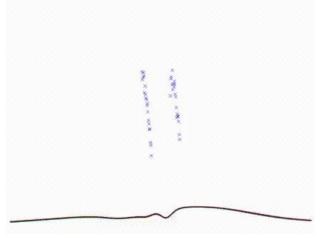
#### ❖ Bayesian neural nets

- ullet treat weight parameters W as a random variable and impose a prior distribution p(W)
- ullet infer a posterior distribution over W instead of point estimation:

$$p(\mathbf{W}|\mathcal{D}) = \frac{p(\mathcal{D}|\mathbf{W})p(W)}{p(\mathcal{D})} = \frac{p(\mathcal{D}|\mathbf{W})p(W)}{\int p(\mathcal{D}|\mathbf{W})p(\mathbf{W})}$$

At test time: predictive distribution is approximated via MC sampling:

$$p(\mathbf{y} \mid \mathbf{x}, \mathcal{D}) = \int p(\mathbf{y} \mid \mathbf{x}, \mathbf{W}) p(\mathbf{W} \mid \mathcal{D}) d\mathbf{W} = \frac{1}{S} \sum_{s=1}^{S} p(\mathbf{y} \mid \mathbf{x}, \mathbf{W}^{(s)})$$



#### ❖ Bayesian neural nets

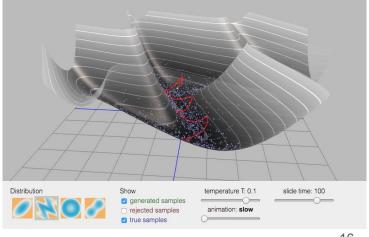
BNN posterior  $p(W|\mathcal{D})$ : intractable, very high dimensional, complicated structure --> approximate inference

- Gradient-based stochastic approximation:
  - energy-based perspective
  - o simulate dynamical systems whose stationary distribution as desired target distribution
  - the true posterior samples is generated via discretizing differential equations describing those dynamics

#### Methods:

- Hamiltonian Monte Carlo (HMC): gold standard
- Stochastic Gradient Hamiltonian Monte Carlo (SGHMC) (ICML-14)
- Stochastic Gradient Langevin Dynamics (SGLD) (<u>ICML-12</u>)

**Pros and Cons:** high fidelity approximation, but large complexity, many potential biases



#### **❖** Bayesian neural nets

BNN posterior  $p(W|\mathcal{D})$ : intractable, very high dimensional, complicated structure --> approximate inference

- **Deterministic approximation:** local approximation
  - $\circ$  Laplace approximation:  $p(W|\mathcal{D}) = \mathcal{N}(W_{MAP}, H^{-1})$  with  $H = \partial^2 \log p(y|x,W)/\partial W^2 + \lambda I$
  - Variational inference: employ a parametric variational distribution  $q_{\phi}(\mathbf{W})$  and minimize  $\mathbb{D}_{KL}(q_{\phi}(\mathbf{W}) || p(\mathbf{W} | \mathcal{D}))$  equivalent to maximizing variational lower bound:

$$\mathcal{L}(\phi) = \mathbb{E}_{q_{\phi}(\mathbf{W})} \log p(\mathcal{D}|\mathbf{W}) - \mathbb{D}_{KL}(q_{\phi}(\mathbf{W}) || p(\mathbf{W}))$$

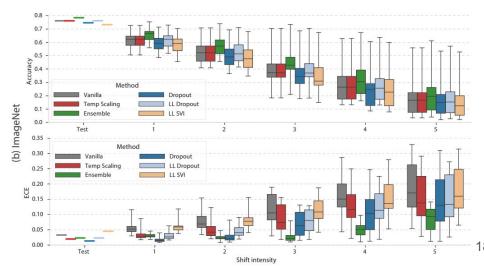
- **Mean-field VI**:  $q_{\phi}(\mathbf{W})$  is factorized distribution (e.g diagonal Gaussian)
- Dropout inference: MC Dropout, Variational Gaussian Dropout --> complementary benefits
- Subspace inference (<u>UAI-19</u>): inspired by effective dimensionality / intrinsic dimension in deep learning

$$\mathcal{S} = \{W|W = \widehat{W} + z_1v_1 + \ldots + z_Kv_K\} = \{W|W = \widehat{W} + Pz\}$$

\*\*sub-network (ICML-21):  $p(\mathbf{W}|\boldsymbol{y},\boldsymbol{X}) \approx p(\mathbf{W}_S|\boldsymbol{y},\boldsymbol{X}) \prod \delta(\mathbf{w}_r - \mathbf{w}_r^*) \approx q(\mathbf{W}_S) \prod \delta(\mathbf{w}_r - \mathbf{w}_r^*)$ 

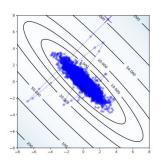
#### Ensemble methods

- Deep ensemble (<u>NeurIPS-16</u>): training (regularized) MLE with different random seeds and averaging final score
  - o inspired by classical ensemble methods: bootstrap, bagging, boosting
  - o loss landscape is highly non-convex --> different local optima --> explore the diversity from multimodality.
  - very simple, but work surprisingly well in practice



#### **Ensemble methods** \*

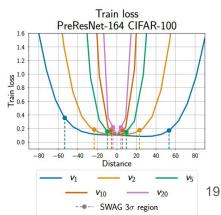
- Stochastic Weight Averaging Gaussian (SWAG) (NeurlPS-19)
  - **Motivated by the theory:** SGD with constant learning rate simulates a Markov chain with a stationary distribution --> SGD iterations is approximately sampling from a Gaussian distribution (JMLR-17)



Utilize SGD iterations  $\{W_i\}_{i=1}^T$  to empirically estimate *first-two moments* of a Gaussian:  $p(W|\mathcal{D}) = \mathcal{N}(\mu, \Sigma)$ 

$$\mu = rac{1}{T} \sum_t W_t \qquad \Sigma = rac{1}{T-1} \sum_t \left( W_t - \overline{W}_t 
ight) \left( W_t - \overline{W}_t 
ight)^T \left[ \left( + rac{1}{T} ext{diag} \left( rac{1}{T} \sum_{i=1}^T W_i^2 - \mu^2 
ight) 
ight) 
ight]$$

- **Properties:** 0
  - require: SGD with *large constant* or *cyclical learning rates*
  - practical runtime ~ SGD training
  - Averaging Weights Leads to Wider Optima and Better Generalization (SWA PyTorch lib) (ICML-18)
  - captures the local geometry of the posterior surprisingly well

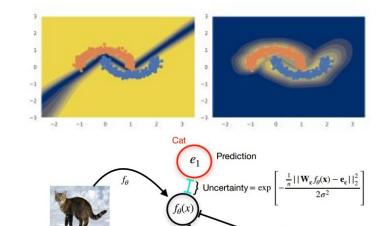


Deterministic uncertainty estimation (DUE)

**Motivation**: overcome limitations of softmax neural nets uncertainty

--> using only single forward-pass

- Deterministic uncertainty estimation (DUE)
- DUE with RBF network. (ICML-20)
  - classes represented by centroids
  - predictive uncertainty computed via RBF kernel
    - --> better than Deep ensemble uncertainty
  - use exponential moving average update to stabilize training
    - --> achieve competitive accuracy softmax models.
  - alleviate feature collapse with two-side Gradient penalty
    - sensitivity: capture changes in inputs
    - smoothness: optimization & generalization



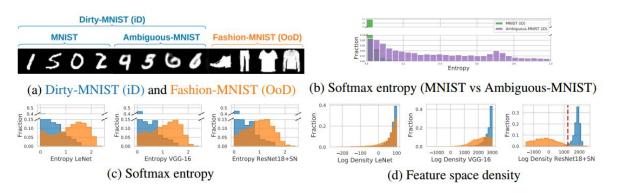
$$K_c(f_{\theta}(\mathbf{x}), \mathbf{e}_c) = \exp\left[-\frac{\frac{1}{n}||\mathbf{W}_c f_{\theta}(\mathbf{x}) - \mathbf{e}_c||_2^2}{2\sigma^2}\right]$$
$$L(\mathbf{x}, \mathbf{y}) = -\sum_c y_c \log(K_c) + (1 - y_c) \log(1 - K_c)$$

$$\lambda \cdot \left[\|
abla_{\mathbf{x}} \sum_c K_c\|_2^2 - L
ight]^2 \longrightarrow \ L_1 \|\mathbf{x}_1 - \mathbf{x}_2\|_I \leq \|K_c(\mathbf{x}_1) - K_c(\mathbf{x}_2)\|_F \leq L_2 \|\mathbf{x}_1 - \mathbf{x}_2\|_I$$

What about softmax nets + enforcing-sensitivity ?

- Deterministic uncertainty estimation (DUE)
- DUE with softmax nets + inductive bias + feature-space density (<u>arXiv-21</u>).
  - o gradient penalty, spectral normalization are appropriate inductive biases enforcing sensitivity
  - o penalize **spectral normal** of deterministic networks weights, then:
    - **softmax entropy** can capture aleatoric uncertainty, but can not estimate epistemic uncertainty
    - ullet use **feature-space density** q(z), with  $z=f_{ heta}(x)$  to capture epistemic uncertainty
    - combine feature-space density and the softmax entropy via Gaussian Discriminant Analysis (GDA)

q(y,z)=q(y)q(z|y) ----> disentangle epistemic and aleatoric uncertainty



# Content

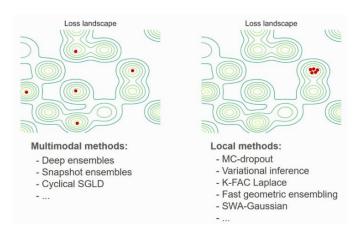
## A. Uncertainty in Deep Learning

- 1. Background
- 2. Main approaches
- 3. The state-of-the-art and a unified view
  - a. Deep ensemble and hybrid variants
  - b. Bayesian model averaging
- 4. Some potential research

- **❖** Deep ensemble and functional perspective (<u>arXiv-20</u>)
- Consistent experimental results: Deep ensemble
  - very simple, but work surprisingly well in practice
  - outperforms SWAG, practical BNNs approximations (MFVI, MC Dropout), particularly under dataset shift.
  - but has much computational overhead

#### • A functional perspective:

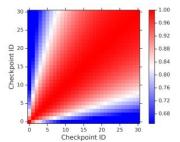
- o desiderata from ensembling for a good approximation of predictive distribution: high-performing but diverse
  - similar predictions will be redundant in the model averaging
  - crucial for quantifying epistemic uncertainty [NeurlPS-17]
- Main point: deep ensembles tend to explore diverse modes in functional space.

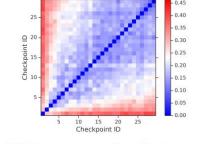


#### \* Deep ensemble and functional perspective

Similarity of functions within and across randomly initialized trajectories

#### SGD single trajectory



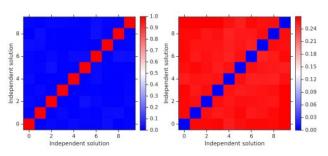


(b) Disagreement of predictions

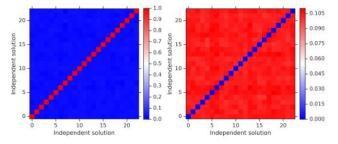
(a) Cosine similarity of weights

 $\cos(W_1,W_2) = rac{W_1^T W_2}{\|W_1\|*\|W_2\|} \quad rac{1}{N} \sum_{n=1}^N [f(x_n;W_1) 
eq f(x_n;W_2)]$ 

#### **Deep Ensemble**



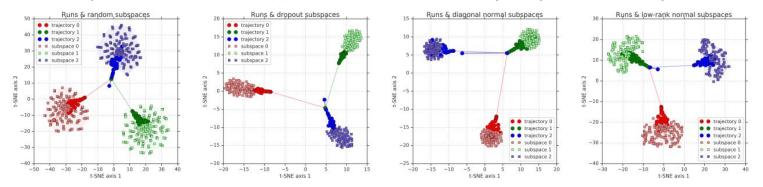
#### (a) Results using SmallCNN



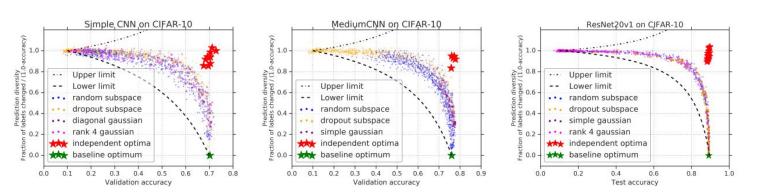
(b) Results using ResNet20v1

#### Deep ensemble and functional perspective

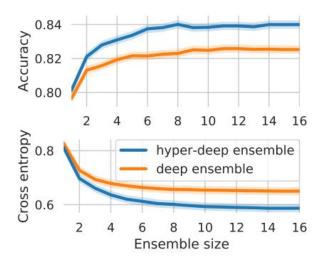
Similarity of functions of local approximations from each trajectory and across trajectories



#### • Diversity versus Accuracy plots



- **❖** Several variants of deep ensemble
  - Hyperparameter ensembles (<u>NeurIPS-20</u>): random search over different hyperparameters



- **Several variants of deep ensemble:** *inspired by sharing parameters*
- Batch ensemble (ICLR-20): efficient ensembles by sharing parameters

$$y_n = \phi\left(\overline{W}_i^{\top} x_n\right)$$

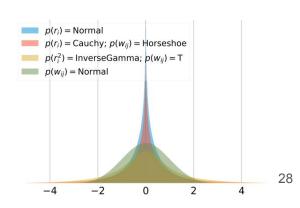
$$= \phi\left(\left(W \circ r_i s_i^{\top}\right)^{\top} x_n\right) \xrightarrow{\text{parallelize}}$$

$$= \phi\left(\left(W^{\top} (x_n \circ r_i)\right) \circ s_i\right) \qquad Y = \phi\left(\left((X \circ R)W\right) \circ S\right)$$

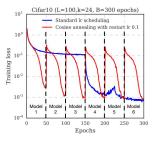
weight matrix (slow weight)...  $\mathbf{s}_1^\top$   $\mathbf{s}_2^\top$   $\mathbf{w}_1 = \mathbf{w} \circ \mathbf{r}_1 \mathbf{s}_1^\top$   $\mathbf{w}_2 = \mathbf{w} \circ \mathbf{r}_2 \mathbf{s}_2^\top$ 

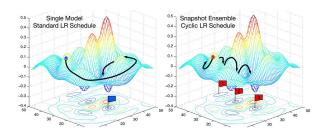
 Rank 1 - BNNs (<u>ICML-20</u>): learn rank-1 perturbation via variational inference, exploit hierarchical prior with non-centered parameterization

$$egin{aligned} \mathcal{L} &= -\mathbb{E}_{q(r)q(s)} \log p(\mathcal{D}|W,r,s) \ &+ \mathbb{KL}(q(r)\|p(r)) + \mathbb{KL}(q(s)\|p(s)) - \log p(W) \end{aligned}$$

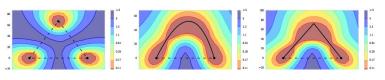


- ❖ Several variants of deep ensemble: inspired by loss landscape
- Snapshot ensemble (ICLR-17): training SGD with cyclicial learning rate schedule --> train 1, get M for free

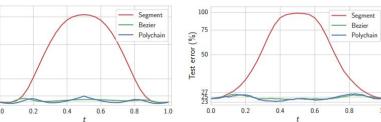




 Fast Geometric Ensemble (<u>NeurIPS-18</u>): ensembling over <u>low-loss tunnel</u> connecting two minima --> cost of conventional training

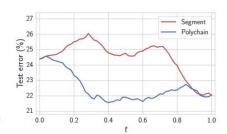


Train loss



Polygonal chain: 
$$\phi_{\theta}(t) = \begin{cases} 2 \left( t\theta + (0.5 - t) \hat{w}_1 \right), & 0 \le t \le 0.5 \\ 2 \left( (t - 0.5) \hat{w}_2 + (1 - t)\theta \right), & 0.5 \le t \le 1. \end{cases}$$

Bezier curve: 
$$\phi_{\theta}(t) = (1-t)^2 \hat{w}_1 + 2t(1-t)\theta + t^2 \hat{w}_2, \ 0 \le t \le 1.$$



\*\* high-performing but diverse ensemble not need different minima.

Bayesian model averaging: unifying ensemble and Bayes

## Bayes vs Ensembles: What's the difference?

Both aggregate predictions over a collection of models. There are two core distinctions.

#### The space of models.

**Bayes** posits a prior that weighs different probability to different functions, and over an infinite collection of functions.

**Ensembles** weigh functions equally a priori and use a finite collection

#### Model aggregation.

**Bayesian** models apply averaging, weighted by the posterior.

**Ensembles** can apply any strategy and have non-probabilistic interpretations.

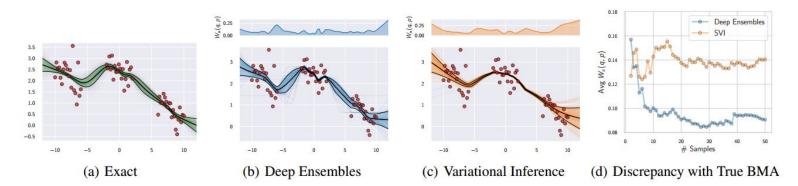
- --> but all for **same goal**: to compute an accurate predictive distribution
- --> do not need samples from a posterior, or even a faithful approximation to the posterior.

- **Bayesian model averaging (NeurIPS-20):** unifying ensemble and Bayes
  - derived from marginalization procedure: key distinguishing property of Bayesian method.
  - an ensemble containing many **high-performing** but **diverse** models:

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

- o consider the BMA integral *separately from* the simple Monte Carlo approximation in BNNs
- $\circ$  Deep ensemble is non-Bayesian method, but can be treated as a compelling approach of BMA with  $p(w|\mathcal{D})pprox \sum_j \delta(w=w_j)$

is a mixture of delta functions. (facilitates D.E to disentangle epistemic from predictive uncertainty)



# The state-of-the-art and a unified perspective

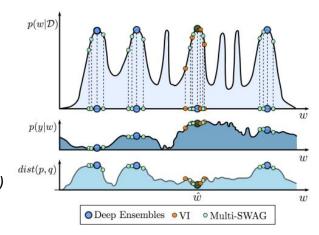
**Bayesian model averaging:** unifying ensemble and Bayes

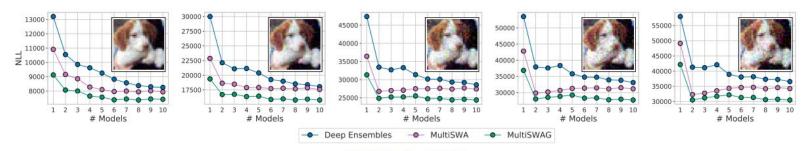
#### Why BMA is actually compelling for deep learning?

- motivated by classical theory of statistical models
- evidenced by extensive empirical results
- provide complementary benefits:

Ensemble MC-Dropout, Multi-SWAG, Multi-SWA

(Ensemble + local approximate/SWA can outperform Deep ensemble)



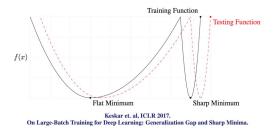


# The state-of-the-art and a unified perspective

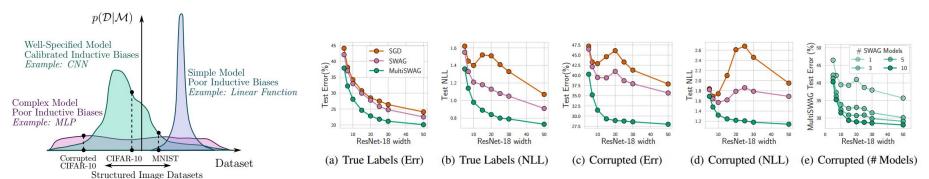
**❖ Bayesian model averaging:** unifying ensemble and Bayes

#### Why BMA is actually compelling for deep learning?

provide intriguing perspectives on many problems of deep learning







# **Content**

## A. Uncertainty in Deep Learning

- 1. Background
- 2. Main approaches
- 3. The state-of-the-art and a unified perspective
- 4. Some potential research

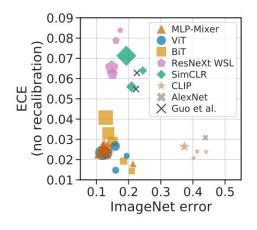
# Some potential research

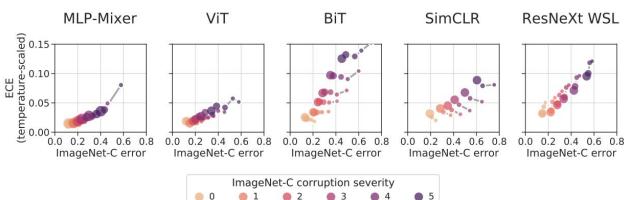
#### Some comments:

- improving model calibration under **distribution shift** is challenging, but prerequisite in practice: **robustness**
- understanding **predictive distribution** is promising to improving model calibration
  - o exploring functional Bayesian neural nets
- subspace inference suggests integrating **Bayesian-like layers** into deep architectures.

# Some potential research

- **Beyond principled approaches:** Stop thinking about just probability distributions. Leverage the inductive biases of core DL techniques --> improve significantly model calibration.
  - test-time data augmentation
  - ullet mixup training:  $x=lpha x_1+(1-lpha)x_2, y=lpha y_1+(1-lpha)y_2$
  - more modern and more accurate architectures (<u>arXiv-21</u>): MLP-Mixer, Vision Transformer --> **reversed trends** 
    - o in-distribution: calibration slightly deteriorates with increasing model size
    - o under distribution shift: accuracy and calibration are correlated, calibration improves with model size





# Content

## B. Bayesian neural network and its controversies

- 1. Why Bayesian neural nets
- 2. Expressive or simple approximate posterior distribution
- 3. Tempered or original true posterior distribution
- 4. Informative or vague prior distribution