



# **Trustworthy Machine Learning on Imbalance Data**

## **Jiangchao Yao**

**CMIC, Shanghai Jiao Tong University**

饮水思源。爱国荣校

#### Large-scale natural sources are very imbalance, usually following a long-tailed distribution.









[1] Van Horn et al. The iNaturalist Species Classification and Detection Dataset. CVPR 2018. [2] Gregory et al. CXR-LT challenge. ICCV CVAMD 2023.

#### [3]<https://worldmapper.org/maps/urban-population-relative-2014/> [4]<https://seopressor.com/blog/short-tail-or-long-tail-keywords/>

#### **A direct decomposition on the risk minimization**

$$
\min_{f} R(f) = E_{P(x,y)}[\ell(f(x), y)] = \sum_{k=1}^{K} P(y = k) E_{P(x|y=k)}[\ell(f(x), y)]
$$

Minority ("generalized" conceptual) classes have weak importance for training, which can be easily ignored in the early phase especially for overparameterized DNNs [1] *(or namely, will be sacrificed first if it is not sufficient for the model to learn)*.

**However**, in real applications, the value of classes cannot be absolutely characterized by their quantity, and instead, sometimes **less is more** for sustainable long-term development.

- **Fairness** w.r.t. diversity e.g., small populations of gender, race and consumers
- **Cost-sensitive scenarios** e.g., medical disease diagnosis and treatment





#### **A critical highlight on the evaluation, different from the ordinary IID learning**



The change in evaluation metric induces **an statistical consistency problem** on applying conventional learning methods, that is,

*What we design during training should be statistically consistent with what we pursue about the evaluation.*



### The development of imbalance learning



[1] Karakoulas et al. Optimizing Classifers for Imbalanced Training Sets. NIPS 1998.

- [2] He et al. Learning from Imbalanced Data. TKDE 2009.
- [3] Fernández et al. Learning from Imbalanced Data Sets. Springer, 2018.
- [4] Zhang et al. Deep Long-tailed Learning: A Survey. TPAMI 2023.



# **Retrospection-I: Re-Sampling**



## SMOTE: Synthetic Minority Over-sampling Technique

Motivation: Replication of the minority class does not cause its decision boundary to spread into the majority class region (but overfitting).



The main idea of SMOTE: augmentation for minority class by interpolation instead of over-sampling with replacement.



Interpolation is limited by the samples. Thus, SMOTE also always runs with the under-sampling for majority class.

Increase minority diversity and decrease majority diversity

Chawla, Nitesh V., et al. "SMOTE: Synthetic Minority Over-Sampling Technique." *JAIR 2002*.

# **Retrospection-II: Threshold-Moving Method**

## Threshold-Moving: adjust the prediction in a post-hoc manner.

Motivation: The over-confident prediction for majority or the low-confident prediction for minority can be calibrated after training.

THE THRESHOLD-MOVING ALGORITHM

#### **Training phase:**

- Let  $S$  be the original training set.
- Train a neural network from  $S$ . 2.

#### **Test phase:**

- Generate real-value outputs with the trained neural network.
- For every output, multiply it with the sum of the costs of misclassifying the corresponding class to other classes.
- Return the class with the biggest output.

#### **Moving function**

$$
\hat{p}_k = \frac{p_k * \sum_{k'=1}^K C[k][k']}{\eta}
$$

where  $p_k$  is the probabilistic prediction,  $C[k][k']$  is the cost mis-predicted from class k to  $k'$ , and  $\eta$  is renormalization parameter.

Sampling methods might not always show promise in multi-class imbalance learning, but threshold-moving way does.



Let  $p_k = \frac{e^{z_k}}{\sum_{k=0}^{k} a_k^2}$  $\sum_{k=1}^{e^{-k}} C[k][k'] = e^{-\tau \log \pi_k}$ <br>  $\sum_{k=1}^{K} C[k][k'] = e^{-\tau \log \pi_k}$ where  $\pi_k$  is the class prior and  $\tau$  is the temperature, the threshold-moving method recovers the popular **logit adjustment** method for long-tailed learning.

Majority classes have the smaller cost than minority classes, e.g.,  $e^{-\tau \log \pi_k}$  is monotonously decreasing.

Zhou, Z. H., & Liu, X. Y. Training Cost-Sensitive Neural Networks with Methods Addressing the Class Imbalance Problem. *TKDE, 2005*.

# **Retrospection-III: Pseudo Labeling**



# COG: Local Decomposition for Rare Class Analysis

Intuition: Quantity imbalance limits the learning pace of minority over majority. We can adjust the quantities by decompositi on.

**How to properly decompose the majority classes (or including minority classes) into subclasses to balance the training?** 



Wu. J. J. et al. COG: Local Decomposition for Rare Class Analysis. *DMKD, 2010*.

# **Retrospection-IV: Theory for Imbalance Learning**

### On Statistical Consistency of Binary Classification with Balanced Accuracy

Motivation: The early ERM theory is developed for the instance-wise evaluation, but cannot guarantee the consistency for balanced measure.

$$
\text{Accuracy} = \mathbb{E}_{p(x,y)}[h(x) = y] \qquad \qquad \text{Balanced Accuracy} = \frac{\sum_{k \in \{-1,1\}} \mathbb{E}_{p(x|y=k)}[h(x) = k]}{2}
$$

#### **If we consider the balanced accuracy, how to modify the algorithm to satisfy the statistical consistency?**

**Theorem 3.** Let D be a probability distribution on  $\mathcal{X} \times \{\pm 1\}$  satisfying Assumption A. Let  $\widehat{p}_S$  denote any estimator of  $p = P(y = 1)$  satisfying  $\widehat{p}_S \in (0, 1)$  and  $\widehat{p}_S \stackrel{P}{\rightarrow} p$ . Let  $\widehat{\eta}_S : \mathcal{X} \rightarrow [0,1]$  denote any class probability estimator satisfying  $\mathbf{E}_{x}[\widehat{\eta_{S}}(x) - \eta(x)^{r}] \stackrel{P}{\to} 0$  for some  $r \ge 1$ , and let  $h_{S}(x) = \frac{\text{sign}(\widehat{\eta}_{S}(x) - \widehat{p}_{S})}{\text{sign}(\widehat{\eta}_{S}(x) - \widehat{p}_{S})}$ . Then regret ${}_{D}^{\text{AM}}[h_S] \stackrel{P}{\rightarrow} 0$ .

\n- **Algorithm 1** Plug-in with Empirical Threshold
\n- 1: **Input:** 
$$
S = ((x_1, y_1), \ldots, (x_n, y_n)) \in (\mathcal{X} \times \{\pm 1\})^n
$$
\n- 2: **Select:** (a) Proper (composite) loss  $\ell : \{\pm 1\} \times \mathbb{R} \to \mathbb{R}_+$ , with link function  $\psi : [0, 1] \to \mathbb{R}$ ; (b) RKHS  $\mathcal{F}_K$  with positive definite kernel  $K : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ ; (c) regularization parameter  $\lambda_n > 0$
\n- 3:  $f_S \in \text{argmin}_{f \in \mathcal{F}_K} \left\{ \frac{1}{n} \sum_{i=1}^n \ell(y_i, f(x_i)) + \lambda_n \|f\|_K^2 \right\}$
\n- 4:  $\hat{\eta}_S = \psi^{-1} \circ f_S$
\n- 5:  $\hat{p}_S = (\text{as in Eq. (2)})$
\n- 6: **Output:** Classifier  $h_S(x) = \text{sign}(\hat{\eta}_S(x) - \hat{p}_S)$
\n





## Summary of imbalanced learning in the early years







### **What is the new of this topic in the recent years?**



The recent advances of imbalance learning powered by deep learning







## **It has been contributed with very broad explorations**





[1] Zhang et al. "Deep Long-Tailed Learning: A Survey" TPAMI 2023.



#### loss re-weighting by effective number

➢ **Intuition:** Non-overlapping sample number, instead of the vanilla quantity number, playing the role of imbalance



- ➢ **Effective Number:** The effective number of examples is the expected volume of samples.
	- $E_n = (1 \beta^n)/(1 \beta)$ where  $\beta = (N-1)/N$  $\lim_{\beta \to 1} E_n = n$
- ➢ **Class-Balanced Loss:** Training from imbalanced data by introducing a weighting factor that is inversely proportional to the effective number of samples.

The class-balanced loss term can be applied to a wide range of deep networks and loss functions.



➢ **Class-Balanced Loss:** The class-balanced (CB) loss can be written as:

$$
CB(\mathbf{p}, y) = \frac{1}{E_{n_y}} \mathcal{L}(\mathbf{p}, y) = \frac{1 - \beta}{1 - \beta^{n_y}} \mathcal{L}(\mathbf{p}, y) \quad CB_{\text{softmax}}(\mathbf{z}, y) = -\frac{1 - \beta}{1 - \beta^{n_y}} \log \left( \frac{\exp(z_y)}{\sum_{j=1}^{C} \exp(z_j)} \right)
$$

It can also be combined with **sigmoid cross-entropy loss, focal loss**, etc.





The proposed framework provides a non-parametric means of quantifying data overlap.

[1] Cui et al. "Class-Balanced Loss Based on Effective Number of Samples" CVPR 2019.



#### Class-wise margin calibration

➢ **Motivation:** for imbalanced learning, there is a class-distribution-aware margin trade-off for generalization error.

The generalization error is proportional to the following (two classes, and same holds for multiple classes)



[1] Cao et al. "Learning Imbalanced Datasets with Label-Distribution-Aware Margin Loss" NeurIPS 2019.





➢ **LDAM:** The authors define their hinge loss function (and its relaxed version via Softmax)

$$
\mathcal{L}_{\text{LDAM-HG}}((x, y); f) = \max(\max_{j \neq y} \{z_j\} - z_y + \Delta_y, 0)
$$
  
where  $\Delta_j = \frac{C}{n_j^{1/4}}$  for  $j \in \{1, ..., k\}$ 





The margin definition is an approximation to the truth value, and whether we should directly add on the logit space?

<sup>17</sup> [1] Cao et al. "Learning Imbalanced Datasets with Label-Distribution-Aware Margin Loss" NeurIPS 2019.

#### Class-wise logit adjustment [1]

➢ **Motivation:** Design a consistent loss function that allows for a relatively elastic margin in the logit for head and tail.

➢ **Balanced error:** Under class imbalance, to measure balanced error:

$$
\operatorname{BER}(f) \doteq \frac{1}{L} \sum\nolimits_{y \in [L]} \mathbb{P}_{x|y} \Big( y \notin \operatorname{argmax}_{y' \in \mathcal{Y}} f_{y'}(x) \Big)
$$

Under Bayes-optimal prediction, if  $\mathbb{P}^{\text{bal}}(y \mid x) \propto \mathbb{P}(y \mid x)/\mathbb{P}(y)$ 

Then

$$
\mathrm{argmax}_{y \in [L]} \mathbb{P}^{\mathrm{bal}}(y \mid x) = \mathrm{argmax}_{y \in [L]} \exp(s_y^*(x)) / \mathbb{P}(y) = \mathrm{argmax}_{y \in [L]} s_y^*(x) - \ln \mathbb{P}(y)
$$

[1] Menon et al. "Long-tailed Learning via Logit Adjustment" ICLR 2021.

#### ➢ **The logit adjusted softmax cross-entropy**

$$
\ell(y, f(x)) = -\log \frac{e^{f_y(x) + \tau \cdot \log \pi_y}}{\sum_{y' \in [L]} e^{f_{y'}(x) + \tau \cdot \log \pi_{y'}}} = \log \left[1 + \sum_{y' \neq y} \left(\frac{\pi_{y'}}{\pi_y}\right)^{\tau} \cdot e^{(f_{y'}(x) - f_y(x))}\right]
$$

 $w_1^{\top} \Phi(x)/\pi_1 < w_2^{\top} \Phi(x)/\pi_2 \nleftrightarrow_{\leftarrow} \exp(w_1^{\top} \Phi(x))/\pi_1 < \exp(w_2^{\top} \Phi(x))/\pi_2.$ 

➢ **Post-hoc logit adjustment**

$$
\operatorname{argmax}_{y \in [L]} \exp(w_y^\top \Phi(x)) / \pi_y^\tau = \operatorname{argmax}_{y \in [L]} f_y(x) - \tau \cdot \log \pi_y
$$



<sup>19</sup> [1] Menon et al. "Long-tailed Learning via Logit Adjustment" ICLR 2021.

➢ **An remarkable point on the statistical consistency of long-tailed multi-class classification** 

$$
\ell(y, f(x)) = \alpha_y \cdot \log \left[ 1 + \sum_{y' \neq y} e^{\Delta_{yy'}} \cdot e^{(f_{y'}(x) - f_y(x))} \right]
$$

**Theorem 1.** For any  $\delta \in \mathbb{R}^L_+$ , the pairwise loss in (11) is Fisher consistent with weights and margins

$$
\alpha_y = \delta_y / \mathbb{P}(y) \qquad \Delta_{yy'} = \log (\delta_{y'}/\delta_y).
$$

Letting  $\delta_y = \pi_y$ , we immediately deduce that the logit-adjusted loss of (10) is consistent, *provided* our  $\pi_y$  is a consistent estimate of  $\mathbb{P}(y)$ . Similarly,  $\delta_y = 1$  recovers the classic result that the balanced loss is consistent. While Theorem 1 only provides a sufficient condition in multi-class setting, one can provide a necessary and sufficient condition that rules out other choices of  $\Delta$  in the binary case.

<sup>20</sup> [1] Menon et al. "Long-tailed Learning via Logit Adjustment" ICLR 2021.

# **Supervised Long-tailed Learning**



#### Dynamic adjustment based on a fine-grained generalization bound

**Proposition 3** (Data-Dependent Bound for the VS Loss). Given the function set  $F$  and the VS loss  $L_{VS}$ , for any  $\delta \in (0,1)$ , with probability at least  $1-\delta$  over the training set S, the following generalization bound holds for all  $f \in \mathcal{F}$ :

$$
\mathcal{R}_{bal}^{L}(f) \precsim \Phi(L_{VS}, \delta) + \frac{\hat{\mathfrak{C}}_{\mathcal{S}}(\mathcal{F})}{C\pi_C} \sum_{y=1}^{C} \alpha_y \tilde{\beta}_y \sqrt{\pi_y} \left[1 - \text{softmax} \left(\beta_y B_y(f) + \Delta_y\right)\right]
$$

$$
L_{\text{VS}}(f(\boldsymbol{x}), y) = -\alpha_y \log \left( \frac{e^{\beta_y f(\boldsymbol{x})_y + \Delta_y}}{\sum_{y'} e^{\beta_{y'} f(\boldsymbol{x})_{y'} + \Delta_{y'}}} \right).
$$



[1] Wang et al. "A Unified Generalization Analysis of Re-Weighting and Logit-Adjustment for Imbalanced Learning" NeurIPS  $2023<sub>21</sub>$ 

### Is self-supervised learning more robust to data imbalance?



- Supervised learning (SL) only extracts features that are useful for predicting labels  $(e_1)$
- Self-supervised learning (SSL) learns task-irrelevant features regardless of the labels, which enables richer and more robust representation  $(e_1, e_2)$

[1] Liu et al. "Self-supervised Learning is More Robust to Dataset Imbalance." ICLR 2021.

### Self-supervised learning still suffers from data imbalance

 $\triangleright$  Performance degeneration: Linear probing on imbalanced data  $(D_i)$  and balanced data  $(D_b)$  with same data amount



➢ Representation learning disparity: head classes dominate the feature regime but tail classes passively collapse



[1] Jiang et al. "Self-damaging contrastive learning." ICML 2021.

[2] Zhou et al. "Combating Representation Learning Disparity with Geometric Harmonization." NeurIPS 2023.

# **Model-based Self-Supervised Long-tailed Learning**



## SDCLR: Self-damaging Contrastive Learning

- ➢ **Intuition:** The sensitivity of head and tail samples to the model pruning, are very different, which helps us to anchor and promote the training of tail samples.
- ➢ **Pruning identified exemplars (PIE)** systematically investigates the model output changes introduced by pruning and finds that certain examples are particularly sensitive to sparsity. They are high likely to be rare and atypical samples, which probably comes from tail classes.





Non-PIE

PIE



[1] Jiang et al. "Self-damaging contrastive learning." ICML 2021.

# BCL: Boosted Contrastive Learning

- ➢ Motivation I: Memorization effect still holds under long-tailed distribution.
- ➢ Motivation II: Stronger information discrepancy motivates tail samples mining.
- ➢ **Challenge:** how to **detect tail data**  and how to construct the **desired information discrepancy**





➢ Motivated from the observation that *learning speed-based proxy* shows strong correlation with the memorization score[1], BCL extends the memorization estimation to *self-supervised learning.*

$$
\mathcal{L}_{i,0}^{m} = \mathcal{L}_{i,0}, \quad \mathcal{L}_{i,t}^{m} = \beta \mathcal{L}_{i,t-1}^{m} + (1-\beta) \mathcal{L}_{i,t} \qquad \mathbf{M}_{i,t} = \frac{1}{2} \left( \frac{\mathcal{L}_{i,t}^{m} - \bar{\mathcal{L}}_{t}^{m}}{\max \{ |\mathcal{L}_{i,t}^{m} - \bar{\mathcal{L}}_{t}^{m}| \}_{i=0,...,N}} + 1 \right)
$$
\n
$$
\Psi(x_i; \mathcal{A}, \mathbf{M}_i) = a_1(x_i) \circ \dots \circ a_k(x_i),
$$
\n
$$
a_j(x_i) = \begin{cases} A_j(x_i; \mathbf{M}_i \zeta) & u \sim \mathcal{U}(0,1) \& u < \mathbf{M}_i \\ x_i & \text{otherwise} \end{cases} \quad \mathcal{L}_{\text{BCL}} = \frac{1}{N} \sum_{i=1}^N -\log \frac{\exp \left( \frac{f(\Psi(x_i))^\top f(\Psi(x_i^+))}{\tau} \right)}{\sum_{x_i' \in X'} \exp \left( \frac{f(\Psi(x_i))^\top f(\Psi(x_i'))}{\tau} \right)}
$$

Adaptively assigns the appropriate augmentation strength for the individual sample according to the feedback from the memorization clues

[1] Jiang et al. "Characterizing structural regularities of labeled data in overparameterized models." ICML 2021 [2] Zhou et al. "Contrastive learning with boosted memorization. " ICML 2022.

### BCL: Boosted Contrastive Learning



- ➢ Calculate memorization scores based on historical statistics to detect tail.
- ➢ Construct instance-wise augmentations to enhance representation learning.



[1] Zhou et al. "Contrastive learning with boosted memorization. " ICML 2022.

### GH: Geometric Harmonization

➢ Why the conventional contrastive learning underperforms in self-supervised long-tailed context?

Conventional contrastive loss motivates *sample-level uniformity*, which is biased towards the head classes.



Contrastive learning causes severer representation learning disparity when enlarging the imbalance ratios.

#### **Geometric Uniform Structure Surrogate Label Allocation**  $\mathbf{M}_i^{\top} \cdot \mathbf{M}_j = C, \ \forall i, j \in \{1, 2, ..., K\}, i \neq j,$

Any two vectors in **M** have the same angle, namely, the unit space are equally partitioned by the vectors.



$$
\min_{\hat{\mathbf{Q}} = [\hat{\boldsymbol{q}}_1, \dots, \hat{\boldsymbol{q}}_N]} \mathcal{L}_{\text{GH}} = -\frac{1}{|\mathcal{D}|} \sum_{\boldsymbol{x}_i \sim \mathcal{D}} \hat{\boldsymbol{q}}_i \log \boldsymbol{q}_i, \\ \text{s.t.} \quad \hat{\mathbf{Q}} \cdot \mathbb{1}_N = N \cdot \boldsymbol{\pi}, \ \hat{\mathbf{Q}}^\top \cdot \mathbb{1}_K = \mathbb{1}_N,
$$

#### **Overall objective**

$$
\min_{\theta, \hat{\mathbf{Q}}} \mathcal{L} = \mathcal{L}_{\text{InfoNCE}} + w_{\text{GH}} \mathcal{L}_{\text{GH}},
$$

[1] Zhou et al. "Combating Representation Learning Disparity with Geometric Harmonization." NeurIPS 2023.



### Still require more efforts on this way









