# Learning Bounds for Open-Set Learning

Zhen Fang

ICML | 2021

AAII, University of Technology Sydney

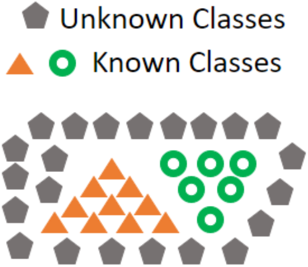
June 2021

# Open-Set Learning

**Definition (Domain)**

Given a feature space $\mathcal{X} \subset \mathbb{R}^d$ and a label space $\mathcal{Y}$, a domain is a joint distribution $P_{X,Y}$, where random variables $X \in \mathcal{X}$, $Y \in \mathcal{X}$.

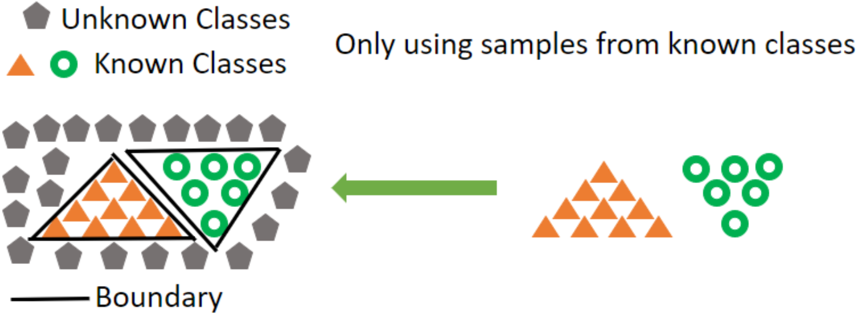
*Known classes* are a subset of $\mathcal{Y}$. We define the label space of known classes as $\mathcal{Y}_k$. Then, the *unknown classes* are from the space $\mathcal{Y}/\ \mathcal{Y}_k$.



# Open-Set Learning

**Definition (Open-Set Learning)**

Given i.i.d. samples $S = \{(\mathrm{x}^i, \mathrm{y}^i)\}_{i=1}^n$ drawn from $P_{X,Y|Y \in \mathcal{Y}_k}$. The aim of open-set learning is to train a classifier $f$ using $S$ such that $f$ can classify
1) the sample from known classes into correct known classes;
2) the sample from unknown classes into unknown classes.



# Main Idea

Aim to construct an auxiliary domain, which has larger support set than that of the known distribution $P_{X,Y|Y\in\mathcal{Y}_k}$. By transferring unknown information from unknown classes of the auxiliary domain, we can recognize the unknown classes.

**Step 1.** Given an auxiliary distribution $U$ such that $P_{X,Y|Y\in\mathcal{Y}_k} \ll U$;

**Step 2.** Construct a weight function $w$ such that $P_{X,Y|Y\in\mathcal{Y}_k} \approx wU$;

**Step 3.** Construct a weight transformation $L_{\tau,\beta}$ such that the density $L_{\tau,\beta}(w)U$ of unknown classes is $\beta$;

**Step 4.** Transfer knowledge from $L_{\tau,\beta}(w)U$ to $P_{X,Y}$.

# Main Theoretical Results

**Generalization Error for Open-Set Learning**

Given mild assumptions, any $\epsilon_0 > 0$ and samples $S$ with size $n$, there exists an algorithm $A_{\epsilon_0}$ whose output belongs to a hypothesis space $\mathcal{H}$, the estimation error of $A_{\epsilon_0}$ is close to $O(\sqrt{1/n})$, i.e.,

$$|R_P^\alpha(A_{\epsilon_0}(S)) - \min_{\boldsymbol{h}\in\mathcal{H}} R_P^\alpha(\boldsymbol{h})| \leq O_p(\sqrt{1/n}) + \epsilon_0,$$

where $R_P^\alpha$ is the risk for open-set learning and $O_p$ is related to $\epsilon_0$.

The generalization error bound proved in our work provides the first almost-PAC-style guarantee on open-set learning.

# Proposed Algorithm

Based on our theory, we minimize a proxy risk:

$$\widetilde{R}^{\tau,\beta}_{S,T}(\boldsymbol{h}) := \widehat{R}_S(\boldsymbol{h}) + \frac{\alpha\gamma'}{1-\alpha}\widehat{R}^{\tau,\beta}_{S,T,u}(\boldsymbol{h}),$$

where $\widehat{R}_S(\boldsymbol{h})$ is the risk for known classes and $\widehat{R}^{\tau,\beta}_{S,T,u}(\boldsymbol{h})$ is the risk for unknown classes, i.e., given $m$ auxiliary data $T$ from $U$,

$$\widehat{R}^{\tau,\beta}_{S,T,u}(\boldsymbol{h}) := \frac{1}{m}\sum_{\mathrm{x}\in T} L^{-}_{\tau,\beta}(\widehat{w}(\mathrm{x}))\ell(\boldsymbol{h}(\mathrm{x}), \mathrm{y}_{C+1}),$$

here

$$L^{-}_{\tau,\beta}(x) = \begin{cases} x+\beta, & x \leq \tau; \\ 0, & 2\tau \leq x; \\ -\dfrac{\tau+\beta}{\tau}x + 2\tau + 2\beta, & \tau < x < 2\tau. \end{cases} \quad (1)$$

# Experiments

- The performance on dataset MNIST, CIFAR-10 using F1 scores. Dark colour means best performance.

| Algorithm | Omniglot | MNIST-Noise | Noise |
|---|---|---|---|
| Openmax | 0.780 | 0.816 | 0.826 |
| CROSR | 0.793 | 0.827 | 0.826 |
| CGDL | **0.850** | 0.887 | 0.859 |
| Ours (AOSR) | 0.825 | **0.953** | **0.953** |

| Algorithm | ImageNet-crop | ImageNet-resize | LSUN-crop | LSUN-resize |
|---|---|---|---|---|
| Openmax | 0.660 | 0.684 | 0.657 | 0.668 |
| CROSR | 0.721 | 0.735 | 0.720 | 0.749 |
| CGDL | **0.840** | **0.832** | 0.806 | 0.812 |
| Ours (AOSR) | 0.798 | 0.795 | **0.839** | **0.838** |

# Acknowledgements

Acknowledgements: The work introduced in this paper was supported by the Australian Research Council (ARC) under FL190100149.

# Thank You

Thank You !