PGADA:

Perturbation-Guided Adversarial Alignment for Few-shot Learning Under the Support-Query Shift

Siyang Jiang[1,2], Wei Ding[1], Hsi-Wen Chen[1], Ming-Syan Chen[1]

May 18, 2022

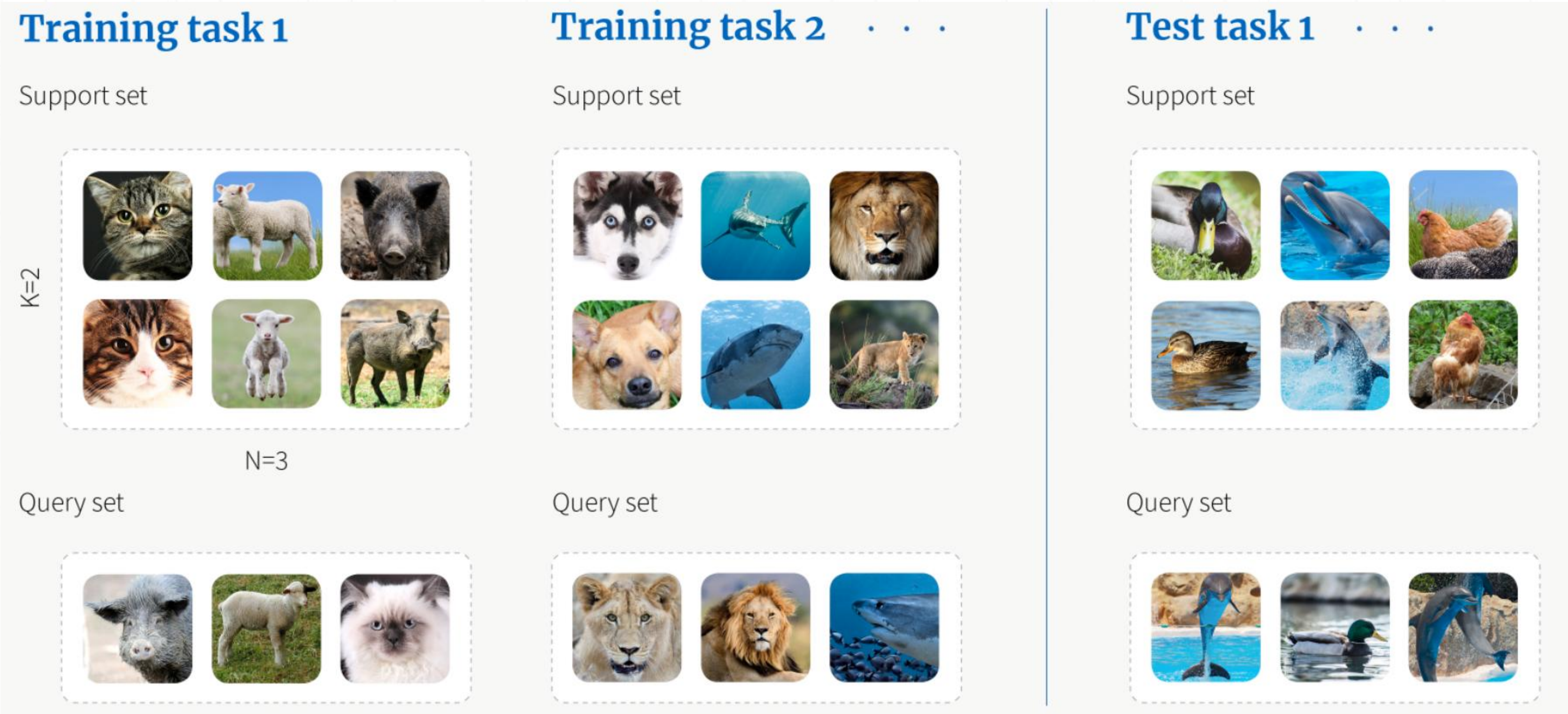
1.National Taiwan Univerisity;
2.Huizhou University

Outlines

- Background
- Challenges
- Motivation
- Methodology
- Result
- Conclusion

Background

- Few-shot Learning (FSL)



Few-Shot Learning

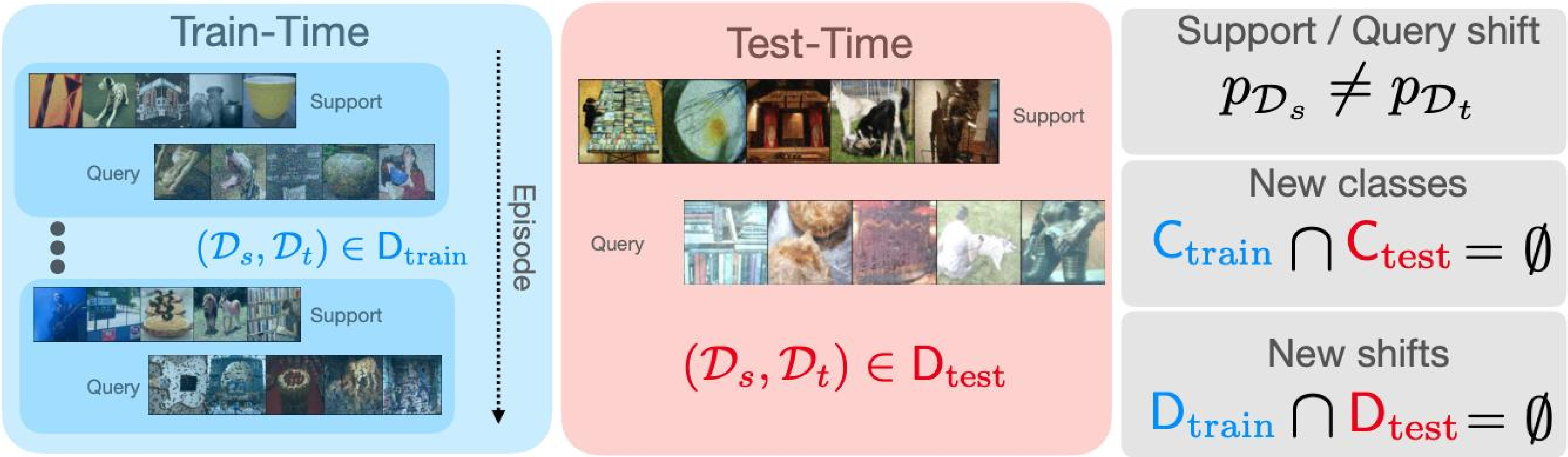
Background

◆ Support-Query Shift Few-shot Learning (SQS-FSL)

FSL

SQS-FSL

Chanllenges



Motivation

- Theoretical foundation
- A robust feature from images
- A better alignment plan for the support and query set

Motivation

- Theoretical foundation

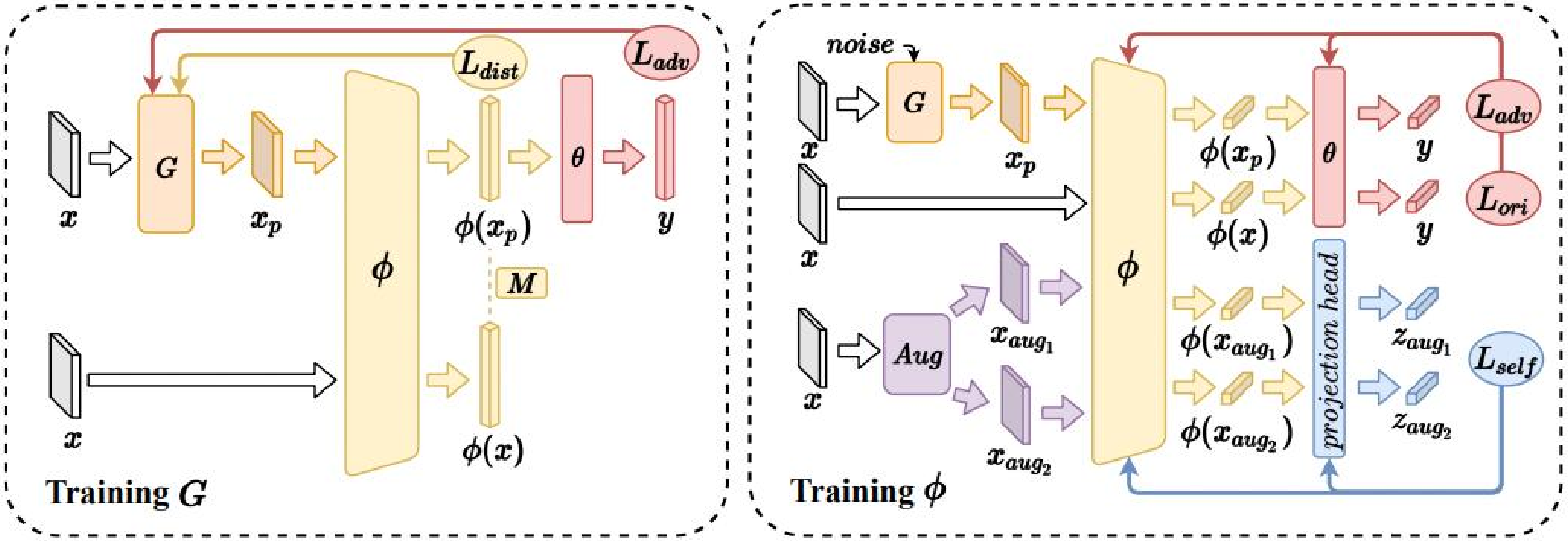
Theorem 1. *The error of the transported embedding is*

$$E[\|\hat{\phi}(x_{s,i}) - \hat{\phi}_{\sigma}(x_{s,i})\|_2^2] = \sqrt{d(\sigma_s^2 + \sigma_q^2)},$$

where $\hat{\phi}_{\sigma}(x_{s,i})$ *is the transported embedding from the perturbed distribution* $W_{\sigma}(\mu_s, \mu_q)$. $W_{\sigma}(\mu_s, \mu_q) := W(\mu_s * \mathcal{N}_{\sigma_s}, \mu_q * \mathcal{N}_{\sigma_q})$ *denotes the original support and query set distributions* μ_s *and* μ_q *being perturbed with Gaussian noises* σ_s *and* σ_q, *and* $*$ *is the convolution operator.*

Methodology

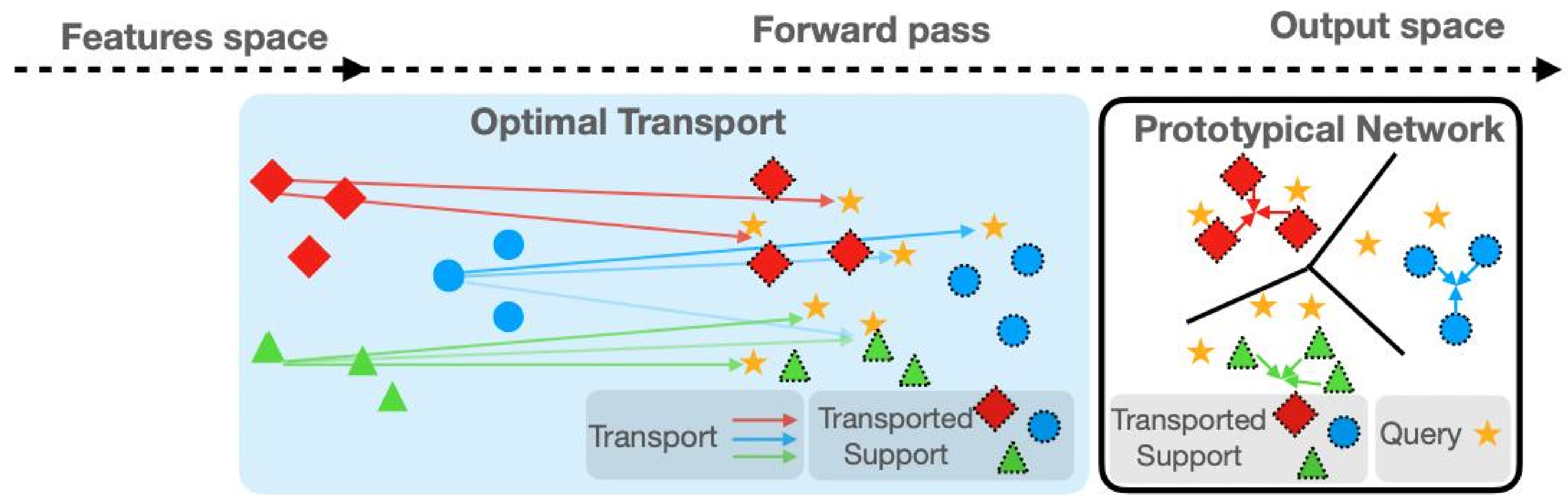
- A robust feature from images



$$\min_{\phi,\theta} L_{ori} + \lambda_1 L_{adv} + \lambda_2 L_{self},$$

Methodology

- A better alignment plan for support and query set



Methodology

- A better alignment plan for support and query set

$$\pi^* = \arg\min_{\pi} \sum_{\substack{x_{s,i} \sim \hat{\mu}_s \\ x_{q,j} \sim \hat{\mu}_q}} \beta w(x_{s,i}, x_{q,j}) \pi(x_{s,i}, x_{q,j}) + \boxed{(1-\beta)\pi(x_{s,i}, x_{q,j}) \log \pi(x_{s,i}, x_{q,j}),}$$

Result

Dataset	CIFAR100				miniImageNet				FEMNIST
	8-target		16-target		8-target		16-target		1-target
	1-shot	5-shot	1-shot	5-shot	1-shot	5-shot	1-shot	5-shot	1-shot
Few-shot Learning									
MatchingNet [30]	$30.71_{\pm 0.38}$	$41.15_{\pm 0.45}$	$31.00_{\pm 0.34}$	$41.83_{\pm 0.39}$	$35.26_{\pm 0.50}$	$44.75_{\pm 0.55}$	$37.20_{\pm 0.48}$	$44.22_{\pm 0.52}$	$84.25_{\pm 0.71}$
ProtoNet [26]	$30.02_{\pm 0.40}$	$42.77_{\pm 0.47}$	$30.29_{\pm 0.33}$	$42.52_{\pm 0.41}$	$36.37_{\pm 0.50}$	$47.58_{\pm 0.57}$	$35.69_{\pm 0.45}$	$46.29_{\pm 0.53}$	$84.31_{\pm 0.73}$
TransPropNet [21]	$34.15_{\pm 0.39}$	$47.39_{\pm 0.42}$	$34.20_{\pm 0.40}$	$44.31_{\pm 0.38}$	$24.10_{\pm 0.27}$	$27.24_{\pm 0.33}$	$25.38_{\pm 0.30}$	$28.05_{\pm 0.30}$	$86.42_{\pm 0.76}$
FTNET [10]	$28.91_{\pm 0.37}$	$37.28_{\pm 0.40}$	$28.66_{\pm 0.31}$	$37.37_{\pm 0.33}$	$39.02_{\pm 0.46}$	$51.27_{\pm 0.45}$	$39.70_{\pm 0.40}$	$52.00_{\pm 0.37}$	$86.13_{\pm 0.71}$
TP [2]	$34.00_{\pm 0.46}$	$49.71_{\pm 0.47}$	$35.55_{\pm 0.41}$	$50.24_{\pm 0.39}$	$40.49_{\pm 0.54}$	$59.85_{\pm 0.49}$	$43.83_{\pm 0.51}$	$55.87_{\pm 0.42}$	$93.63_{\pm 0.63}$
Adversarial Data Augmentation									
MixUp [34]	$37.82_{\pm 0.47}$	$52.57_{\pm 0.47}$	$38.52_{\pm 0.42}$	$53.33_{\pm 0.40}$	$42.98_{\pm 0.54}$	$57.22_{\pm 0.48}$	$43.64_{\pm 0.48}$	$57.33_{\pm 0.42}$	$97.22_{\pm 0.46}$
CutMix [33]	$39.36_{\pm 0.48}$	$54.76_{\pm 0.48}$	$40.05_{\pm 0.44}$	$55.44_{\pm 0.40}$	$35.50_{\pm 0.52}$	$45.50_{\pm 0.56}$	$35.78_{\pm 0.48}$	$44.85_{\pm 0.52}$	$96.89_{\pm 0.49}$
Autoencoder [24]	$39.05_{\pm 0.50}$	$53.24_{\pm 0.47}$	$39.82_{\pm 0.44}$	$53.88_{\pm 0.40}$	$45.36_{\pm 0.56}$	$57.69_{\pm 0.51}$	$45.65_{\pm 0.52}$	$57.39_{\pm 0.44}$	$96.53_{\pm 0.43}$
AugGAN [16]	$39.54_{\pm 0.50}$	$53.05_{\pm 0.47}$	$39.50_{\pm 0.45}$	$53.42_{\pm 0.39}$	$44.65_{\pm 0.55}$	$57.55_{\pm 0.50}$	$44.91_{\pm 0.49}$	$57.10_{\pm 0.42}$	$96.42_{\pm 0.52}$
MaxEntropy [36]	$38.14_{\pm 0.40}$	$51.02_{\pm 0.56}$	$38.21_{\pm 0.34}$	$51.33_{\pm 0.52}$	$48.21_{\pm 0.36}$	$57.67_{\pm 0.63}$	$48.99_{\pm 0.21}$	$59.01_{\pm 0.44}$	$97.19_{\pm 0.51}$
MaxUp [13]	$34.84_{\pm 0.44}$	$47.51_{\pm 0.46}$	$35.20_{\pm 0.40}$	$47.63_{\pm 0.39}$	$37.62_{\pm 0.55}$	$48.65_{\pm 0.58}$	$38.13_{\pm 0.50}$	$49.19_{\pm 0.51}$	$96.48_{\pm 0.53}$
Ours									
PGADA (ProtoNet)	$42.16_{\pm 0.52}$	$\mathbf{56.52}_{\pm \mathbf{0.47}}$	$\mathbf{42.73}_{\pm \mathbf{0.46}}$	$\mathbf{56.83}_{\pm \mathbf{0.40}}$	$55.44_{\pm 0.61}$	$\mathbf{67.34}_{\pm \mathbf{0.49}}$	$55.69_{\pm 0.62}$	$\mathbf{66.90}_{\pm \mathbf{0.50}}$	$\mathbf{97.98}_{\pm \mathbf{0.40}}$
PGADA (MatchingNet)	$\mathbf{42.25}_{\pm \mathbf{0.53}}$	$50.98_{\pm 0.45}$	$42.60_{\pm 0.45}$	$51.80_{\pm 0.39}$	$\mathbf{56.15}_{\pm \mathbf{0.61}}$	$63.08_{\pm 0.49}$	$\mathbf{56.12}_{\pm \mathbf{0.57}}$	$63.61_{\pm 0.45}$	$97.96_{\pm 0.39}$

Table 1: Accuracy comparison of the three datasets with two types of baselines.

Result

Dataset	CIFAR100				miniImageNet				FEMNIST
	8-target		16-target		8-target		16-target		1-target
	1-shot	5-shot	1-shot	5-shot	1-shot	5-shot	1-shot	5-shot	1-shot
PGADA	$\mathbf{42.16}_{\pm 0.52}$	$\mathbf{56.52}_{\pm 0.47}$	$\mathbf{42.73}_{\pm 0.46}$	$\mathbf{56.83}_{\pm 0.40}$	$\mathbf{55.44}_{\pm 0.61}$	$\mathbf{67.34}_{\pm 0.49}$	$\mathbf{55.69}_{\pm 0.62}$	$\mathbf{66.90}_{\pm 0.50}$	$\mathbf{97.98}_{\pm 0.40}$
Generator									
fixed G	$38.58_{\pm 0.48}$	$52.41_{\pm 0.47}$	$39.26_{\pm 0.43}$	$52.67_{\pm 0.39}$	$43.50_{\pm 0.55}$	$55.65_{\pm 0.50}$	$43.48_{\pm 0.51}$	$55.42_{\pm 0.43}$	$96.41_{\pm 0.52}$
w/o noise	$37.16_{\pm 0.47}$	$50.12_{\pm 0.46}$	$37.73_{\pm 0.41}$	$50.50_{\pm 0.38}$	$44.06_{\pm 0.56}$	$56.97_{\pm 0.48}$	$44.42_{\pm 0.49}$	$56.96_{\pm 0.42}$	$96.89_{\pm 0.48}$
w/o KL	$37.30_{\pm 0.47}$	$50.79_{\pm 0.46}$	$37.91_{\pm 0.42}$	$51.35_{\pm 0.39}$	$44.22_{\pm 0.54}$	$55.04_{\pm 0.49}$	$44.21_{\pm 0.49}$	$53.96_{\pm 0.41}$	$96.49_{\pm 0.48}$
Regularized Optimal Transport (OT)									
w/o OT	$35.76_{\pm 0.41}$	$54.06_{\pm 0.45}$	$35.66_{\pm 0.35}$	$54.09_{\pm 0.38}$	$44.30_{\pm 0.52}$	$61.23_{\pm 0.53}$	$44.15_{\pm 0.46}$	$60.86_{\pm 0.48}$	$94.03_{\pm 0.48}$
TP [2]	$34.00_{\pm 0.46}$	$49.71_{\pm 0.47}$	$35.55_{\pm 0.41}$	$50.24_{\pm 0.39}$	$40.49_{\pm 0.54}$	$59.85_{\pm 0.49}$	$43.83_{\pm 0.51}$	$55.87_{\pm 0.42}$	$93.63_{\pm 0.63}$
TP w/o OT	$33.07_{\pm 0.38}$	$50.99_{\pm 0.44}$	$32.96_{\pm 0.32}$	$50.71_{\pm 0.37}$	$38.07_{\pm 0.45}$	$55.31_{\pm 0.51}$	$37.94_{\pm 0.41}$	$55.11_{\pm 0.44}$	$91.84_{\pm 0.56}$
Self-supervised Learning (SSL)									
w/o SSL	$39.33_{\pm 0.50}$	$53.66_{\pm 0.47}$	$40.31_{\pm 0.44}$	$54.23_{\pm 0.40}$	$47.96_{\pm 0.57}$	$61.38_{\pm 0.49}$	$48.70_{\pm 0.52}$	$61.44_{\pm 0.43}$	$97.07_{\pm 0.48}$

Table 2: The results of ablation studies.

Conclusion

- PGADA
  - Theoretical foundation
  - Clean representations
  - Accurate Alignment Plans

Thanks for your attention.