

DRO

$$\min_{\theta \in \Theta} \sup_{D \in \mathcal{P}} \mathbb{E}_{(x,y) \sim D} [\ell(\theta, (x, y))]$$

Objective

$$\Omega^A(\alpha_A, \alpha_P, \theta)$$

$$= \min_{\alpha_A \alpha_P \theta_1 \theta_2} (\alpha_A r_A + \alpha_P r_P) + \frac{1}{n_A n_P} \sum_{(i,j) \in M} (f(y_j^P \langle \theta, (x_j^P, a_i^A) \rangle) + \max(y_j^P \langle \theta, (x_j^P, a_i^A) \rangle - \alpha_P \kappa_P, 0) - \alpha_A \|x_i^A - x_j^P\|)$$

$$\Omega^P(\alpha_A, \alpha_P, \theta)$$

$$= \min_{\alpha_A \alpha_P \theta_1 \theta_2} (\alpha_A r_A + \alpha_P r_P) + \frac{1}{n_A n_P} \sum_{(i,j) \in M} (f(y_j^P \langle \theta, (x_i^A, a_i^A) \rangle) + \max(y_j^P \langle \theta, (x_j^P, a_i^A) \rangle - \alpha_P \kappa_P, 0) - \alpha_P \|x_i^A - x_j^P\|)$$

Constrained by

$$C^A = \{(\alpha_A, \alpha_P, \theta) : \|\theta_1\|_* \leq \alpha_A + \alpha_P, \|\theta_2\| \leq \kappa_A \alpha_A, \alpha_A < \alpha_P\}$$

$$C^P = \{(\alpha_A, \alpha_P, \theta) : \|\theta_1\|_* \leq \alpha_A + \alpha_P, \|\theta_2\| \leq \kappa_A \alpha_A, \alpha_A > \alpha_P\}$$

Adversarial Loss

$$L(x_i^p, x_j^a, \theta) = w_1 \cdot \ell(\theta, (x_i^p, y_i^p)) + w_2 \cdot \ell(\theta, (\tilde{x}_i^p, y_i^p)) + w_3 \cdot \ell(\theta, (x_j^a, y_i^p)) + w_4 \cdot \ell(\theta, (\tilde{x}_j^a, y_i^p))$$

Perturbed samples

$$\tilde{x}_i^p = \arg \max_{x \in \mathcal{B}(x_i^p)} \|f(\theta, x) - f(\theta, x_j^a)\|_2$$

$$\tilde{x}_j^a = \arg \max_{x \in \mathcal{B}(x_j^a)} \|f(\theta, x) - f(\theta, x_i^p)\|_2$$