

## Problem

With the rapid development of the Internet and information technology, the problem of information overload is getting more and more critical. To help people efficiently figure out the content of interests from the exponentially increasing information, recommendation systems have been extensively incorporated as one of the core parts in various advanced web applications.

The existing methods generally focus on exploring the latent feature vectors from the user's feedback to predict the user's preference over items. However, the performance of the learning systems are still far away from satisfactory because of the unqualified training data.

Therefore, the robustness as well as performance of the recommendation systems need to be improved.

## Contributions

We propose a novel Collaborative Generative Adversarial Network (CGAN) model which seamlessly incorporates VAE into GAN model to enhance the robustness to adversarial examples.

We introduce the **Wasserstein Distance with gradient penalty** into the item recommendation tasks to depict the distribution divergence between the generated data and ground-truth data.

Extensive experiments performed on two public datasets demonstrate the effectiveness of our framework on both performance and robustness comparing with the state-of-the-art methods.

## Conclusion

We propose a GAN-based framework to strengthen recommendation systems' robustness and performance by performing adversarial training in continuous embedding space.

## Methodology

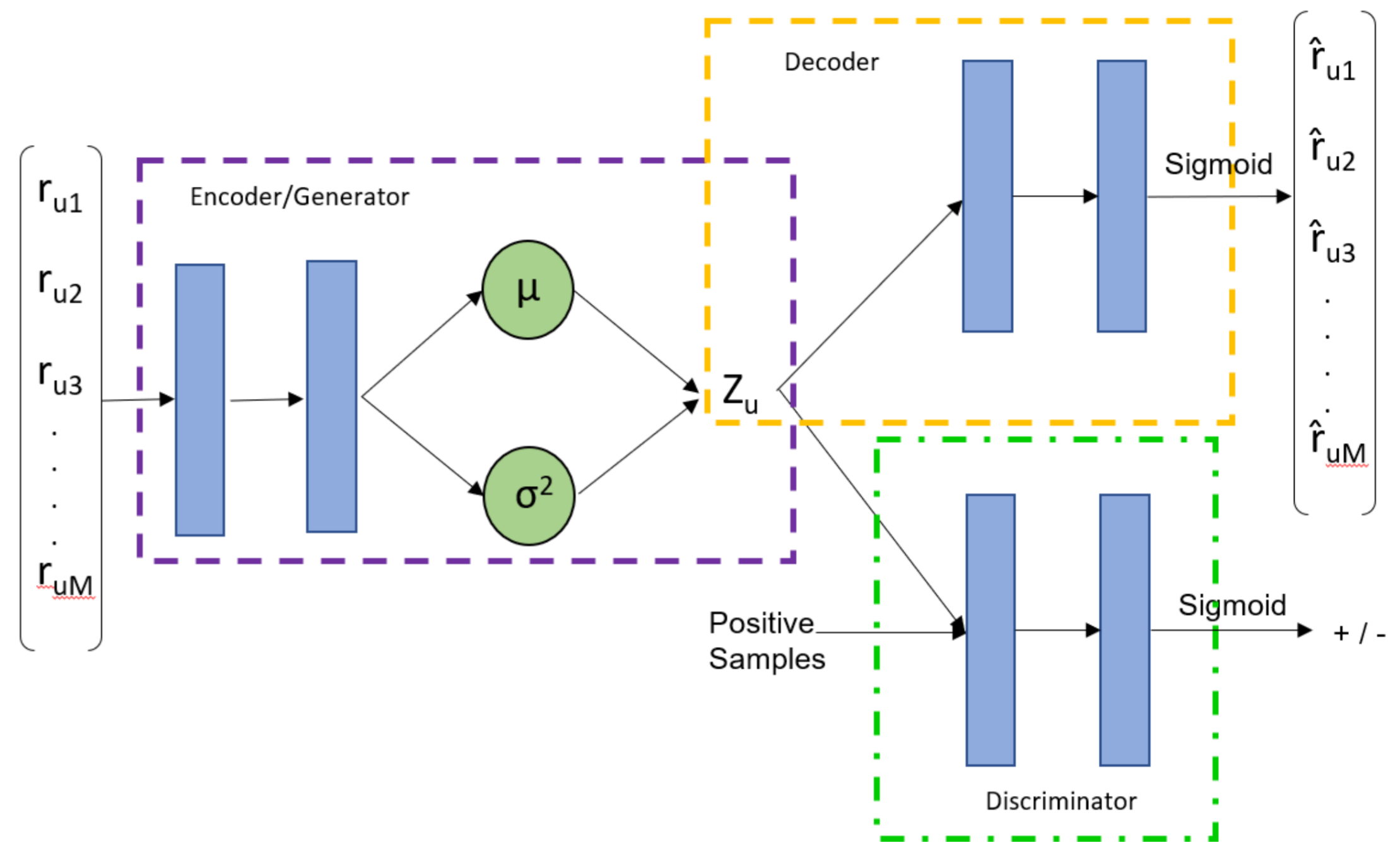


Figure 1. An overview of the framework. It consists of three major components: encoder network, decoder network and discriminator model. The input of the encoder is a row vector  $r_u$  of the rating matrix and the output of the decoder is the reconstructed row vector  $\hat{r}_u$ . Each edge resembles a parametrized mapping with activation function. Without specific label, the activation function is rectified linear.  $Z_u$  stands for the aggregated posterior distribution of VAE.

$$\mathcal{L}_{GAN}^G = -E_{i \sim P_{\theta}(i|u)} [D(v|u)]$$

$$\mathcal{L}_{VAE} = \sum_{i=1}^N [(r_u - \hat{r}_u) \cdot b_u]^2 + \frac{1}{2}(\sigma_i^2 - \log \sigma_i^2 - 1) + \frac{1}{2}\mu_i^2$$

$$\mathcal{J}^D = \mathcal{L}_{GAN}^D + \beta \|\phi\|_2$$

$$\mathcal{J}^G = \frac{1}{2}\mathcal{L}_{GAN}^G + \frac{1}{2}\mathcal{L}_{VAE} + \beta \|\theta\|_2$$

where  $\mathcal{J}^D$  and  $\mathcal{J}^G$  are objective functions of  $D$  and  $G$ , respectively.  $\|\cdot\|_2$  represents the  $L_2$  norm.

## Experiments

Alg.	P@3	P@5	P@10	MAP	NDCG@3	NDCG@5	NDCG@10	MRR
ItemPop	0.279	0.251	0.233	0.124	0.191	0.212	0.256	0.312
MF-BPR	0.381	0.369	0.344	0.163	0.362	0.414	0.432	0.549
CDAE	0.449	0.425	0.402	0.185	0.384	0.428	0.449	0.599
NeuMF	0.461	0.442	0.418	0.197	0.417	0.430	0.462	0.649
GraphGAN	0.354	0.329	0.299	0.125	0.319	0.335	0.341	0.412
IRGAN	0.445	0.433	0.392	0.172	0.409	0.420	0.449	0.637
CGAN	<b>0.472</b>	<b>0.459</b>	<b>0.435</b>	<b>0.207</b>	<b>0.438</b>	<b>0.469</b>	<b>0.478</b>	<b>0.662</b>

Table 1. Recommendation performance on Netflix

Epoch	5		10		15	
	P@5	N@5	P@5	N@5	P@5	N@5
GAN	0.359	0.385	0.367	0.394	0.371	0.399
WGAN	0.361	0.389	0.372	0.402	0.386	0.411
WGANGP	0.374	0.392	0.383	0.417	0.418	0.426

Alg.	P@3	P@5	P@10	N@3	N@5	N@10
MF	0.362	0.313	0.293	0.325	0.364	0.402
AE	0.381	0.363	0.331	0.335	0.372	0.423
VAE	0.449	0.428	0.398	0.369	0.417	0.458

Table 2. Ablation study of WGAN and VAE