2021年度暑期强化课程

8. 生成对抗模型GAN

授课人：曹亚男

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

8.生成对抗模型GAN

8.1	GAN原理
8.2	GAN & NLP
8.3	GAN for NLP

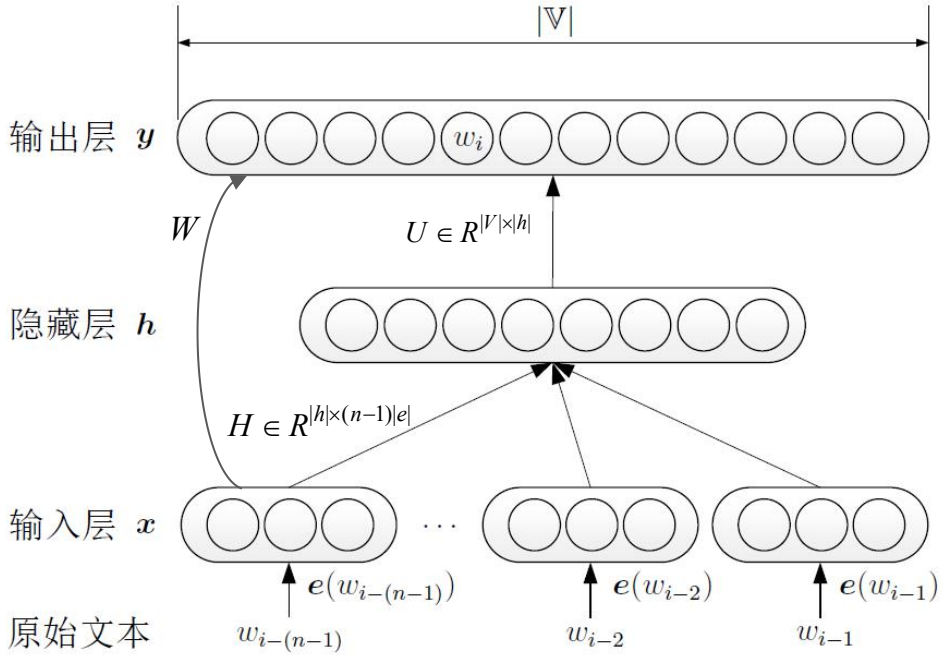
8.生成对抗模型GAN

8.1	GAN原理
8.2	GAN & NLP
8.3	GAN for NLP

判别模型

- 由数据直接学习决策函数$Y=f(X)$或条件概率分布$P(Y|X)$作为预测模型，即判别模型。判别方法关心的是对于给定的输入X，应该预测什么样的输出Y

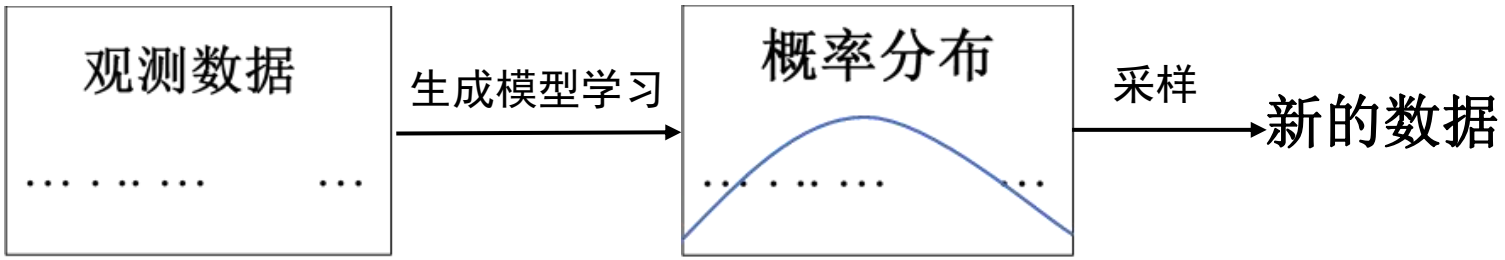
例子：NNLM



- 采用NN结构对n-gram模型进行建模，估算$P(w_i|w_{i-(n-1)}, \ldots, w_{i-1})$的值。输入为条件部分的整个词序列，输出为目标词$w_i$的分布

生成模型

- 生成方法是由数据学习联合概率分布$P(X,Y)$,然后求出条件概率分布$P(Y|X)=P(X,Y)/P(X)$作为预测的模型。该方法表示了给定输入X与产生输出Y的生成关系



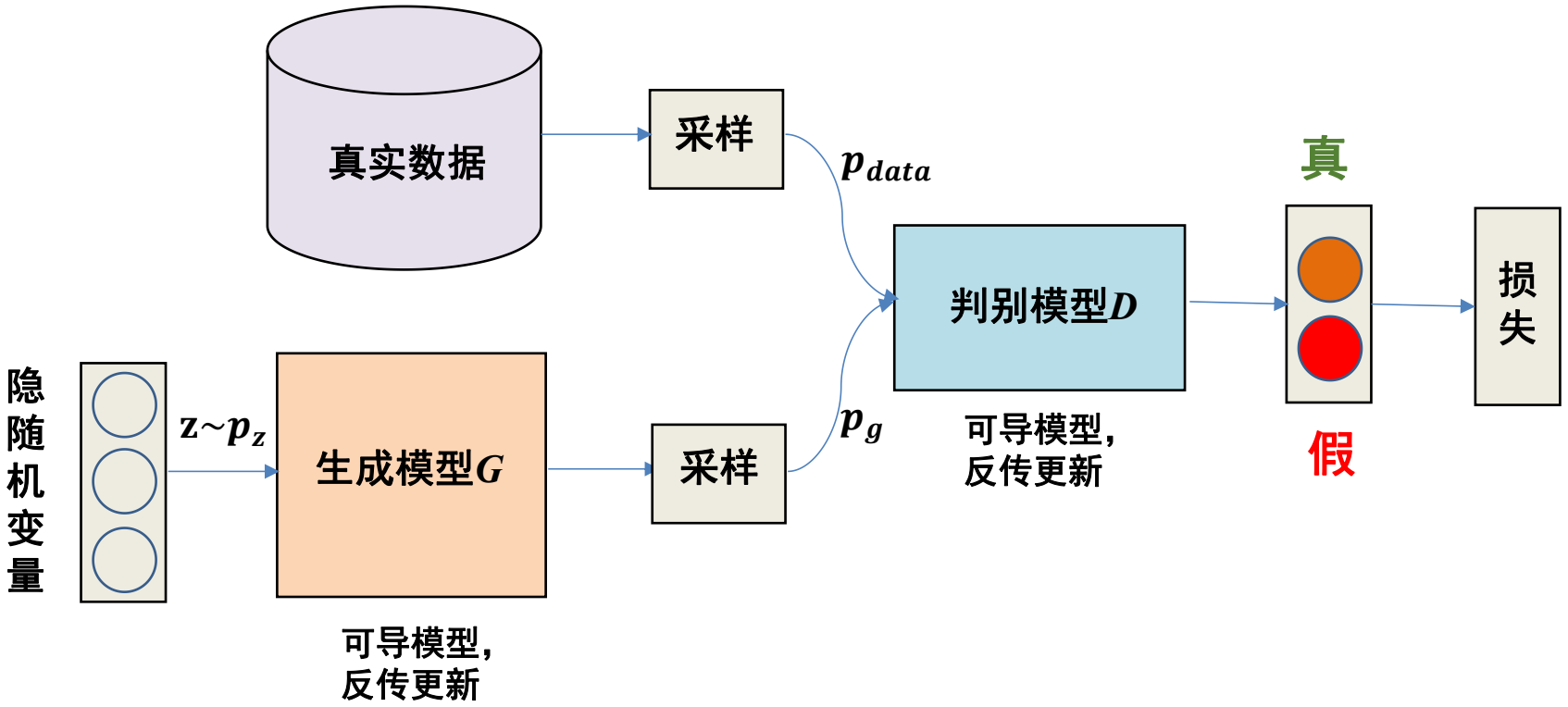
- 生成模型是从大量数据中找规律，属于统计学习；判别模型只关心不同类型的数据之间的差别，利用差别来进行分类

生成模型

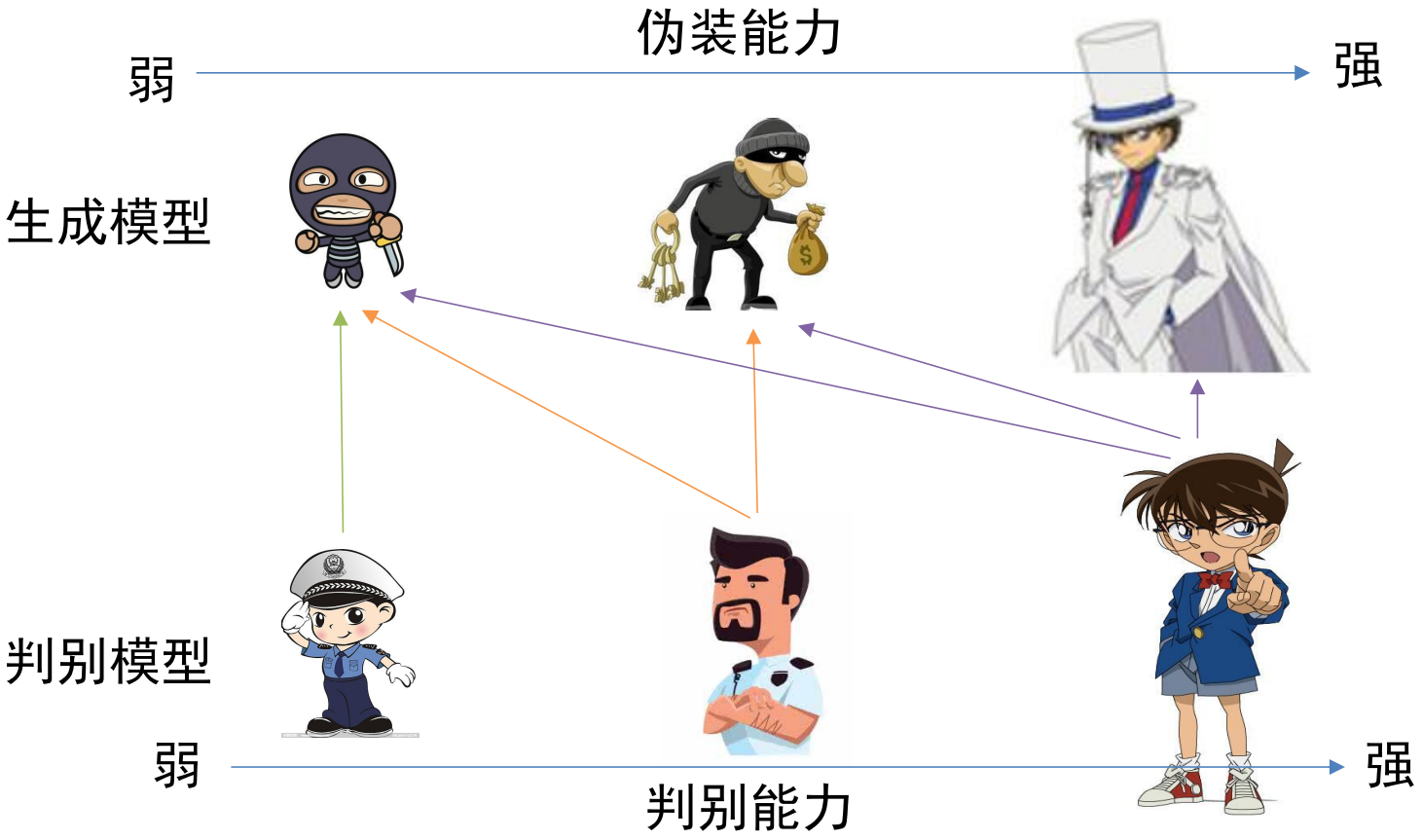
- 用模型来拟合联合概率分布$P(X, Y)$
  - 变分自动编码模型（VAE）
    - 优点：允许带隐变量的概率图模型学习与贝叶斯推理（eg. DRAW, Attened Infer Repeat）
    - 缺点：生成样本模糊
  - 自回归模型（Auto-regressive）
    - 优点：简单，训练过程稳定
    - 缺点：采样效率过低
  - 生成对抗网络（GAN）
    - 优点：生成样本细节清晰
    - 缺点：优化困难（训练过程不稳定）

什么是GAN?

- GAN包括两个多层神经网络模型，一个是生成器、一个是判别器：生成器用于学习数据的分布p_g，判别器用于对生成的采样数据进行判断
- G的训练目标是最小化让D判断正确的概率，D的训练目标是最大化判别器的判断能力

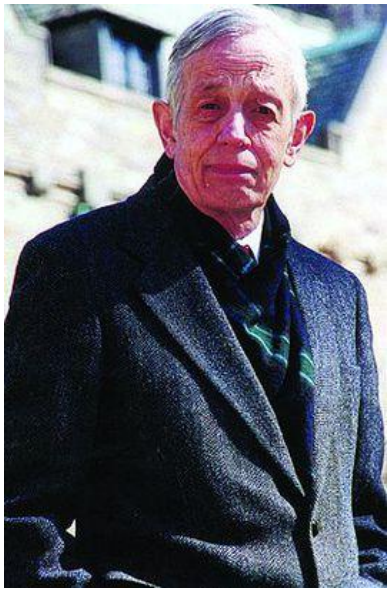


什么是GAN?



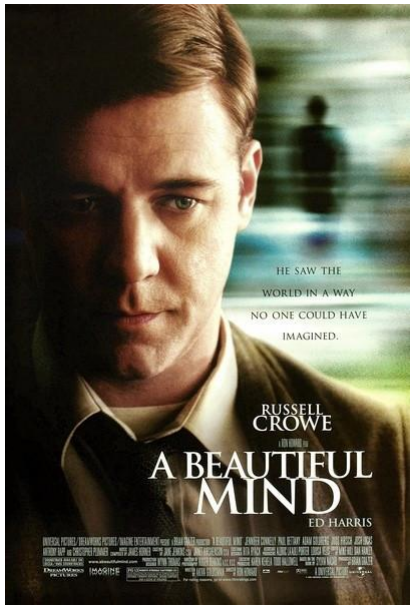
纳什平衡

- 纳什平衡：非合作博弈均衡，是博弈论的一个重要术语。是一种策略组合，使得每个参与人的策略都是对其他参与人策略的最优反应



约翰纳什

因为纳什平衡等理论获得诺贝尔经济学奖



GAN的工作原理

- 目标函数

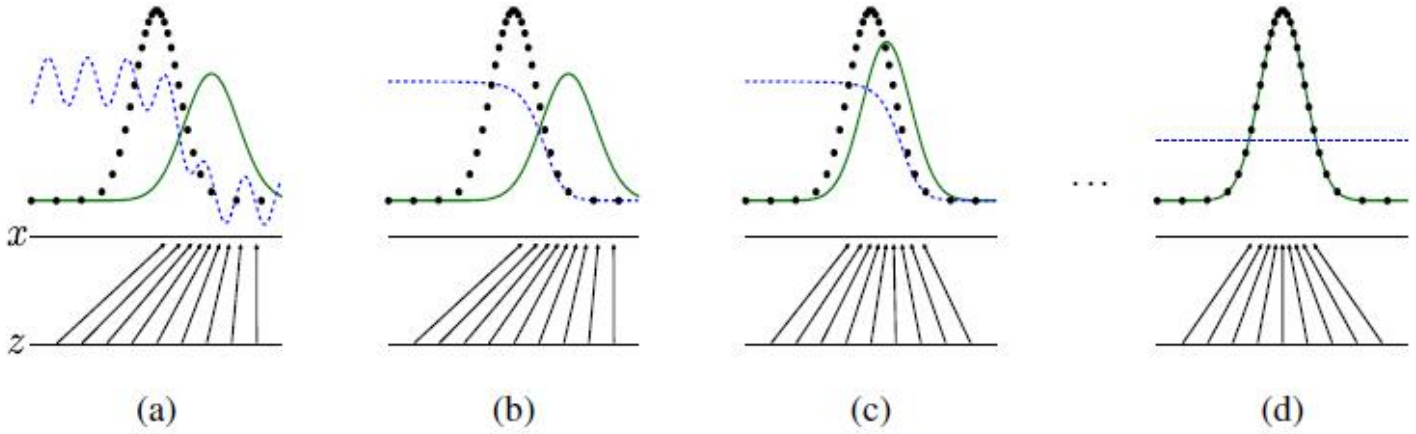
$$\min_G \max_D V(D,G) = E_{x\sim \mathrm{p_{data}}(x)}[logD(x)] + E_{z\sim \mathrm{p}_z(z)}[\log(1-D(G(z)))].$$

- 优化判别模型D：
  - 最大化分配给训练数据x和生成数据$G(z)$正确标签的概率

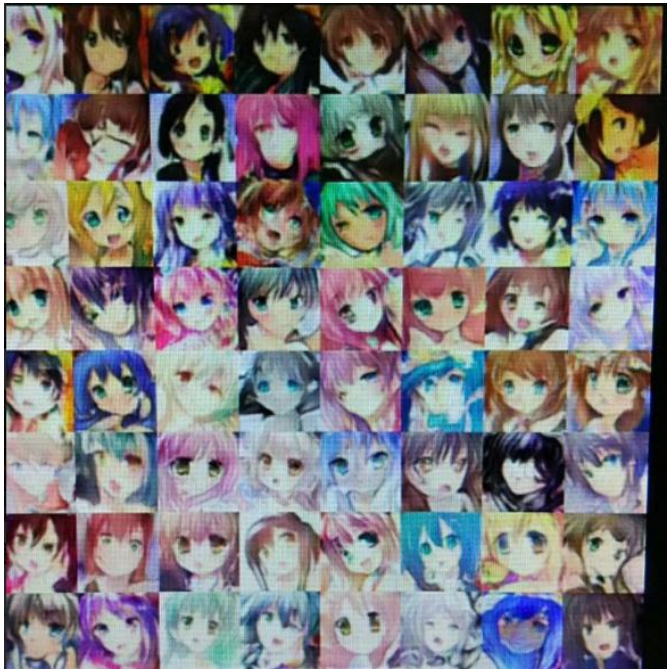
$$\max_D V(D,G) = E_{x\sim \mathrm{p_{data}}(x)}[logD(x)] + E_{z\sim \mathrm{p}_z(z)}[\log(1-D(G(z)))].$$

- 优化生成模型G：将一个随机变量z映射到真实数据空间

$$\min_G V(D,G) = E_{z\sim \mathrm{p}_z(z)}[\log(1-D(G(z)))].$$



GAN for 图像生成

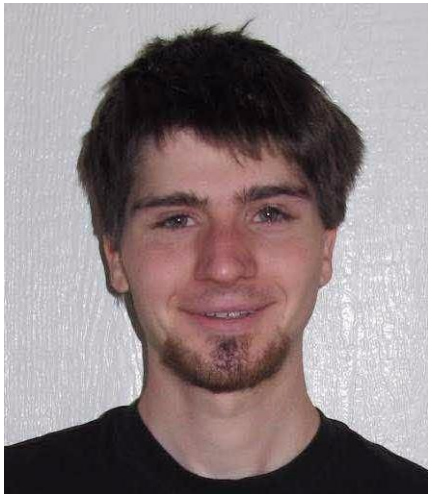


GAN for 图像生成

sample496.jpg

GAN的优缺点

“20年来机器学习领域最酷的想法”



Ian J. Goodfellow

优点

- GAN是一种更好的生成模型
- GAN避免了马尔科夫链式的学习机制
- 各种类型的损失函数都可以整合到GAN模型中
- 概率密度不可计算时，GAN仍能工作

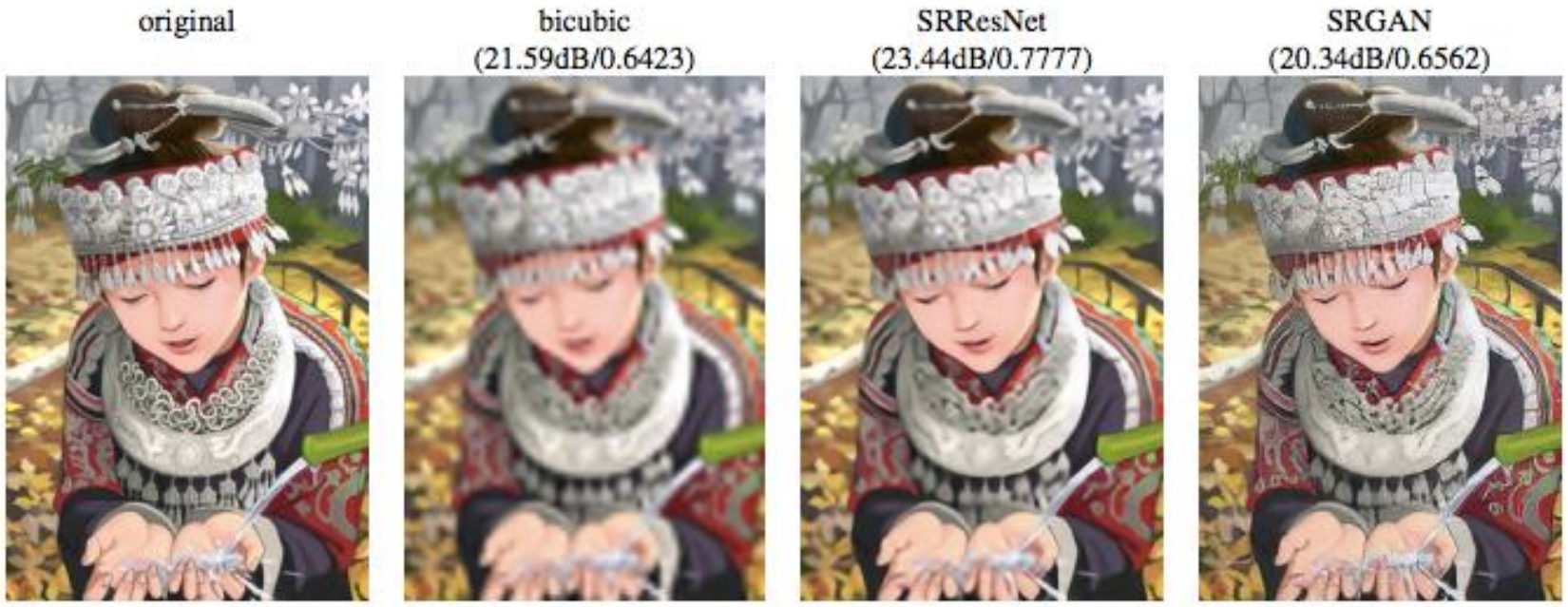
缺点

- 可解释性差：生成模型的分布$\boldsymbol{P_g(G)}$没有显示表达
- 较难训练，D与G之间需要很好地协调

Goodfellow, Ian J. et.al. (2014). "Generative Adversarial Networks". arXiv:1406.2661

GAN for CV -- Image Super-Resolution

- SRGAN：将GAN用于图像超分辨率重建；当图像采样倍数较高时，重建的得到的图片会过于平滑、丢失细节；通过使用对抗训练，能够得到更多的细节信息、更细腻的画质.



Ledig C, Theis L, Huszár F, et al. Photo-realistic single image super-resolution using a generative adversarial network[J]. arXiv preprint arXiv:1609.04802, 2016.

GAN for CV -- Object Detection

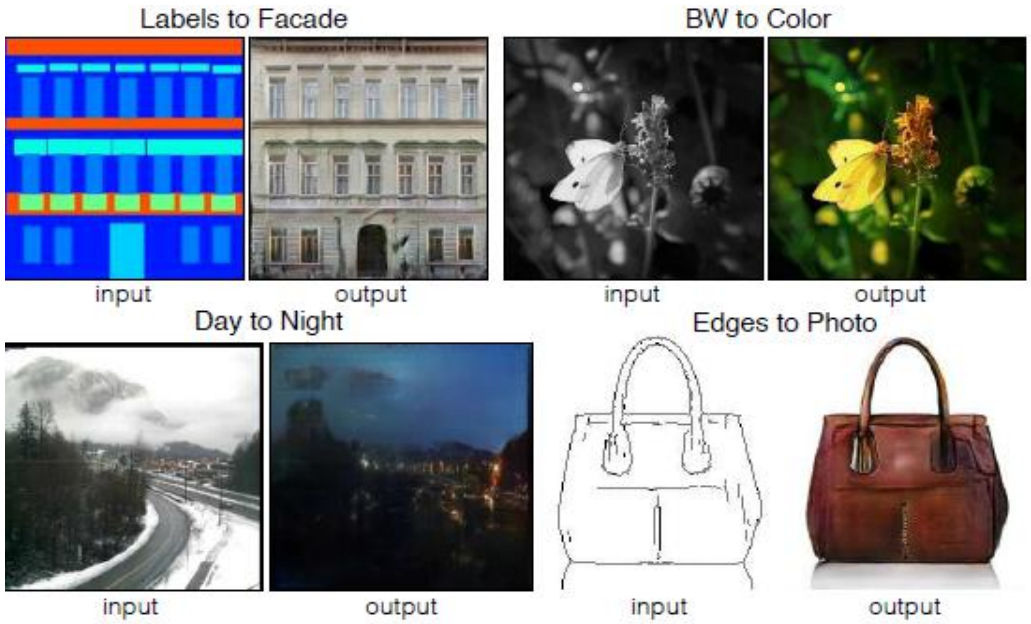
- A-Fast-RCNN：利用GAN来自动生成遮挡和变形的样本

- Perceptual GAN：目标是检测小物体，*G*采用深度残差特征生成模型，将原始的特征转换为高分变形的特征；*D*用于分辨小物体生成的高分辨率特征与真实大物体特征

A-fast-rcnn: Hard positive generation via adversary for object detection[J], 2017.
Perceptual Generative Adversarial Networks for Small Object Detection[J]., 2017.

GAN for CV -- Image translation

- Pix2pix：学习从输入到输出图片的映射，实现图片“翻译”



- Text2image：根据输入的自然语言描述生成图像

the flower has petals that are bright pinkish purple with white stigma

Image-to-image translation with conditional adversarial networks[J]. 2016.
Generative adversarial text to image synthesis[J]. ,2016.

8.生成对抗模型GAN

8.1 GAN原理

8.2 GAN & NLP

8.3 GAN for NLP

GAN & NLP ?

- 问题一：GAN最开始设计是用于生成连续数据（实数空间），不能应用于生成离散数据（如文本）

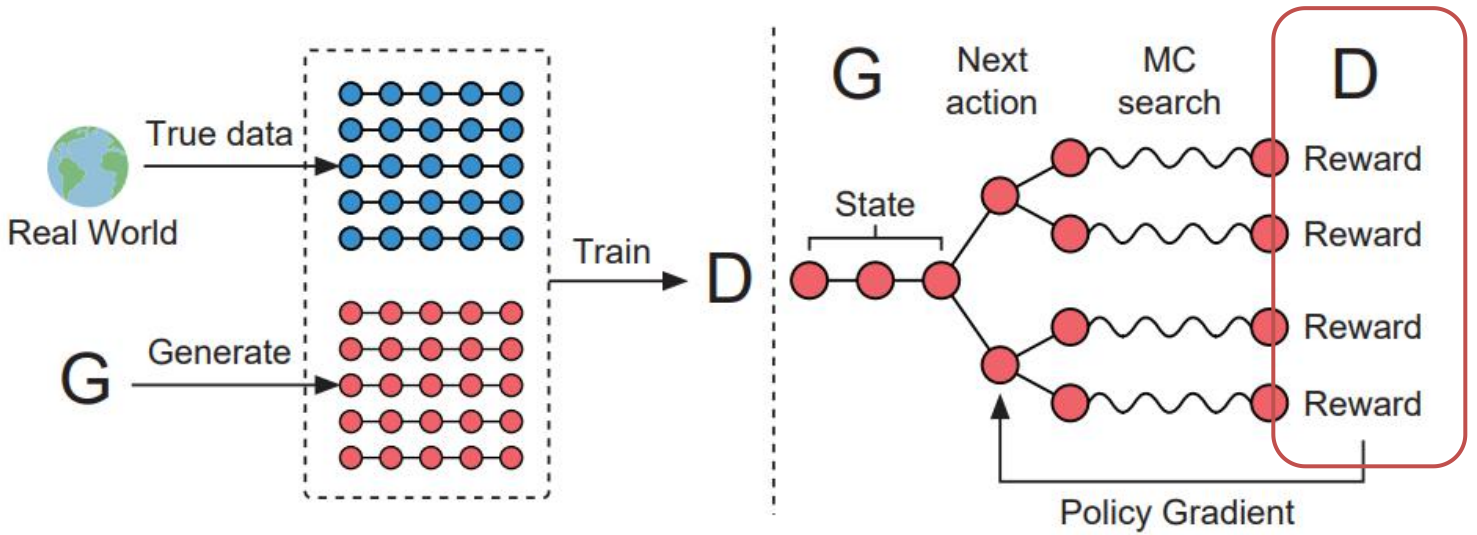
连续数据

+0.001 =

离散数据

$$enjoy = \begin{bmatrix} -0.256 \\ 0.274 \\ 0.159 \end{bmatrix}$$ +0.001 = ?

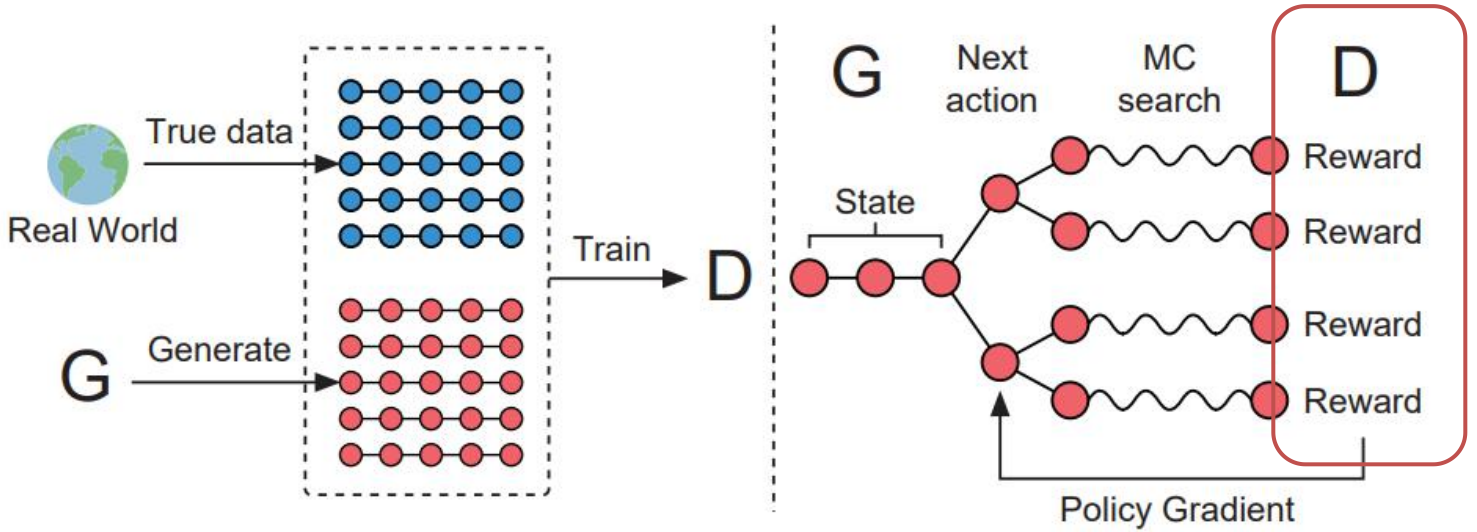
SeqGAN



- 解决问题一：将D的输出作为Reward，采用策略梯度方法(Policy Gradient)来训练G
  - 将GAN训练过程看成一个强化学习的过程，G是强化学习的主体，state是目前G生成的序列，action就是下一步要生成的标记。判别器用于评估G的生成序列，并且将评估结果作为reward

Yu L, Zhang W, Wang J, et al. SeqGAN: Sequence Generative Adversarial Nets with Policy Gradient[C]//AAAI. 2017: 2852-2858.

SeqGAN



- 解决问题一：将D的输出作为Reward，采用策略梯度方法(RL)来训练G

$$\nabla_\theta J(\theta) \simeq \sum_{t=1}^{T} \sum_{y_t \in \mathcal{Y}} \nabla_\theta G_\theta(y_t|Y_{1:t-1}) \cdot Q_{D_\phi}^{G_\theta}(Y_{1:t-1}, y_t)$$

$$= \sum_{t=1}^{T} \sum_{y_t \in \mathcal{Y}} G_\theta(y_t|Y_{1:t-1}) \nabla_\theta \log G_\theta(y_t|Y_{1:t-1}) \cdot Q_{D_\phi}^{G_\theta}(Y_{1:t-1}, y_t)$$

$$= \sum_{t=1}^{T} \mathbb{E}_{y_t \sim G_\theta(y_t|Y_{1:t-1})} [\nabla_\theta \log G_\theta(y_t|Y_{1:t-1}) \cdot Q_{D_\phi}^{G_\theta}(Y_{1:t-1}, y_t)]$$

Yu L, Zhang W, Wang J, et al. SeqGAN: Sequence Generative Adversarial Nets with Policy Gradient[C]//AAAI. 2017: 2852-2858.

GAN for NLP ?

- 问题二：GAN只能对已生成的完整序列进行打分，对于部分(partially)生成的序列，很难判断目前部分序列和之后生成整个序列的分数

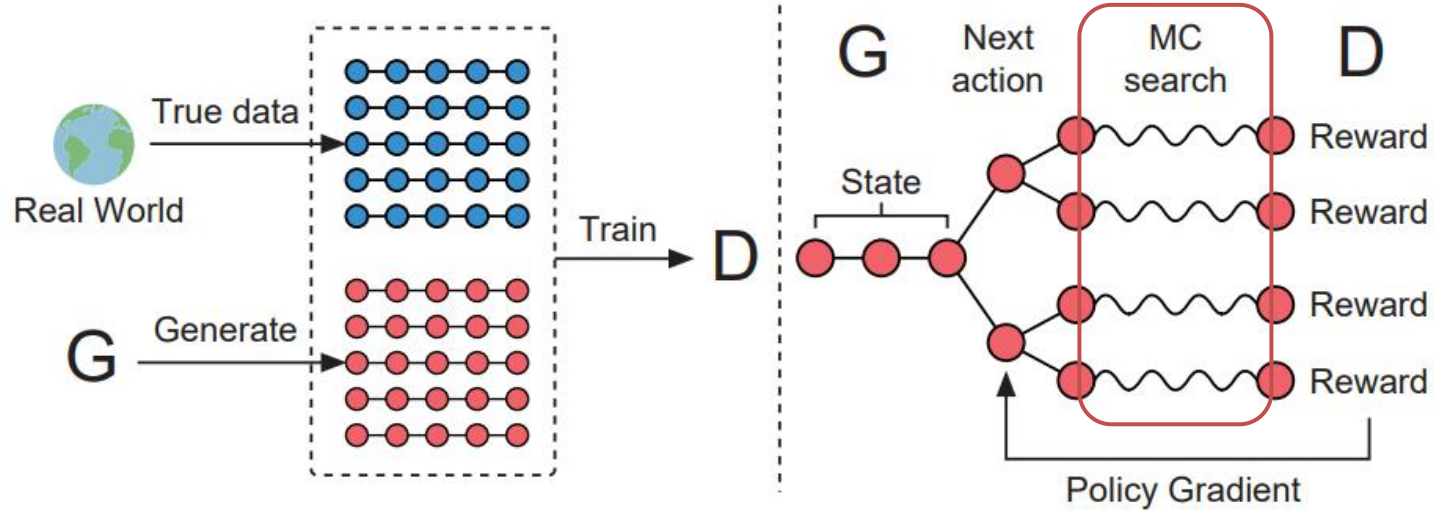
先帝创业未半而中道崩殂，今天下三分，益州疲弊，此诚危急存亡之秋也。然侍卫之臣不懈于内，忠志之士忘身于外者，盖追先帝之殊遇，欲报之于陛下也。诚宜开张圣听，以光先帝德，恢弘志士之气，不宜妄自菲薄，引喻失义，以塞忠谏之遗路也。

√

先帝创业未半而中道崩殂，今天下三分，益州先帝……

?

SeqGAN



- 解决问题二：采用Monto-carlo搜索，针对部分生成的序列，用一个循环神经网络来采样完整的序列，再交给*D*打分，然后对得到的Reward求平均值

Yu L, Zhang W, Wang J, et al. SeqGAN: Sequence Generative Adversarial Nets with Policy Gradient[C]//AAAI. 2017: 2852-2858.

中文诗词生成

Real data	Generated data
南陌春风早，东邻去日斜。	山夜有雪寒，桂里逢客时。
紫陌追随日，青门相见时。	此时人且饮，酒愁一节梦。
胡风不开花，四气多作雪。	四面客归路，桂花开青竹。

Yu L, Zhang W, Wang J, et al. SeqGAN: Sequence Generative Adversarial Nets with Policy Gradient[C]//AAAI. 2017: 2852-2858.

奥巴马演讲生成

Real data	Generated data
• i stood here today i have one and most important thing that not on violence throughout the horizon is OTHERS American fire and OTHERS but we need you are a strong source • for this business leadership will remember now i cant afford to start with just the way our european support for the right thing to protect those American story from the world and • i want to acknowledge you were going to be an outstanding job times for student medical education and warm the republicans who like my times if he said is that brought the	• When he was told of this extraordinary honor that he was the most trusted man in America • But we also remember and celebrate the journalism that Walter practiced -- a standard of honesty and integrity and responsibility to which so many of you have committed your careers. It's a standard that's a little bit harder to find today • I am honored to be here to pay tribute to the life and times of the man who chronicled our time.

Yu L, Zhang W, Wang J, et al. SeqGAN: Sequence Generative Adversarial Nets with Policy Gradient[C]//AAAI. 2017: 2852-2858.

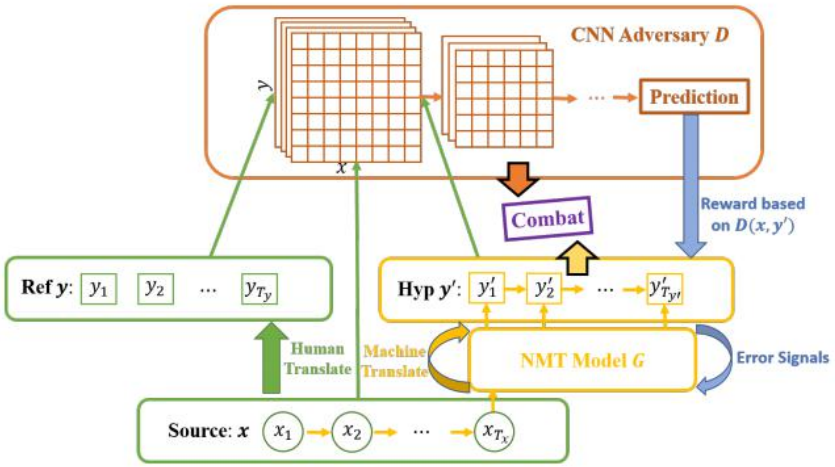
8.生成对抗模型GAN

8.1 GAN原理

8.2 GAN & NLP

8.3 GAN for NLP

GAN for MT (ANMT)



ANMT框架图
（D:CNN; G: LSTM-seq2seq）

- 生成器采用LSTM-Seq2seq
- 判别器采用CNN

1. Experimental results on English→French

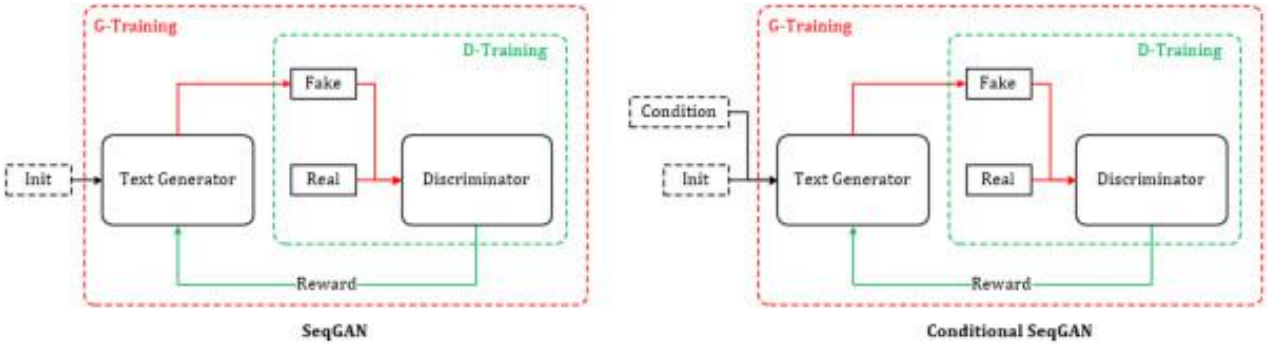
System	System Configurations	BLEU
	Representative end-to-end NMT systems	
Bahdanau et al. (2014)	RNNSearch	23.87 [a]
Ranzato et al. (2015)	CNN encoder + Sequence level objective	21.83
Bahdanau et al. (2016)	CNN encoder + Sequence level actor-critic objective	22.45
Wiseman et al. (2016)	RNNSearch + Beam search optimization	25.48
Shen et al. (2016)	RNNSearch + Minimum Risk Training Objective	25.84 [b]
	Adversarial-NMT	
this work	RNNSearch + Adversarial Training Objective	26.98†
	RNNSearch + Adversarial Training Objective + UNK Replace	27.94

2. Experimental results on German→French

System	System Configurations	BLEU
	Representative end-to-end NMT systems	
Sutskever et al. (2014)	LSTM with 4 layers + $80K$ vocabs	30.59
Bahdanau et al. (2014)	RNNSearch	29.97[a]
Jean et al. (2015)	RNNSearch + UNK Replace	33.08
Jean et al. (2015)	RNNSearch + $500k$ vocabs + UNK Replace	34.11
Luong et al. (2015)	LSTM with 4 layers + $40K$ vocabs	29.50
Luong et al. (2015)	LSTM with 4 layers + $40K$ vocabs + PosUnk	31.80
Shen et al. (2016)	RNNSearch +Minimum Risk Training Objective	31.30
Sennrich et al. (2016)	RNNSearch +Monolingual Data	30.40 [b]
He et al. (2016)	RNNSearch+ Monolingual Data + Dual Objective	32.06
	Adversarial-NMT	
this work	RNNSearch + Adversarial Training Objective	31.91†
	RNNSearch + Adversarial Training Objective + UNK Replace	34.78

Lijun Wu, Yingce Xia, Li Zhao, et al. Adversarial neural machine translation. arXiv:1704.06933, 2017.

GAN for Dialogue Generation



- 生成器：Seq2seq
- 判别器:二元分类器（层次编码+softmax）

For number of training iterations **do**
. **For** i=1,D-steps **do**
. Sample (X,Y) from real data
. Sample $\hat{Y} \sim G(\cdot|X)$
. Update D using (X, Y) as positive examples and $(X, \hat{Y})$ as negative examples.
. **End**
.
. **For** i=1,G-steps **do**
. Sample (X,Y) from real data
. Sample $\hat{Y} \sim G(\cdot|X)$
. Compute Reward r for $(X, \hat{Y})$ using D.
. Update G on $(X, \hat{Y})$ using reward r
. Teacher-Forcing: Update G on (X, Y)
. **End**
End

Input	tell me ... how long have you had this falling sickness ?
Vanilla-MLE	i 'm not a doctor .
Vanilla-Sample	well everything you did was totally untrue .
REINFORCE	i don 't know how long it 's been .
REGS Monte Carlo	A few months, I guess .
Input	so i had the doctors test sammy 's response to conditioning .
Vanilla-MLE	sammy wrote the test sammy wrote the test .
Vanilla-Sample	objects pick objects up objects objects objects objects objects
REINFORCE	i 'm not sure that 's relevant .
REGS Monte Carlo	so he took the pills .
Input	what are you going to do ?
Vanilla-MLE	i 'm going to the movies .
Vanilla-Sample	get him outta here first !
REINFORCE	i 'm going to get you .
REGS Monte Carlo	i 'm going to get you a new car .
Input	they fear your power your intellect .
Vanilla-MLE	you 're the only one who knows what 's going on .
Vanilla-Sample	when they are conquered and you surrender they will control all of us .
REINFORCE	i 'm afraid i 'm not ready yet .
REGS Monte Carlo	i 'm not afraid of your power .

Li J.W., et al. Adversarial Learning for Neural Dialogue Generation
https://github.com/jiweil/Neural-Dialogue-Generation

GAN for Text Summarization

- 生成器采用双层Attention的Seq2seq，判别器采用Triple-RNN

System	$Rouge_1$	$Rouge_2$	$Rouge_L$
LexRank	21.23	8.98	19.15
Abs	29.47	11.91	26.14
Abs+INRNN	33.15	13.20	26.36
Abs+	35.46	13.30	32.65
DeepRL	39.87	15.82	***36.90**
ANMT	39.92	17.65	36.71
ATRNNs	***41.56**	***18.42**	36.68

Table 1: Rouge-score on CNN/Daily mail corpus

System	$Rouge_1$	$Rouge_2$	$Rouge_L$
LexRank	22.03	0.72	13.01
Abs	11.35	1.67	14.17
Abs+INRNN	24.49	8.72	21.81
Abs+	26.82	9.19	24.12
DeepRL	29.90	10.36	26.59
ANMT	29.91	10.53	27.21
ATRNNs	***31.40**	***10.66**	***27.58**

Table 2: Rouge-score on NLPCC corpus

S(1):	two amish girls , apparently abducted (189 words)
R:	new : two girls found safe , authorities tell cnn
AB:	new : girl found TAGNUM girl say
AT:	new TAGNUM girl found safe TAGNUM girl say cnn
S(2):	paintings said gangster reggie kray(350 tokens)
R:	three paintings killer expected fetch TAGNUM
AB:	paintings killer killer fetch TAGNUM year
AT:	TAGNUM paintings killer killer expected fetch fetch TAGNUM TAGNUM
S(3):	britain launch world 's first spaceport (350 tokens)
R:	britain leading space race world 's first non - american spaceport
AB:	father spaceport daughter son daughter TAGNUM spaceport son TAGNUM kill first crash
AT:	uk uk early leading space big business uk TAGNUM spaceport space space space

Table 3: Examples from the CNN/Daily Mail test dataset showing the outputs of Abs and ATRNNs models, after tokenizing, truncating to 350 tokens and replacing Arabic numbers in "TAGNUM"

Sequence Generative Adversarial Network for Long Text Summarization. 2018.

探讨：GAN与NLP的结合

- 质疑的声音
  - 效果似乎没有那么好：许多应用场景下，seq2seq模型已经足够好
  - 模型复杂度高：G+D+RL
  - 训练非常困难

欢迎加入DL4NLP！

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS