

# Unsupervised Learning & & Generative Adversarial Networks

DL4DS – Spring 2025

# April Dates 💢

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	April 1	2	3	4 GANs	5	6
7	8	9 VAEs	10 Discussion	11 Diffusion Models	12	13
14	15	16 Graph Neural Nets	17 Discussion	18 Reinforcement Learning	19	20
21	22	23 TBD/Overflow	24 Discussion	25 ★ Project Presentations 1 ★	26	27
28	29	30 ★ Project Presentations 2 ★	May 1 Discussion??	2 Study Period	3 Study Period	4
5	6 Final Exams	7	8	9	10 Final report & Repo **	11

<sup>\*\*</sup> Might be earlier. Depends on when grades are due.

### **Project Presentations**

Looking for volunteers for April 25. Then I will randomly draw remainder of April 25 spots.

### April 25 – 75 minutes

- Slot 1
- Slot 2
- Slot 3
- Slot 4
- Slot 5
- Slot 6
- Slot 7
- Slot 8

### Format:

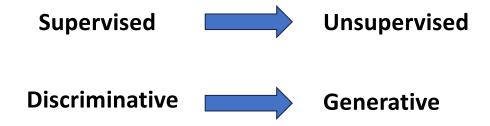
- ≤ 3 minutes screencast/video
- ≤ 2 minutes additional presentation
- ~2 minutes Q&A

### April 30 – 75 minutes

- Slot 9
- Slot 10
- Slot 11
- Slot 12
- Slot 13
- Slot 14
- Slot 15
- Slot 16
- Slot 17

### Up to this point...

- we looked at discriminative supervised learning models
- Exceptions:
  - Transformers pretrained *unsupervised* (then usually finetuned *supervised*)
  - and the Transformer decoder which *generated* text



# Supervised vs. Self/Unsupervised Learning

### **Supervised Learning**

Data: (x, y)

x is data, y is a label

Goal: Learn function to map

 $x \rightarrow y$ 

**Applications**: Classification, regression, object detection, semantic segmentation, etc.

**Self/Unsupervised Learning** 

Data: x

x is data, no labels!

**Goal**: Learn the hidden or underlying structure of the data.

**Applications**: Clustering, dimensionality reduction, compression, find outliers, generating new examples, denoising, interpolating between data points, etc.

# Supervised vs. Self/Unsupervised Learning

### **Supervised Learning**

Data: (x, y)

x is data, y is a label

Goal: Learn function to map

$$x \rightarrow y$$

**Applications**: Classification, regression, object detection, semantic segmentation, etc.

### **Self/Unsupervised Learning**

Data: x

x is data, no labels! Or labels part of the data

**Goal**: Learn the hidden or underlying structure of the data.

**Applications**: Clustering, dimensionality reduction, compression, find outliers, generating new examples, denoising, interpolating between data points, etc.

### We'll consider two attributes of models

• Probabilistic Models

• Latent Variable Models

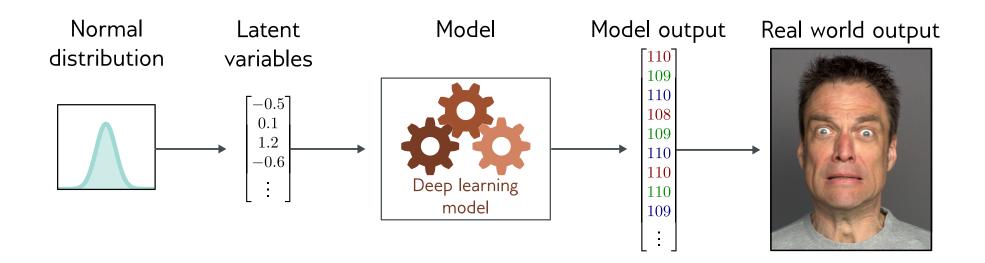
### Probabilistic models

Maximize log likelihood of training data

$$\hat{\phi} = \underset{\phi}{\operatorname{argmax}} \left[ \sum_{i=1}^{I} \log[\Pr(x_i | \phi)] \right]$$

• Find the parameters,  $\phi$ , of some parametric probability distribution so that the training data is most likely under that distribution

### Latent variable models

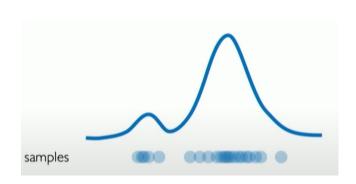


Latent variable models map a random "latent" variable to create a new data sample

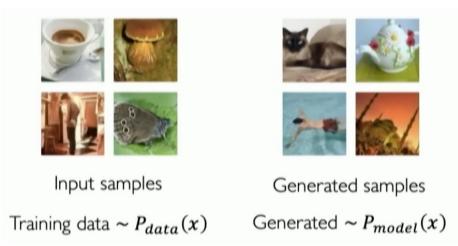
# Generative Modeling

Goal: Take as input training samples from some distribution and learn a model that represents that distribution

### **Probability Density Estimation**



### **Sample Generations**



How can we learn  $P_{model}(x)$  similar to  $P_{data}(x)$ ?

# Types of unsupervised generative model

- Generative adversarial networks (GANs) (LV)
- Variational auto-encoders (VAEs) (P, LV)
- Diffusion models (P, LV)
- Normalizing flows (P, LV)
- Energy models (P)
- Autoregressive models (P)

### Decoder model: GPT3

- One job: predict the next word in a sequence
- More formally builds an autoregressive probability model

$$Pr(t_1, t_2, \dots t_N) = Pr(t_1) \prod_{n=2}^{N} Pr(t_n | t_1 \dots t_{n-1})$$

- Doesn't use latent variables, but is probabilistic and generative
  - Can generate new examples
  - Can assign a probability to new data

# Why generative models? Debiasing

Capable of uncovering underlying features in a dataset

VS



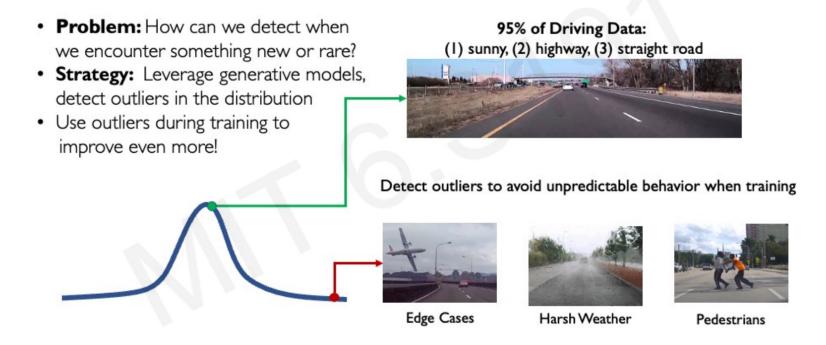
Homogeneous skin color, pose



Diverse skin color, pose, illumination

How can we use this information to create fair and representative datasets?

### Why generative models? Outlier detection



# More outlier examples



# Why generative models? image, video and audio creation



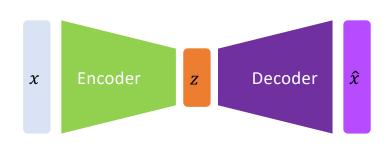
A teenage superhero fighting crime in an urban setting shown in the style of claymation.



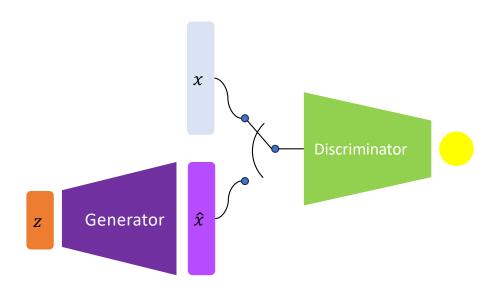
Write a short pop song about students wanting to learn about neural networks and do great things with them.

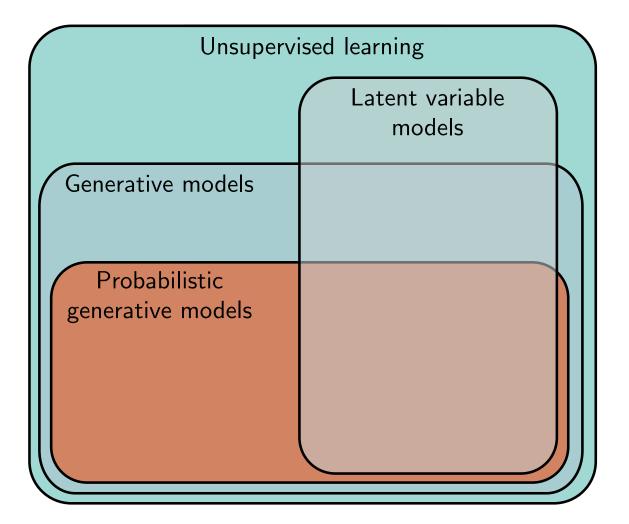
### Latent Variable Models

### **Autoencoders and Variational Autoencoders (VAEs)**



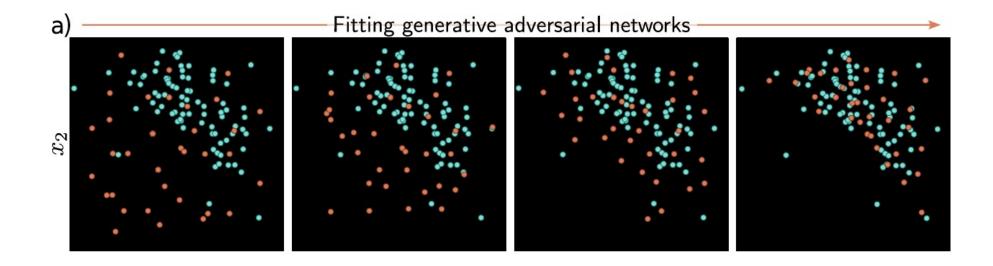
### **Generative Adversarial Networks**

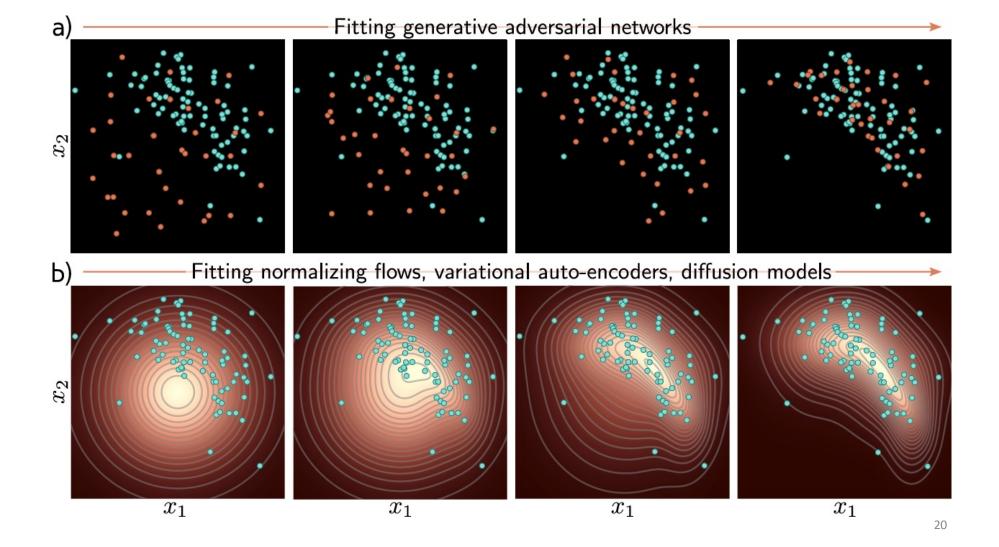




Generative = can generate new examples

Probabilistic = can assign probability to data examples





# What makes a good model?

- **Efficient sampling:** Generating samples from the model should be computationally inexpensive and take advantage of the parallelism of modern hardware.
- **High-quality sampling:** The samples should be indistinguishable from the real data that the model was trained with.
- **Coverage:** Samples should represent the entire training distribution. It is insufficient to only generate samples that all look like a subset of the training data.
- Well-behaved latent space: Every latent variable z should correspond to a plausible data example x and smooth changes in z should correspond to smooth changes in x.
- Interpretable latent space: Manipulating each dimension of z should correspond to changing an interpretable property of the data. For example, in a model of language, it might change the topic, tense or degree of verbosity.
- Efficient likelihood computation: If the model is probabilistic, we would like to be able to calculate the probability of new examples efficiently and accurately

# Do we have good models?

	GANs	VAEs	Flows	Diffusion
Efficient sampling	✓	<b>√</b>	<b>√</b>	X
High quality	✓	X	Х	<b>√</b>
Coverage	Х	?	?	?
Well-behaved latent space	✓	✓	✓	Х
Interpretable latent space	?	?	?	Х
Efficient likelihood	n/a	X	✓	Х

How to measure performance within or between categories?

• Open research area.

### "Generative adversarial networks", Goodfellow et al

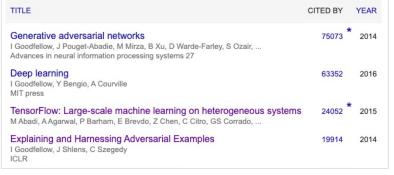


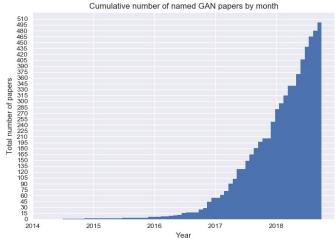
### Ian Goodfellow

PhD ML, U de Montréal 2014

- Google (TensorFlow, Google Brain)
- OpenAl
- Google Staff/Sr. Staff Research
   Scientist
- Apple Director of ML
- Google Deep Mind, Research Scientist

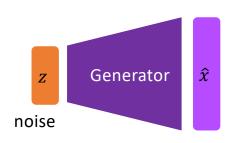






The GAN Zoo (Github)

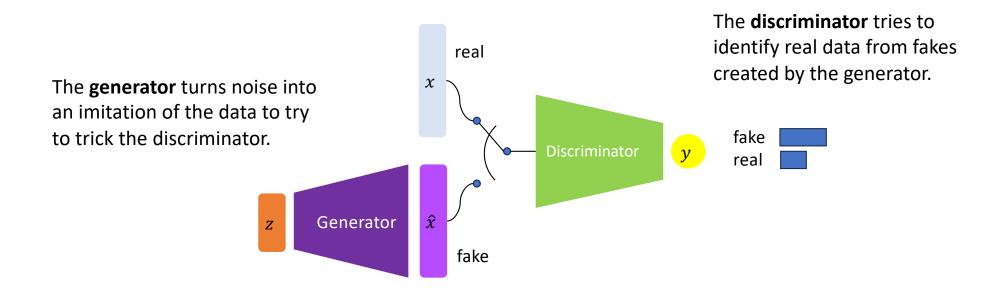
### General Idea of GANs



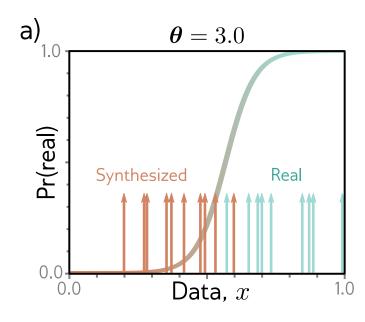
- Don't try to build a probability model directly
- Learn a transformation from a sample of noise to look similar to training data distribution

### Generative Adversarial Networks

Train a generative model to try to fool a "discriminator" model.

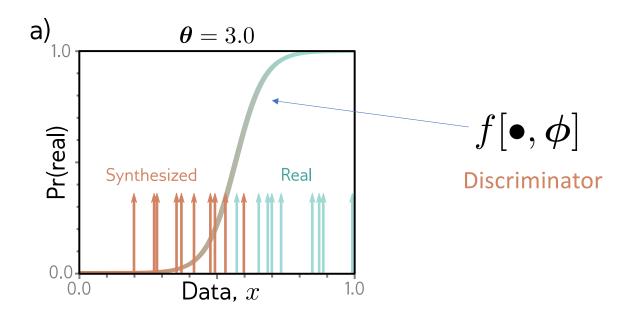


$$x_j^* = g[z_j, \theta] = z_j + \theta$$



- We take examples from a real distribution (e.g. shifted standard gaussian)
- We generate synthesized samples,  $z_j$ , from a standard gaussian and shift by  $\theta$ .
- Train a classifier on the data

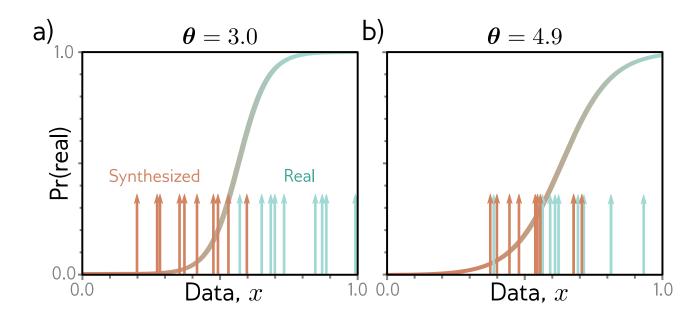
$$x_j^* = g[z_j, \theta] = z_j + \theta$$



- Train the discriminator
- ullet using logistic regression parameterized by  $\phi$
- as a binary classifier on the data

• e.g. 
$$\begin{cases} \text{real if } f[\cdot] \geq .5 \\ \text{fake if } f[\cdot] < .5 \end{cases}$$

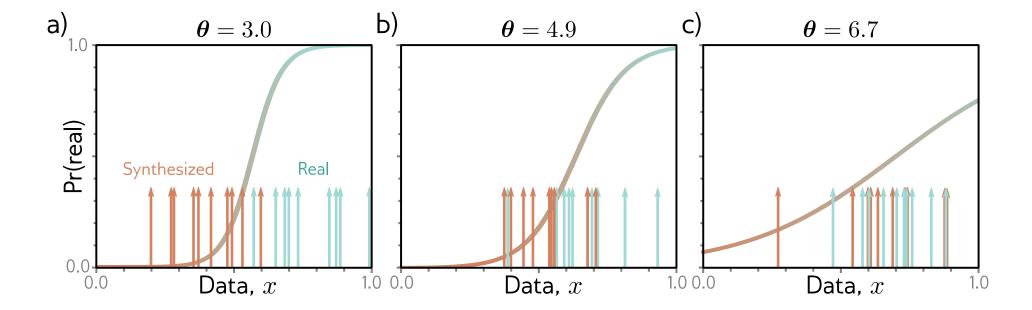
$$x_j^* = g[z_j, \theta] = z_j + \theta$$



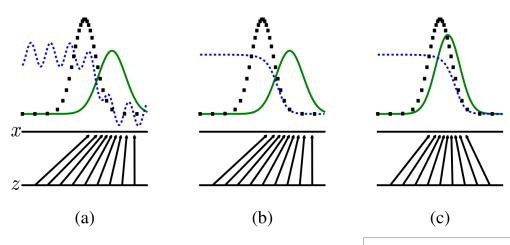
- Train the **generator** to update  $\theta$  in order to *increase* the loss on the discriminator
- Then train the discriminator to decrease the loss

$$x_j^* = g[z_j, \theta] = z_j + \theta$$

 Keep repeating till the discriminator does no better than random chance



# Trained to completion



- o z: uniform latent variable
- x: samples according to a (green solid) generative distribution
- o black dotted curve: real data distribution
- blue dashed curve: discriminator

### 4.1 Global Optimality of $p_g = p_{\text{data}}$

We first consider the optimal discriminator D for any given generator G.

(d)

**Proposition 1.** For G fixed, the optimal discriminator D is

$$D_G^*(oldsymbol{x}) = rac{p_{data}(oldsymbol{x})}{p_{data}(oldsymbol{x}) + p_g(oldsymbol{x})}$$

### **GANs**

- GAN loss function
- DCGAN results and problems
- Tricks for improving performance
- Conditional GANs
- Image translation models

### GAN cost function

**Discriminator** uses standard cross entropy loss (see Section 5.4 – binary classification loss): :

$$\hat{\boldsymbol{\phi}} = \underset{\boldsymbol{\phi}}{\operatorname{argmin}} \left[ \sum_{i} -(1 - y_i) \log \left[ 1 - \operatorname{sig}[f[\mathbf{x}_i, \boldsymbol{\phi}]] \right] - y_i \log \left[ \operatorname{sig}[f[\mathbf{x}_i, \boldsymbol{\phi}]] \right] \right]$$

### **GAN** cost function

**Discriminator** uses standard cross entropy loss (see Section 5.4 – binary classification loss):

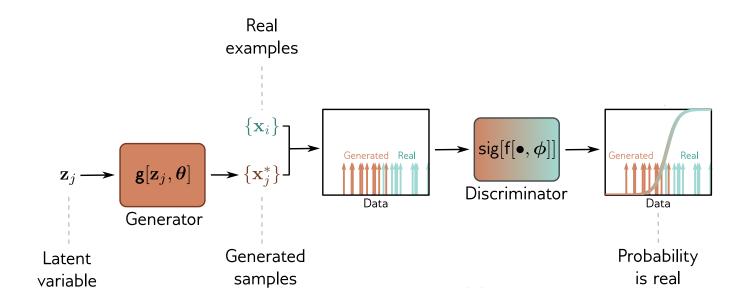
$$\hat{\boldsymbol{\phi}} = \underset{\boldsymbol{\phi}}{\operatorname{argmin}} \left[ \sum_{i} -(1 - y_i) \log \left[ 1 - \operatorname{sig}[f[\mathbf{x}_i, \boldsymbol{\phi}]] \right] - y_i \log \left[ \operatorname{sig}[f[\mathbf{x}_i, \boldsymbol{\phi}]] \right] \right]$$

Generated samples,  $\mathbf{x}_i^*$ ,  $y_i = 0$ , and for real examples,  $\mathbf{x}_i$ ,  $y_i = 1$ :

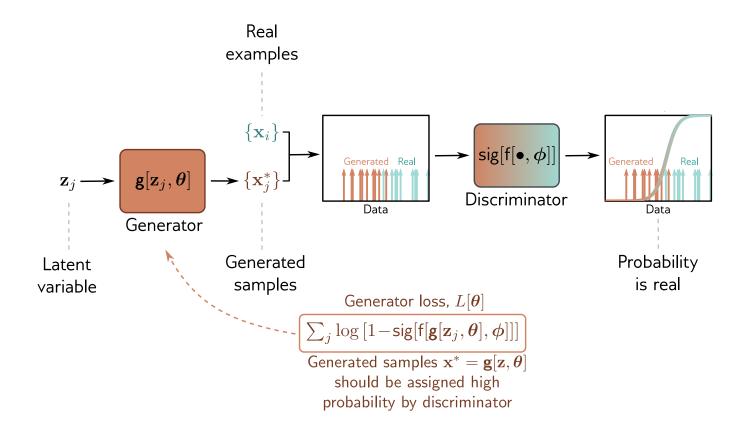
$$\hat{\phi} = \operatorname*{argmin} \left[ \sum_{j} - \log \left[ 1 - \operatorname{sig}[f[\mathbf{x}_{j}^{*}, \phi]] \right] - \sum_{i} \log \left[ \operatorname{sig}[f[\mathbf{x}_{i}, \phi]] \right] \right]$$
 These are *generated* samples so  $y_{j} = 0$  These are *real* samples so  $y_{i} = 1$ 

We can separate into two summations that separately index over the generated samples and the real samples.

### **GAN** loss function

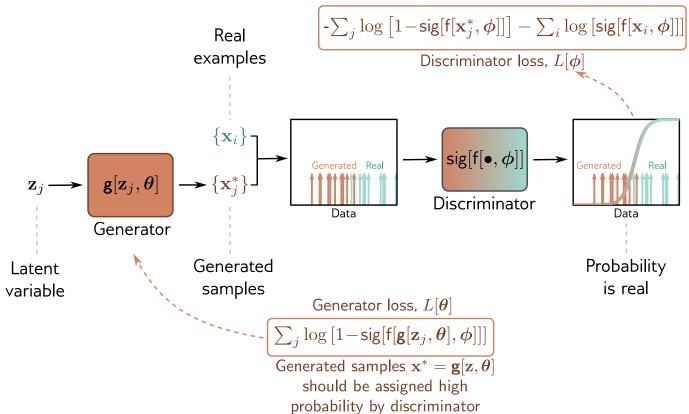


### **GAN** loss function



### **GAN** loss function

Generated samples  $x^*$  should have low probability Real examples x should have high probability



#### GAN cost function

Discriminator uses standard cross entropy loss:

$$\hat{\boldsymbol{\phi}} = \underset{\boldsymbol{\phi}}{\operatorname{argmin}} \left[ \sum_{i} -(1 - y_i) \log \left[ 1 - \operatorname{sig}[f[\mathbf{x}_i, \boldsymbol{\phi}]] \right] - y_i \log \left[ \operatorname{sig}[f[\mathbf{x}_i, \boldsymbol{\phi}]] \right] \right]$$

Discriminator: generated samples, y = 0, real examples, y = 1:

$$\hat{\boldsymbol{\phi}} = \underset{\boldsymbol{\phi}}{\operatorname{argmin}} \left[ \sum_{j} -\log \left[ 1 - \operatorname{sig}[f[\mathbf{x}_{j}^{*}, \boldsymbol{\phi}]] \right] - \sum_{i} \log \left[ \operatorname{sig}[f[\mathbf{x}_{i}, \boldsymbol{\phi}]] \right] \right]$$

Generator loss: make generated samples more likely under discriminator (i.e. make discriminator loss larger)

$$\hat{\boldsymbol{\phi}}, \hat{\boldsymbol{\theta}} = \underset{\boldsymbol{\theta}}{\operatorname{argmax}} \left[ \underset{\boldsymbol{\phi}}{\operatorname{argmin}} \left[ \sum_{j} -\log \left[ 1 - \operatorname{sig}[f[\mathbf{g}[\mathbf{z}_{j}, \boldsymbol{\theta}], \boldsymbol{\phi}]] \right] - \sum_{i} \log \left[ \operatorname{sig}[f[\mathbf{x}_{i}, \boldsymbol{\phi}]] \right] \right] \right]$$

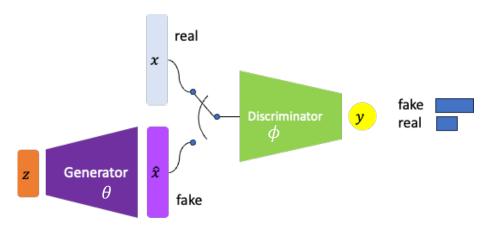
substituted the generator function for the generated sample

#### **GAN** Cost function

$$\hat{\boldsymbol{\phi}}, \hat{\boldsymbol{\theta}} = \underset{\boldsymbol{\theta}}{\operatorname{argmax}} \left[ \underset{\boldsymbol{\phi}}{\operatorname{argmin}} \left[ \sum_{j} - \log \left[ 1 - \operatorname{sig}[f[\mathbf{g}[\mathbf{z}_{j}, \boldsymbol{\theta}], \boldsymbol{\phi}]] \right] - \sum_{i} \log \left[ \operatorname{sig}[f[\mathbf{x}_{i}, \boldsymbol{\phi}]] \right] \right] \right]$$

The **discriminator** parameters,  $\phi$ , are manipulated to *minimize* the loss function

The **generator** parameters,  $\theta$ , are manipulated to *maximize* the loss function.



#### **GAN** Cost function

$$\hat{\boldsymbol{\phi}}, \hat{\boldsymbol{\theta}} = \underset{\boldsymbol{\theta}}{\operatorname{argmax}} \left[ \underset{\boldsymbol{\phi}}{\operatorname{argmin}} \left[ \sum_{j} - \log \left[ 1 - \operatorname{sig}[f[\mathbf{g}[\mathbf{z}_{j}, \boldsymbol{\theta}], \boldsymbol{\phi}]] \right] - \sum_{i} \log \left[ \operatorname{sig}[f[\mathbf{x}_{i}, \boldsymbol{\phi}]] \right] \right] \right]$$

The **discriminator** parameters,  $\phi$ , are manipulated to *minimize* the loss function

The **generator** parameters,  $\theta$ , are manipulated to *maximize* the loss function.

Can divide into two parts:

$$\textbf{discriminator loss:} \quad L[\boldsymbol{\phi}] = \sum_{j} -\log \Big[1 - \mathrm{sig}[\mathrm{f}[\mathbf{g}[\mathbf{z}_{j}, \boldsymbol{\theta}], \boldsymbol{\phi}]]\Big] - \sum_{i} \log \Big[\mathrm{sig}[\mathrm{f}[\mathbf{x}_{i}, \boldsymbol{\phi}]]\Big]$$

negated **generator** loss: 
$$L[m{ heta}] = \sum_j \log \Big[1 - \mathrm{sig}[\mathrm{f}[\mathbf{g}[\mathbf{z}_j, m{ heta}], m{\phi}]]\Big]$$

The 2<sup>nd</sup> term is constant w.r.t.  $\theta$  (gradient  ${^{\partial \mathcal{L}}/_{\partial \theta}}=0$ ) so we can drop it)

#### **GAN Solution**

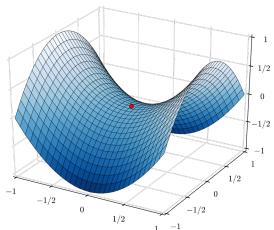
$$\hat{\boldsymbol{\phi}}, \hat{\boldsymbol{\theta}} = \underset{\boldsymbol{\theta}}{\operatorname{argmax}} \left[ \underset{\boldsymbol{\phi}}{\operatorname{argmin}} \left[ \sum_{j} -\log \left[ 1 - \operatorname{sig}[f[\mathbf{g}[\mathbf{z}_{j}, \boldsymbol{\theta}], \boldsymbol{\phi}]] \right] - \sum_{i} \log \left[ \operatorname{sig}[f[\mathbf{x}_{i}, \boldsymbol{\phi}]] \right] \right] \right]$$

- The solution is the Nash equilibrium
- OIt lays at a saddle point
- ols inherently unstable

#### Nash equilibrium

In game theory, the Nash equilibrium, named after the mathematician John Nash, is the most common way to define the solution of a non-cooperative game involving two or more players.

...each player is assumed to know the equilibrium strategies of the other players, and no one has anything to gain by changing only one's own strategy. <u>Wikipedia</u>







### GAN Training Flow Pseudo Python

```
for c_gan_iter in range(n_gan_iters): # GAN Iterations

# Run generator to produce synthesized data
x_syn = generator(z, theta)

# Update/train the discriminator
phi = update_discriminator(x_real, x_syn, n_iter_discrim, phi)

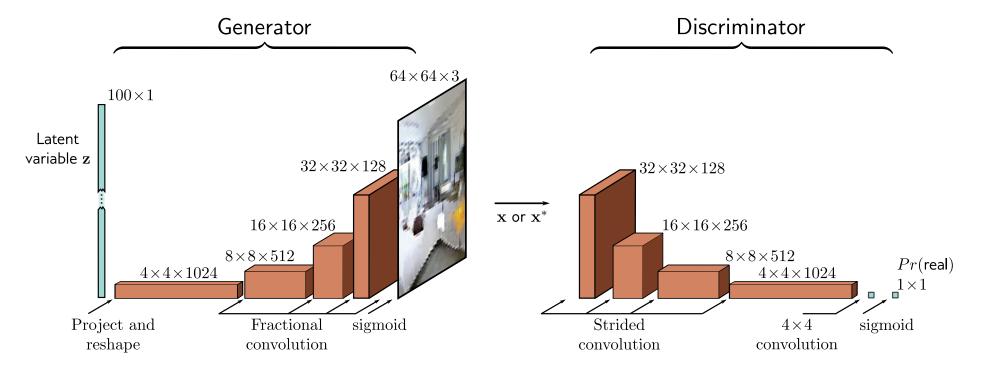
# Update/train the generator
theta = update_generator(z, theta, n_iter_gen, phi)
```

### **GANs**

- GAN loss function
- DCGAN results and problems
- Tricks for improving performance
- Conditional GANs
- Image translation models

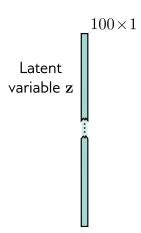
### Deep Convolutional (DC) GAN

• Early GAN specialized in image generation

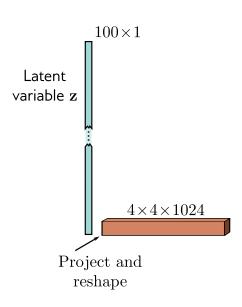


### DCGAN -- Generator

• Input is 100D latent variable, z, drawn from a uniform distribution

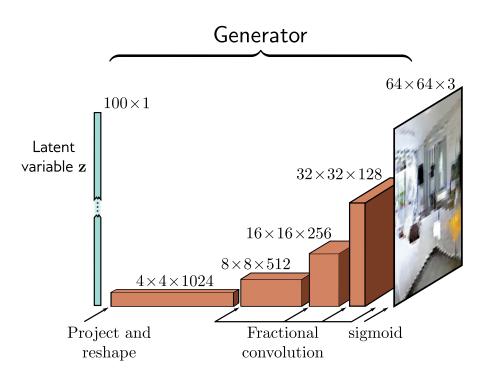


#### DCGAN -- Generator



- Input is 100D latent variable, z, drawn from a uniform distribution
- Maps to 4x4x1024 via a linear transformation

#### DCGAN -- Generator

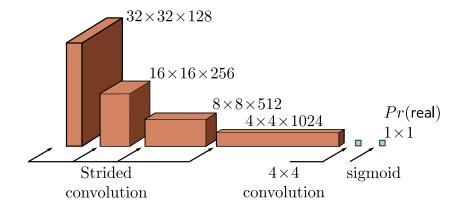


- Input is 100D latent variable, z, drawn from a uniform distribution
- Maps to 4x4x1024 via a linear transformation
- Fractionally strided (stride = 0.5) convolutions to double resolution in each dimension
- Final tanh to limit to [-1,1]
- Rescaled to [0,255]

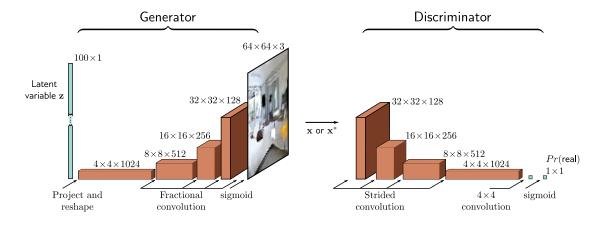
### DCGAN -- Discriminator

- Standard convolution network
- Reduces to 1x1
- Final sigmoid to create output probability





### Deep Convolutional (DC) GAN



#### Trained as in the earlier example.

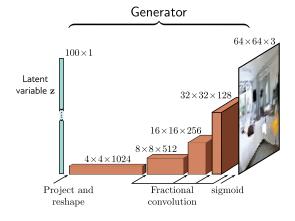
```
for c_gan_iter in range(5): # GAN Iterations

# Run generator to produce synthesized data
x_syn = generator(z, theta)

# Update/train the discriminator
phi = update_discriminator(x_real, x_syn, n_iter_discrim, phi)

# Update/train the generator
theta = update_generator(z, theta, n_iter_gen, phi)
```

### Deep Convolutional (DC) GAN



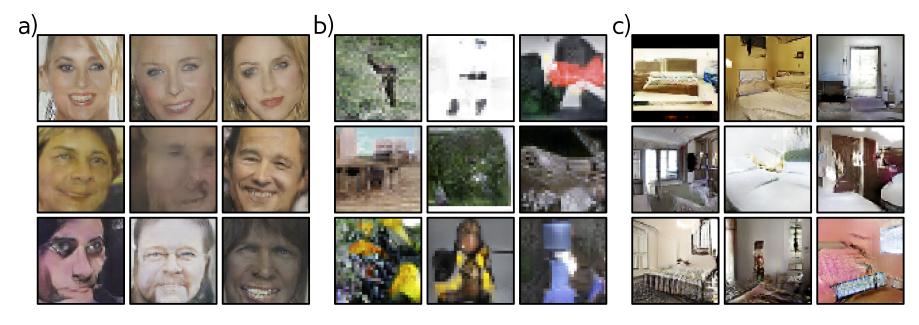
When training is complete

Discard discriminator

Draw new latent variable

Pass through generator

### DC GAN Results



Trained on a faces dataset.

Trained on ImageNet dataset.

Trained on LSUN dataset.

The LSUN classification dataset contains 10 scene categories, such as dining room, bedroom, chicken, outdoor church, and so on.

#### Common Failures with GANs

**Mode Dropping**: Only represent a subset of the training distribution.

Mode Collapse: Extreme case where the generator mostly ignores the latent variable and collapses all samples to a few points



#### GAN Performance and Distribution Distance

$$D_{JS}\left[Pr(\mathbf{x}^*) \mid\mid Pr(\mathbf{x})\right] = \underbrace{\frac{1}{2}D_{KL}\left[Pr(\mathbf{x}^*) \mid\mid \frac{Pr(\mathbf{x}^*) + Pr(\mathbf{x})}{2}\right]}_{\text{quality}} + \underbrace{\frac{1}{2}D_{KL}\left[Pr(\mathbf{x}) \mid\mid \frac{Pr(\mathbf{x}^*) + Pr(\mathbf{x})}{2}\right]}_{\text{coverage}}$$

Summary of lengthy analysis in §15.2.1 "Analysis of GAN loss function" Can be rewritten in terms of dissimilarities between *generated* and *real* probability distributions.

Two important takeaways:

Quality: Generated samples need to occur where real samples are

**Coverage**: Where there is concentrations of real samples, there should be good representation from generated samples

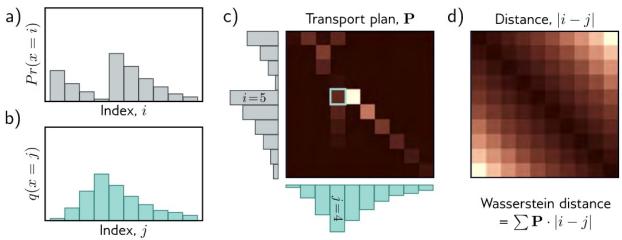
#### We can conclude that:

- (i) the GAN loss can be interpreted in terms of distances between probability distributions and that
- (ii) the gradient of this distance becomes zero when the generated samples are too easy to distinguish from the real examples.

We need a distance metric with better properties.

# Wassertein Distance (for continuous distributions) Earth Mover's Distance (for discrete probabilities)

- The quantity of work required to transport the probability mass from one distribution to create the other.
- Use linear programming to find an optimal "transport plan" that minimizes  $\sum \mathbf{P} \cdot |i-j|$

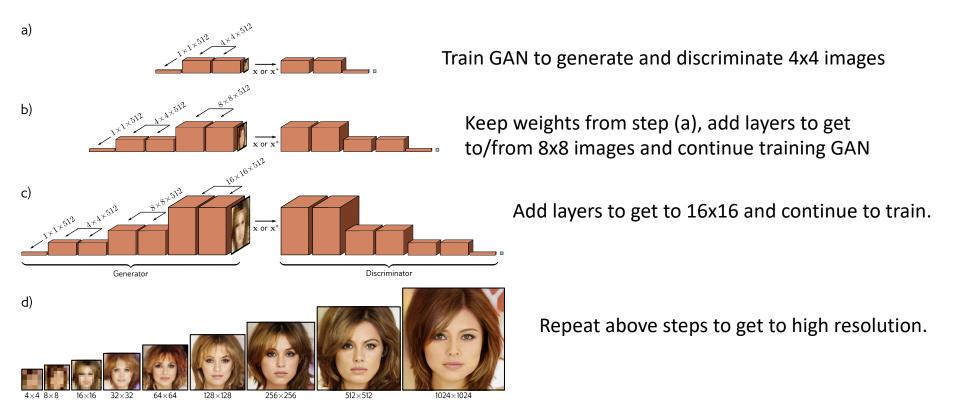


See 15.2.4 Wasserstein distance for discrete distributions

### **GANs**

- GAN loss function
- DCGAN results and problems
- Tricks for improving performance
- Conditional GANs
- Image translation models

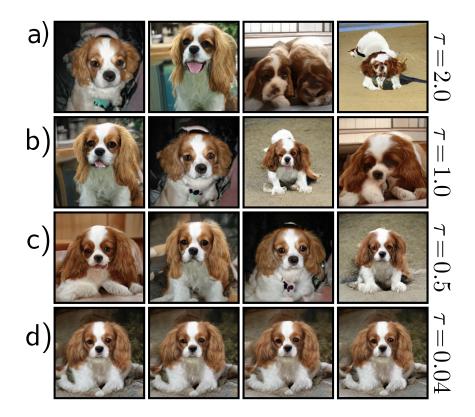
### Trick 1: Progressive growing



#### Trick 2: Minibatch discrimination

- Add in statistics across minibatches of synthesized and real data
- Provided to the discriminator as an additional feature map
- Sends signal back to generator to try to better match real batch statistics

### Trick 3: Truncation



- Only choose random values of latent variables that are less than a threshold  $\tau$  distance from the mean of the latent variables.
- Reduces variation but improves quality

### Interpolation

**Well-behaved latent space:** Every latent variable z should correspond to a plausible data example x and smooth changes in z should correspond to smooth changes in x.











## Interpolation

**Well-behaved latent space:** Every latent variable z should correspond to a plausible data example x and smooth changes in z should correspond to smooth changes in x.



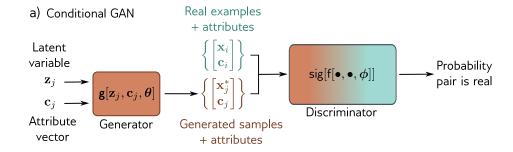
### **GANs**

- GAN loss function
- DCGAN results and problems
- Tricks for improving performance
- Conditional GANs
- Image translation models

#### Lack of control

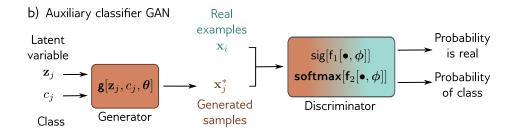
- Cannot specify attributes of generated images from vanilla GANs
- E.g. can't choose ethnicity, age, etc., for a GAN trained on faces.
- Conditional generation models provide this control

#### Conditional GAN models



- Passes a vector **c** of attributes to both the generator and discriminator
- Generator learns to generate sample with correct attribute
- Discriminator learns to distinguish between generated sample with target attribute and real sample with real attribute

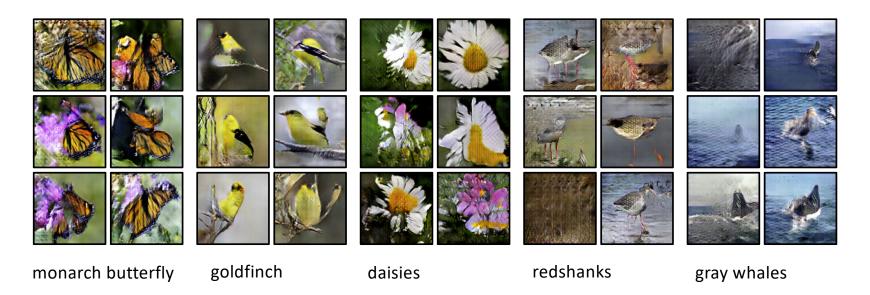
### Auxiliary classifier GAN



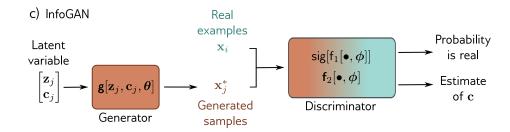
- Similar to Conditional GAN, but use class label instead of attribute vector
- Discriminator produces:
  - Binary real/fake classifier
  - Multi-class classifier

# Auxiliary Classifier GAN results

Trained on ImageNet images and classes.

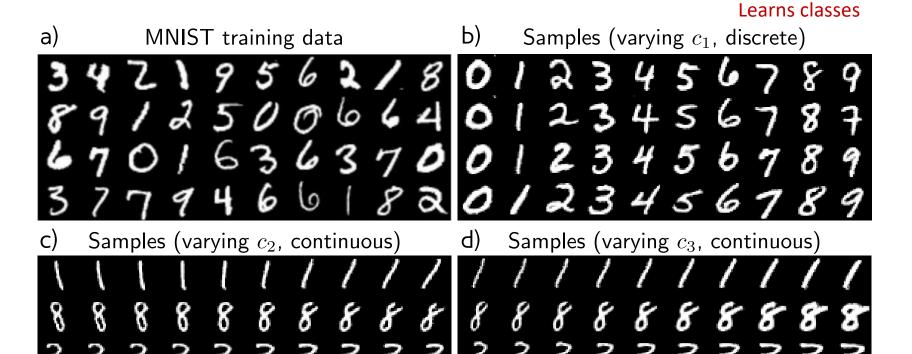


### InfoGAN



- Add random attribute variables c to generator
- Discriminator learns to predict discrete and continuous values of the attributes

#### InfoGAN results



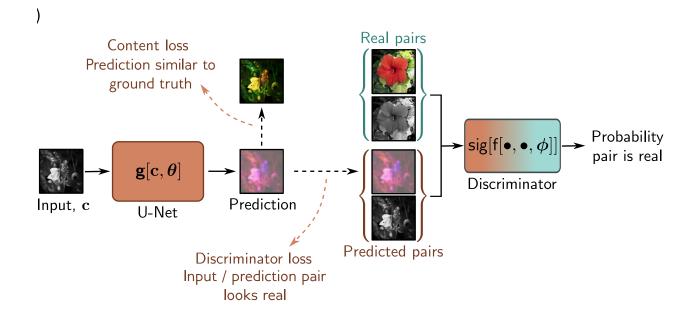
Learns orientation

Learns stroke thickness

### **GANs**

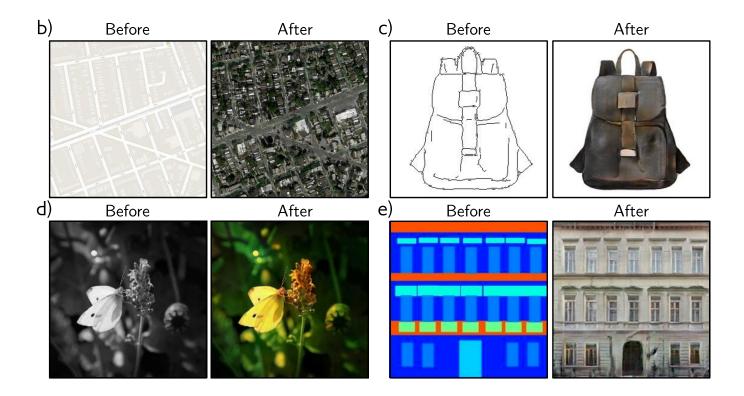
- GAN loss function
- DCGAN results and problems
- Tricks for improving performance
- Conditional GANs
- Image translation models

Image translation: Pix2Pix

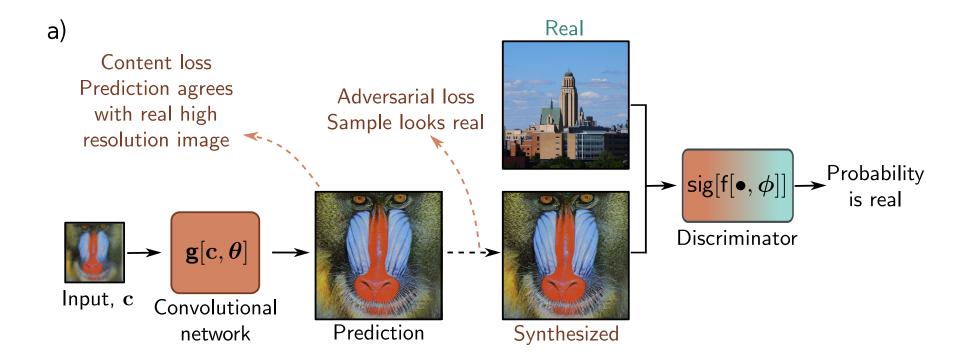


- Maps one image to a different style image using a U-Net type model
- Adds a content loss ( $\ell_1$ norm) to make the input similar to ground truth
- Discriminator fed input/prediction and real/modified pairs to predict real or fake

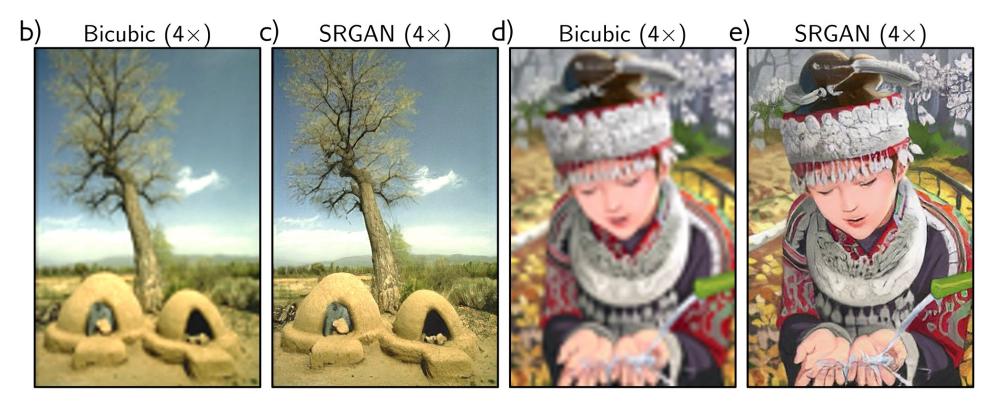
### Image translation: Pix2Pix



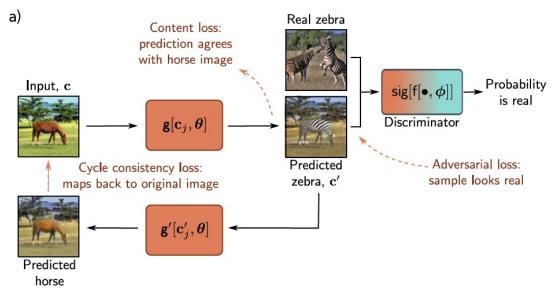
### Image translation: SRGAN



### Image translation: SRGAN



### Image translation: CycleGAN



2<sup>nd</sup> model is also trained.

Encourages the generator to be reversible

Doesn't need labeled or matched training pairs.

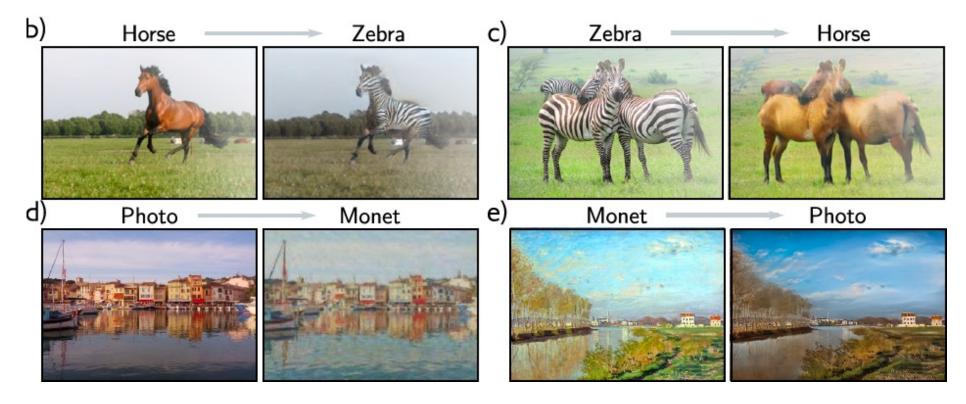
Have two sets of data with distinct styles but no matching pairs.

E.g. Horses and zebras, or photos and Monet paintings

#### Three losses

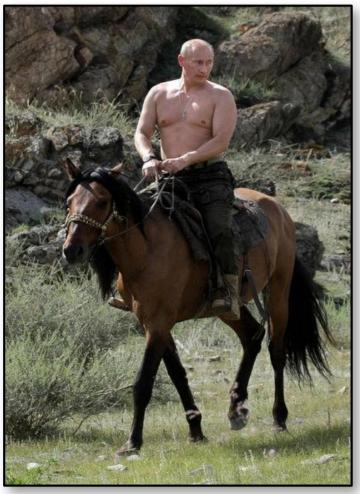
- 1. Content loss based on ( $\ell_1$ norm)
- 2. Discriminator loss (real vs fake)
- 3. Cycle-consistency loss

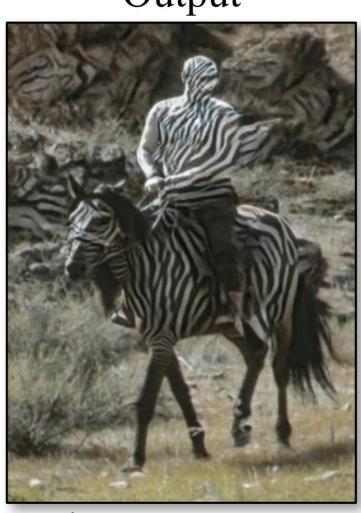
### Image translation: CycleGAN



### Input





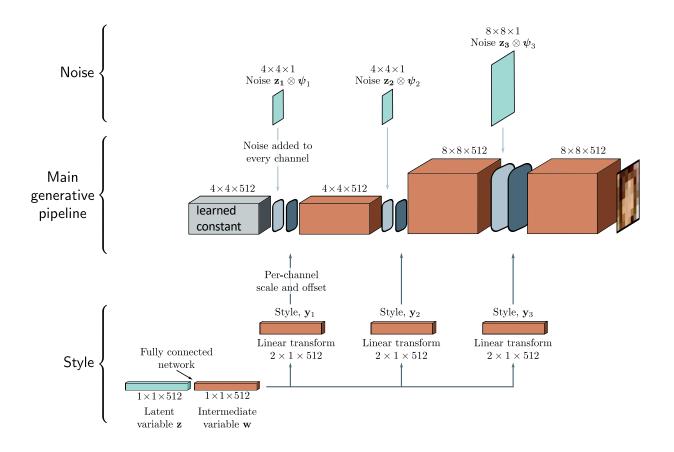


horse → zebra

### **GANs**

- GAN loss function
- DCGAN results and problems
- Tricks for improving performance
- Conditional GANs
- Image translation models
- StyleGAN

### Style GAN



Separates style from noise at different scales

**Face Examples** 

Large style changes: face shape, head pose

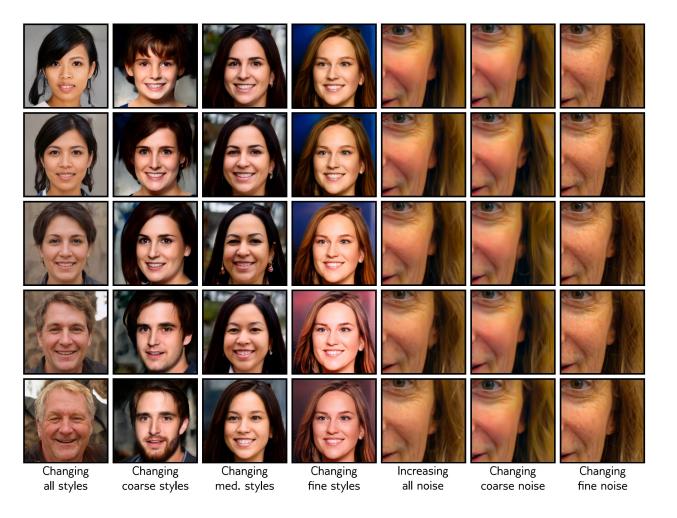
Medium-scale changes: facial features

Fine-scale: hair and skin

color

Noise: hair placement,

freckles



**Figure 15.20** StyleGAN results. First four columns show systematic changes in style at various scales. Fifth column shows the effect of increasing noise magnitude. Last two columns show different noise vectors at two different scales.

### **Upcoming Topics**

- VAEs
- Diffusion Models
- Graph Neural Networks
- Reinforcement Learning

### Feedback



Link