

Topics:

- Image Segmentation and Decoders
- Generative Adversarial Networks

CS 4644-DL / 7643-A

ZSOLT KIRA

- **Assignment 3**
 - Due **March 9th 11:59pm EST**
 - **Oops.** Diffusion models accidentally included. No need to do it by Mar 9th! @258
- **Projects**
 - Project proposal due **March ~~15th~~ 17th**
 - Proposal description out on canvas @256
- Meta office hours today 3pm ET on language models

Self-Attention Layer

One **query** per **input vector**

Inputs:

Input vectors: X (Shape: $N_x \times D_x$)

Key matrix: W_k (Shape: $D_x \times D_Q$)

Value matrix: W_v (Shape: $D_x \times D_v$)

Query matrix: W_Q (Shape: $D_x \times D_Q$)

Computation:

Query vectors: $Q = XW_Q$

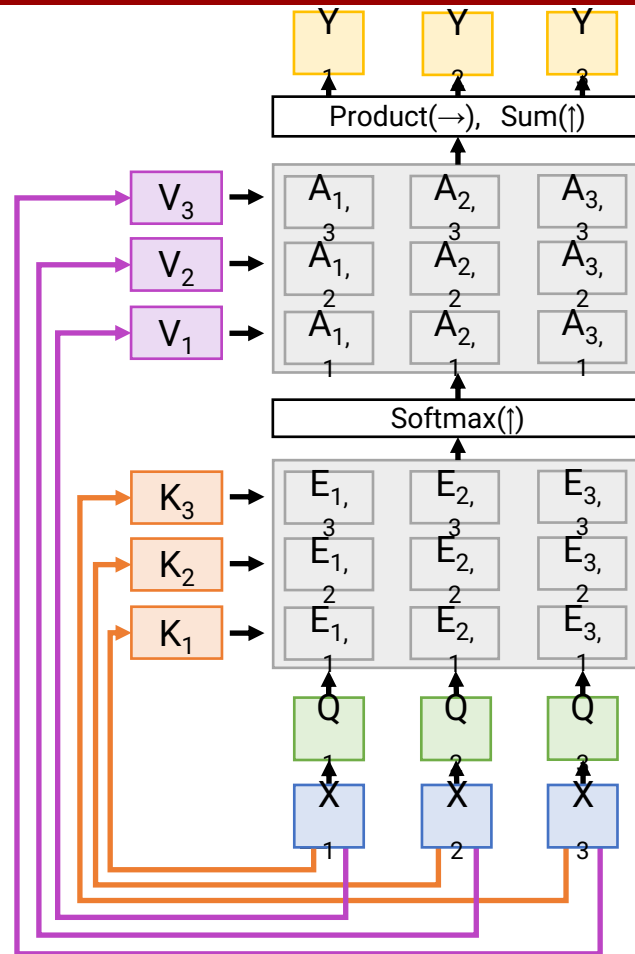
Key vectors: $K = XW_k$ (Shape: $N_x \times D_Q$)

Value vectors: $V = XW_v$ (Shape: $N_x \times D_v$)

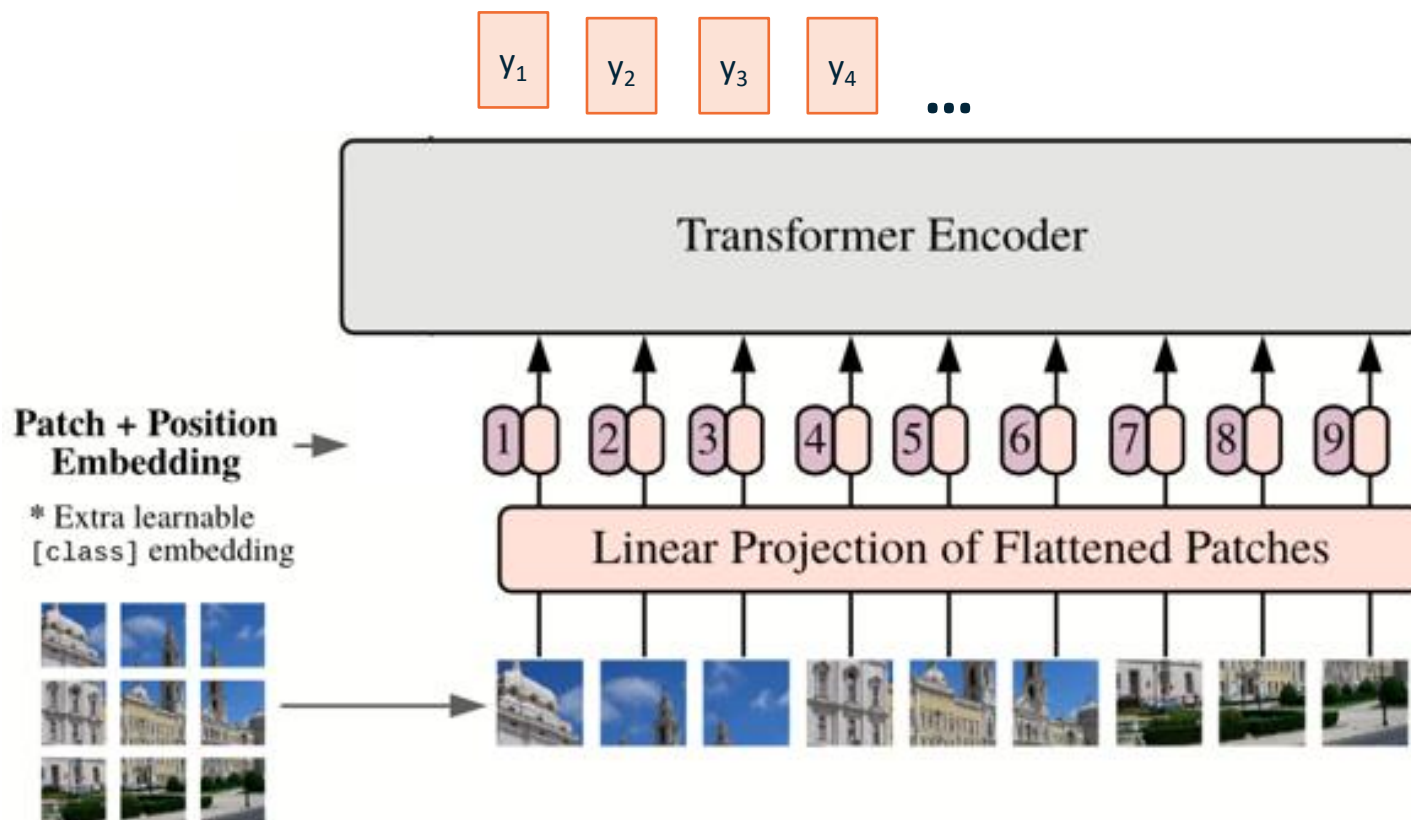
Similarities: $E = QK^T$ (Shape: $N_x \times N_x$) $E_{ij} = Q_i \cdot K_j / \text{sqrt}(D_Q)$

Attention weights: $A = \text{softmax}(E, \text{dim}=1)$ (Shape: $N_x \times N_x$)

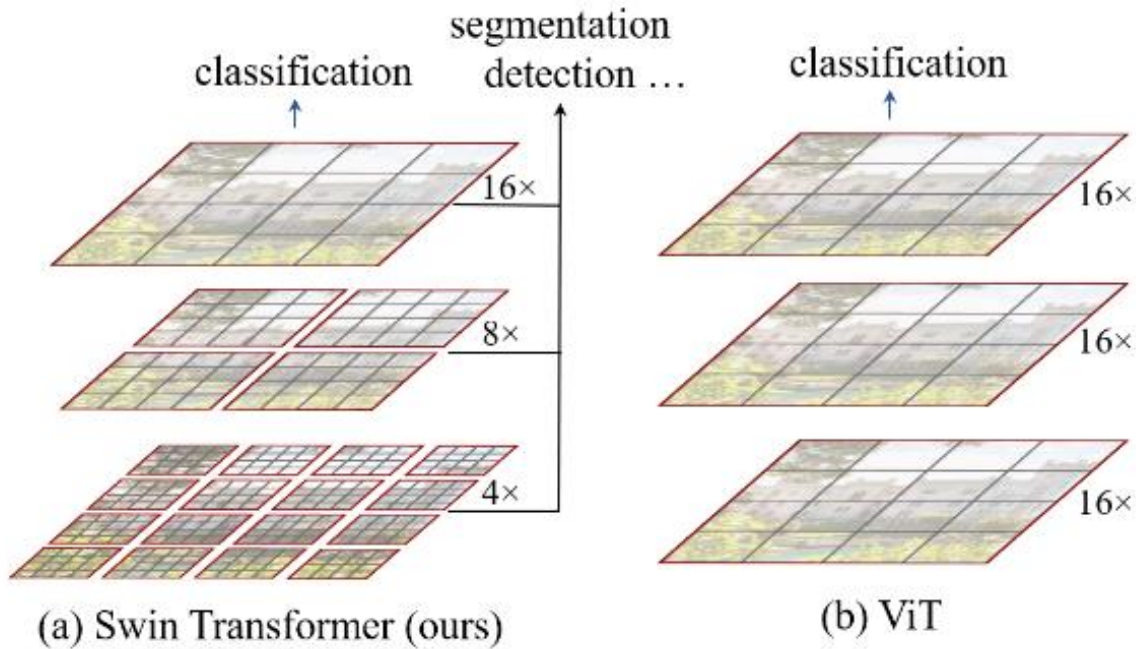
Output vectors: $Y = AV$ (Shape: $N_x \times D_v$) $Y_i = \sum_j A_{ij} V_j$



- How do we do classification?



Patches as input to Self-Attention



Ideas:

- Use smaller patches (4x4x3)
- Project them to lower dimension (4)
- Merge tokens at deeper levels
- Full attention => Window attention
 - => Shifted window attention

Swin Transformer: Hierarchical Vision Transformer using Shifted Windows

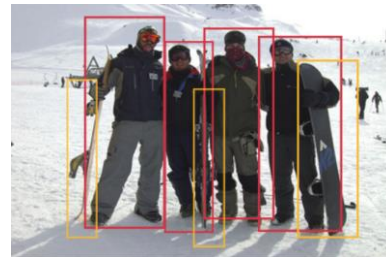
Ze Liu, Yutong Lin, Yue Cao, Han Hu, Yixuan Wei, Zheng Zhang, Stephen Lin, Baining Guo

Image Segmentation Networks



Classification

(Class distribution per image)



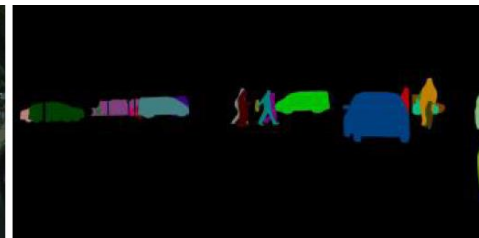
Object Detection

(List of bounding boxes with class distribution per box)



Semantic Segmentation

(Class distribution per pixel)

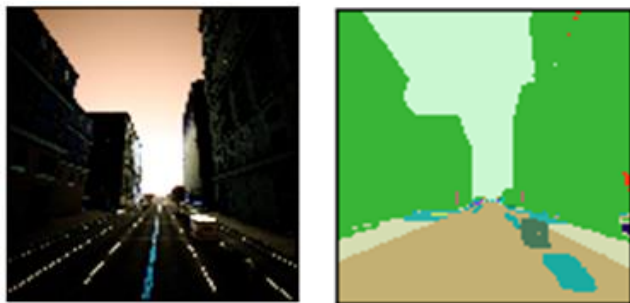


Instance Segmentation

(Class distribution per pixel with unique ID)

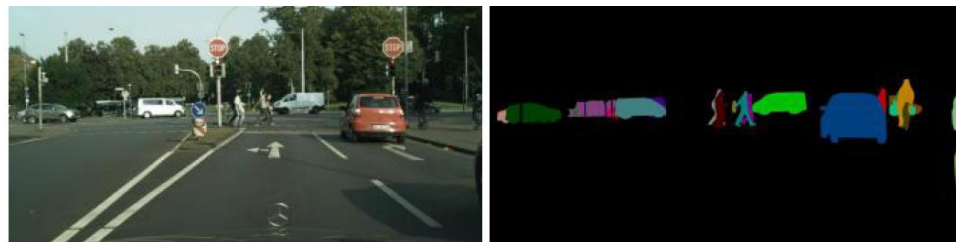
Given an image, output another image

- Each output contains class distribution per pixel
- More generally an image-to-image problem



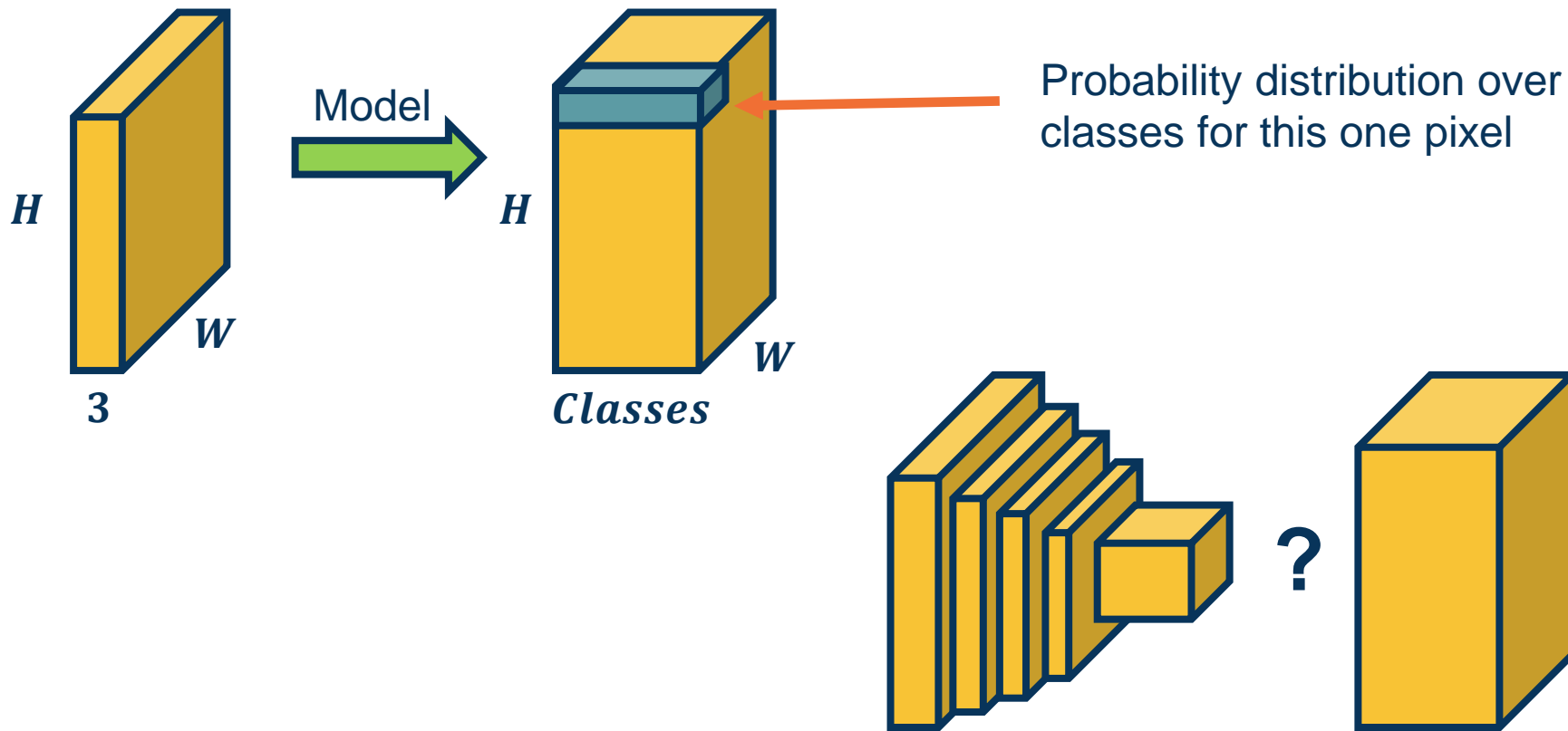
Semantic Segmentation

(Class distribution per pixel)

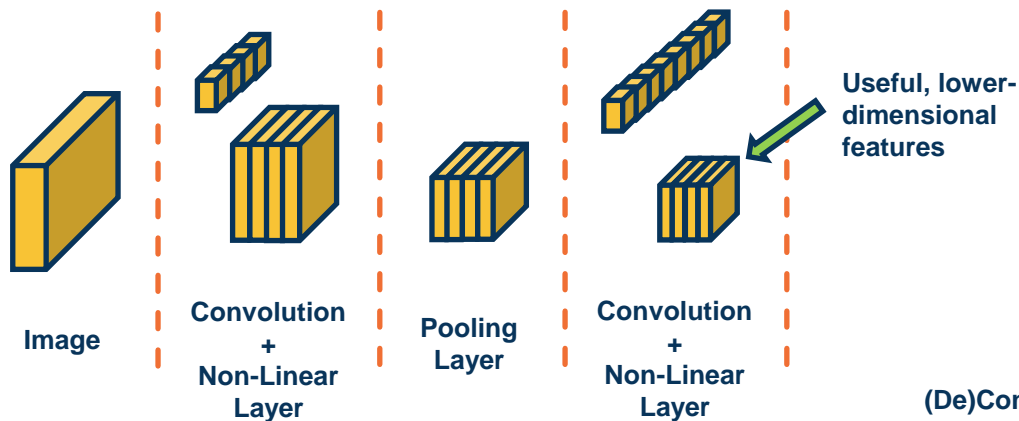


Instance Segmentation

(Class distribution per pixel with unique ID)



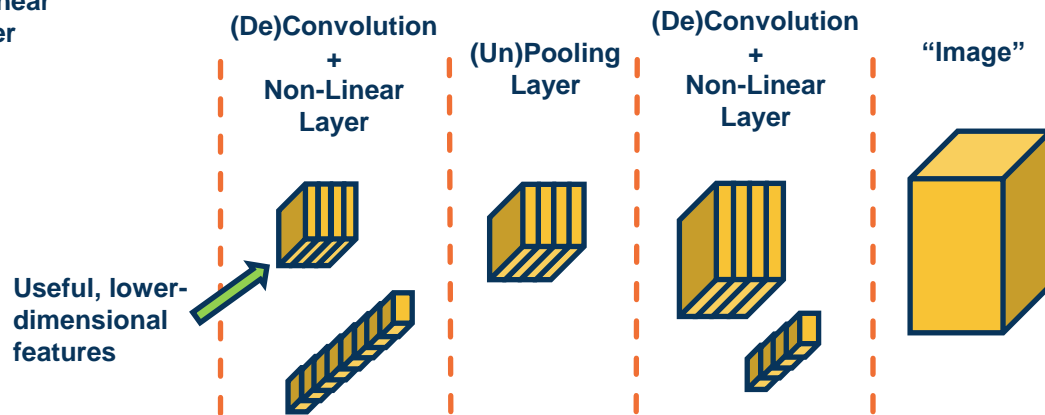
Convolutional Neural Network (CNN)



Encoder

We can develop learnable or non-learnable upsampling layers!

Decoder

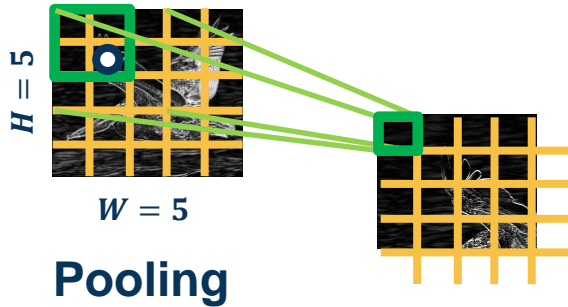


Idea: “De”Convolution and UnPooling

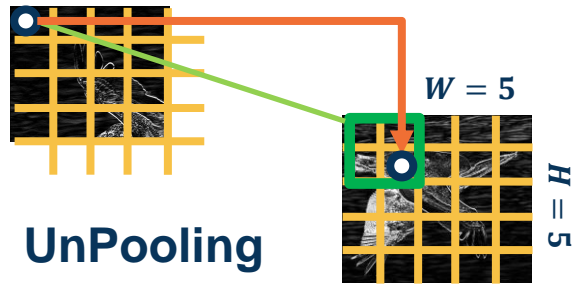
Example : Max pooling

- ◆ Stride window across image but perform per-patch **max operation**

$$X(0:1, 0:1) = \begin{bmatrix} 100 & 150 \\ 100 & 200 \end{bmatrix} \longrightarrow \max(0:1, 0:1) = 200$$



Copy value to position chosen as max in encoder, fill rest of this window with zeros



Idea: Remember max elements in encoder! Copy value from equivalent position, rest are zeros

$$X = \begin{bmatrix} 120 & 150 & 120 \\ 100 & 50 & 110 \\ 25 & 25 & 10 \end{bmatrix} \xrightarrow{\text{2x2 max pool}} Y = \begin{bmatrix} 150 & 150 \\ 100 & 110 \end{bmatrix}$$

Encoder

Decoder

$$X = \begin{bmatrix} 300 & 450 \\ 100 & 250 \end{bmatrix} \xrightarrow{\text{2x2 max unpool}} Y = \begin{bmatrix} 0 & 300 & - \\ 0 & 0 & - \\ - & - & - \end{bmatrix}$$

Max Unpooling Example (one window)

$$X_{\text{enc}} = \begin{bmatrix} 120 & 150 & 120 \\ 100 & 50 & 110 \\ 25 & 25 & 10 \end{bmatrix} \xrightarrow{2 \times 2 \text{ max pool}} Y_{\text{enc}} = \begin{bmatrix} 150 & 150 \\ 100 & 110 \end{bmatrix}$$

Encoder

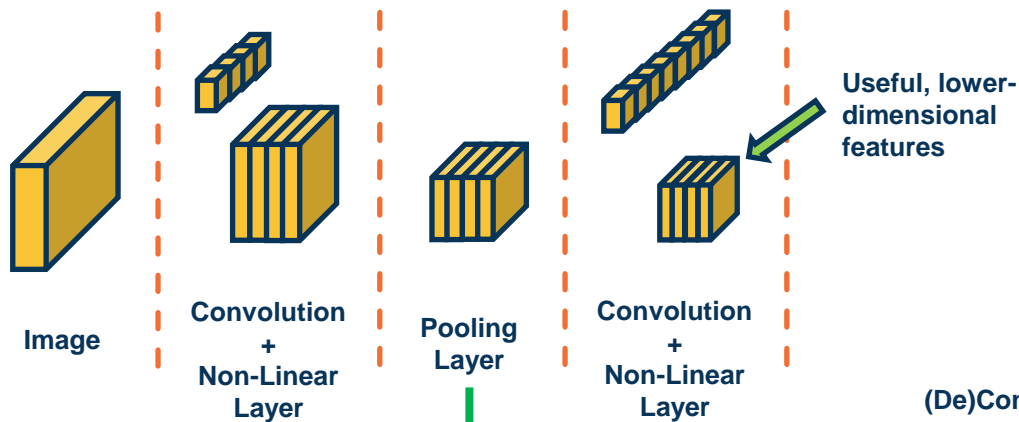
Contributions from multiple windows are summed

$$X_{\text{dec}} = \begin{bmatrix} 300 & 450 \\ 100 & 250 \end{bmatrix} \xrightarrow{2 \times 2 \text{ max unpool}} Y_{\text{dec}} = \begin{bmatrix} 0 & 300 + 450 & 0 \\ 100 & 0 & 250 \\ 0 & 0 & 0 \end{bmatrix}$$

Decoder

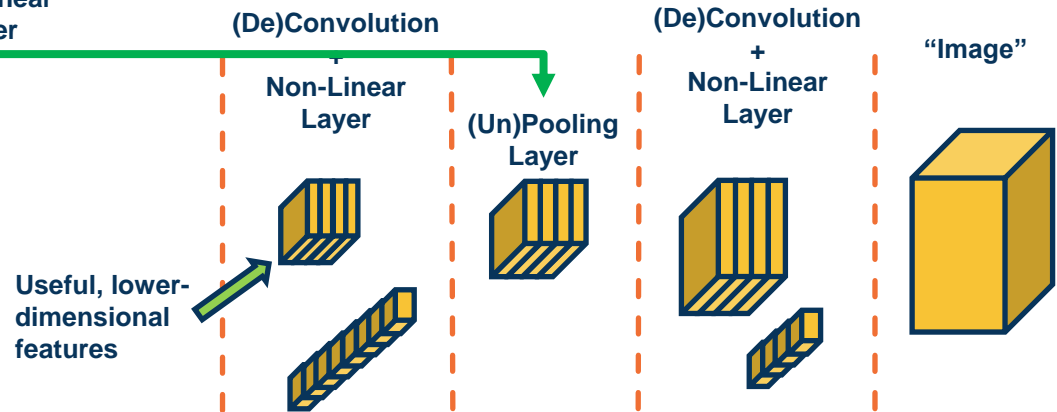
Max Unpooling Example

Convolutional Neural Network (CNN)



We pull max indices from corresponding layers (requires symmetry in encoder/decoder)

Decoder

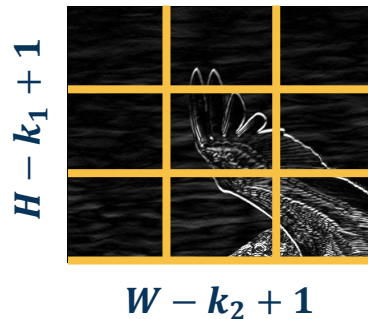
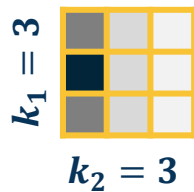


Encoder

Symmetry in Encoder/Decoder

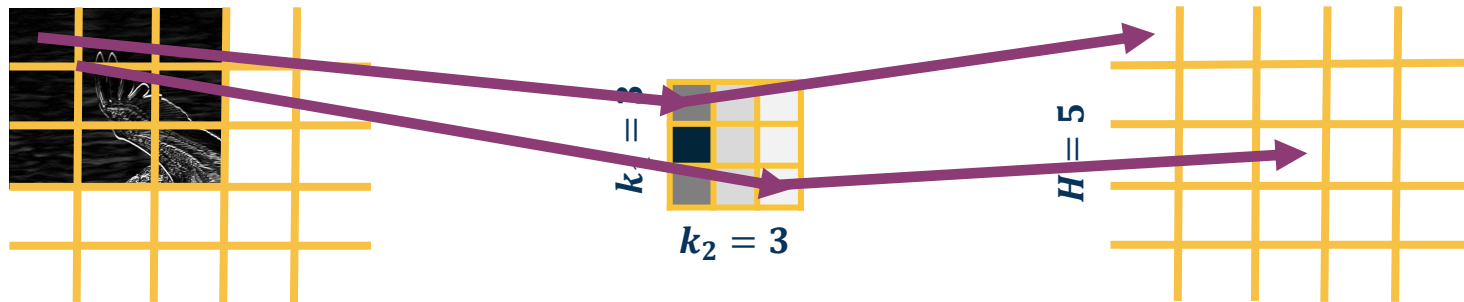
How can we *upsample* using convolutions and learnable kernel?

Normal Convolution



Transposed Convolution (also known as “deconvolution”, fractionally strided conv)

Idea: Take each input pixel, multiply by learnable kernel, “stamp” it on output



“De”Convolution (Transposed Convolution)

$$X = \begin{bmatrix} 120 & 150 & 120 \\ 100 & 50 & 110 \\ 25 & 25 & 10 \end{bmatrix}$$

$$K = \begin{bmatrix} 1 & -1 \\ 2 & -2 \end{bmatrix}$$

Contributions from multiple windows are summed

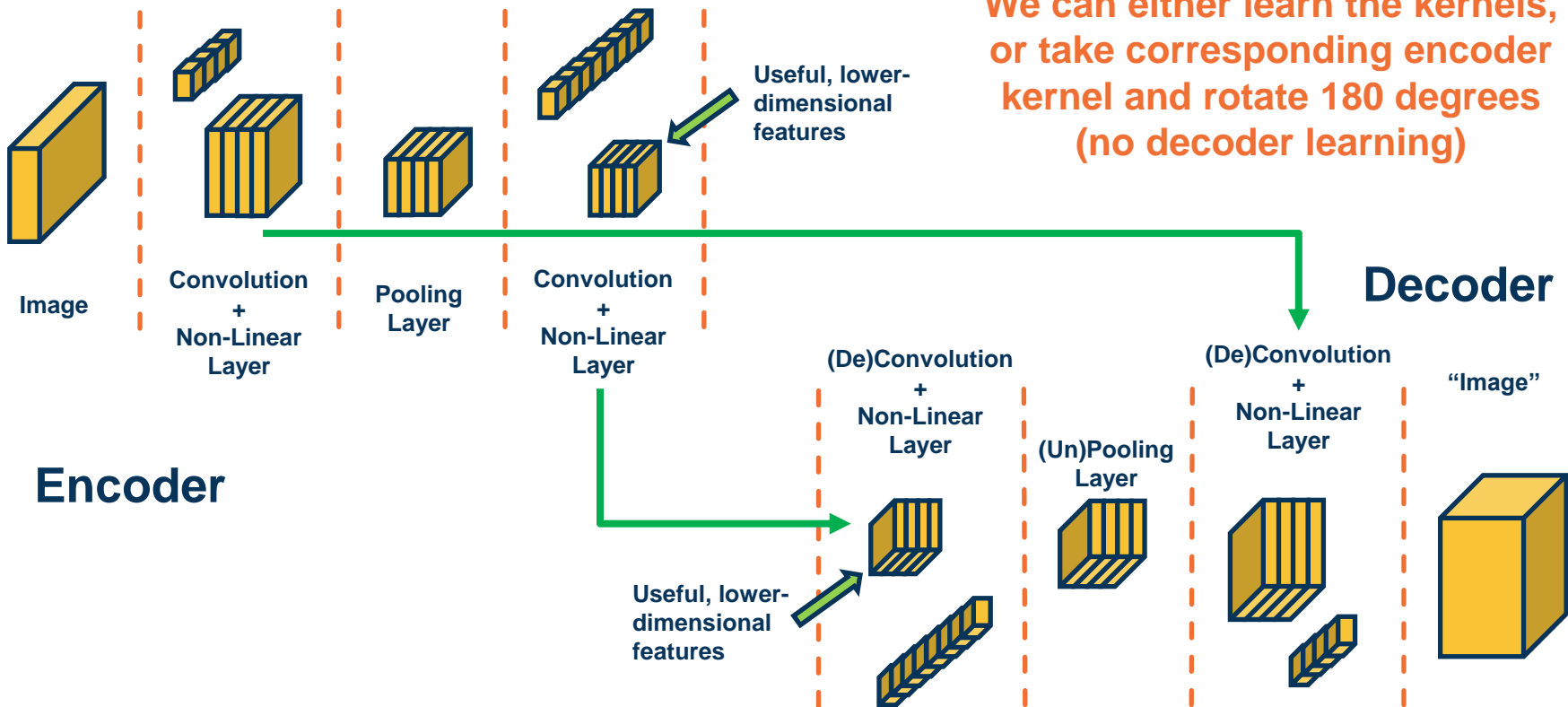
$$\begin{bmatrix} 120 & -120 & 0 & 0 \\ 240 & -240 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Incorporate
X(0,0)

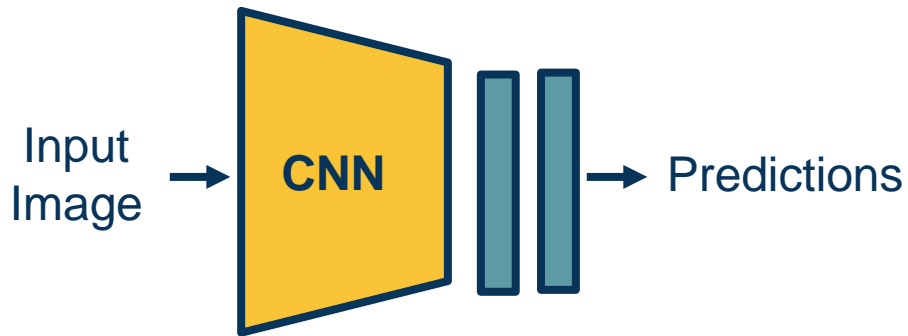
$$\begin{bmatrix} 120 & -120 + 150 & -150 & 0 \\ 240 & -240 + 300 & -300 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Incorporate
X(1,0)

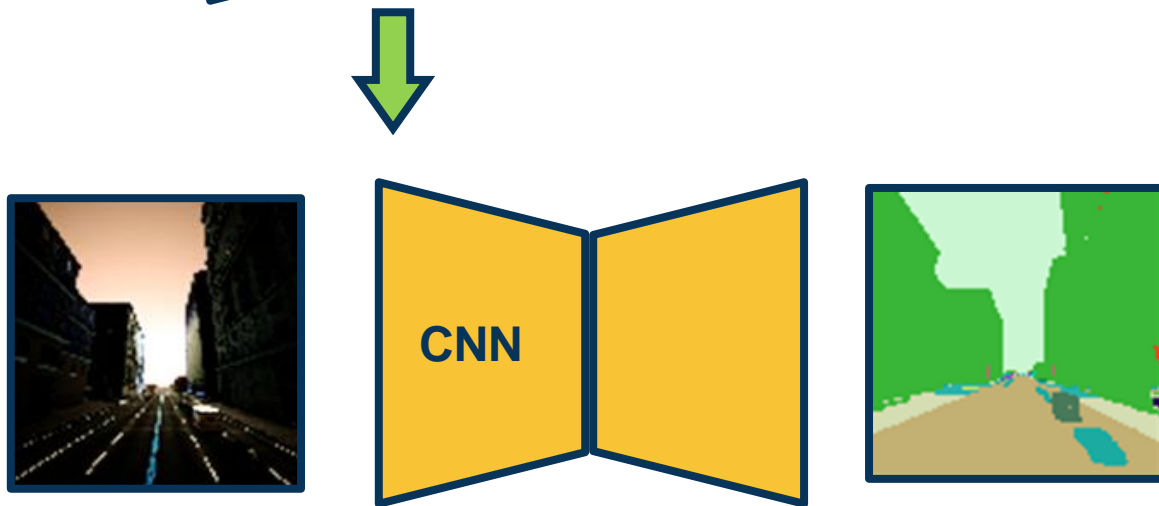
Convolutional Neural Network (CNN)



Symmetry in Encoder/Decoder

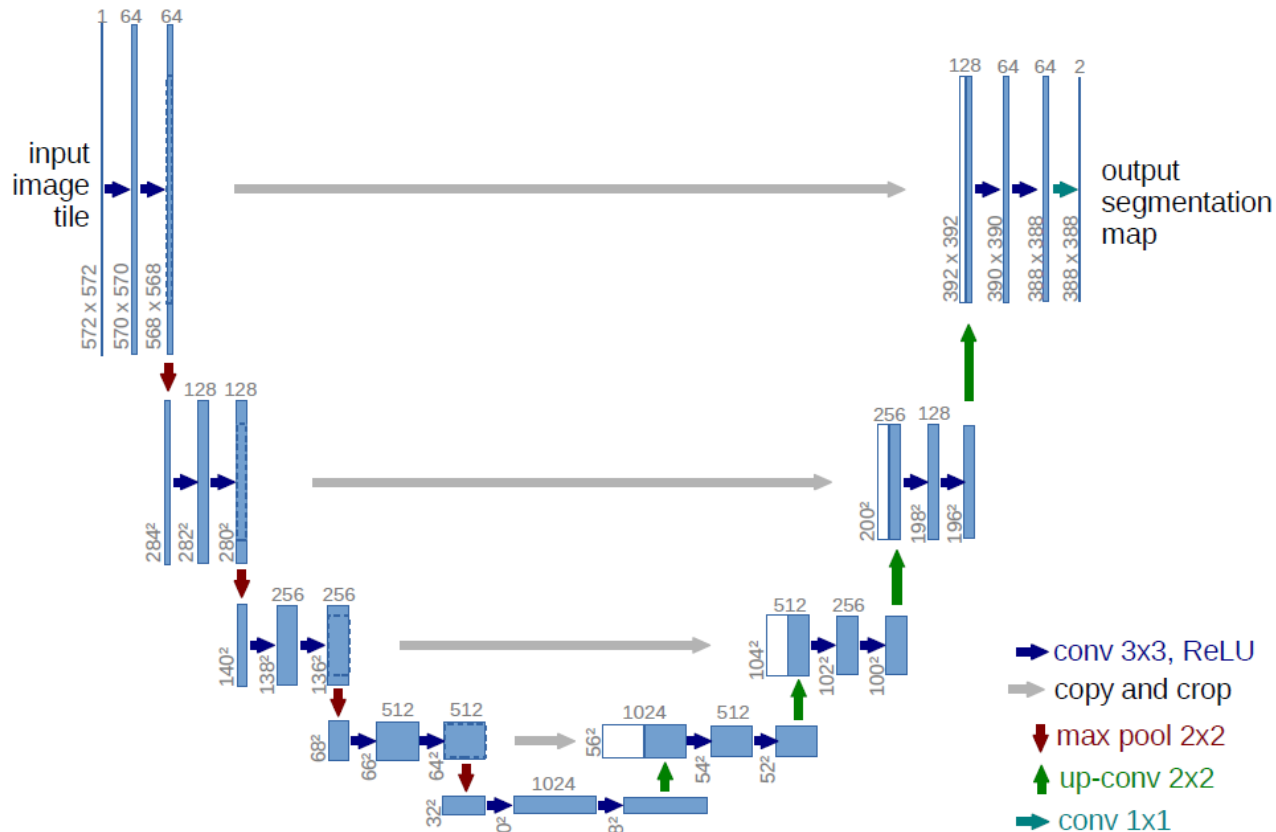


We can start with a pre-trained trunk/backbone (e.g. network pretrained on ImageNet)!



U-Net

You can have skip connections to bypass bottleneck!



Summary

- ◆ Various ways to get **image-like outputs**, for example to predict segmentations of input images
- ◆ We can have various upsampling layers that actually increase the size
- ◆ Encoder/decoder architectures are popular ways to leverage these to perform general image-to-image tasks
- ◆ Other methods exist:
 - ◆ Fully convolutional neural networks



Generative Models: Introduction

Supervised Learning

- Train Input: $\{X, Y\}$
- Learning output:
 $f : X \rightarrow Y, P(y|x)$
- e.g. classification

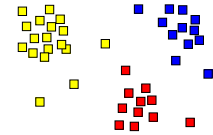


Sheep
Dog
Cat
Lion
Giraffe

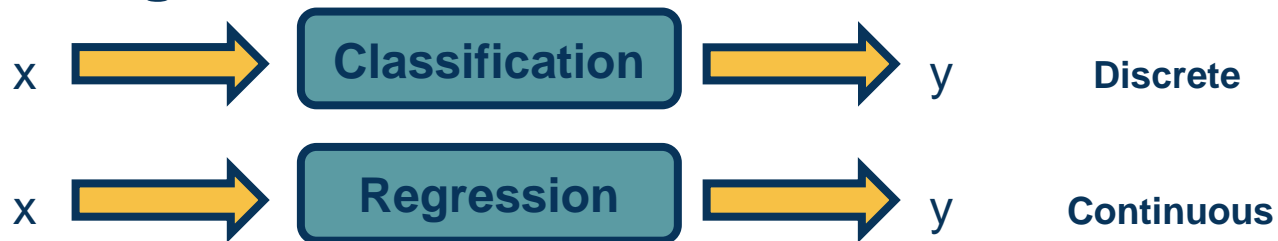


Unsupervised Learning

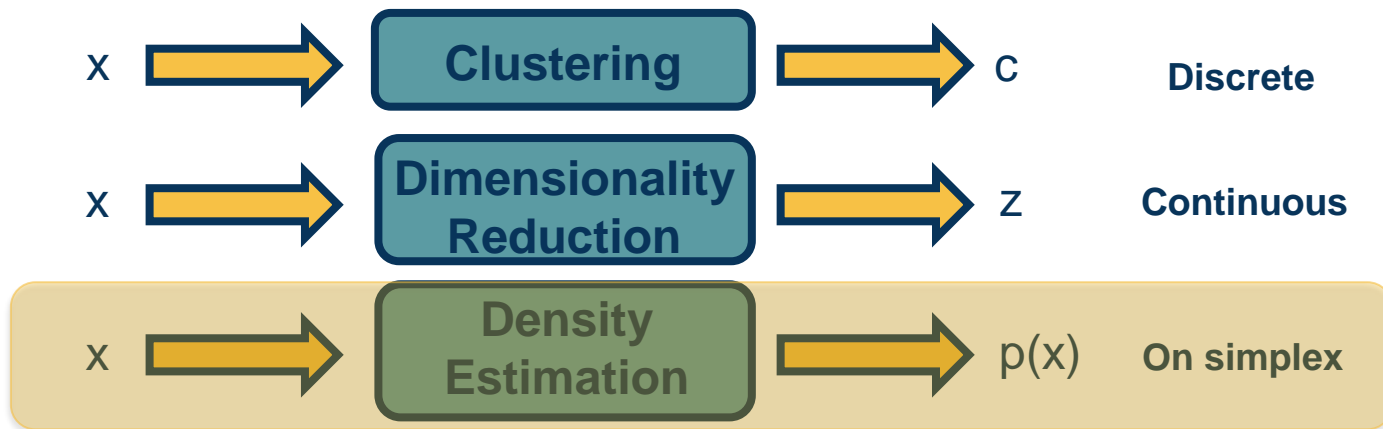
- Input: $\{X\}$
- Learning output: $P(x)$
- Example: Clustering, density estimation, etc.



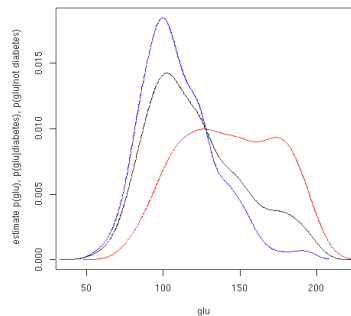
Supervised Learning



Unsupervised Learning



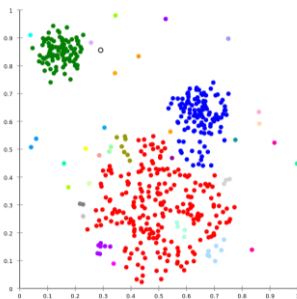
Traditional unsupervised learning methods:



Density
estimation

Modeling $P(x)$

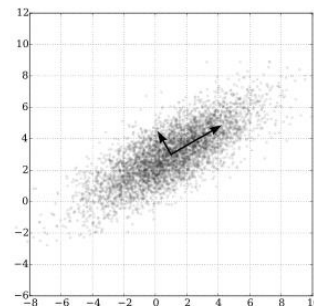
Deep Generative Models



Clustering

**Comparing/
Grouping**

Metric learning & clustering



Principal
Component
Analysis

**Representation
Learning**

Almost all deep learning!

Similar in deep learning, but **from neural network/learning perspective**

What to Learn?

Discriminative vs. Generative Models

- Discriminative models model $P(y|x)$
 - Example: Model this via neural network, SVM, etc.
- Generative models model $P(x)$

Goodfellow, NeurIPS 2016 Tutorial: Generative Adversarial Networks

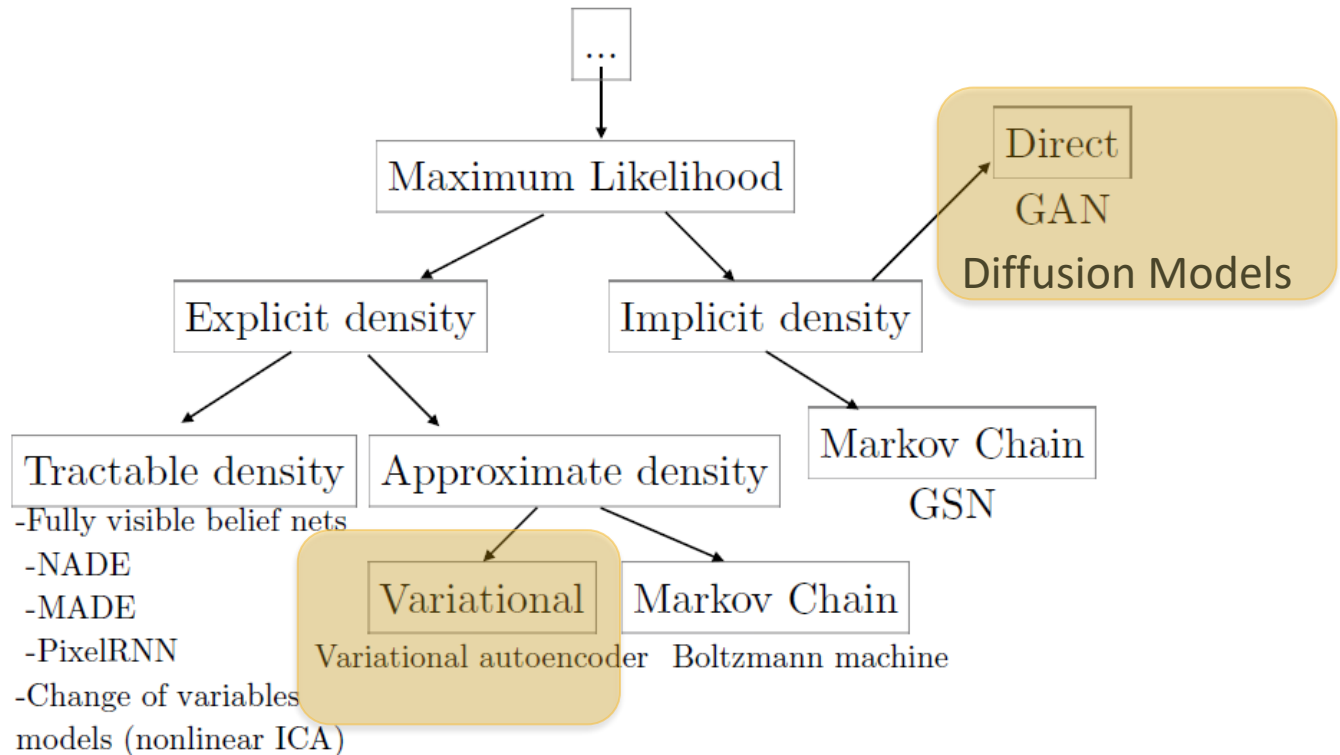
Discriminative vs. Generative Models

- Discriminative models model $P(y|x)$
 - Example: Model this via neural network, SVM, etc.
- Generative models model $P(x)$
- We can parameterize our model as $P(x, \theta)$ and use maximum likelihood to optimize the parameters given an unlabeled dataset:

$$\begin{aligned}\theta^* &= \arg \max_{\theta} \prod_{i=1}^m p_{\text{model}} \left(\mathbf{x}^{(i)}; \theta \right) \\ &= \arg \max_{\theta} \log \prod_{i=1}^m p_{\text{model}} \left(\mathbf{x}^{(i)}; \theta \right) \\ &= \arg \max_{\theta} \sum_{i=1}^m \log p_{\text{model}} \left(\mathbf{x}^{(i)}; \theta \right).\end{aligned}$$

- They are called generative because they can often generate *samples*
 - Example: Multivariate Gaussian with estimated parameters μ, σ

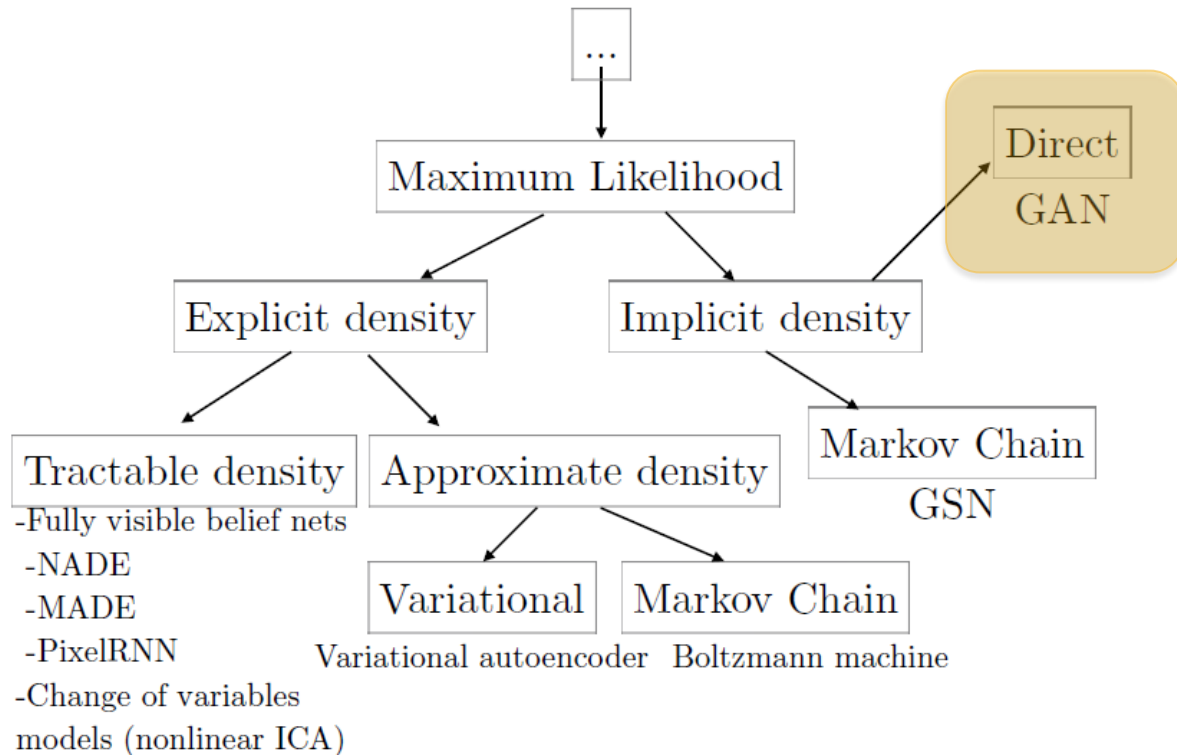
Goodfellow, NeurIPS 2016 Tutorial: Generative Adversarial Networks



Goodfellow, NeurIPS 2016 Tutorial: Generative Adversarial Networks

Generative Models

Generative Adversarial Networks (GANs)



Goodfellow, NeurIPS 2016 Tutorial: Generative Adversarial Networks

Generative Models

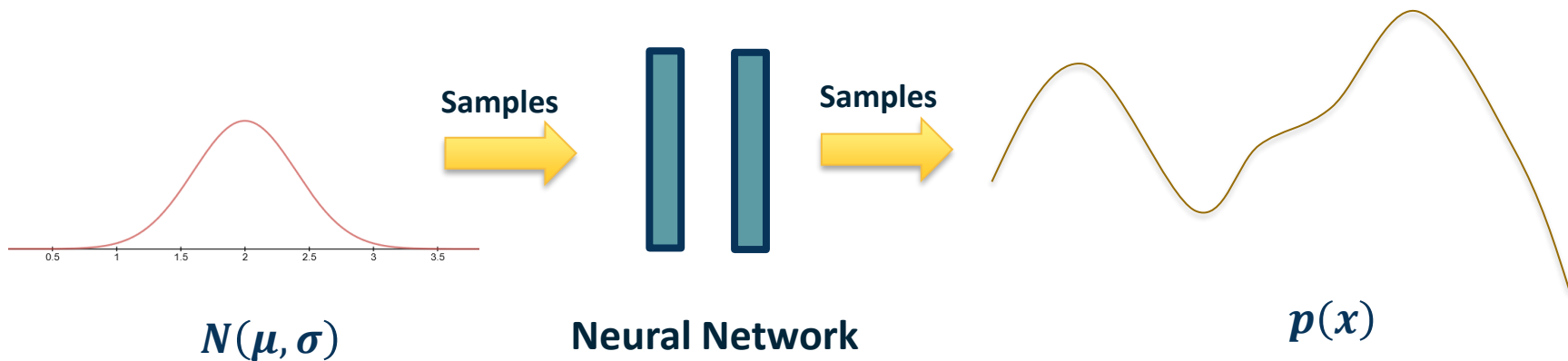
- ◆ *Implicit* generative models do not actually learn an explicit model for $p(x)$
- ◆ Instead, learn to *generate samples* from $p(x)$
 - ◆ Learn good feature representations
 - ◆ Perform data augmentation
 - ◆ Learn world models (a simulator!) for reinforcement learning
- ◆ How?
 - ◆ **Learn to sample** from a neural network output
 - ◆ **Adversarial training** that uses one network's predictions to train the other (dynamic loss function!)
 - ◆ **Lots of tricks** to make the optimization more stable

◆ We would like to *sample* from $p(x)$ using a neural network

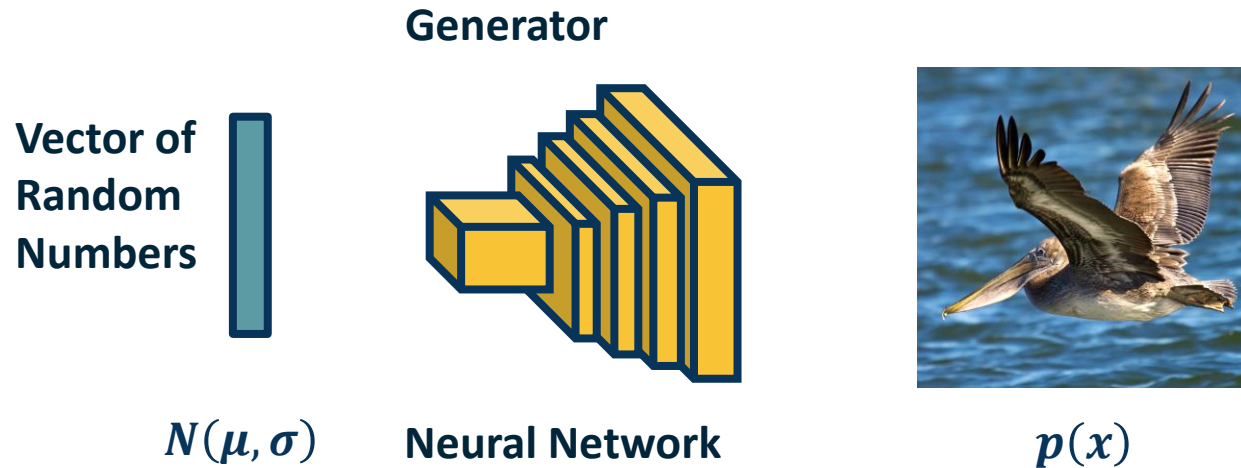
◆ **Idea:**

◆ Sample from a simple distribution (Gaussian)

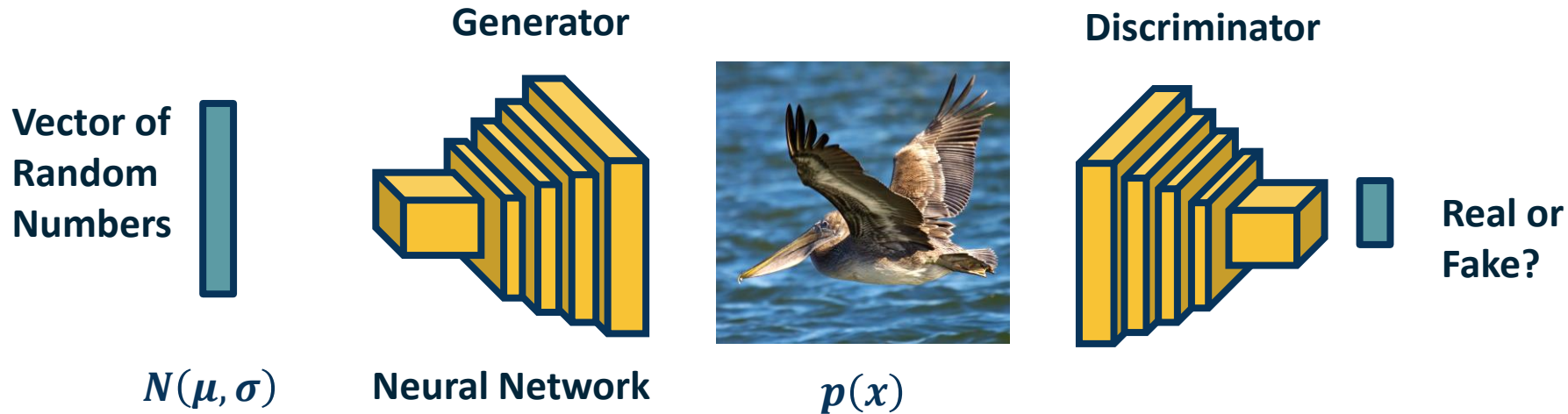
◆ Transform the sample to $p(x)$



- ◆ Input can be a vector with (independent) Gaussian random numbers
- ◆ We can use a CNN to generate images!

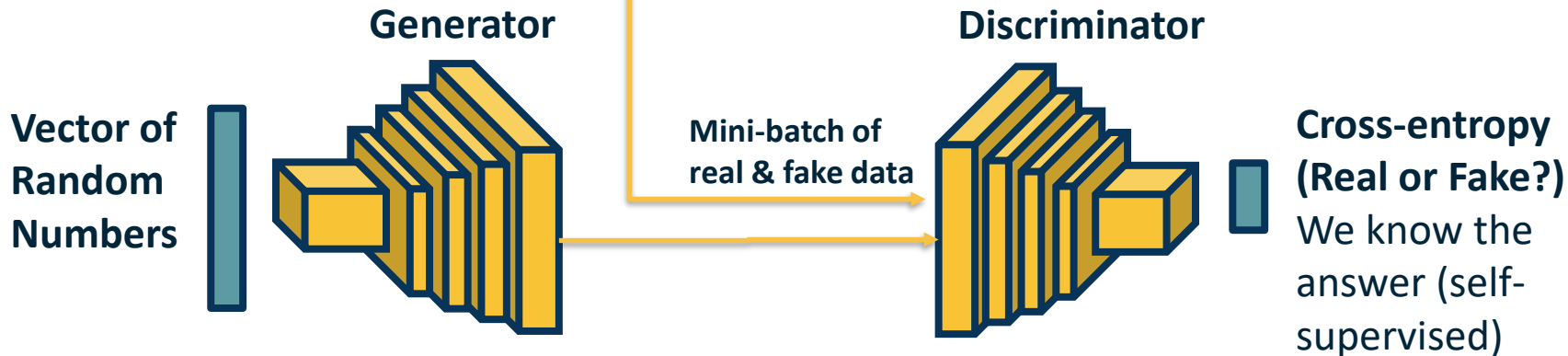


- ◆ **Goal:** We would like to generate *realistic* images. How can we drive the network to learn how to do this?
- ◆ **Idea:** Have *another* network try to distinguish a real image from a generated (fake) image
 - ◆ **Why?** Signal can be used to determine how well it's doing at generation





- ◆ **Generator:** Update weights to improve realism of generated images
- ◆ **Discriminator:** Update weights to better discriminate



Question: What loss functions can we use (for each network)?

- ◆ Since we have two networks competing, this is a mini-max two player game
 - ◆ Ties to game theory
 - ◆ Not clear what (even local) Nash equilibria are for this game

- ◆ Since we have two networks competing, this is a mini-max two player game
 - ◆ Ties to game theory
 - ◆ Not clear what (even local) Nash equilibria are for this game

- ◆ The full mini-max objective is:

$$\min_G \max_D V(D, G) = \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [\log D(\mathbf{x})] + \mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [\log(1 - D(G(\mathbf{z})))]$$

$$\min_G \max_D V(D, G) = \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [\log D(\mathbf{x})] + \mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [\log(1 - D(G(\mathbf{z})))]$$

- ◆ where $D(x)$ is the discriminator outputs probability ($[0,1]$) of **real** image
- ◆ x is a **real image** and $G(z)$ is a **generated** image

- ◆ The discriminator wants to **maximize** this:
 - ◆ $D(x)$ is pushed up (to 1) because x is a real image
 - ◆ $1 - D(G(z))$ is also pushed up to 1 (so that $D(G(z))$ is pushed down to 0)
 - ◆ In other words, discriminator wants to classify real images as real (1) and fake images as fake (0)

$$\min_G \max_D V(D, G) = \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [\log D(\mathbf{x})] + \mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [\log(1 - D(G(\mathbf{z})))]$$

- ◆ where $D(x)$ is the discriminator outputs probability ($[0,1]$) of **real** image
- ◆ x is a **real image** and $G(z)$ is a **generated** image

- ◆ The generator wants to **minimize** this:
 - ◆ $1 - D(G(z))$ is pushed down to 0 (so that $D(G(z))$ is pushed up to 1)
 - ◆ This means that the generator is **fooling** the discriminator, i.e. succeeding at generating images that the discriminator can't discriminate from real

- ◆ Since we have two networks competing, this is a mini-max two player game
 - ◆ Ties to game theory
 - ◆ Not clear what (even local) Nash equilibria are for this game

- ◆ The full mini-max objective is:

$$\min_G \max_D V(D, G) = \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [\log D(\mathbf{x})] + \underbrace{\mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [\log(1 - D(G(\mathbf{z})))]}_{\text{Sample from fake}}$$

Generator *minimizes*

**How well discriminator
does (0 for fake)**

- ◆ where $D(x)$ is the discriminator outputs probability $([0,1])$ of **real** image
- ◆ x is a **real image** and $G(z)$ is a **generated** image

Goodfellow, NeurIPS 2016 Tutorial: Generative Adversarial Networks

- Since we have two networks competing, this is a mini-max two player game
 - Ties to game theory
 - Not clear what (even local) Nash equilibria are for this game

- The full mini-max objective is:

$$\min_G \max_D V(D, G) = \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [\log D(\mathbf{x})] + \mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [\log(1 - D(G(\mathbf{z})))]$$

Discriminator *maximizes*

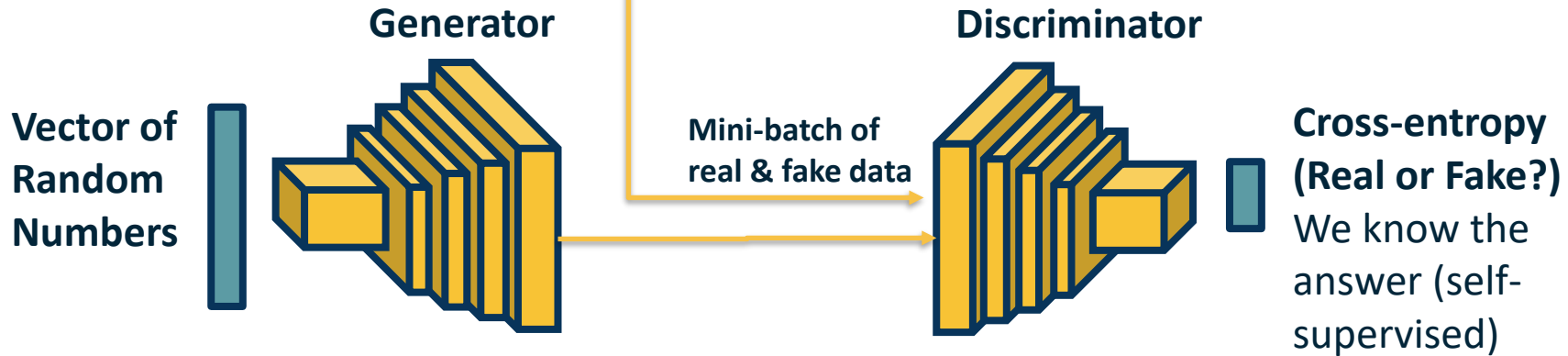
How well discriminator
does (1 for real)

How well discriminator
does (0 for fake)

- where $D(x)$ is the discriminator outputs probability ($[0,1]$) of **real** image
- x is a **real image** and $G(z)$ is a **generated** image

Goodfellow, NeurIPS 2016 Tutorial: Generative Adversarial Networks

Mini-max Two Player Game



$$\nabla_{\theta_g} \frac{1}{m} \sum_{i=1}^m \log \left(1 - D \left(G \left(z^{(i)} \right) \right) \right).$$

Generator Loss

$$\nabla_{\theta_d} \frac{1}{m} \sum_{i=1}^m \left[\log D \left(x^{(i)} \right) + \log \left(1 - D \left(G \left(z^{(i)} \right) \right) \right) \right].$$

Discriminator Loss

Generative Adversarial Networks (GANs)

- The generator part of the objective does not have good gradient properties

$$\min_G \max_D V(D, G) = \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [\log D(\mathbf{x})] + \mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [\log(1 - D(G(\mathbf{z})))]$$

- High gradient when $D(G(\mathbf{z}))$ is high (that is, discriminator is wrong)
- We want it to improve when samples are *bad* (discriminator is right)

- Alternative objective, **maximize**:

$$\max_{\theta_g} \mathbb{E}_{\mathbf{z} \sim p(\mathbf{z})} \log(D_{\theta_d}(G_{\theta_g}(\mathbf{z})))$$



Plot from CS231n, Fei-Fei Li, Justin Johnson, Serena Yeung

Algorithm 1 Minibatch stochastic gradient descent training of generative adversarial nets. The number of steps to apply to the discriminator, k , is a hyperparameter. We used $k = 1$, the least expensive option, in our experiments.

for number of training iterations **do**

for k steps **do**

- Sample minibatch of m noise samples $\{z^{(1)}, \dots, z^{(m)}\}$ from noise prior $p_g(z)$.
- Sample minibatch of m examples $\{x^{(1)}, \dots, x^{(m)}\}$ from data generating distribution $p_{\text{data}}(x)$.
- Update the discriminator by ascending its stochastic gradient:

$$\nabla_{\theta_d} \frac{1}{m} \sum_{i=1}^m \left[\log D(x^{(i)}) + \log \left(1 - D(G(z^{(i)})) \right) \right].$$

end for

- Sample minibatch of m noise samples $\{z^{(1)}, \dots, z^{(m)}\}$ from noise prior $p_g(z)$.
- Update the generator by descending its stochastic gradient:

$$\nabla_{\theta_g} \frac{1}{m} \sum_{i=1}^m \log \left(1 - D(G(z^{(i)})) \right).$$

end for

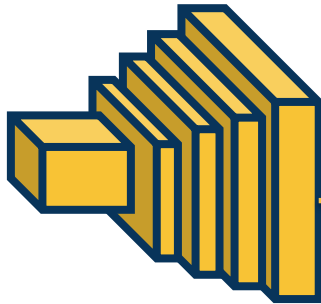
The gradient-based updates can use any standard gradient-based learning rule. We used momentum in our experiments.



Vector of
Random
Numbers

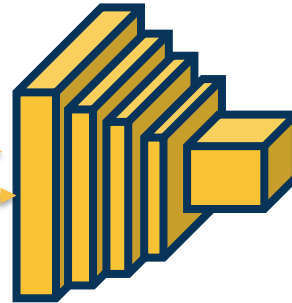


Generator



Mini-batch of
real & fake data

Discriminator

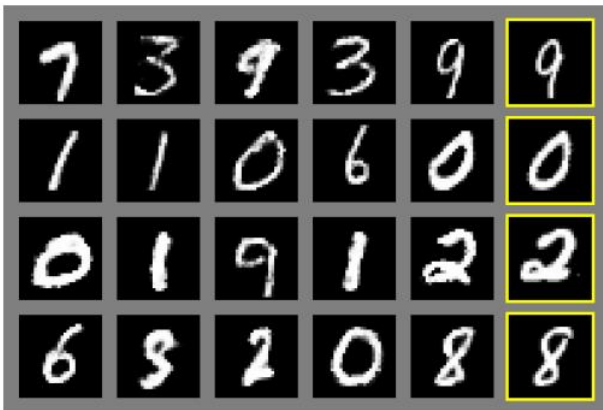


Cross-entropy
(Real or Fake?)

We know the
answer (self-
supervised)

- At the end, we have:
 - An *implicit* generative model!
 - Features from discriminator

Generative Adversarial Networks (GANs)



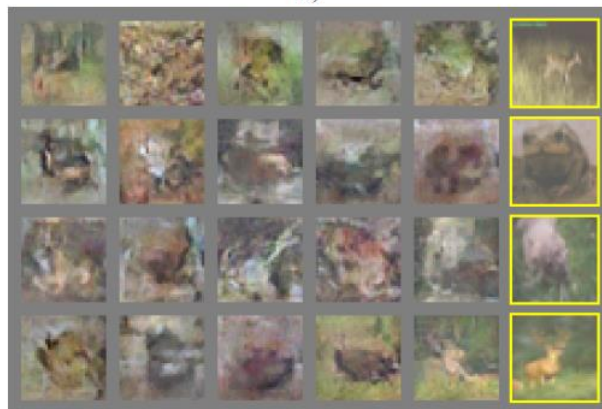
a)



b)



c)



d)

- Low-resolution images but look decent!
- Last column are nearest neighbor matches in dataset

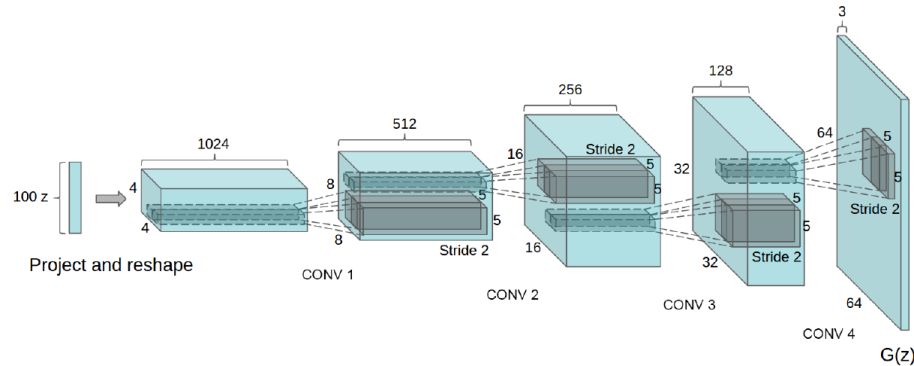
- ◆ GANs are very difficult to train due to the mini-max objective
- ◆ Advancements include:
 - ◆ More stable architectures
 - ◆ Regularization methods to improve optimization
 - ◆ Progressive growing/training and scaling

Goodfellow, NeurIPS 2016 Generative Adversarial Nets

Difficulty in Training

Architecture guidelines for stable Deep Convolutional GANs

- Replace any pooling layers with strided convolutions (discriminator) and fractional-strided convolutions (generator).
- Use batchnorm in both the generator and the discriminator.
- Remove fully connected hidden layers for deeper architectures.
- Use ReLU activation in generator for all layers except for the output, which uses Tanh.
- Use LeakyReLU activation in the discriminator for all layers.



Radford et al., *Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks*

- ◆ Training GANs is difficult due to:
 - ◆ Minimax objective – For example, what if generator learns to memorize training data (no variety) or only generates part of the distribution?
 - ◆ Mode collapse – Capturing only some modes of distribution
- ◆ Several theoretically-motivated regularization methods
 - ◆ Simple example: Add noise to real samples!

$$\lambda \cdot \mathbb{E}_{x \sim P_{real}, \delta \sim N_d(0, cI)} \left[\left\| \nabla_x D_\theta(x + \delta) \right\| - k \right]^2$$

Kodali et al., On Convergence and Stability of GANs (also known as How to Train your DRAGAN)

Generative Adversarial Nets: Convolutional Architectures

Samples from the model look much better!



Radford et al,
ICLR 2016

Generative Adversarial Nets: Convolutional Architectures

Interpolating
between
random
points in
latent space



Radford et al,
ICLR 2016



Brock et al., Large Scale GAN Training for High Fidelity Natural Image Synthesis

Example Generated Images - BigGAN



(a) 128×128



(b) 256×256



(c) 512×512



(d)

Figure 4: Samples from our model with truncation threshold 0.5 (a-c) and an example of class leakage in a partially trained model (d).



<https://www.youtube.com/watch?v=PCBTZh41Ris>

Video Generation

- ◆ Generative Adversarial Networks (GANs) can produce amazing images!
- ◆ Several drawbacks
 - ◆ High-fidelity generation heavy to train
 - ◆ Training can be unstable
 - ◆ No explicit model for distribution
- ◆ Larger number of extensions:
 - ◆ GANs conditioned on labels or other information
 - ◆ Adversarial losses for other applications

Comparison of Methods

