Lecture 12: Unsupervised and Reinforcement Learning

Announcements

- Project milestone due Friday 10/30
- Project milestone presentations next Monday 11/2 in-class
 - See upcoming Piazza post for details
 - Please show up at the beginning of the class time, we will share presentation order at that time
- We want to hear how things are going for you in the class, and your feedback!
 A survey was released on Piazza, please fill this out.

Supervised learning

Data: (x, y)

x is data, y is label

Goal: Learn a *function* to map x -> y

Examples: Classification, regression, semantic segmentation, object detection, instance segmentation



Classification

Now: Unsupervised learning

Data: x

Just data, no labels!

Goal: Learn some underlying hidden *structure* of the data

Examples: Clustering, representation / feature learning, density estimation, etc.

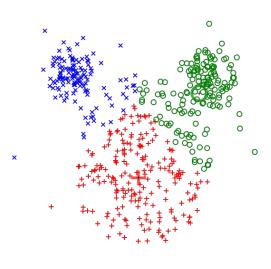
Now: Unsupervised learning

Data: x

Just data, no labels!

Goal: Learn some underlying hidden *structure* of the data

Examples: Clustering, representation / feature learning, density estimation, etc.



K-means clustering

This image is CC0 public domain

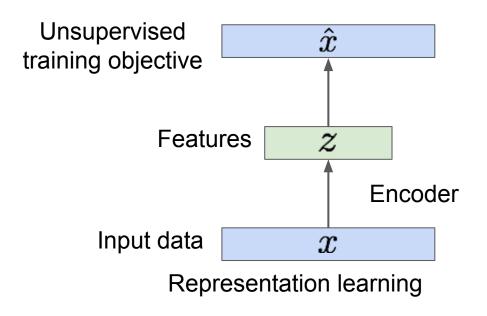
Now: Unsupervised learning

Data: x

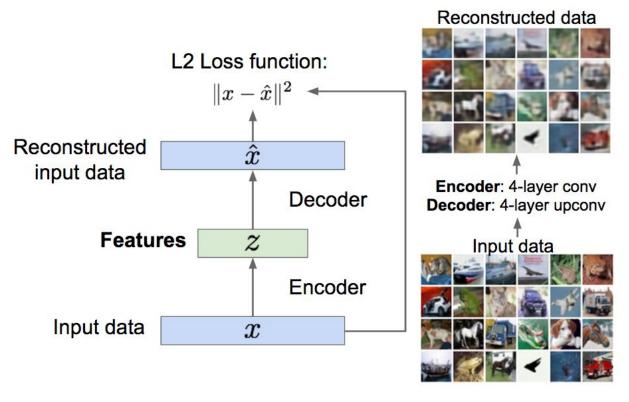
Just data, no labels!

Goal: Learn some underlying hidden *structure* of the data

Examples: Clustering, representation / feature learning, density estimation, etc.



Unsupervised representation learning: autoencoders

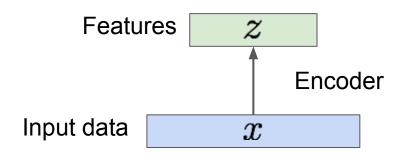


Autoencoders

Unsupervised Reconstructed data L2 Loss function: representation $||x - \hat{x}||^2$ learning: Reconstructed autoencoders input data Encoder: 4-layer conv Decoder Decoder: 4-layer upconv **Features** Input data (Feature Encoder representation) Input data

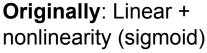
Autoencoders

Unsupervised approach for learning a lower-dimensional feature representation from unlabeled training data



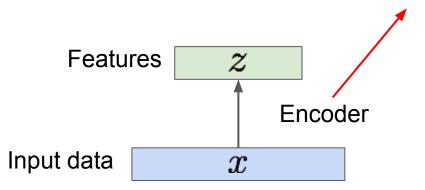


Unsupervised approach for learning a lower-dimensional feature representation from unlabeled training data



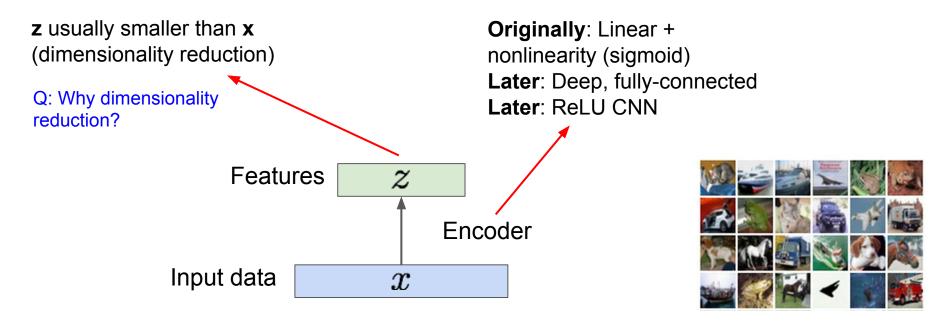
Later: Deep, fully-connected

Later: ReLU CNN

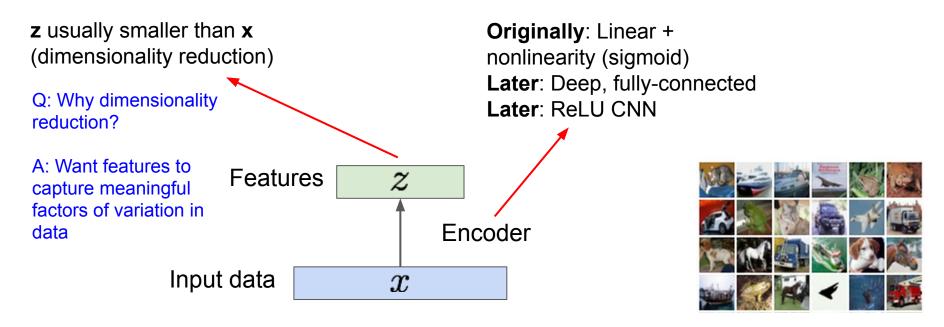




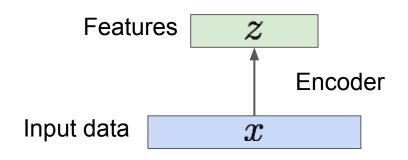
Unsupervised approach for learning a lower-dimensional feature representation from unlabeled training data

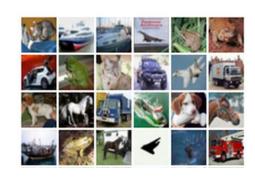


Unsupervised approach for learning a lower-dimensional feature representation from unlabeled training data



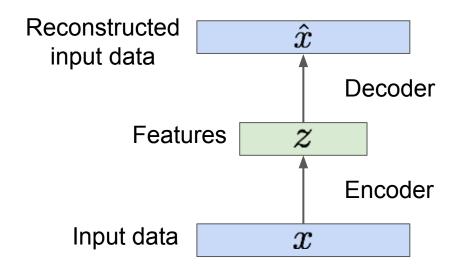
How to learn this feature representation?

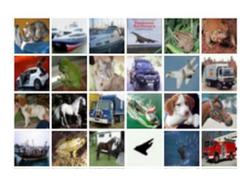




How to learn this feature representation?

Train such that features can be used to reconstruct original data "Autoencoding" - encoding itself

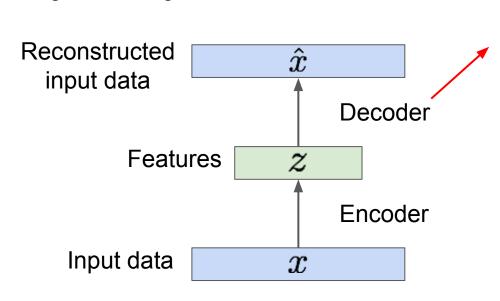




How to learn this feature representation?

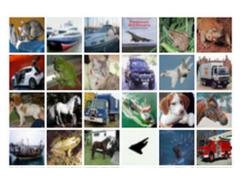
Train such that features can be used to reconstruct original data

"Autoencoding" - encoding itself



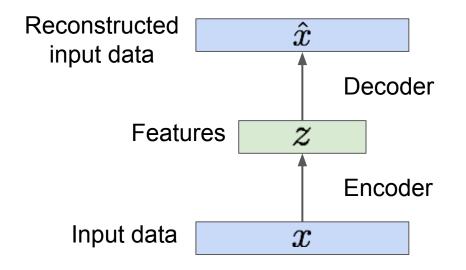
Originally: Linear + nonlinearity (sigmoid)

Later: Deep, fully-connected
Later: ReLU CNN (upconv)



How to learn this feature representation?

Train such that features can be used to reconstruct original data "Autoencoding" - encoding itself



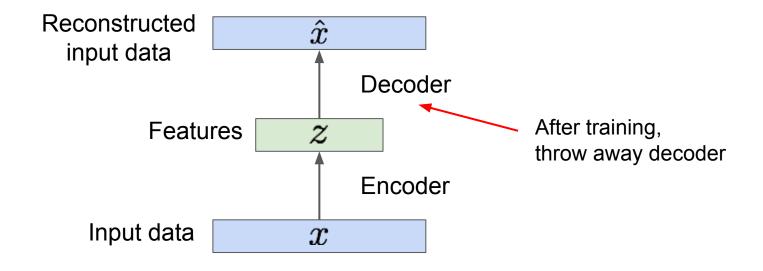


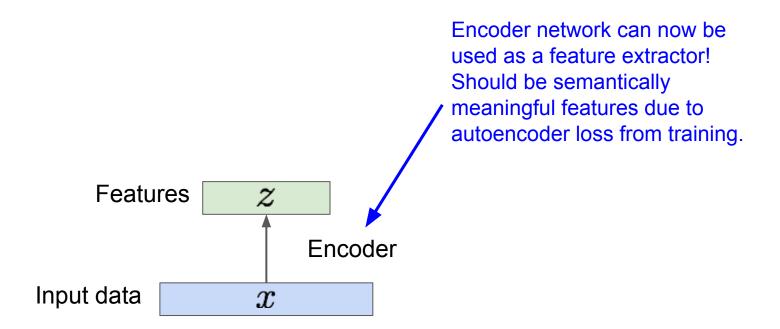
Train such that features 12 Loss function: can be used to reconstruct original data $||x - \hat{x}||^2$ Reconstructed input data Decoder **Features** Encoder Input data x

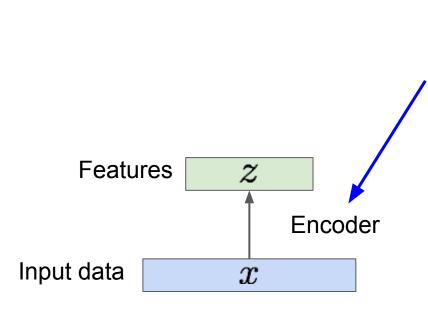


Train such that features Doesn't use labels! L2 Loss function: -> unsupervised can be used to reconstruct original data $||x - \hat{x}||^2$ Reconstructed input data Decoder **Features** Encoder Input data x









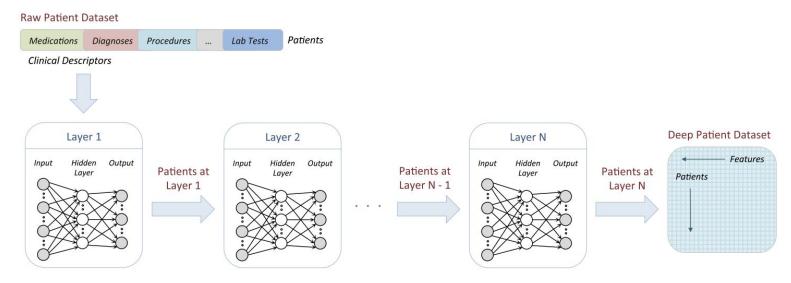
Encoder network can now be used as a feature extractor!
Should be semantically meaningful features due to autoencoder loss from training.

Features can be used for clustering, retrieval (e.g. find the closest patient to this one), etc.

In supervised Loss function learning tasks, an (Softmax, etc) encoder trained in an unsupervised \widehat{y} way (potentially on yPredicted Label larger amounts of Fine-tune data) can also be Classifier encoder used as a feature jointly with extractor for the **Features** classifier task, or to initialize a supervised model Encoder Input data x

Miotto 2016

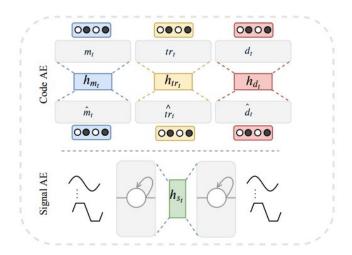
- Used stack of denoising autoencoders (add noise to inputs to avoid overfitting) to learn feature representation from EHR data of 700,000 patients from Mount Sinai
- Used learned feature representation for downstream disease classification tasks



Miotti et al. Deep Patient: An Unsupervised Representation to Predict the Future of Patients from the Electronic Health Records, 2016.

Darabi 2019

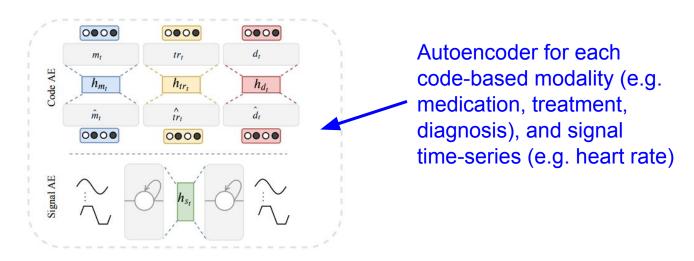
- Autoencoder-based unsupervised representation learning for multimodal data of 200,000 records from 250 hospital sites (eICU collaborative Research Database)
- Used feature representation to train models for downstream mortality, readmission prediction tasks



Darabi et al. Unsupervised Representation for EHR Signals and Codes as Patient Status Vector, 2019.

Darabi 2019

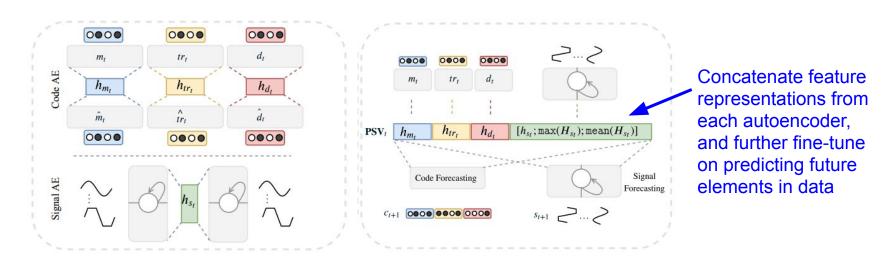
- Autoencoder-based unsupervised representation learning for multimodal data of 200,000 records from 250 hospital sites (eICU collaborative Research Database)
- Used feature representation to train models for downstream mortality, readmission prediction tasks



Darabi et al. Unsupervised Representation for EHR Signals and Codes as Patient Status Vector, 2019.

Darabi 2019

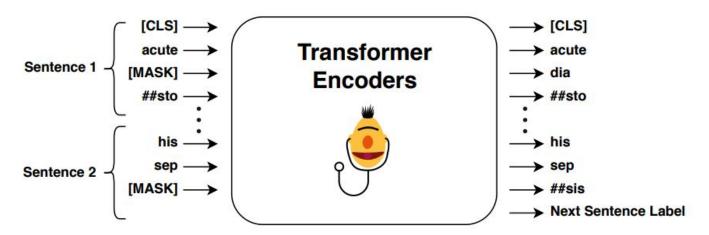
- Autoencoder-based unsupervised representation learning for multimodal data of 200,000 records from 250 hospital sites (eICU collaborative Research Database)
- Used feature representation to train models for downstream mortality, readmission prediction tasks



Darabi et al. Unsupervised Representation for EHR Signals and Codes as Patient Status Vector, 2019.

Aside: self-supervised learning

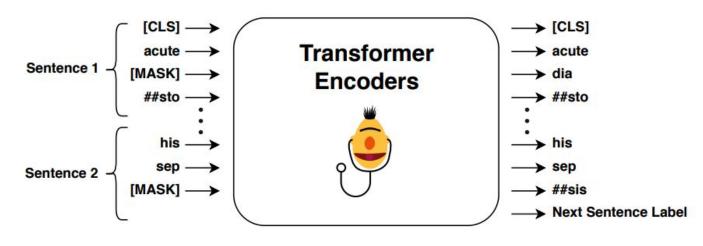
- Also learns representations without external (e.g., manually provided) labels, but instead using labels generated from inherent structure in the data
- Remember BERT training



Huang et al. ClinicalBert: Modeling Clinical Notes and Predicting Hospital Readmission, 2019.

Aside: self-supervised learning

- Also learns representations without external (e.g., manually provided) labels, but instead using labels generated from inherent structure in the data
- Remember BERT training

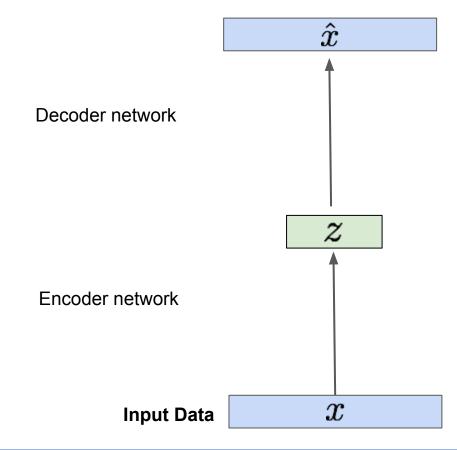


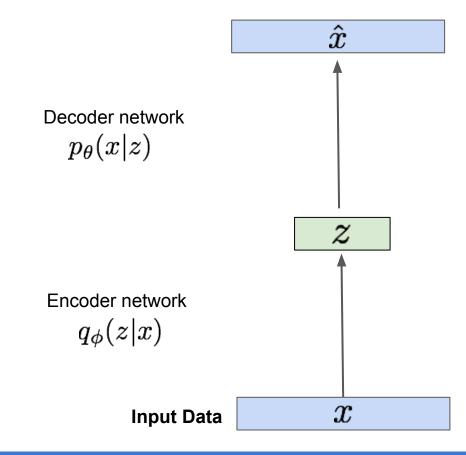
Also a lot of recent work in contrastive learning. E.g., two transformed versions of an image should have similar representations to each other, and different from transformed versions of other images

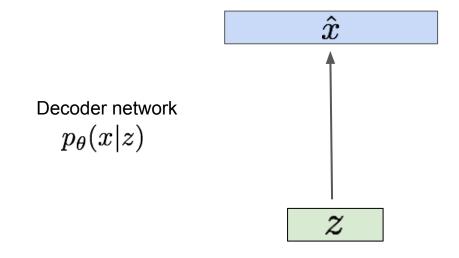
Huang et al. ClinicalBert: Modeling Clinical Notes and Predicting Hospital Readmission, 2019.

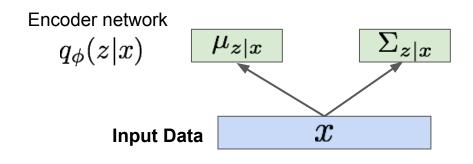
Train such that features Doesn't use labels! L2 Loss function: -> unsupervised can be used to reconstruct original data $||x - \hat{x}||^2$ Reconstructed input data Decoder **Features** Encoder Input data x

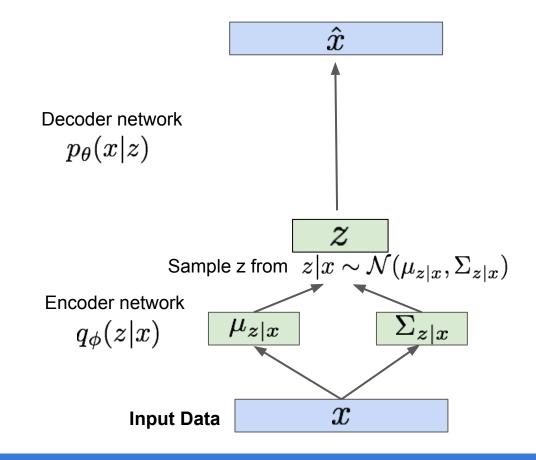




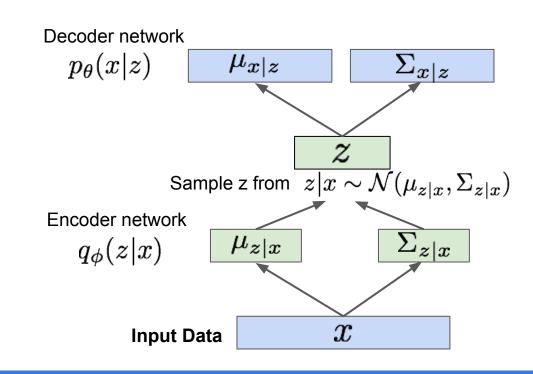


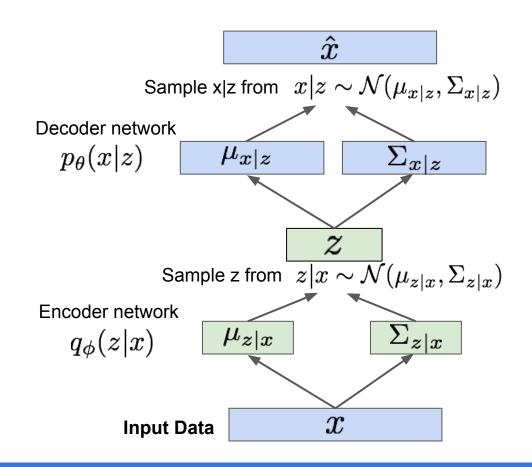






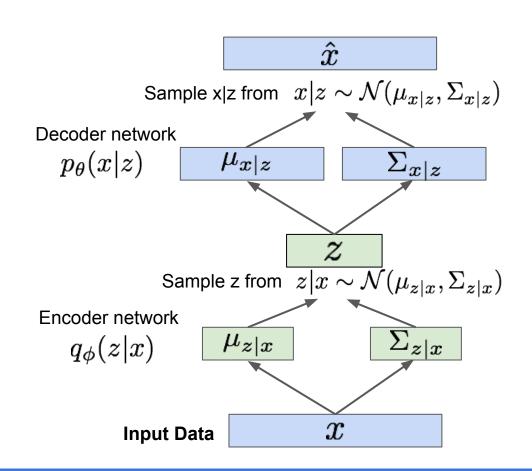






Loss function

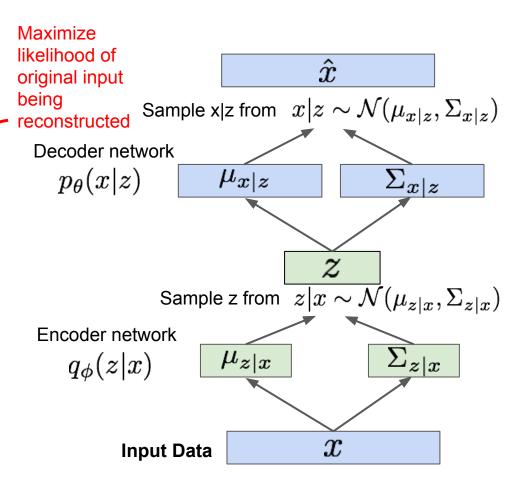
$$\underbrace{\mathbf{E}_{z} \left[\log p_{\theta}(x^{(i)} \mid z) \right] - D_{KL}(q_{\phi}(z \mid x^{(i)}) \mid\mid p_{\theta}(z))}_{\mathcal{L}(x^{(i)}, \theta, \phi)}$$



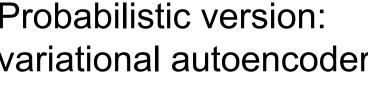
Probabilistic version: variational autoencoder

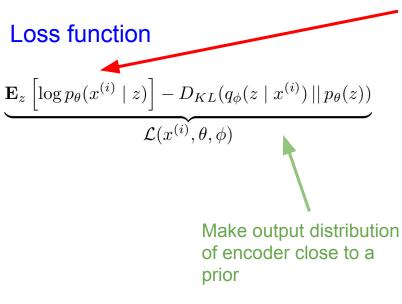
Loss function

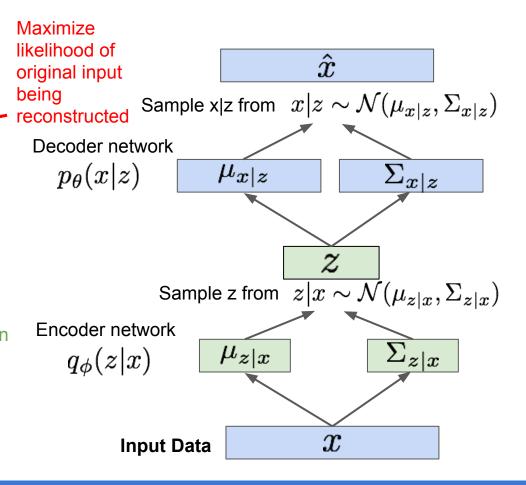
$$\underbrace{\mathbf{E}_{z} \left[\log p_{\theta}(x^{(i)} \mid z) \right] - D_{KL}(q_{\phi}(z \mid x^{(i)}) \mid\mid p_{\theta}(z))}_{\mathcal{L}(x^{(i)}, \theta, \phi)}$$



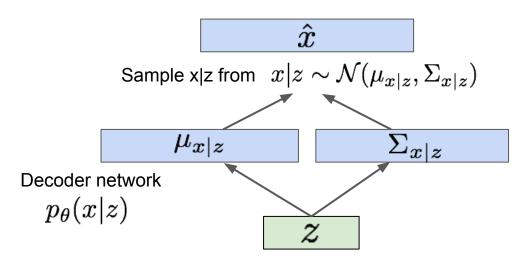
Probabilistic version: variational autoencoder







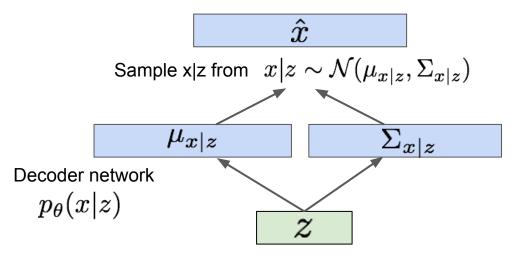
Use decoder network. Now sample z from prior!



Sample z from $\,z \sim \mathcal{N}(0,I)\,$

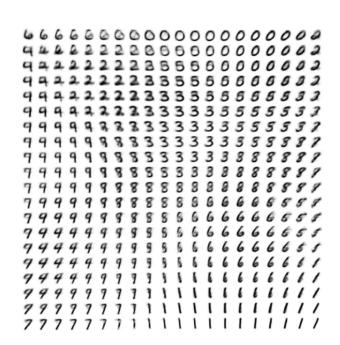
Kingma and Welling, "Auto-Encoding Variational Bayes", ICLR 2014

Use decoder network. Now sample z from prior!

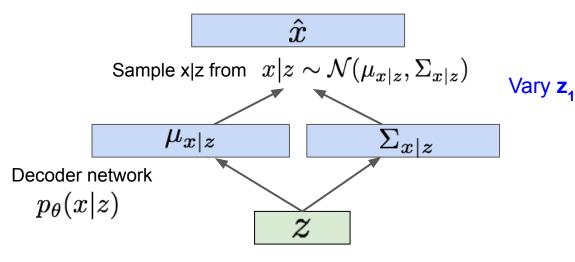


Sample z from $z \sim \mathcal{N}(0, I)$

Kingma and Welling, "Auto-Encoding Variational Bayes", ICLR 2014

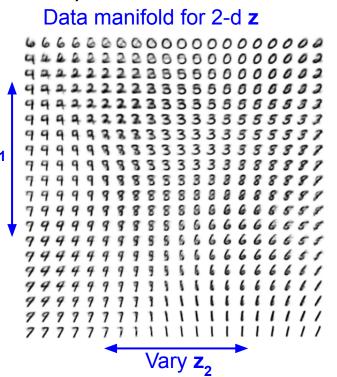


Use decoder network. Now sample z from prior!

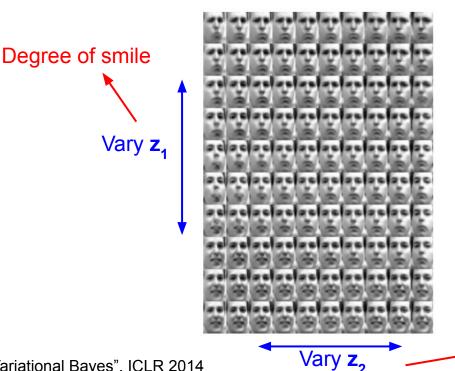


Sample z from $\,z \sim \mathcal{N}(0,I)\,$

Kingma and Welling, "Auto-Encoding Variational Bayes", ICLR 2014



Different dimensions of **z** encode interpretable factors of variation



Kingma and Welling, "Auto-Encoding Variational Bayes", ICLR 2014

Head pose

Another approach for learning to generate data: generative adversarial networks (GANs)

Motivation: Want to sample (generate data) from complex, high-dimensional training distribution. No direct way to do this!

Solution: Sample from a simple distribution, e.g. random noise. Learn transformation to training distribution.

Q: What can we use to represent this complex transformation?

Another approach for learning to generate data: generative adversarial networks (GANs)

Motivation: Want to sample (generate data) from complex, high-dimensional training distribution. No direct way to do this!

Solution: Sample from a simple distribution, e.g. random noise. Learn transformation to

training distribution.

Q: What can we use to represent this complex transformation?

A: A neural network!

Output: Sample from training distribution

Generator Network

Input: Random noise

Another approach for learning to generate data: generative adversarial networks (GANs)

Motivation: Want to sample (generate data) from complex, high-dimensional training distribution. No direct way to do this!

Solution: Sample from a simple distribution, e.g. random noise. Learn transformation to

training distribution.

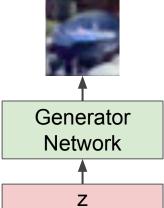
Q: What can we use to represent this complex transformation?

A: A neural network!

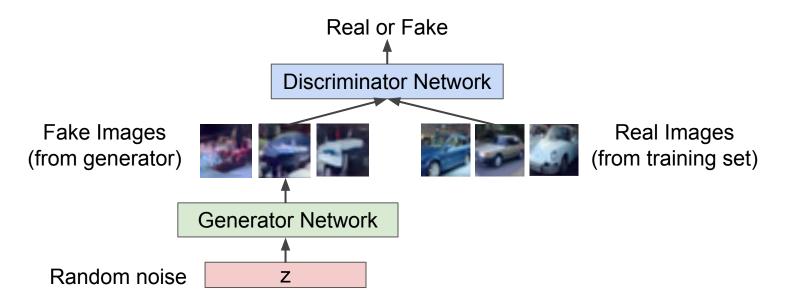
If goal is generating high quality samples, most current state-of-the-art approaches based on this

Output: Sample from training distribution

Input: Random noise



Generator network: try to fool the discriminator by generating real-looking images **Discriminator network**: try to distinguish between real and fake images



Fake and real images copyright Emily Denton et al. 2015. Reproduced with permission.

Generator network: try to fool the discriminator by generating real-looking images **Discriminator network**: try to distinguish between real and fake images

Train jointly in minimax game

Minimax objective function:

$$\min_{\theta_g} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

Generator network: try to fool the discriminator by generating real-looking images **Discriminator network**: try to distinguish between real and fake images

Train jointly in minimax game

Discriminator outputs likelihood in (0,1) that image is real

Minimax objective function:

$$\min_{\theta_g} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$
Discriminator output for for real data x
$$\min_{\theta_g} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$
Discriminator output for generated fake data G(z)

Generator network: try to fool the discriminator by generating real-looking images **Discriminator network**: try to distinguish between real and fake images

Train jointly in minimax game

Discriminator outputs likelihood in (0,1) that image is real

Minimax objective function:

$$\min_{\theta_g} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$
Discriminator output for for real data x
$$\min_{\theta_d} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

- Discriminator (θ_d) wants to **maximize objective** such that D(x) is close to 1 (real) and D(G(z)) is close to 0 (fake)
- Generator (θ_g) wants to **minimize objective** such that D(G(z)) is close to 1 (discriminator is fooled into thinking generated G(z) is real)

Minimax objective function:

$$\min_{\theta_g} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

Alternate between:

Gradient ascent on discriminator

$$\max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

2. Gradient descent on generator

$$\min_{\theta_g} \mathbb{E}_{z \sim p(z)} \log(1 - D_{\theta_d}(G_{\theta_g}(z)))$$

Minimax objective function:

$$\min_{\theta_g} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

Alternate between:

Gradient ascent on discriminator

$$\max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

2. In practice: Gradient ascent on generator, different objective

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

Minimax objective function:

$$\min_{\theta_g} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

Alternate between:

Gradient ascent on discriminator

$$\max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

2. In practice: Gradient ascent on generator, different objective

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

Instead of minimizing likelihood of discriminator being correct, now maximize likelihood of discriminator being wrong.

Minimax objective function:

$$\min_{\theta_g} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

Alternate between:

Gradient ascent on discriminator

$$\max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

2. In practice: Gradient ascent on generator, different objective

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

Instead of minimizing likelihood of discriminator being correct, now maximize likelihood of discriminator being wrong.

Same objective of fooling discriminator, but this objective has some nice properties that make optimization work better in practice

Ian Goodfellow et al., "Generative Adversarial Nets", NIPS 2014

Minimax objective function:

$$\min_{\theta_a} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right]$$

Alternate between:

Gradient ascent on discriminator

$$\max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log D_{\theta_d}(x) + \mathbb{E}_{z \sim p(z)} \log (1 - D_{\theta_d}(G_{\theta_g}(z))) \right] \text{ can be unstable. Lots of active research to improve the property of the prop$$

Aside: Jointly training two active research to improve GAN training.

In practice: Gradient ascent on generator, different objective

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

Instead of minimizing likelihood of discriminator being correct, now maximize likelihood of discriminator being wrong.

Same objective of fooling discriminator, but this objective has some nice properties that make optimization work better in practice

Putting it together: GAN training algorithm

for number of training iterations do

for k steps do

- Sample minibatch of m noise samples $\{z^{(1)}, \ldots, z^{(m)}\}$ from noise prior $p_q(z)$.
- 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:

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

end for

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

$$\nabla_{\theta_g} \frac{1}{m} \sum_{i=1}^m \log(D_{\theta_d}(G_{\theta_g}(z^{(i)})))$$

end for

Putting it together: GAN training algorithm

for number of training iterations do

for k steps do

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

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

More recent GAN variants alleviate this problem, better stability!

Some find k=1

others use k > 1,

more stable,

no best rule.

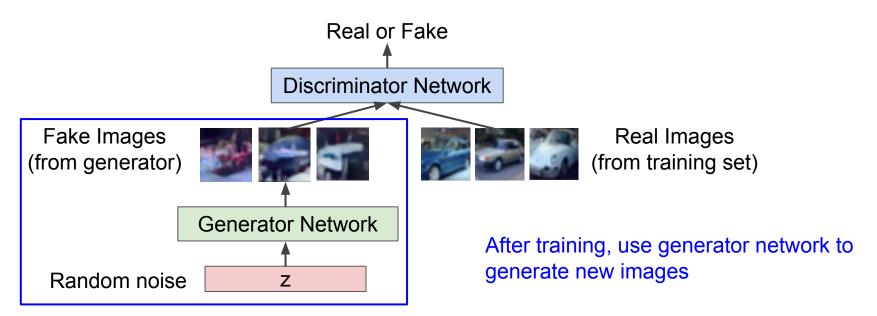
end for

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

$$\nabla_{\theta_g} \frac{1}{m} \sum_{i=1}^m \log(D_{\theta_d}(G_{\theta_g}(z^{(i)})))$$

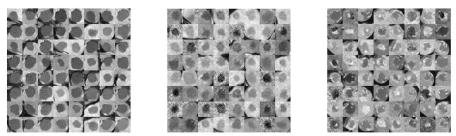
end for

Generator network: try to fool the discriminator by generating real-looking images **Discriminator network**: try to distinguish between real and fake images

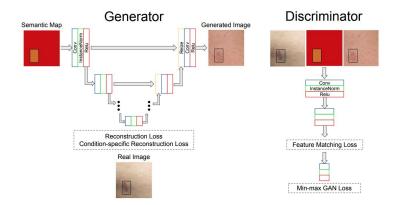


Fake and real images copyright Emily Denton et al. 2015. Reproduced with permission.

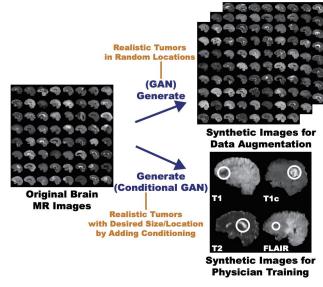
Example: GAN-based medical image synthesis



Liver lesions of different types (Frid-Adar 2018)



Dermatology lesions (Ghorbani 2019)



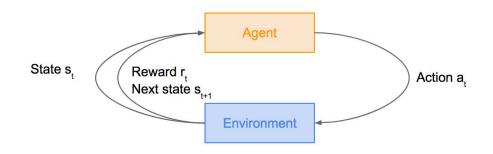
Brain MRIs with lesions (Han 2018)

Can be used for data augmentation!

A third paradigm of learning: reinforcement learning

Problems involving an **agent** interacting with an **environment**, which provides numeric **reward** signals

Goal: Learn how to take actions in order to maximize reward

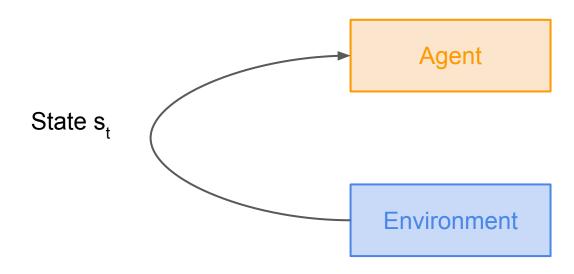


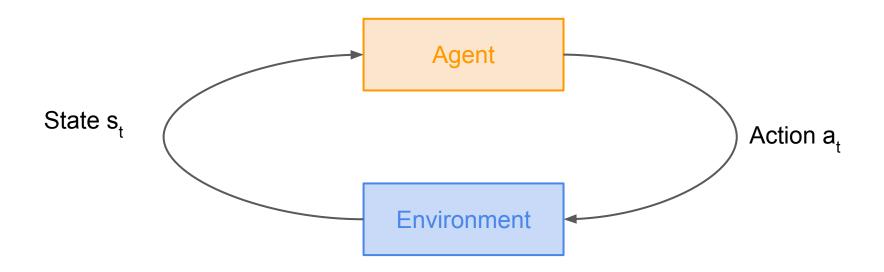


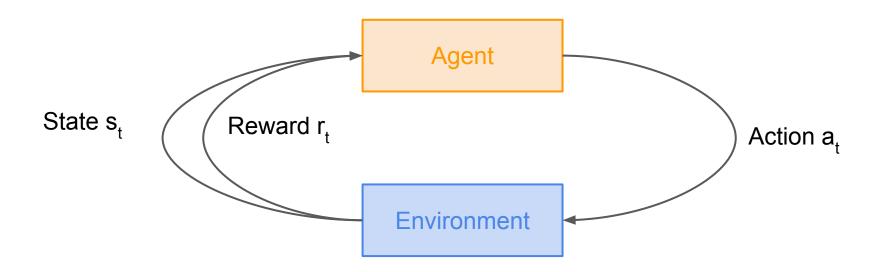
Atari games figure copyright Volodymyr Mnih et al., 2013. Reproduced with permission.

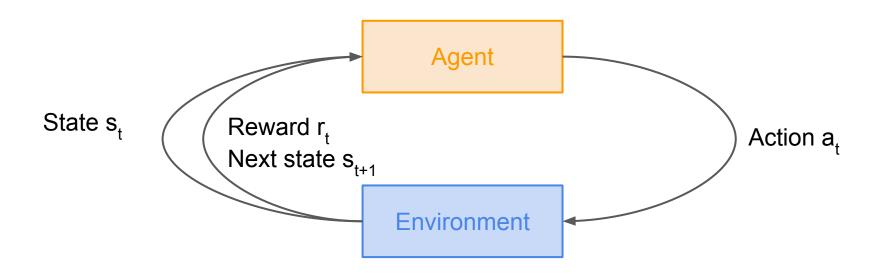
Agent

Environment









Q-learning (one class of RL methods)

Learn a function (called Q-function) to estimate the expected future reward from taking a particular action from any given state:



Q-learning (one class of RL methods)

Learn a function (called Q-function) to estimate the expected future reward from taking a particular action from any given state:

$$Q(s,a; heta)$$
 function parameters (weights)

If the function is a deep neural network => **deep q-learning!**

Famous example: playing Atari games



Objective: Complete the game with the highest score

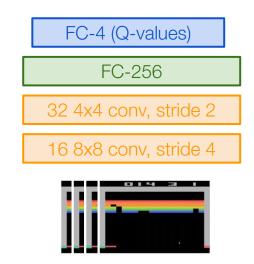
State: Raw pixel inputs of the game state

Action: Game controls e.g. Left, Right, Up, Down

Reward: Score increase/decrease at each time step

Q-network architecture

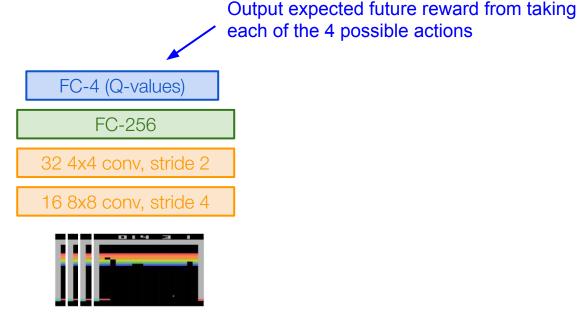
Q(s,a; heta) : neural network with weights heta



Current state s_t: 84x84x4 stack of last 4 frames (after RGB->grayscale conversion, downsampling, and cropping)

Q-network architecture

Q(s,a; heta) : neural network with weights heta



Current state s_t: 84x84x4 stack of last 4 frames (after RGB->grayscale conversion, downsampling, and cropping)

Policy gradients (another class of RL methods)

What is a problem with Q-learning? The Q-function can be very complicated!

Example: a robot grasping an object has a very high-dimensional state => hard to learn exact value of every (state, action) pair

What is a problem with Q-learning?
The Q-function can be very complicated!

Example: a robot grasping an object has a very high-dimensional state => hard to learn exact value of every (state, action) pair

But the policy can be much simpler: just close your hand Can we learn a policy directly, e.g. finding the best policy from a collection of policies?

Formally, let's define a class of parameterized policies: $\Pi = \{\pi_{\theta}, \theta \in \mathbb{R}^m\}$

For each policy, define its value:

$$J(heta) = \mathbb{E}\left[\left| \sum_{t \geq 0} \gamma^t r_t | \pi_ heta
ight]$$

Formally, let's define a class of parameterized policies: $\Pi = \{\pi_{\theta}, \theta \in \mathbb{R}^m\}$

For each policy, define its value:

$$J(heta) = \mathbb{E}\left[\sum_{t \geq 0} \gamma^t r_t | \pi_ heta
ight]$$

We want to find the optimal policy $\theta^* = \arg \max_{\theta} J(\theta)$

How can we do this?

Formally, let's define a class of parameterized policies: $\Pi = \{\pi_{\theta}, \theta \in \mathbb{R}^m\}$

For each policy, define its value:

$$J(heta) = \mathbb{E}\left[\sum_{t \geq 0} \gamma^t r_t | \pi_ heta
ight]$$

We want to find the optimal policy $\ heta^* = \arg\max_{ heta} J(heta)$

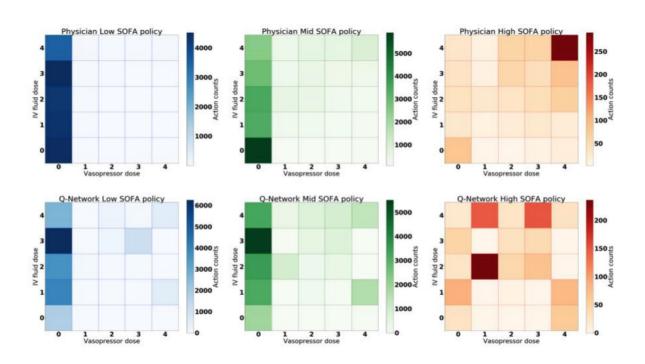
How can we do this?

Gradient ascent on policy parameters!

Example: Raghu et al. 2017

Learned a Q-learning based policy to take treatment actions for sepsis patients, using the MIMIC dataset

5x5 possible policy actions at any timestep



Raghu et al. Deep Reinforcement Learning for Sepsis Treatment, 2017.

Next time

Your milestone presentations!