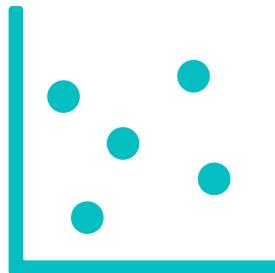


Lecture Notes for **Neural Networks** **and Machine Learning**



Holy GAN-Zooks



Logistics and Agenda

- Logistics
 - None!
- Agenda
 - More-GANs:
 - ◆ LSGAN
 - ◆ InfoGAN
 - ◆ CycleGAN
 - ◆ Paper Presentation
 - ◆ GAIA (next lecture)
 - ◆ Text-to-image Synthesis (next lecture)



Last Time

- Loss function for generator is really difficult and unstable
 - hard to optimize based on feedback only from discriminator output!
- Since generator is trying to statistically match features inside the discriminator (to fool it)
 - try to make generator match statistics of discriminator activations

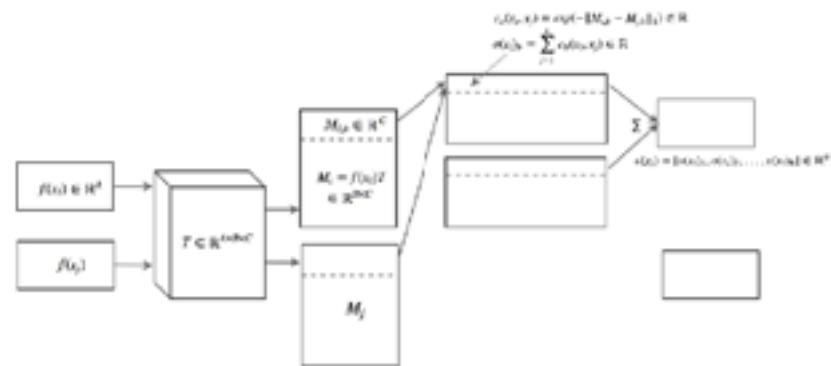
$$\| \mathbb{E}_{x \leftarrow \text{data}} [\mathbf{f}(x)] - \mathbb{E}_{x \leftarrow q(z)} [\mathbf{f}(G(z))] \|_2^2$$

mean discriminator activation
from real data mean discriminator activation
from fake data

- How much do I need to change one distribution to get it to match another?
- Could use KL divergence, but we already know that has many problems associated with vanishing gradients
- We will only have samples from the distributions (not the actual equations)
- Wasserstein Distance** for continuous probabilities:

$$W(p_{\text{data}}, p_g) = \inf_{\gamma \in \Pi(p_{\text{data}}, p_g)} \mathbb{E}_{x, y \sim \gamma} [\|x - y\|]$$

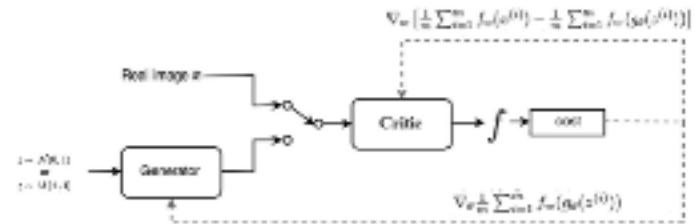
- inf is greatest lower bound
- gamma is completely and utterly intractable to compute



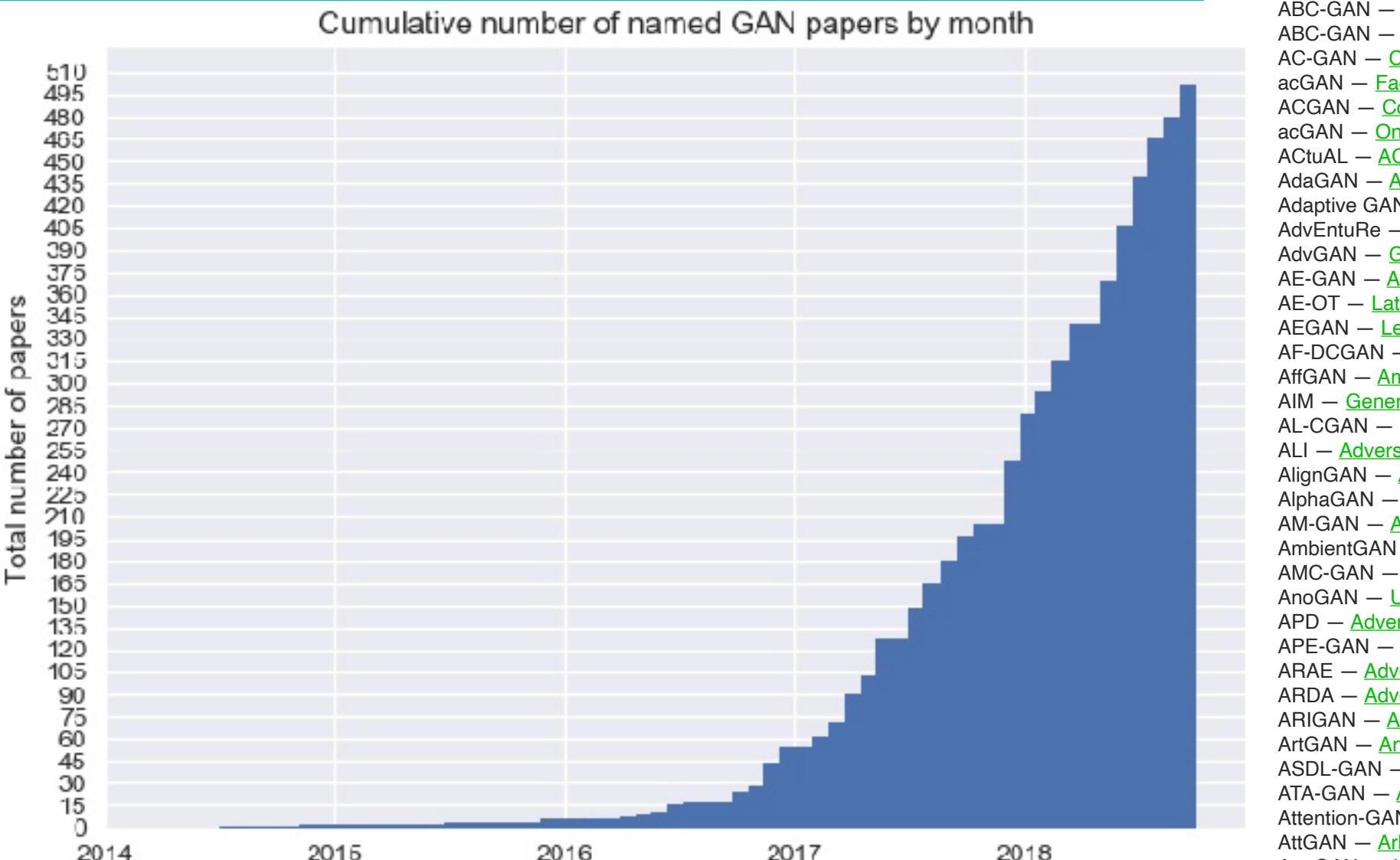
- 1-Lipschitz constraint: $|f(x_1) - f(x_2)| \leq |x_1 - x_2|$.
- Wasserstein Duality Formula:

$$W(\mathbb{P}_r, \mathbb{P}_g) = \sup_{\|f\|_{L^1} \leq 1} \mathbb{E}_{x \sim \mathbb{P}_r} [f(x)] - \mathbb{E}_{x \sim \mathbb{P}_g} [f(x)]$$

- where sup is the least upper bound (which we cannot find directly, so we assume its a maximization)



Example GANs, Abridged



LSGAN

Least Squares Generative Adversarial Networks

Xudong Mao^{*1}, Qing Li^{†1}, Haoran Xie^{‡2}, Raymond Y.K. Lau^{§3},
Zhen Wang^{¶4}, and Stephen Paul Smolley^{||5}

¹Department of Computer Science, City University of Hong Kong

²Department of Mathematics and Information Technology, The
Education University of Hong Kong

³Department of Information Systems, City University of Hong
Kong

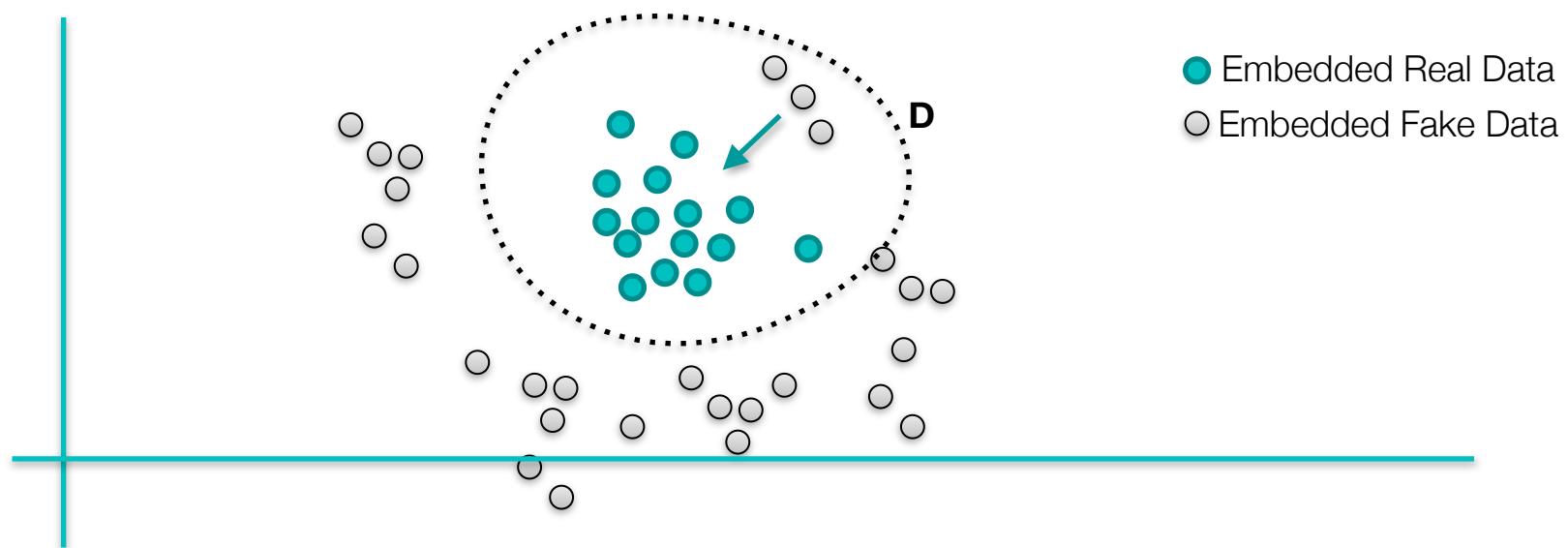
⁴Center for OPTical IMagery Analysis and Learning (OPTIMAL),
Northwestern Polytechnical University

⁵CodeHatch Corp.



The Least Squares GAN

- **Observation:** Generated points may (by chance) be classified as real by Discriminator—but they are still not representative of the real data
- **Solution:** Incentivize even correctly classified labels to move toward real data distribution



Mao, Xudong, Qing Li, Haoran Xie, Raymond YK Lau, Zhen Wang, and Stephen Paul Smolley. "Least squares generative adversarial networks." In *Proceedings of the IEEE International Conference on Computer Vision*, pp. 2794-2802. 2017.



Incentivizing with Least Squares

- Assume a =fake label, b =real label, c =misleading label
- The new loss function is:

$$\min_D V_{\text{LSGAN}}(D) = \frac{1}{2} \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [(D(\mathbf{x}) - b)^2] + \frac{1}{2} \mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [(D(G(\mathbf{z})) - a)^2]$$
$$\min_G V_{\text{LSGAN}}(G) = \frac{1}{2} \mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [(D(G(\mathbf{z})) - c)^2],$$

- Here we can take advantage of the labels, even when they are classified correct/incorrect
 - ...because we have a distance to margin
 - ...that's it!



But that results is not publishable!

- We need to find a way to complicate the math to make it less approachable and therefore publishable
 - Yay for ethics!
- **Discussion:** is this wrong for the authors to do?

In the original GAN paper [7], the authors has shown that minimizing Equation 1 yields minimizing the Jensen-Shannon divergence:

$$C(G) = KL \left(p_{\text{data}} \left\| \frac{p_{\text{data}} + p_g}{2} \right\| \right) + KL \left(p_g \left\| \frac{p_{\text{data}} + p_g}{2} \right\| \right) - \log(4). \quad (3)$$

Here we also explore the relation between LSGANs and f-divergence. Consider the following extension of Equation 2:

$$\begin{aligned} \min_D V_{\text{LSGAN}}(D) &= \frac{1}{2} \mathbb{E}_{x \sim p_{\text{data}}(x)} [(D(x) - b)^2] + \frac{1}{2} \mathbb{E}_{z \sim p_g(z)} [(D(G(z)) - a)^2] \\ \min_G V_{\text{LSGAN}}(G) &= \frac{1}{2} \mathbb{E}_{x \sim p_{\text{data}}(x)} [(D(x) - c)^2] + \frac{1}{2} \mathbb{E}_{z \sim p_g(z)} [(D(G(z)) - c)^2]. \end{aligned} \quad (4)$$

Note that adding the term $\mathbb{E}_{x \sim p_{\text{data}}(x)} [(D(x) - c)^2]$ to $V_{\text{LSGAN}}(G)$ does not change the optimal values since this term does not contain parameters of G .

We first derive the optimal discriminator D for a fixed G as below :

$$D^*(x) = \frac{bp_{\text{data}}(x) + ap_g(x)}{p_{\text{data}}(x) + p_g(x)}. \quad (5)$$

In the following equations we use p_d to denote p_{data} for simplicity. Then we can reformulate Equation 4 as follows:

$$\begin{aligned} 2C(G) &= \mathbb{E}_{x \sim p_d} [(D^*(x) - c)^2] + \mathbb{E}_{x \sim p_g} [(D^*(x) - c)^2] \\ &= \mathbb{E}_{x \sim p_d} \left[\left(\frac{bp_d(x) + ap_g(x)}{p_d(x) + p_g(x)} - c \right)^2 \right] + \mathbb{E}_{x \sim p_g} \left[\left(\frac{bp_d(x) + ap_g(x)}{p_d(x) + p_g(x)} - c \right)^2 \right] \\ &= \int_X p_d(x) \left(\frac{(b-c)p_d(x) + (a-c)p_g(x)}{p_d(x) + p_g(x)} \right)^2 dx + \int_X p_g(x) \left(\frac{(b-c)p_d(x) + (a-c)p_g(x)}{p_d(x) + p_g(x)} \right)^2 dx \\ &= \int_X \frac{\left((b-c)p_d(x) + (a-c)p_g(x) \right)^2}{p_d(x) + p_g(x)} dx \\ &= \int_X \frac{\left((b-c)(p_d(x) + p_g(x)) - (b-a)p_g(x) \right)^2}{p_d(x) + p_g(x)} dx. \end{aligned} \quad (6)$$

If we set $b - c = 1$ and $b - a = 2$, then

$$\begin{aligned} 2C(G) &= \int_X \frac{\left(2p_g(x) - (p_d(x) + p_g(x)) \right)^2}{p_d(x) + p_g(x)} dx \\ &= \chi_{\text{Pearson}}^2(p_d + p_g \| 2p_g), \end{aligned} \quad (7)$$

where χ_{Pearson}^2 is the Pearson χ^2 divergence. Thus minimizing Equation 4 yields minimizing the Pearson χ^2 divergence between $p_d + p_g$ and $2p_g$ if a , b , and c satisfy the conditions of $b - c = 1$ and $b - a = 2$.



LS-GAN Parameter Selection

3.2.3 Parameters Selection

One method to determine the values of a , b , and c in Equation 2 is to satisfy the conditions of $b - c = 1$ and $b - a = 2$, such that minimizing Equation 2 yields minimizing the Pearson χ^2 divergence between $p_d + p_g$ and $2p_g$. For example, by setting $a = -1$, $b = 1$, and $c = 0$, we get the following objective functions:

$$\begin{aligned} \min_D V_{\text{LSGAN}}(D) &= \frac{1}{2} \mathbb{E}_{x \sim p_{\text{data}}(x)} [(D(x) - 1)^2] + \frac{1}{2} \mathbb{E}_{z \sim p_z(z)} [(D(G(z)) + 1)^2] \\ \min_G V_{\text{LSGAN}}(G) &= \frac{1}{2} \mathbb{E}_{z \sim p_z(z)} [(D(G(z)))^2]. \end{aligned} \tag{8}$$

Another method is to make G generate samples as real as possible by setting $c = b$. For example, by using the 0-1 binary coding scheme, we get the following objective functions:

$$\begin{aligned} \min_D V_{\text{LSGAN}}(D) &= \frac{1}{2} \mathbb{E}_{x \sim p_{\text{data}}(x)} [(D(x) - 1)^2] + \frac{1}{2} \mathbb{E}_{z \sim p_z(z)} [(D(G(z)))^2] \\ \min_G V_{\text{LSGAN}}(G) &= \frac{1}{2} \mathbb{E}_{z \sim p_z(z)} [(D(G(z)) - 1)^2]. \end{aligned} \tag{9}$$

In practice, we observe that Equation 8 and Equation 9 show similar performance. Thus either one can be selected. In the following sections, we use Equation 9 to train the models.

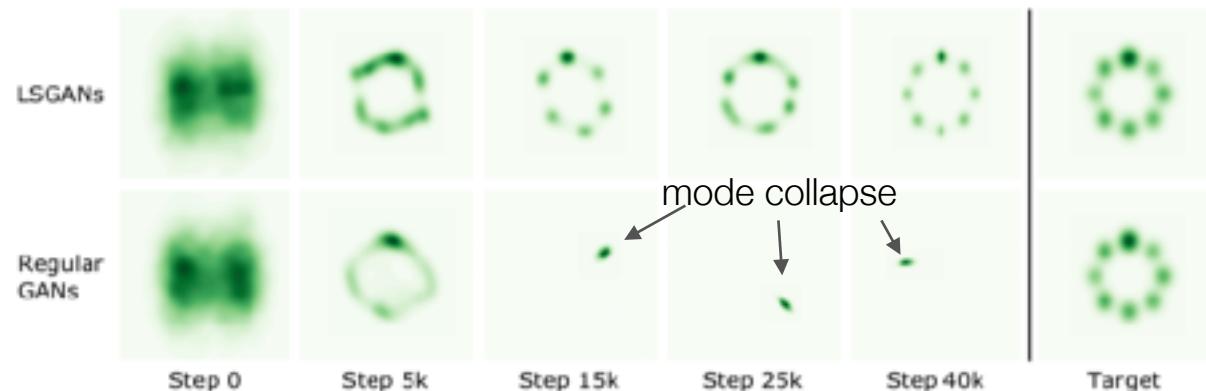


LS-GAN Results

- Some takeaways:
 - RMSProp works better than Adam
 - Reasonable values for a,b,c have similar performance
 - Mode collapse is still a problem, but not nearly as bad as regular GANs

Experiment:

Generate 2D samples from known Mix of Gaussian Distributions, then train 3 layer GANs to generate the same 2D data.

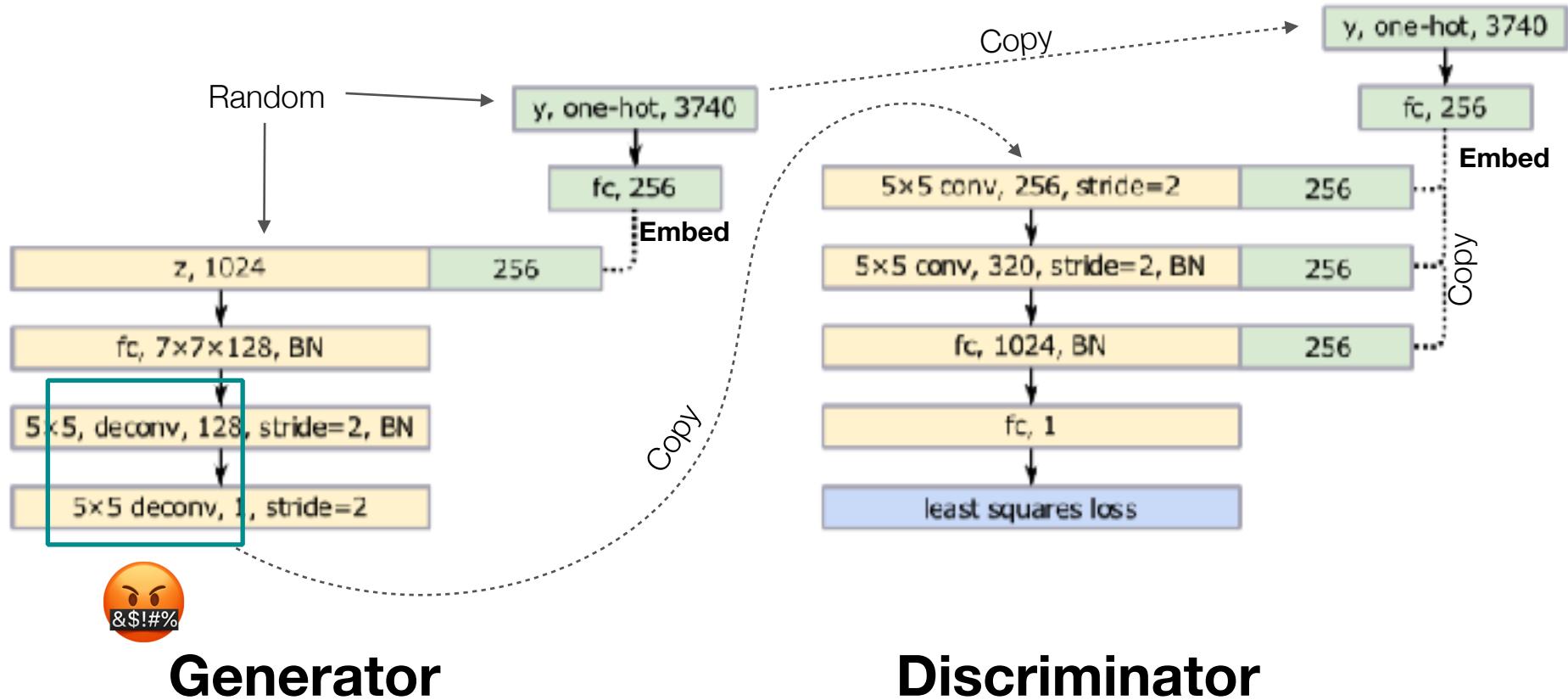


Does one learn the distribution?

Figure 8: Dynamic results of Gaussian kernel estimation for LSGANs and regular GANs. The final column shows the real data distribution.



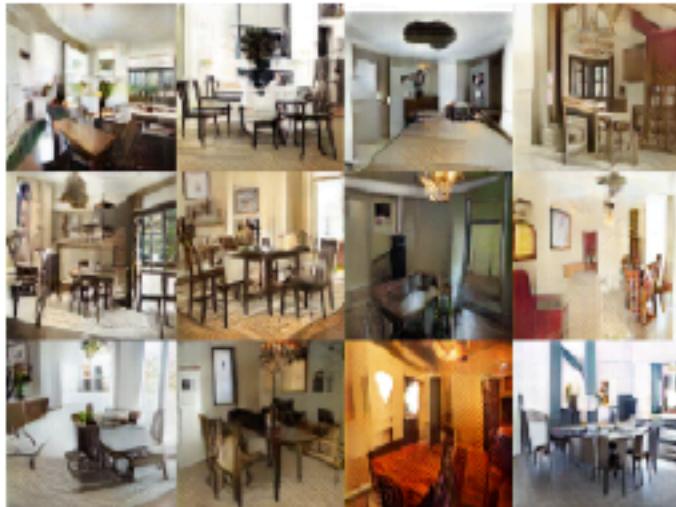
Architecture Employed



Qualitative Results



(a) Church outdoor.



(b) Dining room.



(c) Kitchen.



(d) Conference room.

More Qualitative Results



(a) Generated by LSGANs.



(b) Generated by DCGANs (Reported in [11]).



(c) Generated by EBGANs (Reported in [26]).



How can we trust the results?

- Do we trust that the authors are not cherry picking the results?
- If I perform random seed optimization and run my algorithms for longer, can I always claim its better
 - ...but maybe not for the reasons I publish...
- Without strong quantitative evaluation criteria for image generation, can there be a solution to this?
 - Require human subjects evaluation?
 - But can't they still tune the results for their algorithm before the human subjects testing?
 - What about open sourcing the weights of a tuned algorithm?



InfoGAN

InfoGAN: Interpretable Representation Learning by Information Maximizing Generative Adversarial Nets

Xi Chen^{†‡}, Yan Duan^{†‡}, Rein Houthooft^{†‡}, John Schulman^{†‡}, Ilya Sutskever[‡], Pieter Abbeel^{†‡}

† UC Berkeley, Department of Electrical Engineering and Computer Sciences

‡ OpenAI

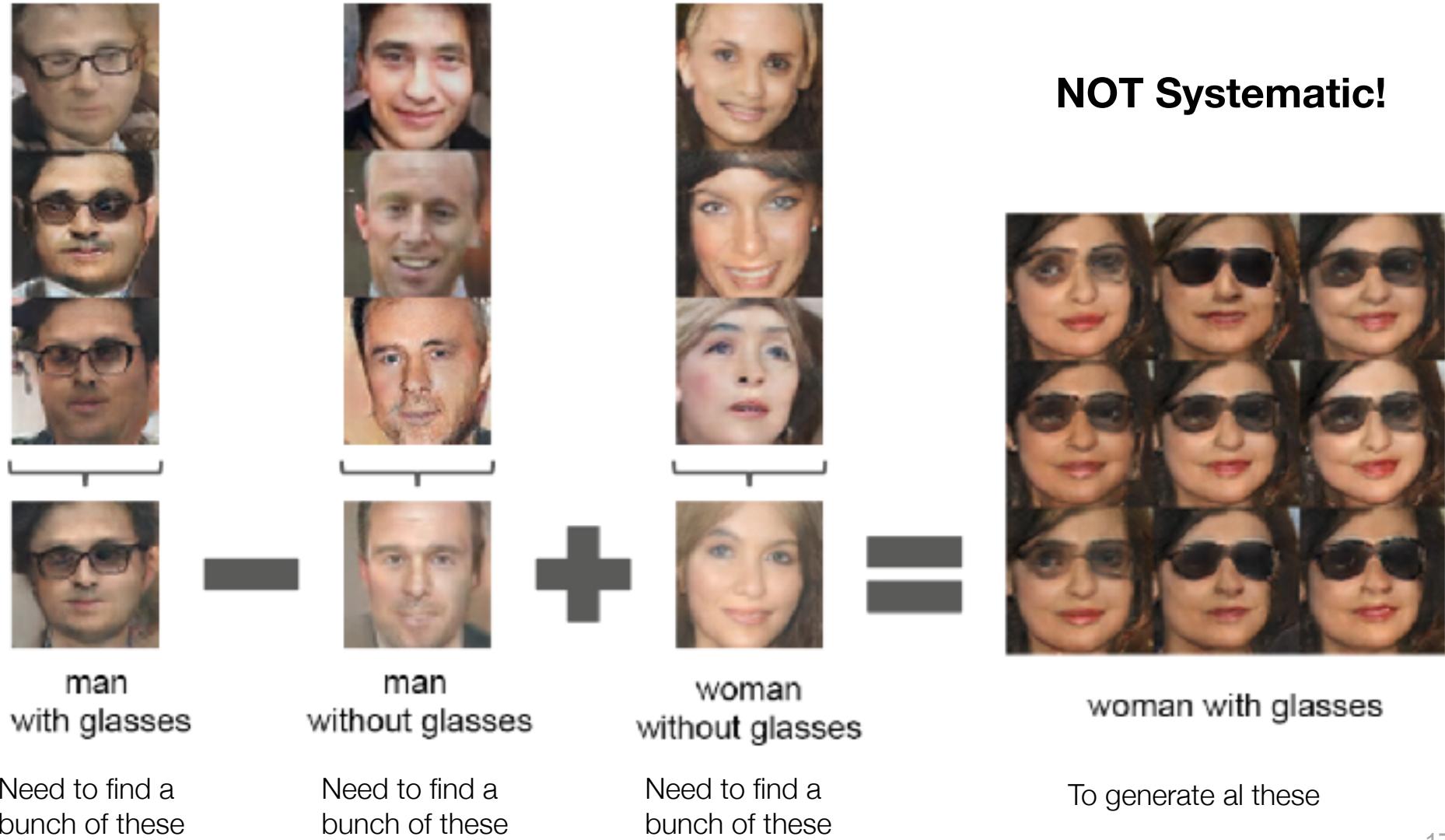


InfoGAN Problem Statement

- We need to disentangle information in the latent space for it to be truly useful
- Disentangling should be ascertained by the ability of the generator to have interpretable latent space axes
- Each axis should have little impact on the other axes, which is not imposed by any GAN structure yet
 - *For example, for a dataset of faces, a useful disentangled representation may allocate a separate set of dimensions for each of the following attributes: facial expression, eye color, hairstyle, presence or absence of eyeglasses, and the identity of the corresponding person.*



How to perform latent space arithmetic?



The InfoGAN Money Back Guarantee

However, many domains naturally decompose into a set of semantically meaningful factors of variation. For instance, when generating images from the MNIST dataset, it would be ideal if the model automatically chose to allocate a discrete random variable to represent the numerical identity of the digit's angle and by simply specifying continuous variables.

**Authors: by Maximizing Mutual Information
the network will learn to disentangle latent space**

- Decompose latent variable representation into
 - z : continuous incompressible noise
 - c : latent code, hopefully learns semantic features
- We want mutual information of c and $G(z,c)$ to be large
- Using standard entropy definition: $I(X;Y)=H(X)-H(X|Y)$
- New Loss Function: $\min_G \max_D V_I(D, G) = V(D, G) - \lambda I(c; G(z, c))$
Regular GAN Loss MI Loss



Maximizing Mutual Information

- You guessed it, Mutual Information with P is intractable to compute!
- So let's dust off our approximation pants and put some ELBO grease into this
- Variational Inference Maximization, Assume there is an approximation of P from Q :

$$\begin{aligned} I(c; G(z, c)) &= H(c) - H(c|G(z, c)) \\ &= \mathbb{E}_{x \sim G(z, c)} [\mathbb{E}_{c' \sim P(c|x)} [\log P(c'|x)]] + H(c) && \text{Expand Def. of Conditional Entropy} \\ &= \mathbb{E}_{x \sim G(z, c)} [\underbrace{D_{\text{KL}}(P(\cdot|x) \parallel Q(\cdot|x))}_{\text{make Q close to P}} + \mathbb{E}_{c' \sim P(c|x)} [\log Q(c'|x)]] + H(c) && \begin{array}{l} \text{Insert Q Approximation} \\ \text{sample from Q} \end{array} \\ &\geq \mathbb{E}_{x \sim G(z, c)} [\mathbb{E}_{c' \sim P(c|x)} [\log Q(c'|x)]] + H(c) && \begin{array}{l} \text{Define a Lower Bound to Maximize because} \\ \text{we don't like other terms...} \end{array} \end{aligned}$$

Lemma 5.1 *For random variables X, Y and function $f(x, y)$ under suitable regularity conditions:*
 $\mathbb{E}_{x \sim X, y \sim Y|x} [f(x, y)] = \mathbb{E}_{x \sim X, y \sim Y|x, x' \sim X|y} [f(x', y)].$



Maximizing Mutual Information (kinda)

$$I(c; G(z, c)) \geq \mathbb{E}_{x \sim G(z, c)} [\mathbb{E}_{c' \sim P(c|x)} [\log Q(c'|x)]] + H(c)$$

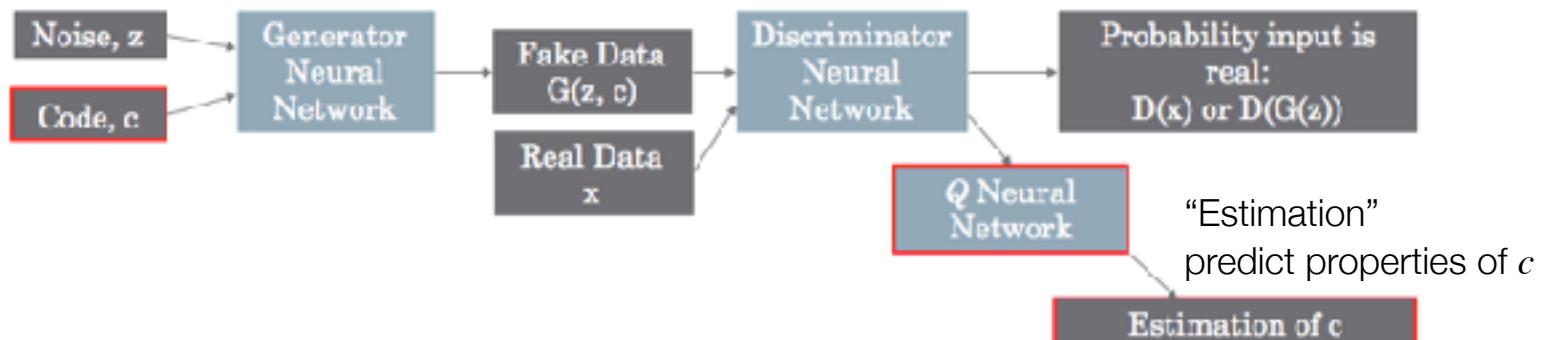
Lemma 5.1 For random variables X, Y and function $f(x, y)$ under suitable regularity conditions:
 $\mathbb{E}_{x \sim X, y \sim Y|x} [f(x, y)] = \mathbb{E}_{x \sim X, y \sim Y|x, x' \sim X|y} [f(x', y)].$

$$\begin{aligned} L_I(G, Q) &= \mathbb{E}_{c \sim P(c), x \sim G(z, c)} [\log Q(c|x)] + H(c) \\ &= \mathbb{E}_{x \sim G(z, c)} [\mathbb{E}_{c' \sim P(c|x)} [\log Q(c'|x)]] + H(c) \\ &\leq I(c; G(z, c)) \end{aligned}$$

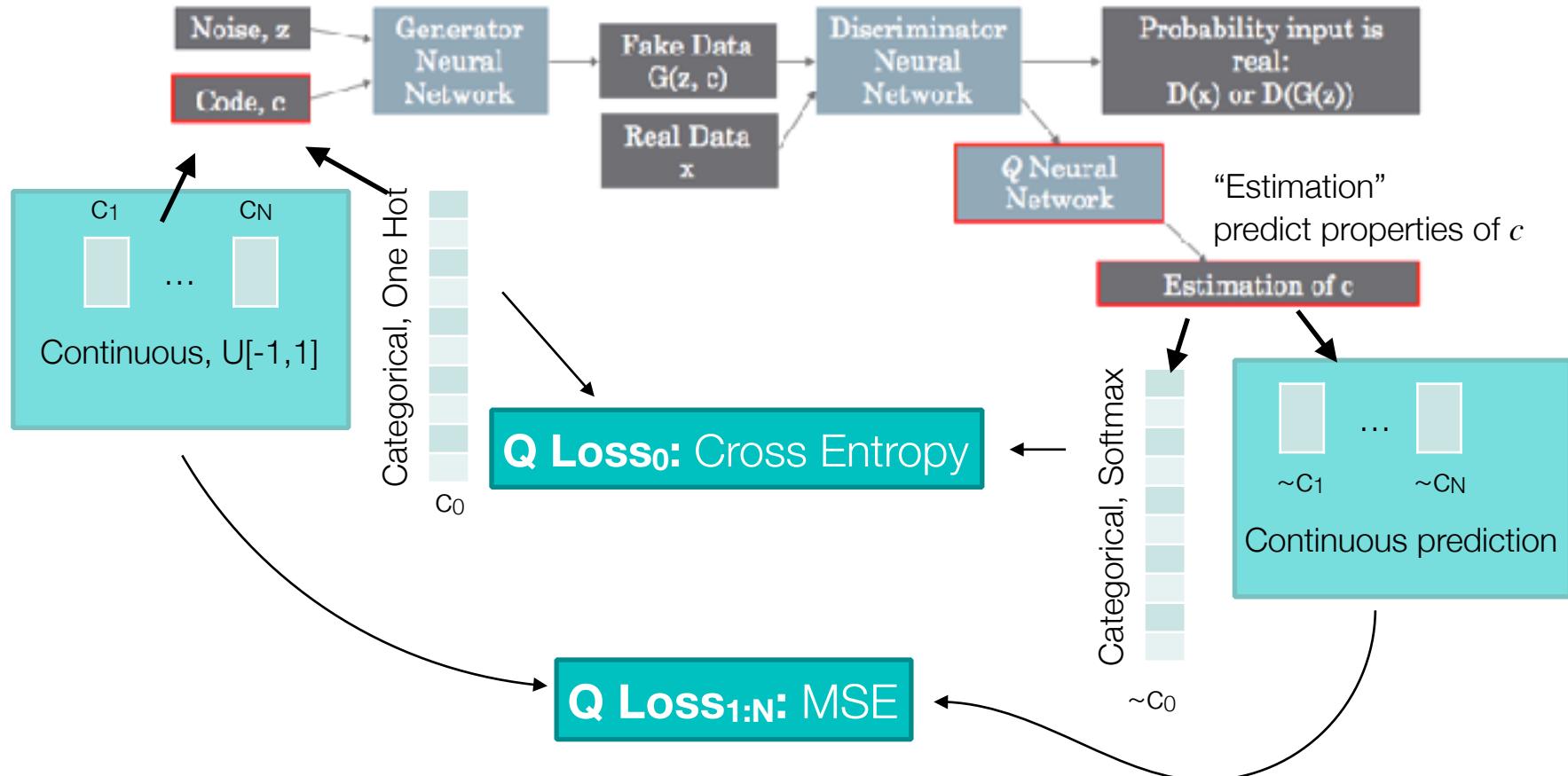
Re-parameterize:

Q will be good if we can measure
 c from the Generator network

New Objective Function Becomes: $\min_{G, Q} \max_D V_{\text{InfoGAN}}(D, G, Q) = V(D, G) - \lambda L_I(G, Q)$



Measuring Latent Codes in Loss



Intuition: If the generator starts to use these codes and variables semantically, then the Q network (and therefore the discriminator) can start learning to predict these semantics. By learning these semantics, the generator is incentivized to produce disentangled, meaningful features from the codes.



Implementation: D and Q

```
# define the standalone discriminator model
def define_discriminator(n_cat, in_shape=(28,28,1)):
    # weight initialization
    init = RandomNormal(stddev=0.02)
    # image input
    in_image = Input(shape=in_shape)
    # downsample to 14x14
    d = Conv2D(64, (4,4), strides=(2,2), padding='same', kernel_initializer=init)(in_image)
    d = LeakyReLU(alpha=0.1)(d)
    # downsample to 7x7
    d = Conv2D(128, (4,4), strides=(2,2), padding='same', kernel_initializer=init)(d)
    d = LeakyReLU(alpha=0.1)(d)
    d = BatchNormalization()(d)
    # normal
    d = Conv2D(256, (4,4), padding='same', kernel_initializer=init)(d)
    d = LeakyReLU(alpha=0.1)(d)
    d = BatchNormalization()(d)
    # flatten feature maps
    d = Flatten()(d)
    # real/fake output
    out_classifier = Dense(1, activation='sigmoid')(d)
    # define d model
    d_model = Model(in_image, out_classifier)
    # compile d model
    d_model.compile(loss='binary_crossentropy', optimizer=Adam(lr=0.0002, beta_1=0.5))
    # create q model layers
    q = Dense(128)(d)
    q = BatchNormalization()(q)
    q = LeakyReLU(alpha=0.1)(q)
    # q model output
    out_codes = Dense(n_cat, activation='softmax')(q)
    # define q model
    q_model = Model(in_image, out_codes)
    return d_model, q_model
```



Implementation: G and Q Trained

```
# define the combined discriminator, generator and q network model
def define_gan(g_model, d_model, q_model):
    # make weights in the discriminator (some shared with the q model) as not trainable
    d_model.trainable = False
    # connect g outputs to d inputs
    d_output = d_model(g_model.output)
    # connect g outputs to q inputs
    q_output = q_model(g_model.output)
    # define composite model
    model = Model(g_model.input, [d_output, q_output])
    # compile model
    opt = Adam(lr=0.0002, beta_1=0.5)
    model.compile(loss=['binary_crossentropy', 'categorical_crossentropy'], optimizer=opt)
    return model
```

```
# generate points in latent space as input for the generator
```

```
def generate_latent_points(latent_dim, n_cat, n_samples):
```

```
    # generate points in the latent space
```

```
    z_latent = randn(latent_dim * n_samples)
```

```
    # reshape into a batch of inputs for the network
```

```
    z_latent = z_latent.reshape(n_samples, latent_dim)
```

```
    # generate categorical codes
```

```
    cat_codes = randint(0, n_cat, n_samples)
```

Only uses codes, not continuous “c” vars

```
    # one hot encode
```

```
    cat_codes = to_categorical(cat_codes, num_classes=n_cat)
```

```
    # concatenate latent points and control codes
```

```
    z_input = hstack((z_latent, cat_codes))
```

```
    return [z_input, cat_codes]    Input to generator and labels for Q network returned (repeats “c”)
```

<https://machinelearningmastery.com/how-to-develop-an-information-maximizing-generative-adversarial-network-infogan-in-keras/>

23



Implementation: Training

```
# train the generator and discriminator
def train(g_model, d_model, gan_model, dataset, latent_dim, n_cat, n_epochs=100, n_batch=64):
    # calculate the number of batches per training epoch
    bat_per_epo = int(dataset.shape[0] / n_batch)
    # calculate the number of training iterations
    n_steps = bat_per_epo * n_epochs
    # calculate the size of half a batch of samples
    half_batch = int(n_batch / 2)
    # manually enumerate epochs
    for i in range(n_steps):
        # get randomly selected 'real' and 'fake' samples
        X_real, y_real = generate_real_samples(dataset, half_batch)
        X_fake, y_fake = generate_fake_samples(g_model, latent_dim, n_cat, half_batch)
        # update discriminator and q model weights
        d_loss1 = d_model.train_on_batch(X_real, y_real)
        d_loss2 = d_model.train_on_batch(X_fake, y_fake)
        # prepare points in latent space as input for the generator
        z_input, cat_codes = generate_latent_points(latent_dim, n_cat, n_batch)
        # create inverted labels for the fake samples
        y_mislead = ones((n_batch, 1))
        # update the g via the d and q error
        _,g_1,g_2 = gan_model.train_on_batch(z_input, [y_mislead, cat_codes])
        # summarize loss on this batch
        print('>%d, d[%.*f,%.*f], g[%.*f] q[%.*f]' % (i+1, d_loss1, d_loss2, g_1, g_2))
        # evaluate the model performance every 'epoch'
        if (i+1) % (bat_per_epo * 10) == 0:
            summarize_performance(i, g_model, gan_model, latent_dim, n_cat)
```



Did they really disentangle?

$c_1 = 10$ discrete codes with equal probability 0.1

c_2 and c_3 = uniformly sampled data from -1 to 1

0 1 2 3 4 5 6 7 8 9	7 7 7 7 7 7 7 7 7 7
0 1 2 3 4 5 6 7 8 7	0 0 0 0 0 0 0 0 0 0
0 1 2 3 4 5 6 7 8 9	7 7 7 7 7 7 7 7 7 7
0 1 2 3 4 5 6 7 8 9	9 9 9 9 9 9 9 9 9 9
0 1 2 3 4 5 6 7 8 9	8 8 8 8 8 8 8 8 8 8

(a) Varying c_1 on InfoGAN (Digit type)

(b) Varying c_1 on regular GAN (No clear meaning)

1 1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1
8 8 8 8 8 8 8 8 8 8	8 8 8 8 8 8 8 8 8 8
3 3 3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3 3 3
9 9 9 9 9 9 9 9 9 9	9 9 9 9 9 9 9 9 9 9
5 5 5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5 5 5

(c) Varying c_2 from -2 to 2 on InfoGAN (Rotation)

(d) Varying c_3 from -2 to 2 on InfoGAN (Width)

Columns: Hold other variables constant, Rows: Vary named variable



Did they really disentangle?



(a) Azimuth (pose)

(b) Elevation



(c) Lighting

(d) Wide or Narrow

Figure 3: **Manipulating latent codes on 3D Faces:** We show the effect of the learned continuous

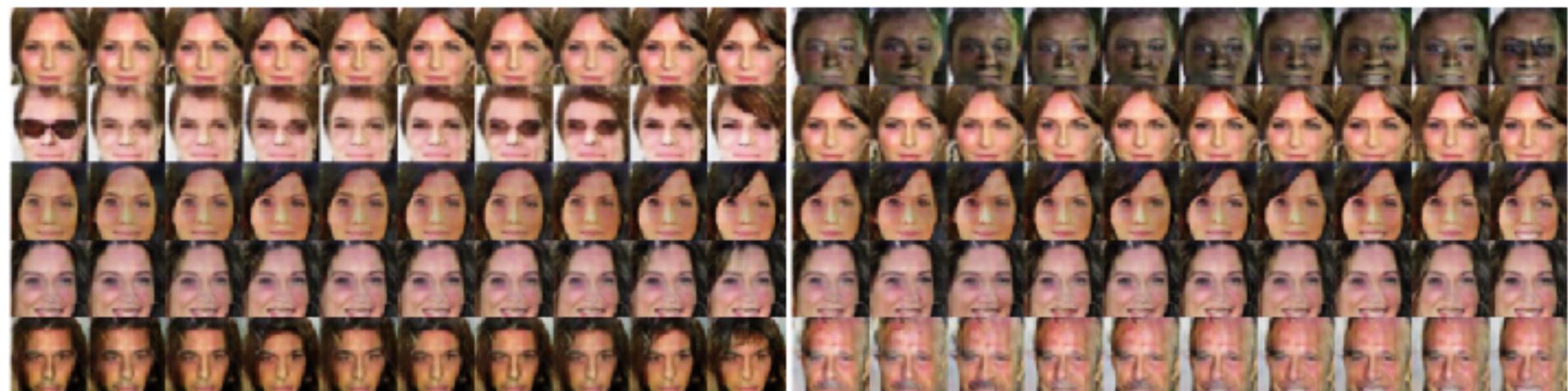


Did they really disentangle?



(a) Azimuth (pose)

(b) Presence or absence of glasses



(c) Hair style

(d) Emotion



CycleGAN

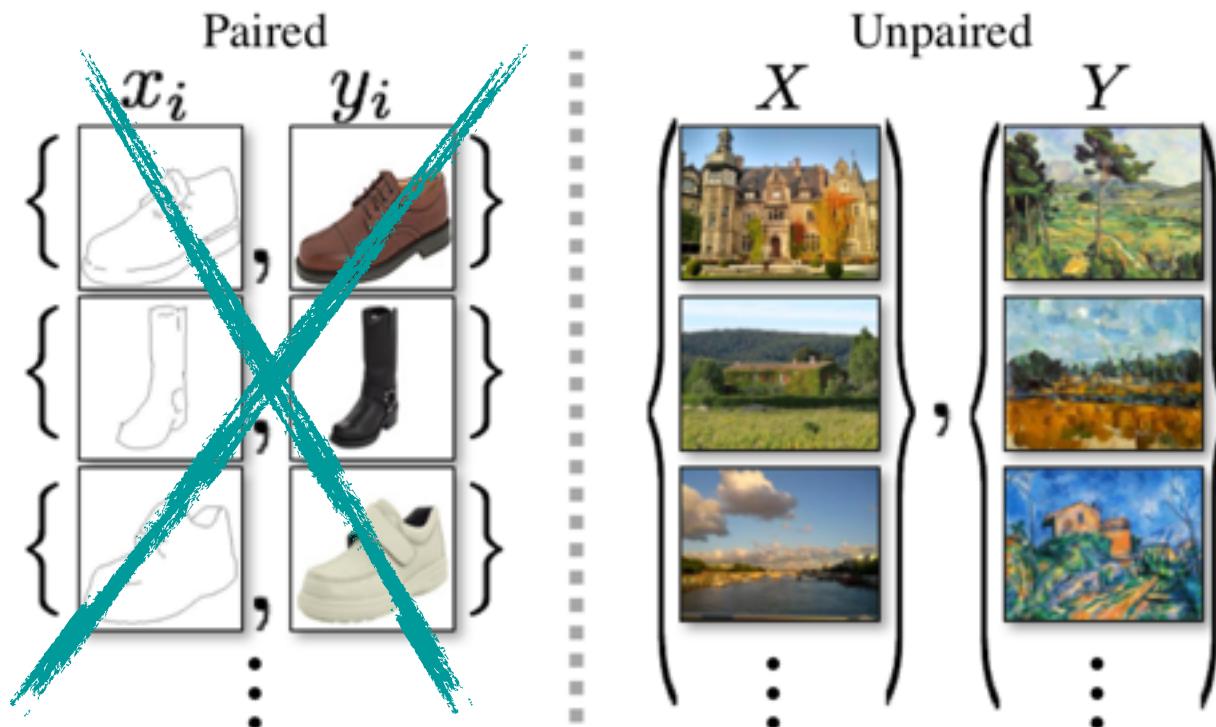
Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks

Jun-Yan Zhu* Taesung Park* Phillip Isola Alexei A. Efros
Berkeley AI Research (BAIR) laboratory, UC Berkeley

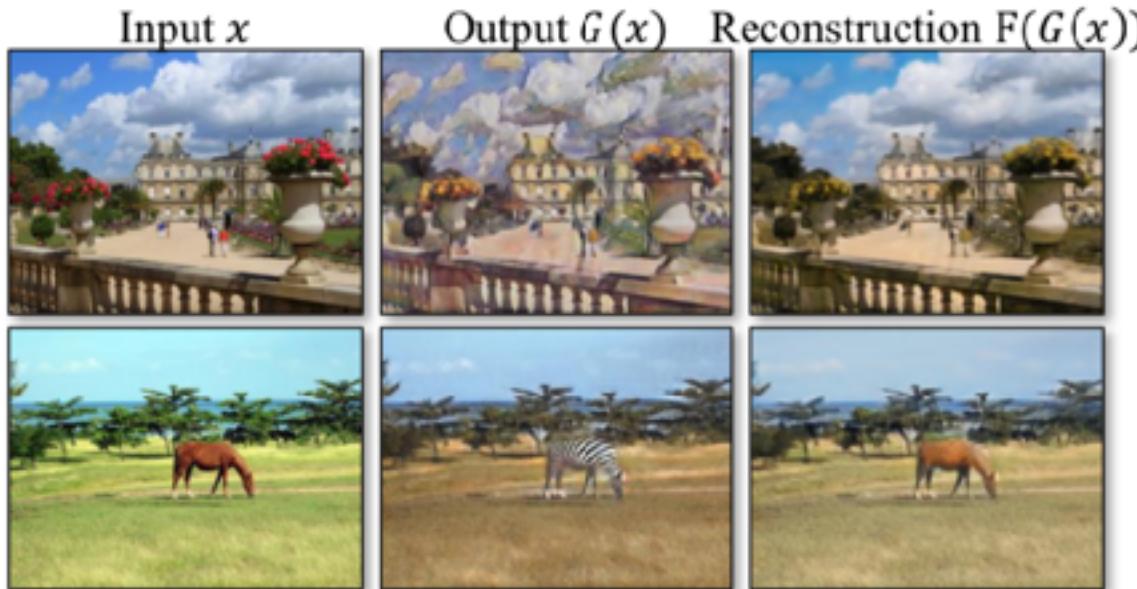
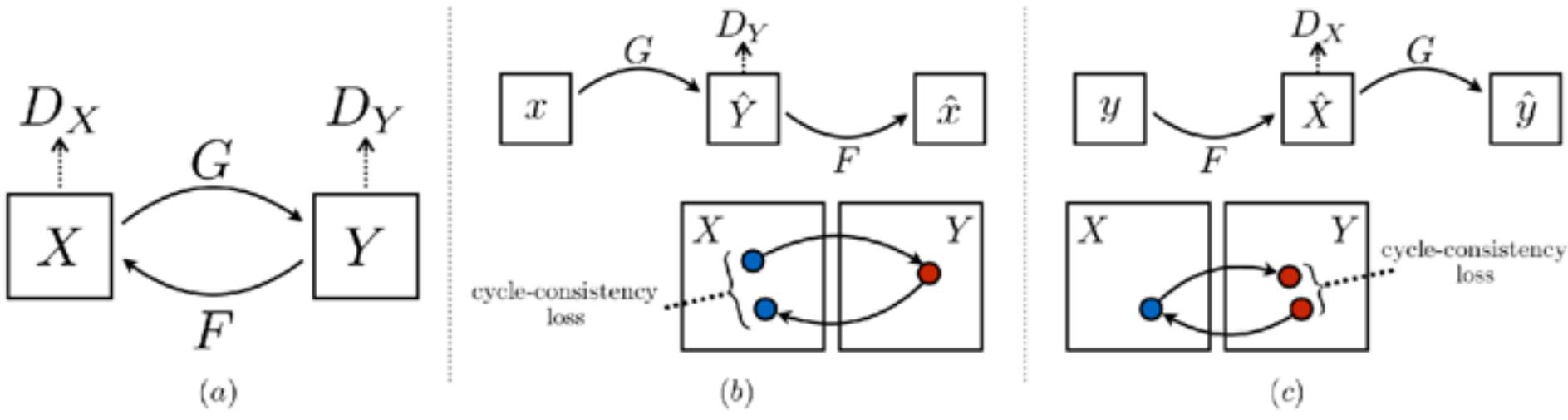


Unpaired Cycles

- Idea: Try to find specialized unpaired translations that are consistent between domains



Defining Cycle Consistency



Adding to the loss function

- Have two discriminator losses for two auto encoders:

$$\begin{aligned}\mathcal{L}_{\text{GAN}}(G, D_Y, X, Y) = & \mathbb{E}_{y \sim p_{\text{data}}(y)} [\log D_Y(y)] \\ & + \mathbb{E}_{x \sim p_{\text{data}}(x)} [\log(1 - D_Y(G(x)))]\end{aligned}$$

- Enforce cycle consistency and self consistency:

$$\begin{aligned}\mathcal{L}_{\text{cyc}}(G, F) = & \mathbb{E}_{x \sim p_{\text{data}}(x)} [\|F(G(x)) - x\|_1] \\ & + \mathbb{E}_{y \sim p_{\text{data}}(y)} [\|G(F(y)) - y\|_1].\end{aligned}$$

$$\mathcal{L}_{\text{identity}}(G, F) = \mathbb{E}_{y \sim p_{\text{data}}(y)} [\|G(y) - y\|_1] + \mathbb{E}_{x \sim p_{\text{data}}(x)} [\|F(x) - x\|_1]$$

- Put it all together:

$$\begin{aligned}\mathcal{L}(G, F, D_X, D_Y) = & \mathcal{L}_{\text{GAN}}(G, D_Y, X, Y) \\ & + \mathcal{L}_{\text{GAN}}(F, D_X, Y, X) \\ & + \lambda \mathcal{L}_{\text{cyc}}(G, F),\end{aligned}$$



Training Notes

Training details We apply two techniques from recent works to stabilize our model training procedure. First, for \mathcal{L}_{GAN} (Equation 1), we replace the negative log likelihood objective by a least-squares loss [35]. This loss is more stable during training and generates higher quality results. In particular, for a GAN loss $\mathcal{L}_{\text{GAN}}(G, D, X, Y)$, we train the G to minimize $\mathbb{E}_{x \sim p_{\text{data}}(x)}[(D(G(x)) - 1)^2]$ and train the D to minimize $\mathbb{E}_{y \sim p_{\text{data}}(y)}[(D(y) - 1)^2] + \mathbb{E}_{x \sim p_{\text{data}}(x)}[D(G(x))^2]$.

Second, to reduce model oscillation [15], we follow generators using a history of generated images rather than the ones produced by the latest generators. We keep an image buffer that stores the 50 previously created images.

For all the experiments, we set $\lambda = 10$ in Equation 3. We use the Adam solver [26] with a batch size of 1. All networks were trained from scratch with a learning rate of 0.0002. We keep the same learning rate for the first 100 epochs and linearly decay the rate to zero over the next 100 epochs. Please see the appendix (Section 7) for more details about the datasets, architectures, and training procedures.

So, not using Entropy?

Yes! Experience Replay!

Linear learning rate decay.



Show me the Code!

Discriminators

```
# Build and compile the discriminators
self.d_A = self.build_discriminator()
self.d_B = self.build_discriminator()
self.d_A.compile(loss='mse',
    optimizer=optimizer,
    metrics=['accuracy'])
self.d_B.compile(loss='mse',
    optimizer=optimizer,
    metrics=['accuracy'])
```

Cycle Producers

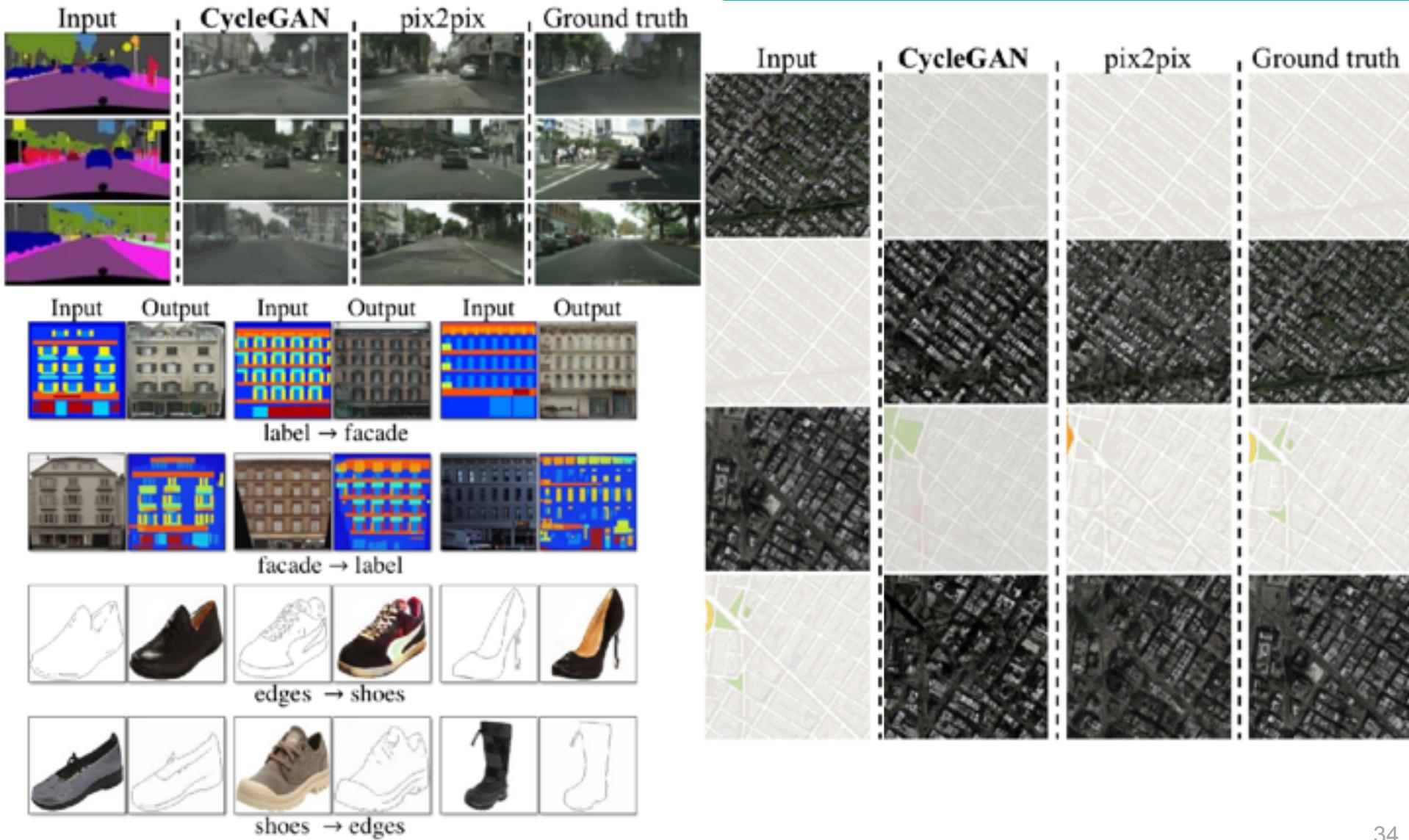
```
# Translate images to the other domain
fake_B = self.g_AB(img_A)
fake_A = self.g_BA(img_B)
# Translate images back to original domain
reconstr_A = self.g_BA(fake_B)
reconstr_B = self.g_AB(fake_A)
# Identity mapping of images
img_A_id = self.g_BA(img_A)
img_B_id = self.g_AB(img_B)
```

```
# Combined model trains generators to fool discriminators
self.combined = Model(inputs=[img_A, img_B],
                      outputs=[ valid_A, valid_B,
                                reconstr_A, reconstr_B,
                                img_A_id, img_B_id ])
self.combined.compile(loss=['mse', 'mse', discriminator MSE, 0,1
                           'mae', 'mae', cycle consistency
                           'mae', 'mae'], self consistency
                      loss_weights=[ 1, 1,
                                     self.lambda_cycle, self.lambda_cycle,
                                     self.lambda_id, self.lambda_id ],
                      optimizer=optimizer)
```

<https://github.com/eriklindernoren/Keras-GAN/blob/master/cyclegan/cyclegan.py>



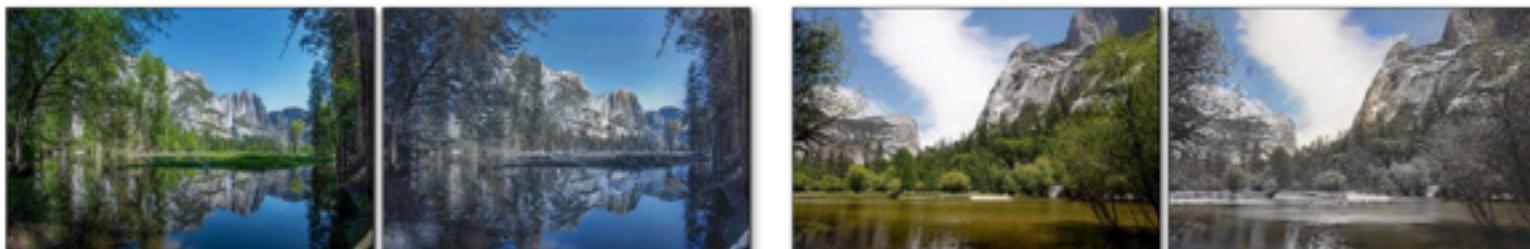
Results



Fun Results



winter Yosemite → summer Yosemite



summer Yosemite → winter Yosemite



apple → orange

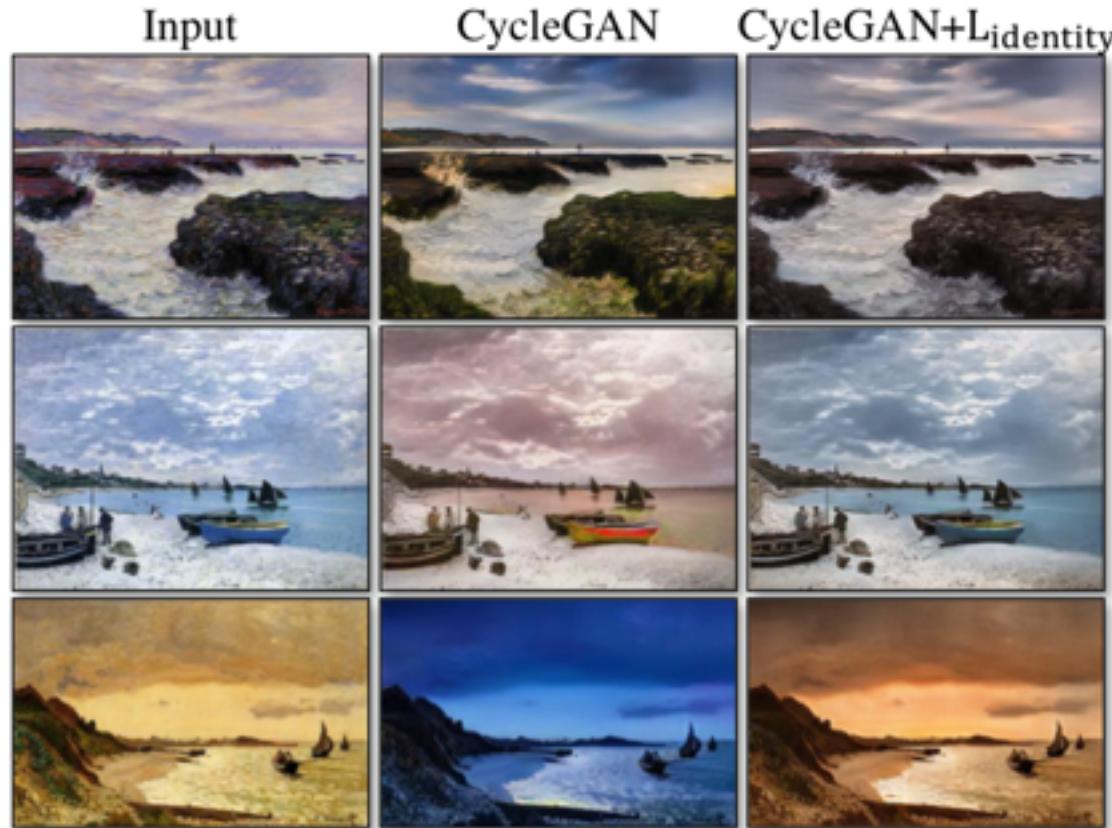


orange → apple



Results: Fixing Hue Changes

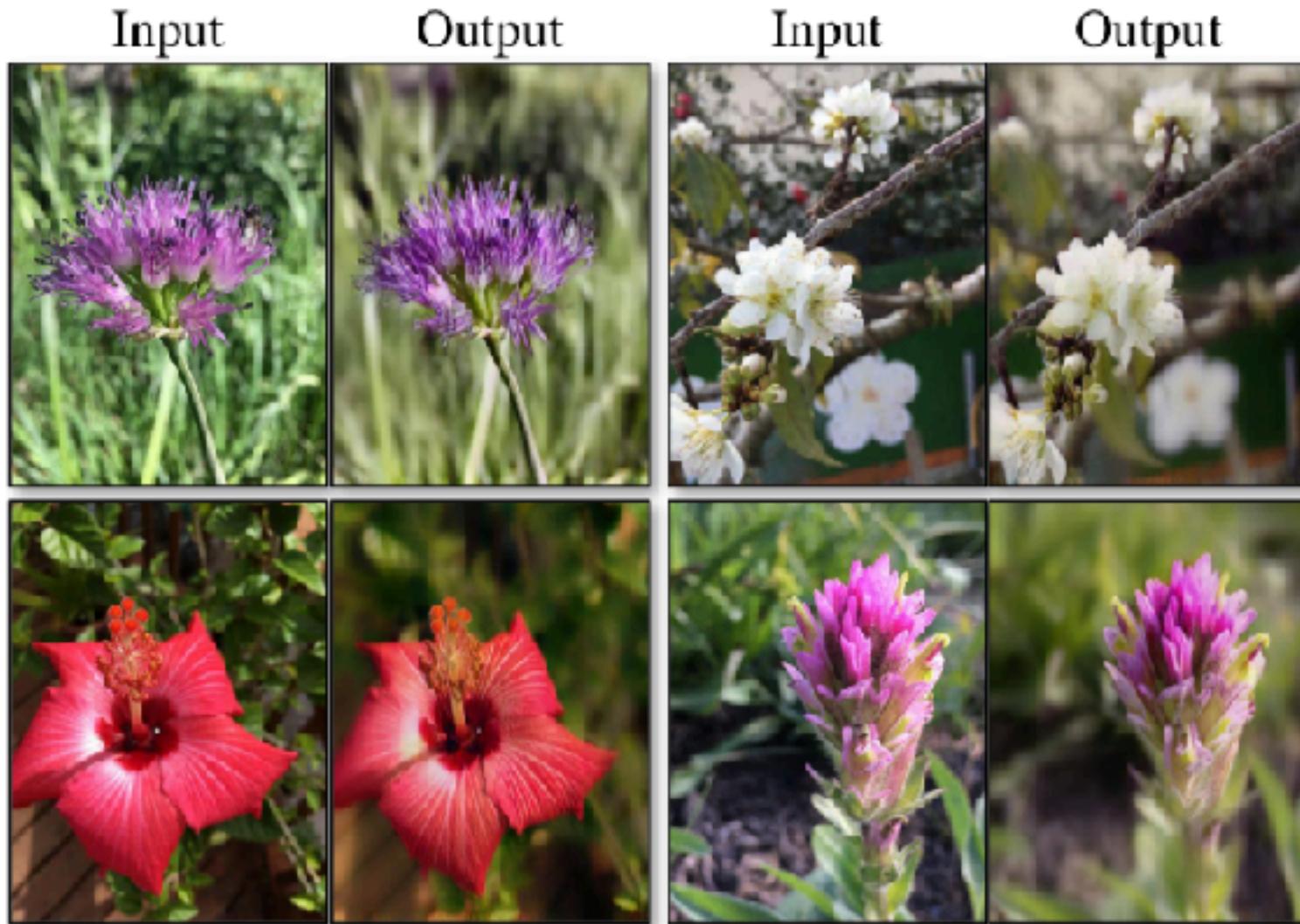
- Self consistency is mostly about preserving color



$$\begin{aligned}\mathcal{L}_{\text{identity}}(G, F) = \\ \mathbb{E}_{y \sim p_{\text{data}}(y)} [\|G(y) - y\|_1] + \\ \mathbb{E}_{x \sim p_{\text{data}}(x)} [\|F(x) - x\|_1]\end{aligned}$$



Image Enhancement



Map from iPhone Images to DSLR Photos



Full Circle: Back to Style Transfer

Input



Monet



Van Gogh



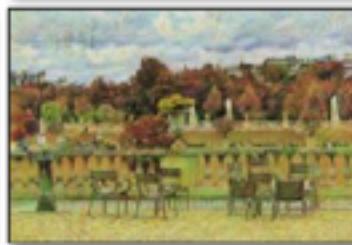
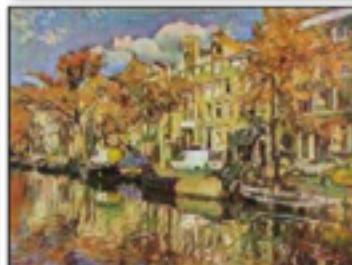
Cezanne



Ukiyo-e



Input



They can't all be gold

Input

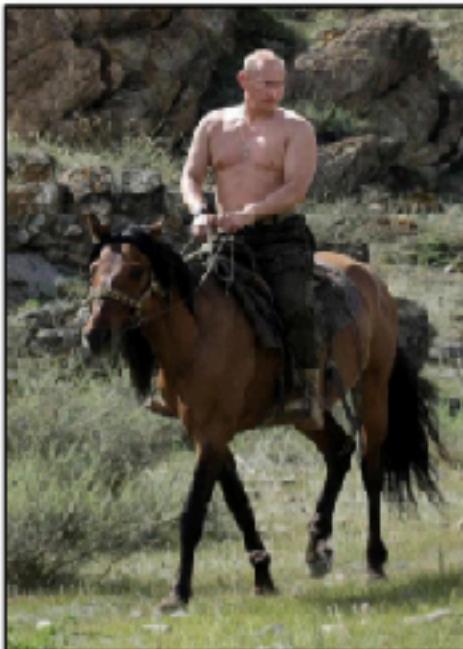


Output



winter → summer

Input



Output



horse → zebra

Monet → photo



iPhone photo → DSLR photo



ImageNet “wild horse” training images



GAN Town Hall

Asking a friend about adversarial attacks

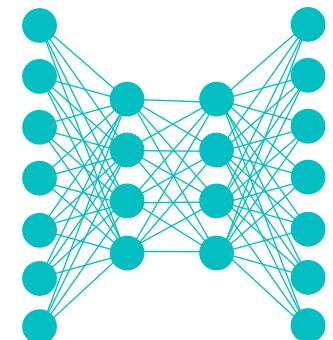


Lecture Notes for **Neural Networks** **and Machine Learning**

Holy GAN Zooks



Next Time:
Continued
Reading: None

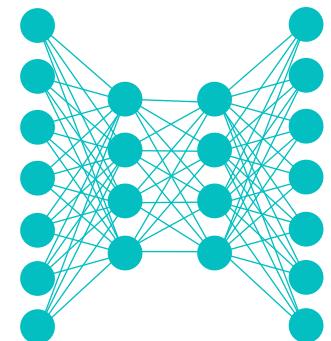




Lecture Notes for **Neural Networks** **and Machine Learning**



Holy GAN-Zooks
Continued



Logistics and Agenda

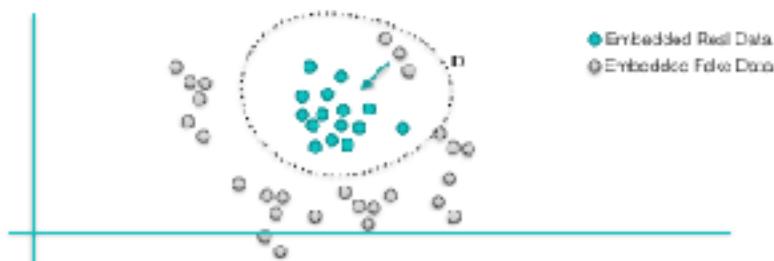
- Logistics
- Agenda
 - More GANs:
 - ◆ GAIA
 - ◆ Conditional GAN
 - ◆ Text-to-image Synthesis
 - ◆ BigGAN



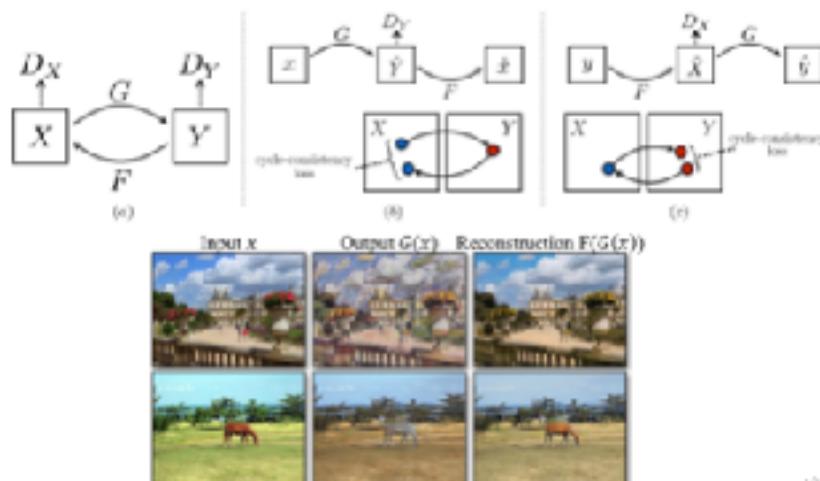
Last Time

The Least Squares GAN

- Observation:** Generated points may (by chance) be classified as real by Discriminator—but they are still not representative of the real data
- Solution:** Incentivize even correctly classified labels to move toward real data distribution



Defining Cycle Consistency



Maximizing Mutual Information (kinda)

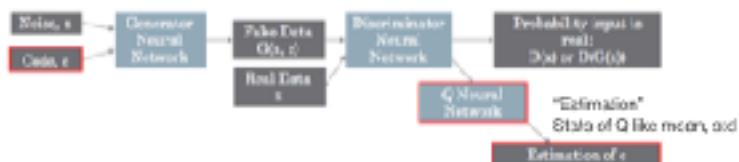
$$J(c; G(z, c)) \geq \mathbb{E}_{z \sim G(z, c)} [\mathbb{E}_{x' \sim P(x|z, c)} [\log Q(x'|x)]] + H(c)$$

Lemma 5.1: For random variables X, Y and function $f(x, y)$ under suitable regularity conditions: $\mathbb{E}_{x \sim N, y \sim Y} [f(x, y)] = \mathbb{E}_{x \sim N, y \sim Y} [\mathbb{E}_{x' \sim N|y} [f(x', y)]]$

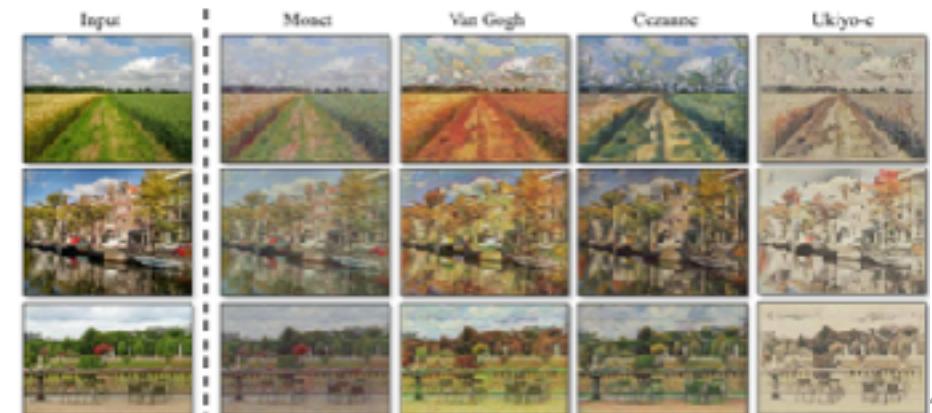
$$\begin{aligned} L_I(G, Q) &= \mathbb{E}_{z \sim P(z), x \sim G(z, c)} [\log Q(c|x)] + H(c) \\ &= \mathbb{E}_{z \sim P(z, c)} [\mathbb{E}_{x' \sim P(x|z, c)} [\log Q(x'|x)]] + H(c) \\ &\leq I(c; G(z, c)) \end{aligned}$$

Re-parameterization:
Define λ what your children can
you want to sample from!

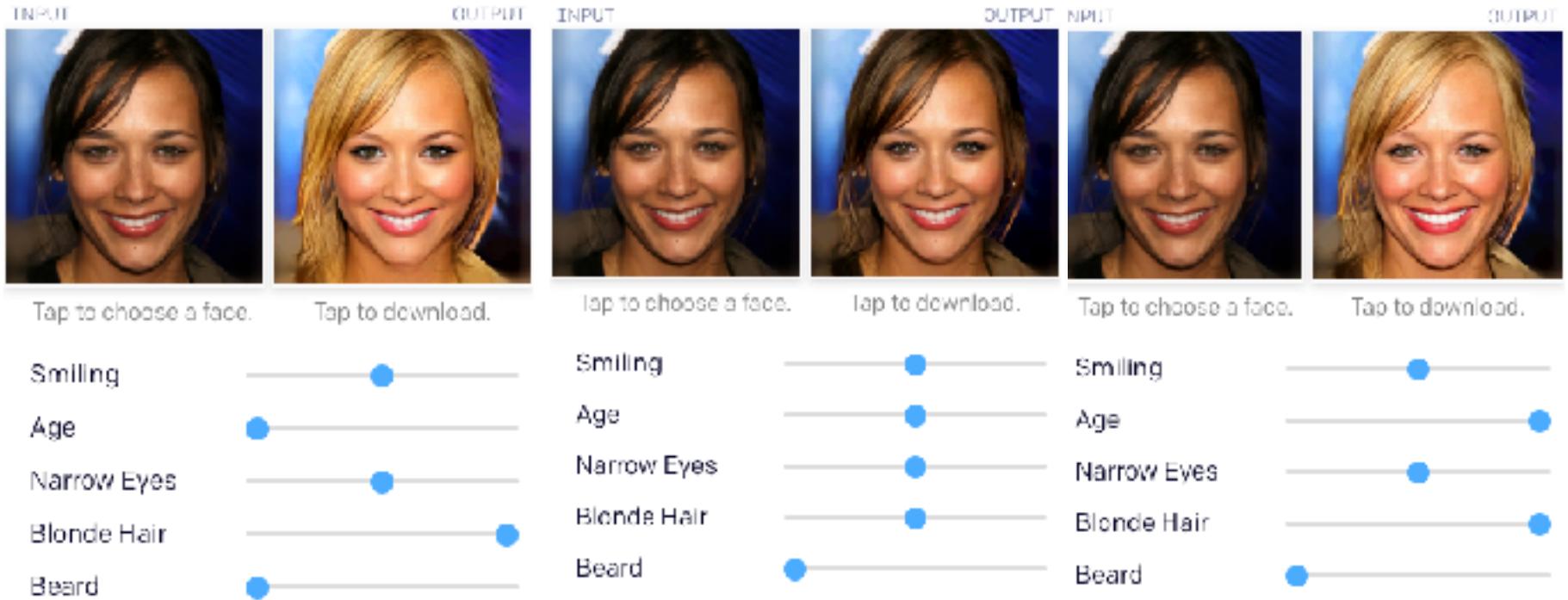
$$\text{New Objective Function becomes } \min_{G, Q} \max_D V_{\text{InfoGAN}}(D, G, Q) = V(D, G) - \lambda L_I(G, Q)$$



Full Circle: Back to Style Transfer



GLOW



GAIA



Tim Sainburg

PhD Student @ UCSD studying
Psychology, Neuroscience,
Anthropogeny, Animal Communication,
and Machine Learning

Generative adversarial interpolative autoencoding: adversarial training on latent space interpolations encourage convex latent distributions

Tim Sainburg
UC San Diego
tsainbur@ucsd.edu

Marvin Thielk
UC San Diego
mthielk@ucsd.edu

Brad Theilman
UC San Diego
btheilm@ucsd.edu

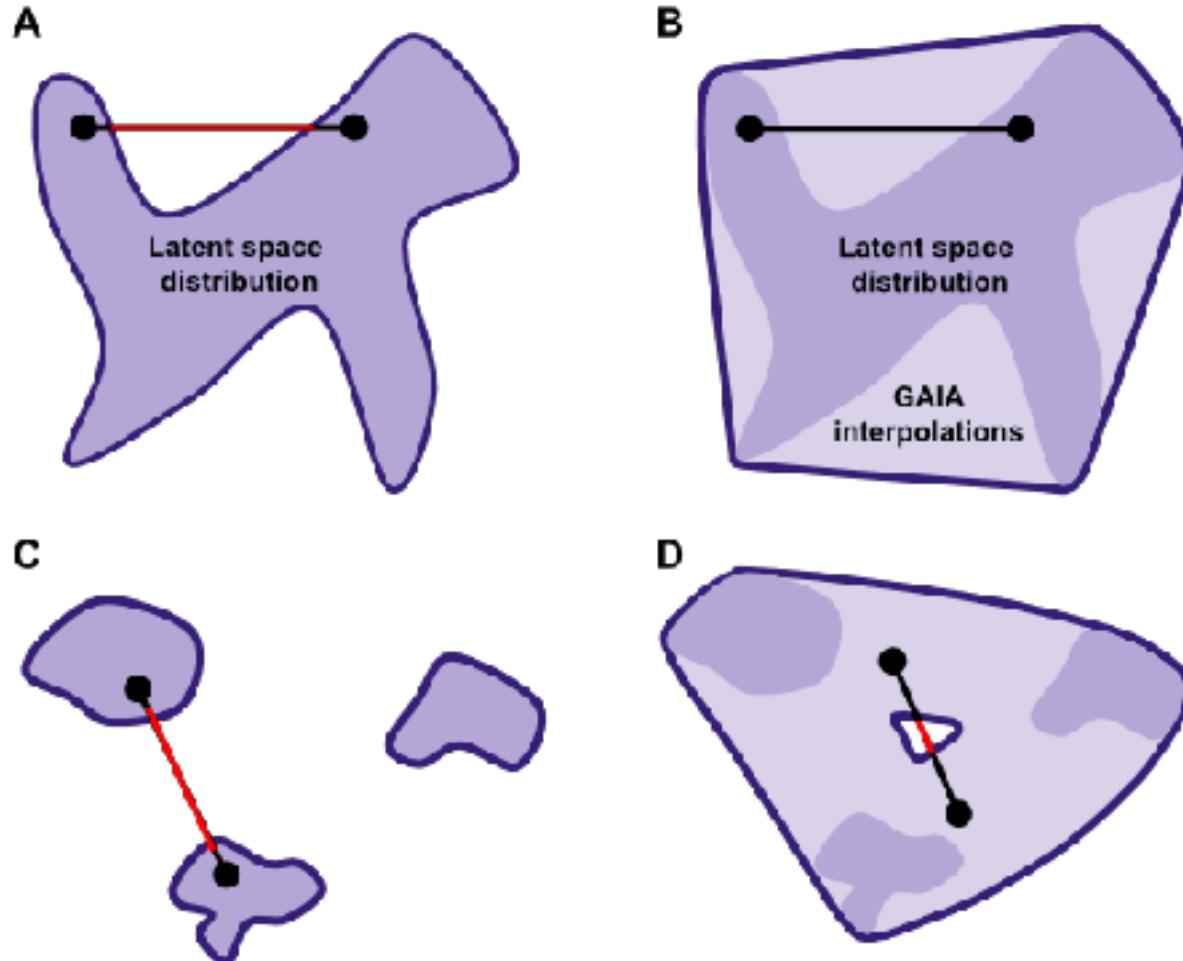
Benjamin Migliori
SPAWAR
migliori@spawar.navy.mil

Timothy Gentner
UC San Diego
tgentner@ucsd.edu



What does GAIA address?

- Explicitly Interpolate to make latent space as **convex** as possible



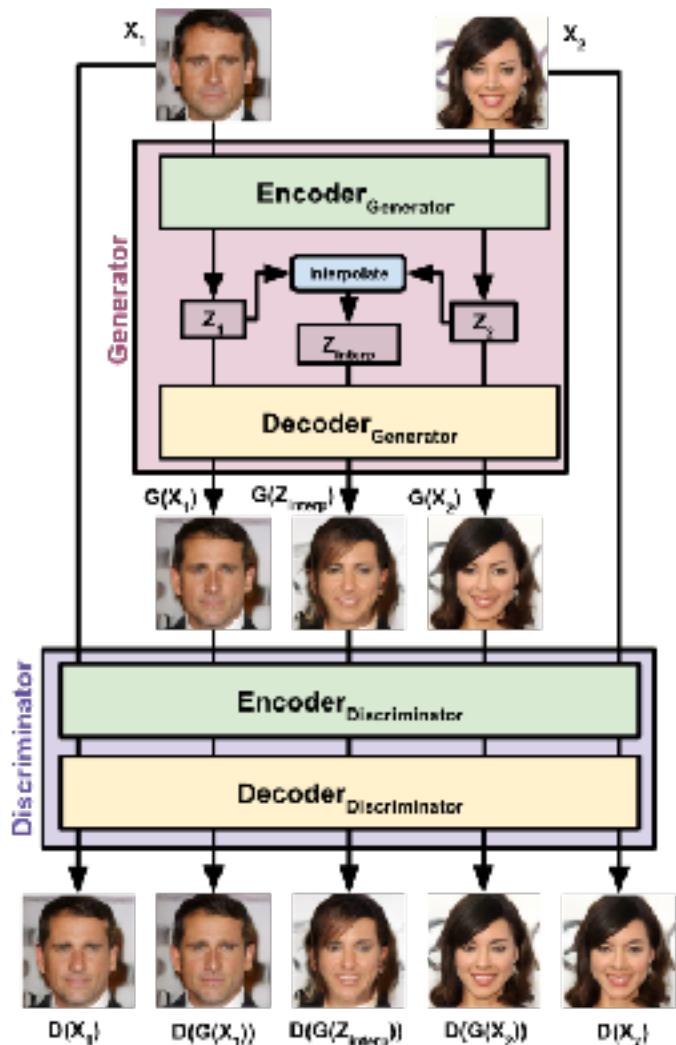
<https://timsainburg.com/gaia.html#gaia>

How to enforce convexity?

- Change discriminator function entirely
 - Discriminator also auto-encodes an image
 - Maximize **reconstruction error** in generated image for **fake**
 - Minimize **reconstruction error** in generated image for **real**
- Generator takes two images and outputs three
 - Two are simply auto encoded
 - Third Image is interpolated



How to enforce convexity?



Generator: Minimize

$$\mathcal{L}_{Gen} = \|X - D(G(X))\|_1 + \|G(Z_{\text{interp}}) - D(G(G(Z_{\text{interp}})))\|_1$$

Discriminator: Minimize

$$\begin{aligned}\mathcal{L}_{Disc} = & \|X - D(X)\|_1 + \\ & - \|G(X) - D(G(X))\|_1 + \\ & - \|G(Z_{\text{interp}}) - D(G(G(Z_{\text{interp}})))\|_1\end{aligned}$$

Regularize, for each mini-batch:

$$\begin{aligned}\mathcal{L}_{dist}(X, Z) = & \frac{1}{B} \sum_{i,j}^B \left[\log_2 \left(1 + \frac{(X_i - X_j)^2}{\frac{1}{N} \sum_{i,j} (X_i - X_j)^2} \right) \right. \\ & \left. - \log_2 \left(1 + \frac{(Z_i - Z_j)^2}{\frac{1}{N} \sum_{i,j} (Z_i - Z_j)^2} \right) \right]\end{aligned}$$



Results



Results



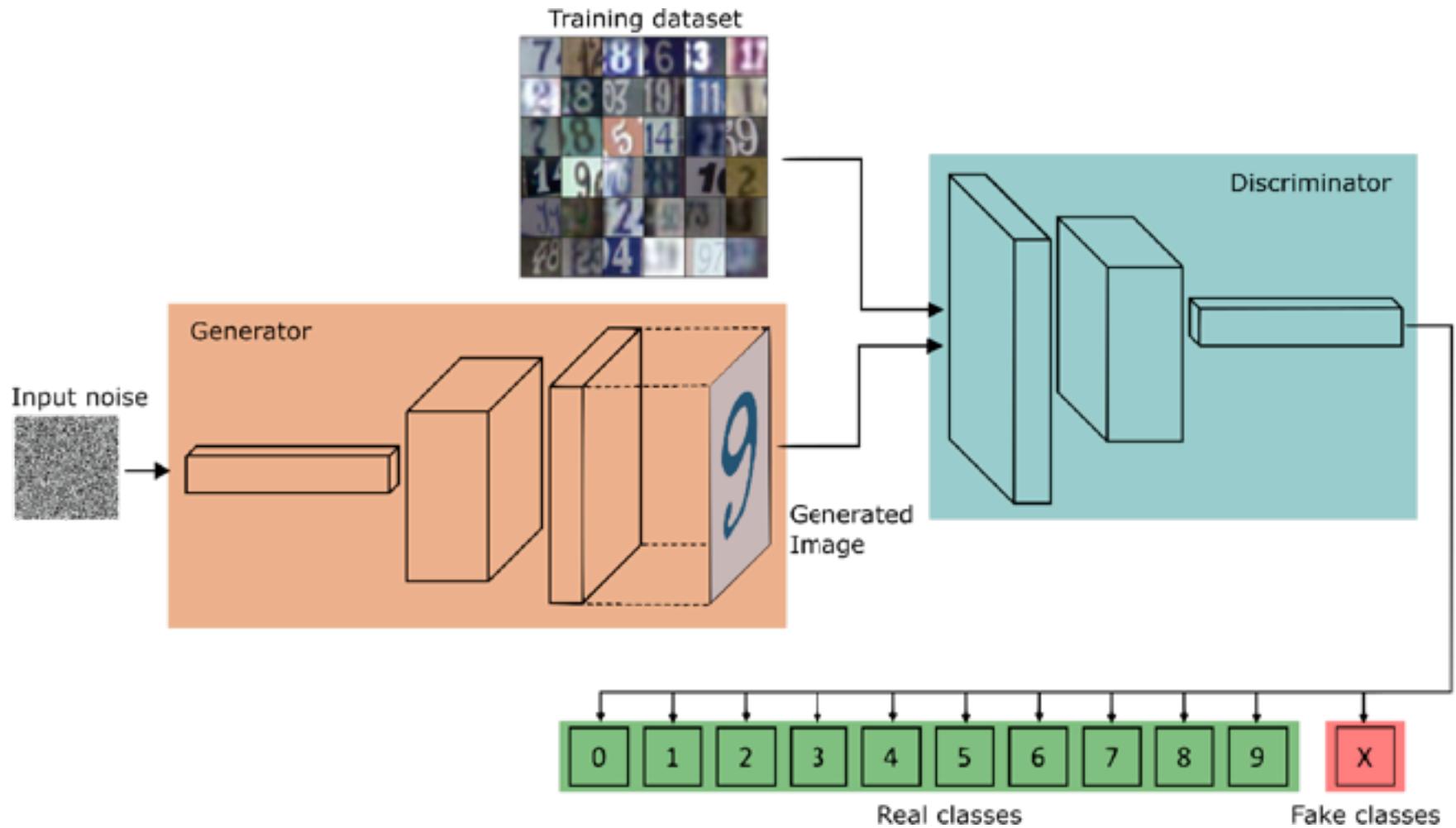
GANs for Improving Classifiers



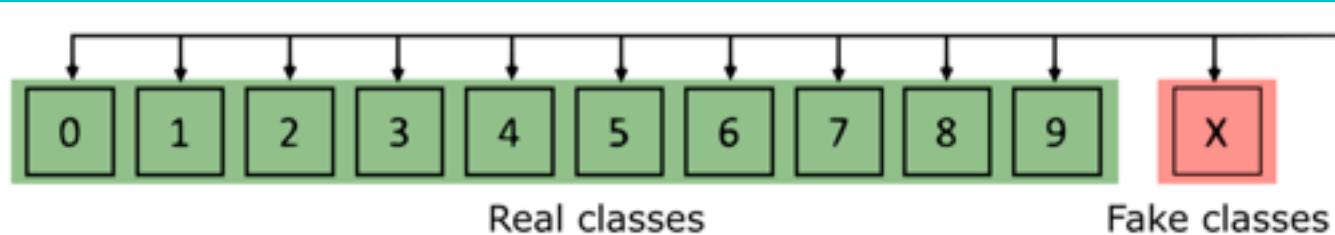
hadou-GAN



Fewer Labels, Still Lots of Data



Minimizing Labels



- MNIST Performance
 - 60,000 labels → 1,000 labels
 - 0.6% Error (~SOA)
- SVHN Performance
 - 73,000 labels → 1,000 labels
 - 1.3% Error (~SOA)

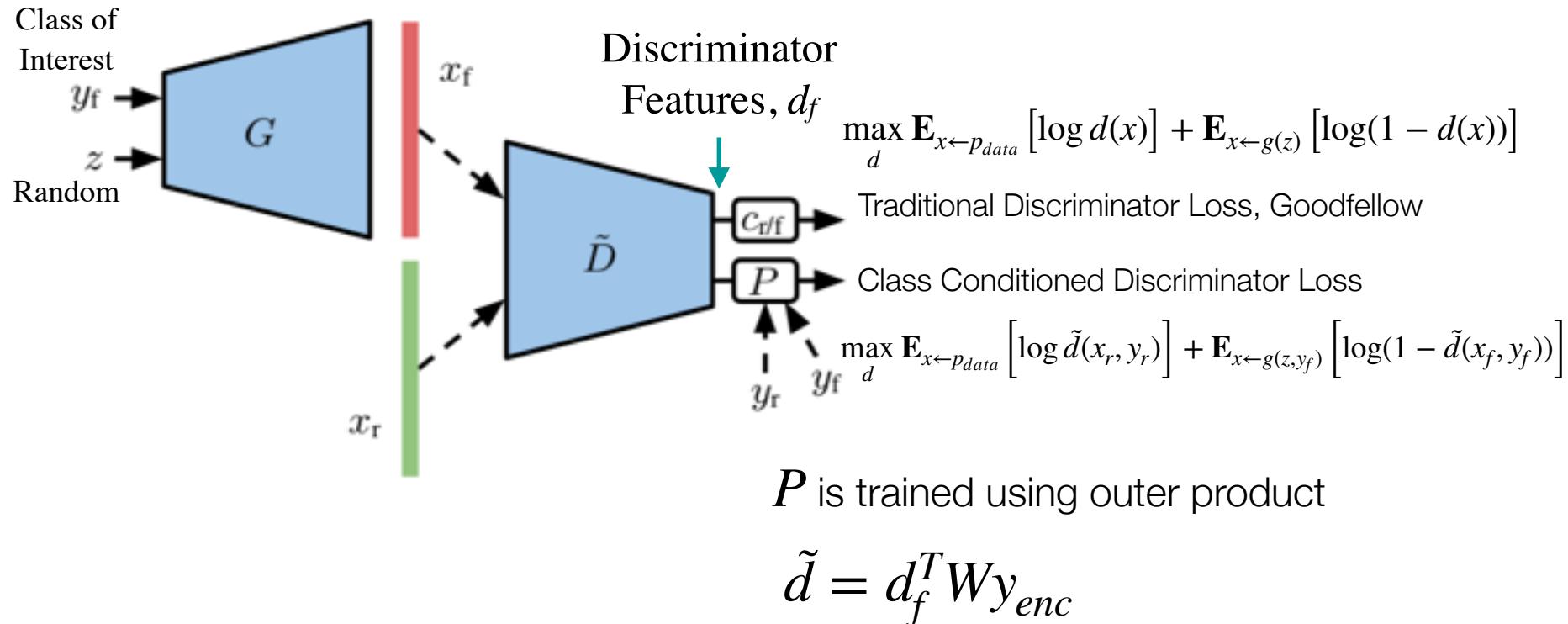
- ImageNet
 - 20% Labels (of 1.3M)
 - 10.3% Top-5 Error (slightly worse than SOA)

Need a slightly more complicated loss function



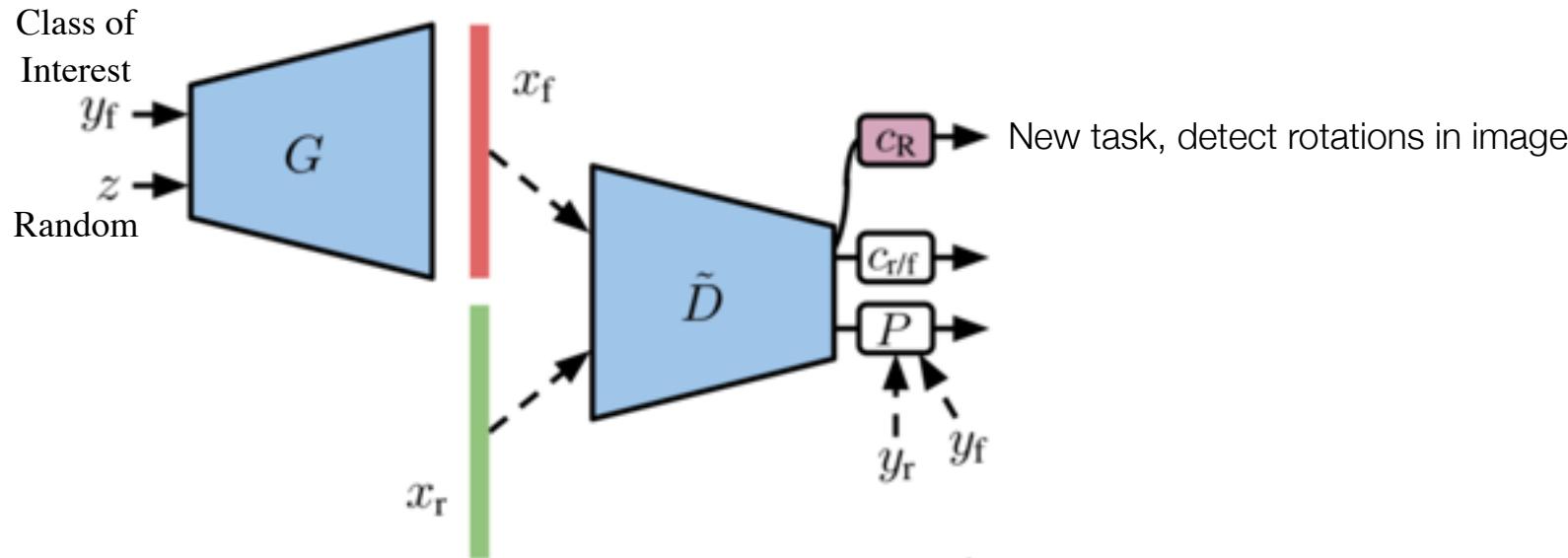
Conditional GANs and Self-Supervision

Lucic, Mario, Michael Tschannen, Marvin Ritter, Xiaohua Zhai, Olivier Bachem, and Sylvain Gelly. "High-Fidelity Image Generation With Fewer Labels." *arXiv preprint arXiv:1903.02271* (2019).



Conditional GANs and Self-Supervision

Lucic, Mario, Michael Tschannen, Marvin Ritter, Xiaohua Zhai, Olivier Bachem, and Sylvain Gelly. "High-Fidelity Image Generation With Fewer Labels." *arXiv preprint arXiv:1903.02271* (2019).



All these equations are saying is that they classify rotations from real and fake images.

and

And... nothing in these equations is meaningful except α, β

$$-\frac{\beta}{|\mathcal{R}|} \sum_{r \in \mathcal{R}} \mathbb{E}_{x \sim p_{\text{data}}(x)} [\log p(c_R(\tilde{D}(x^r) = r)]$$

$$-\frac{\alpha}{|\mathcal{R}|} \mathbb{E}_{(z,y) \sim p(z,y)} [\log p(c_R(\tilde{D}(G(z,y)^r) = r)],$$



Summary

- When we care about the discriminator for classification:
 - More unsupervised tasks helps feature extraction
 - Conditioning on classes with outer product helps
 - Many other attempts have been tried...
 - ◆ But not many work...
 - Open research topic!



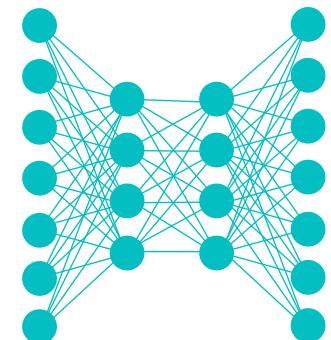


Lecture Notes for **Neural Networks** **and Machine Learning**

Holy GAN-Zooks



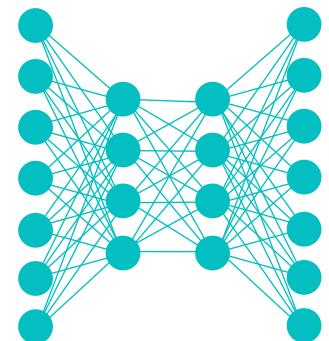
Next Time:
Lapan Ch. 1
Reading: None



Lecture Notes for
Neural Networks
and Machine Learning



Beyond Generation
with GANs



Logistics and Agenda

- Logistics
- Agenda
 - Text to image synthesis
 - BigGAN
 - Adversarial Auto Encoding



Text to Image Synthesis with GANs

Generative Adversarial Text to Image Synthesis

**Scott Reed, Zeynep Akata, Xinchen Yan, Lajanugen Logeswaran
Bernt Schiele, Honglak Lee**

REEDSCOT¹, AKATA², XCYAN¹, LLAJAN¹
SCHIELE², HONGLAK¹

¹ University of Michigan, Ann Arbor, MI, USA (UMICH.EDU)

² Max Planck Institute for Informatics, Saarbrücken, Germany (MPI-INF.MPG.DE)



Correspondence Images/Text Features

- Need a correspondence function for text and image representations:

sampled from text
for class y

$$f_v(v) = \arg \max_{y \in \mathcal{Y}} \mathbb{E}_{t \sim \mathcal{T}(y)} [\phi(v)^T \varphi(t)]$$

sampled from images
for class y

$$f_t(t) = \arg \max_{y \in \mathcal{Y}} \mathbb{E}_{v \sim \mathcal{V}(y)} [\phi(v)^T \varphi(t))]$$

text description * image description

When text and image match, these products should be large, else smaller. Therefore f_v and f_t will learn to make similar text and image features.

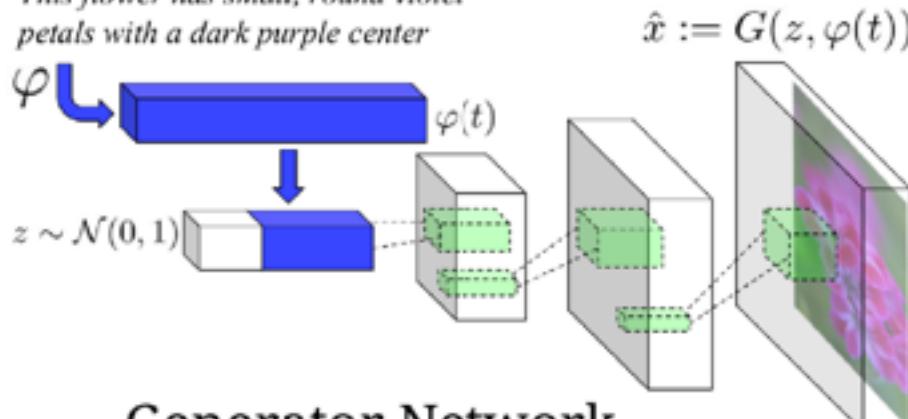
Can also add to loss function by interpolating
text descriptors of the same class

$$\mathbb{E}_{t_1, t_2 \sim p_{data}} [\log(1 - D(G(z, \beta t_1 + (1 - \beta)t_2)))]$$



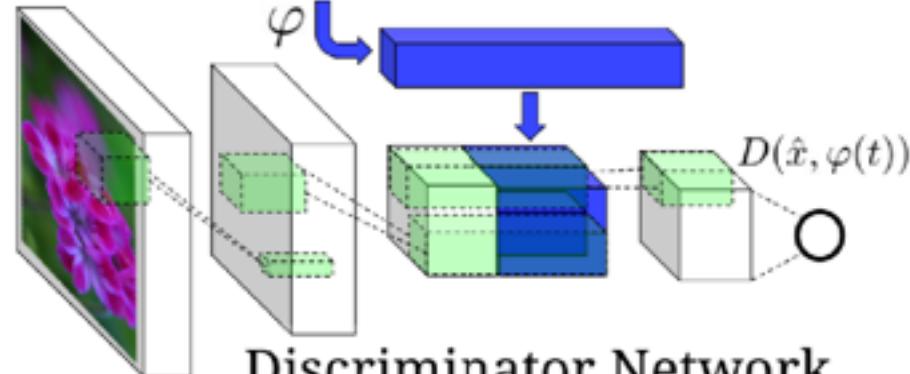
Architecture

This flower has small, round violet petals with a dark purple center



Generator Network

This flower has small, round violet petals with a dark purple center



Discriminator Network

Figure 2. Our text-conditional convolutional GAN architecture. Text encoding $\varphi(t)$ is used by both generator and discriminator. It is projected to a lower-dimensions and depth concatenated with image feature maps for further stages of convolutional processing.

Algorithm 1 GAN-CLS training algorithm with step size α , using minibatch SGD for simplicity.

```
1: Input: minibatch images  $x$ , matching text  $t$ , mis-  
   matching  $\hat{t}$ , number of training batch steps  $S$   
2: for  $n = 1$  to  $S$  do  
3:    $h \leftarrow \varphi(t)$  {Encode matching text description}  
4:    $\hat{h} \leftarrow \varphi(\hat{t})$  {Encode mis-matching text description}  
5:    $z \sim \mathcal{N}(0, 1)^Z$  {Draw sample of random noise}  
6:    $\hat{x} \leftarrow G(z, h)$  {Forward through generator}
```

```
7:    $s_r \leftarrow D(x, h)$  {real image, right text}  
8:    $s_w \leftarrow D(x, \hat{h})$  {real image, wrong text}  
9:    $s_f \leftarrow D(\hat{x}, h)$  {fake image, right text}  
10:   $\mathcal{L}_D \leftarrow \log(s_r) + (\log(1 - s_w) + \log(1 - s_f))/2$   
11:   $D \leftarrow D - \alpha \partial \mathcal{L}_D / \partial D$  {Update discriminator}  
12:   $\mathcal{L}_G \leftarrow \log(s_f)$   
13:   $G \leftarrow G - \alpha \partial \mathcal{L}_G / \partial G$  {Update generator}  
14: end for
```



Results Not Satisfying

- So we need more processing!
- Add attention!

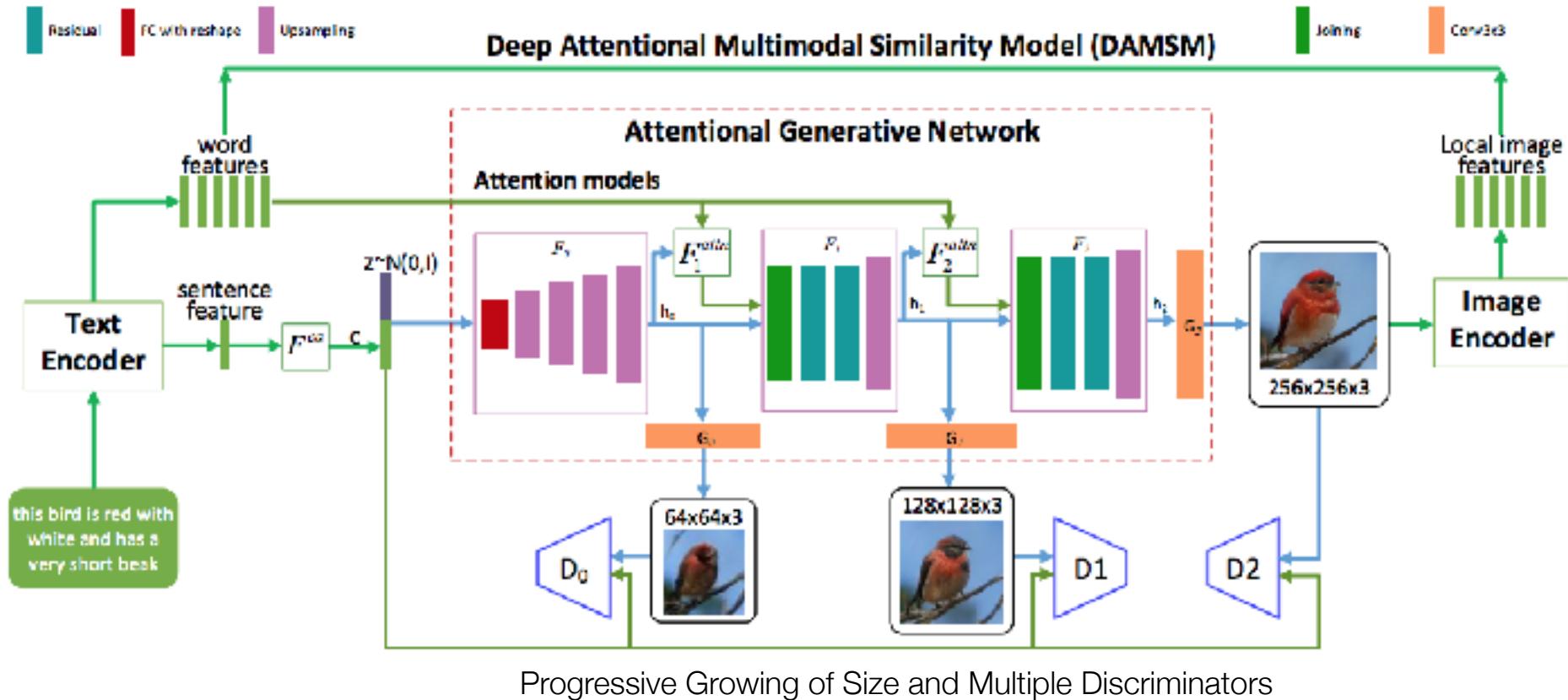
AttnGAN: Fine-Grained Text to Image Generation with Attentional Generative Adversarial Networks

Tao Xu^{*1}, Pengchuan Zhang², Qiuyuan Huang²,
Han Zhang³, Zhe Gan⁴, Xiaolei Huang¹, Xiaodong He²

¹Lehigh University ²Microsoft Research ³Rutgers University ⁴Duke University
{tax313, xih206}@lehigh.edu, {penzhan, qihua, xiaohe}@microsoft.com
han.zhang@cs.rutgers.edu, zhe.gan@duke.edu



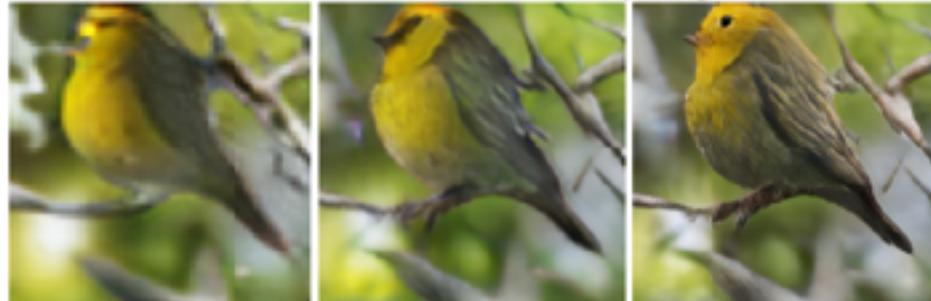
New Process is Similar



Results are very satisfying!



the bird has a yellow crown and a black eyering that is round



this bird has a green crown black primaries and a white belly



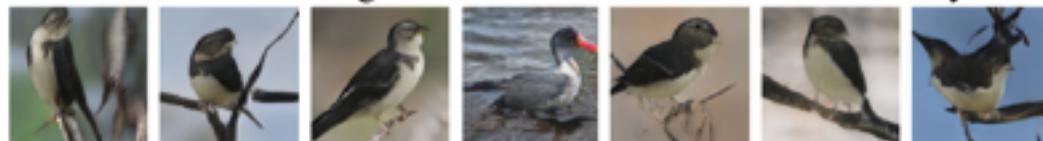
a photo of a homemade swirly pasta with broccoli carrots and onions



a fruit stand display with bananas and kiwi



this bird has wings that are black and has a white belly



this bird has wings that are red and has a yellow belly



this bird has wings that are blue and has a red belly



BigGAN

In a field with 1000's of competing papers,
BigGAN is here to use the most meaningful
Portions of each paper and put them into
One BIG paper.



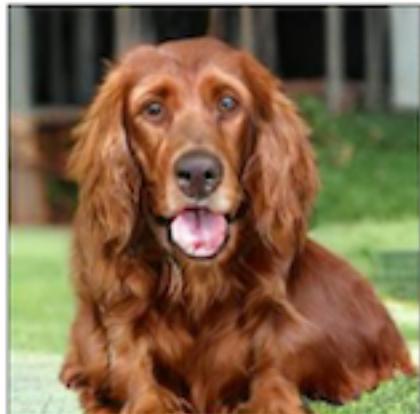
BigGAN

- This is simply an agglomeration of everything we already know about GANs from 2016-2019
 - Training is hard, so use good loss and heuristics
 - large batches, feature matching
 - Scale up progressively, with multiple discriminators at each scale
 - use attention, conditional classes, spectral normalization, moving average of weights, orthogonal weight initialization, skip connections, orthogonal regularizers
 - truncation trick: sample a wide range during training, then truncate for generating results
- [Large Scale GAN Training for High Fidelity Natural Image Synthesis](#), 2018.
 - [Large Scale GAN Training for High Fidelity Natural Image Synthesis, ICLR 2019](#). 2019
 - [Self-Attention Generative Adversarial Networks](#), 2018.
 - [A Learned Representation For Artistic Style](#), 2016.
 - [Spectral Normalization for Generative Adversarial Networks](#), 2018.
 - [Progressive Growing of GANs for Improved Quality, Stability, and Variation](#), 2017.
 - [Exact Solutions To The Nonlinear Dynamics Of Learning In Deep Linear Neural Networks](#), 2013.
 - [Neural Photo Editing with Introspective Adversarial Networks](#), 2016.



BigGAN Results

- Go read that paper!



(a) 128×128

(b) 256×256

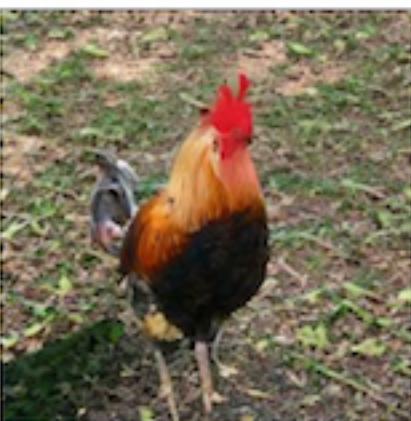
(c) 512×512



BigGAN Results

- Go read that paper!

256 x 256



BigGAN Results

- Go read that paper!

512 x 512



The GAN Takeaways

- Approximation reigns supremum, err maximum
 - But do not be too skeptical
 - ... be skeptical of your skepticism
- Intractable mathematics encourages researchers to find their method works through poor practices
- It's still unclear what loss actually works and how to incentivize different behaviors, but we are getting better



François Chollet  @fchollet · 23h
We will soon have a large enough dataset of pairs of Disney animated movies + matching photorealistic CG renderings that we will be able to train an end-to-end deep learning model to do the conversion automatically.



Disney  @Disney · 1d

In 100 days, the king arrives. Watch the brand new trailer for #TheLionKing now.



7

40

225



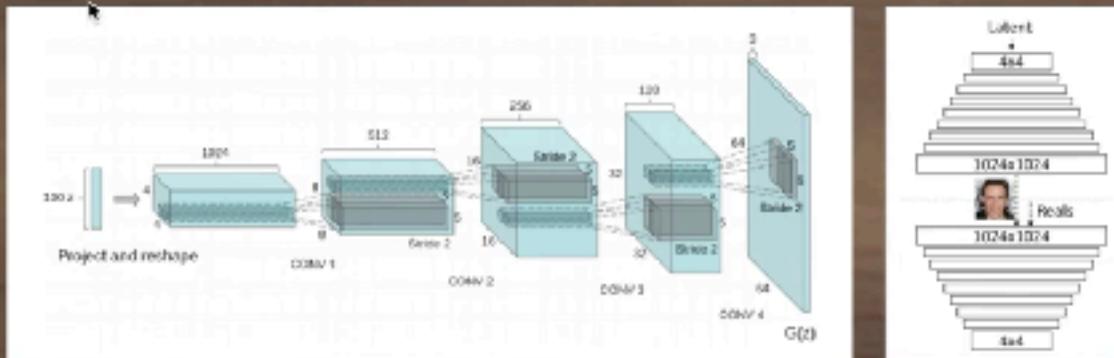
François Chollet  @fchollet · 23h
Usual disclaimer: this is a tongue in cheek joke. Stop taking it literally 😊



A Quick Summary

Press **esc** to exit full screen

Must-Read Papers on GANs



www.henryailabs.com

<https://towardsdatascience.com/must-read-papers-on-gans-b665bbae3317>



Generative Teaching Networks

- Insert Explanation here for future semesters
- Released December 2019
- <https://eng.uber.com/generative-teaching-networks/>



Adversarial Auto Encoding



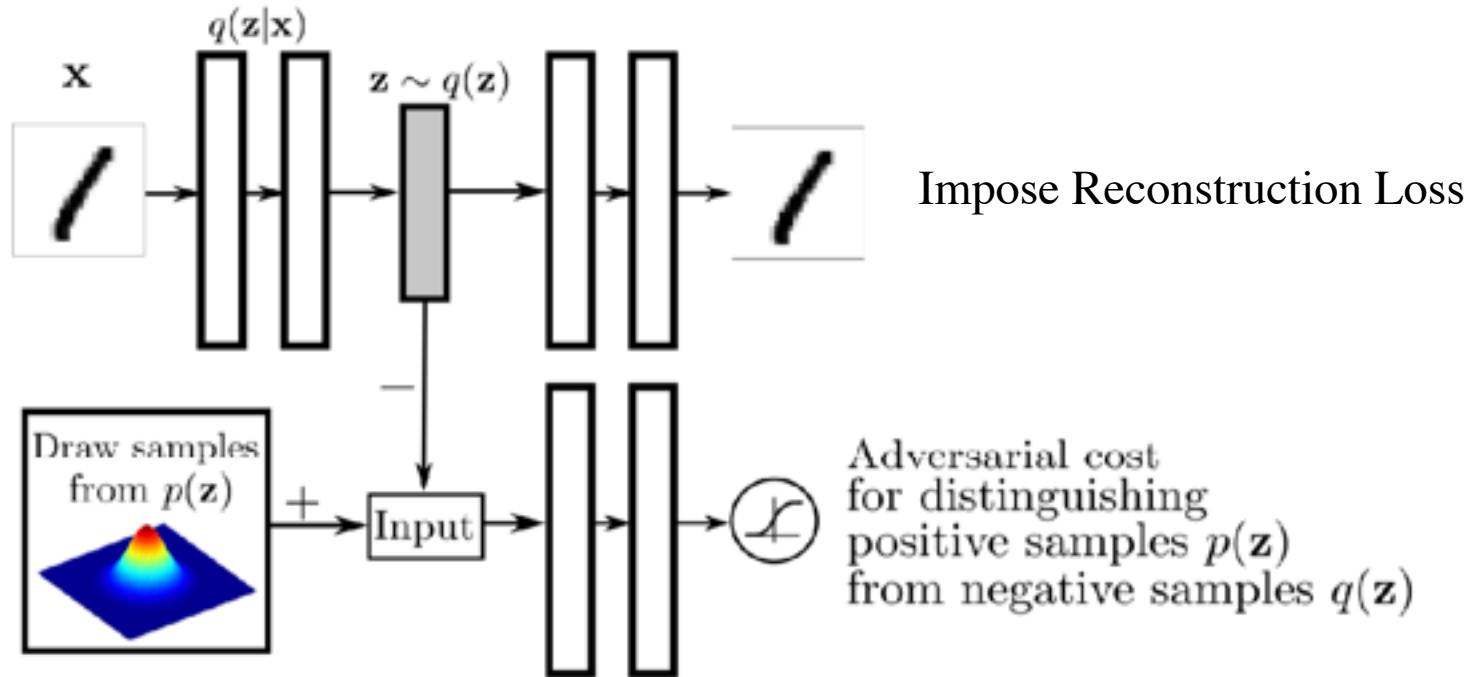
Do we need something more than VAE?

- Arguments for Yes:
 - ELBO is flawed!
 - Assumption of Normal distributions to $q(z)$ is limiting
 - Training tends to be slow
 - Manifold of distributions do not cover the latent space completely
 - We can't incorporate distributions separately for different classes without reformulating loss function
- Arguments for No:
 - It seems hard, how can we research methods that aren't low hanging fruit? Plus the VAE math was like really hard for me to understand so this is not going to be very fun, guaranteed. Ah, fine lets look at it.



The Main Idea

- How can we enforce constraints on the latent space with GANs?

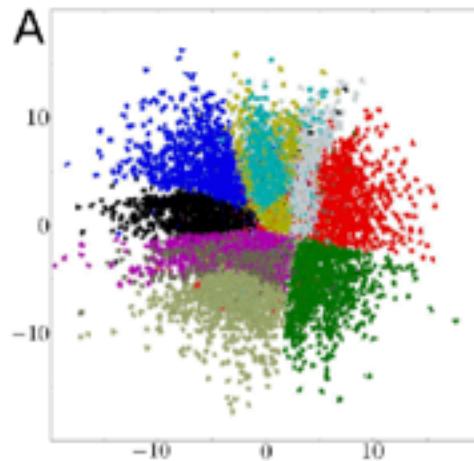


Makhzani, Alireza, Jonathon Shlens, Navdeep Jaitly, Ian Goodfellow, and Brendan Frey. "Adversarial autoencoders." *arXiv preprint arXiv:1511.05644* (2015).

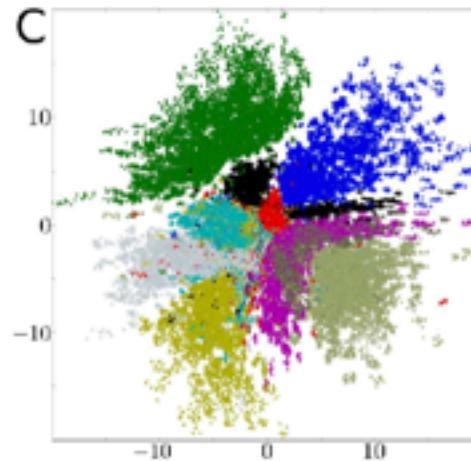


Arbitrary Prior Distributions

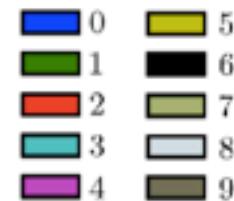
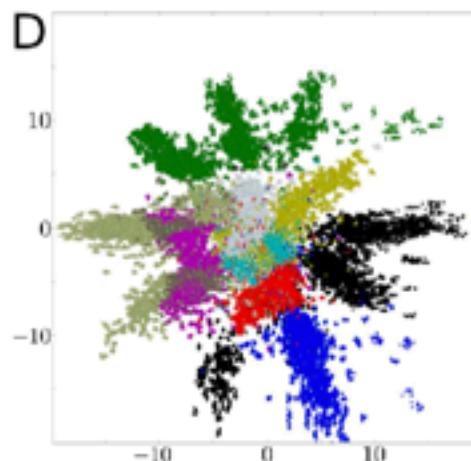
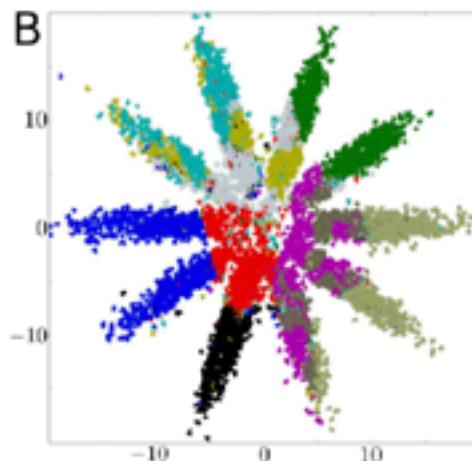
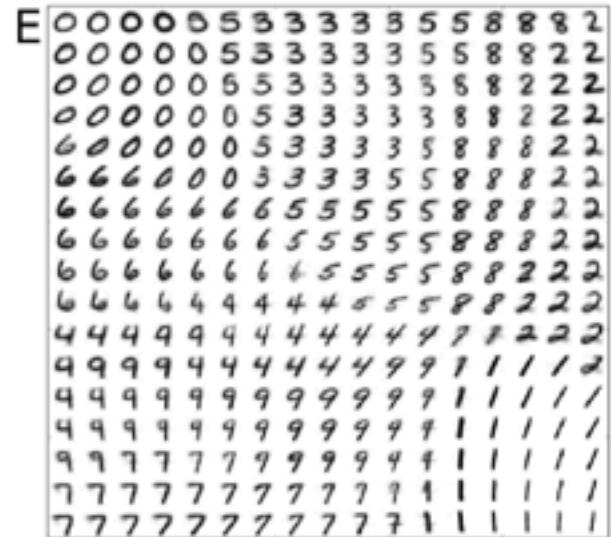
Adversarial Autoencoder



Variational Autoencoder



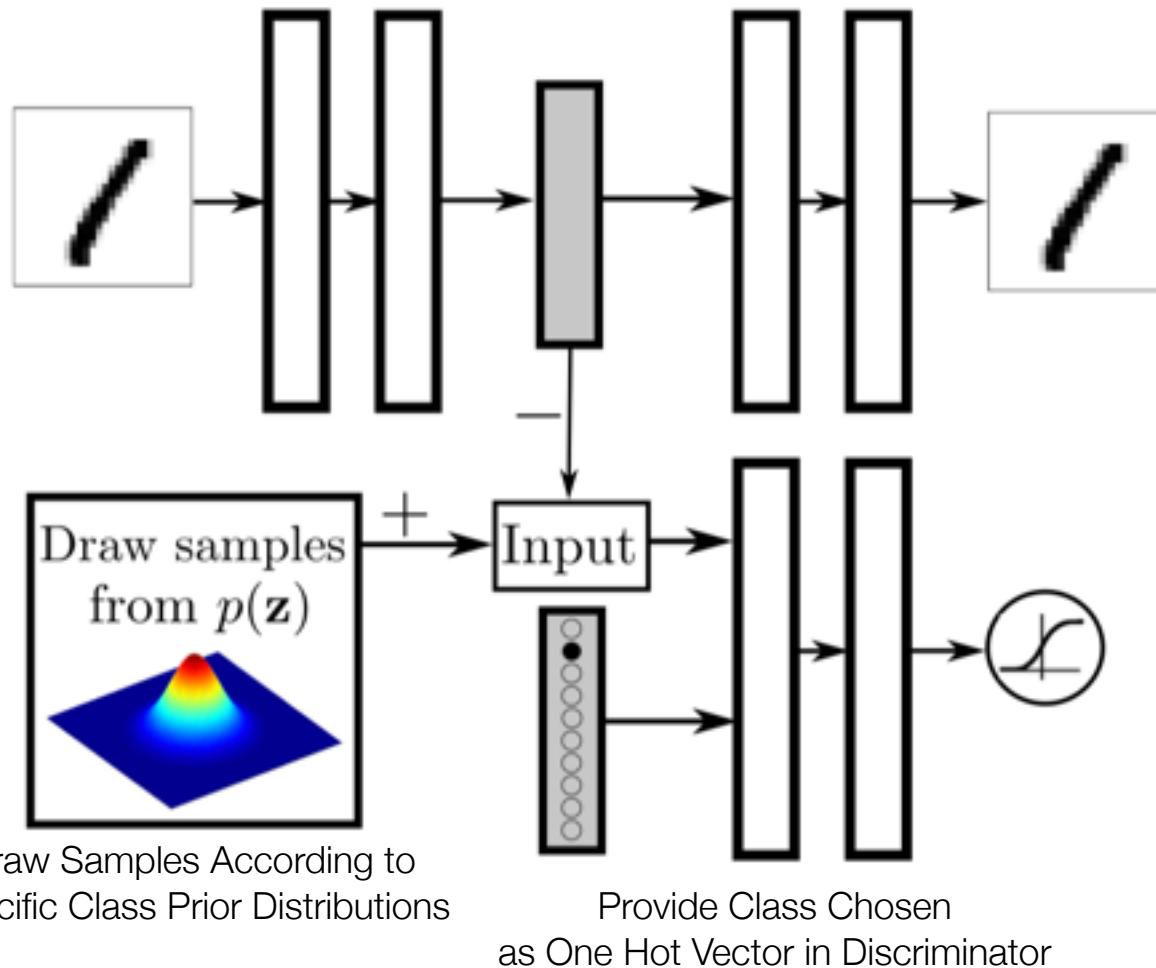
Manifold of
Adversarial Autoencoder



Makhzani, Alireza, Jonathon Shlens, Navdeep Jaitly, Ian Goodfellow, and Brendan Frey. "Adversarial autoencoders." *arXiv preprint arXiv:1511.05644* (2015).



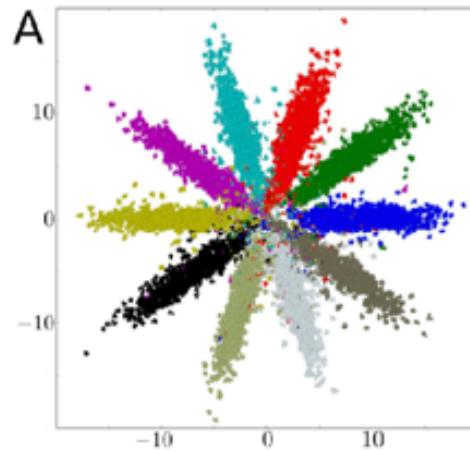
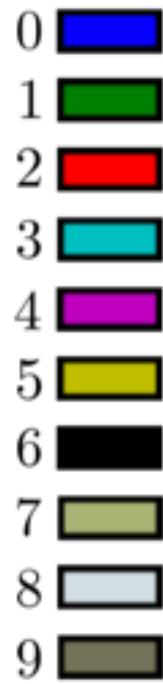
Sampling From Classes



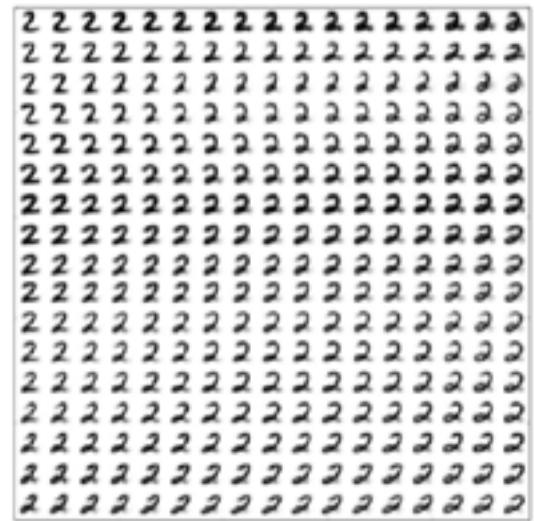
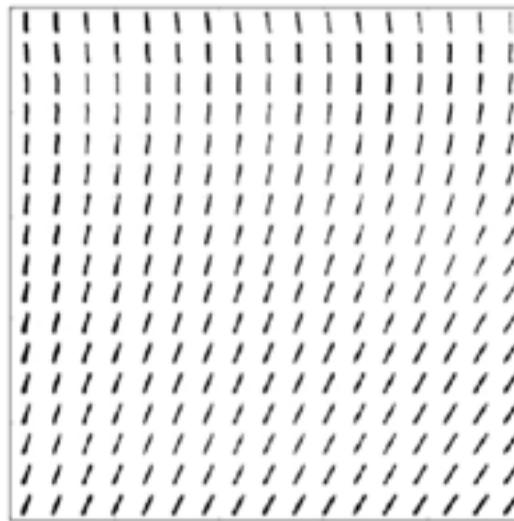
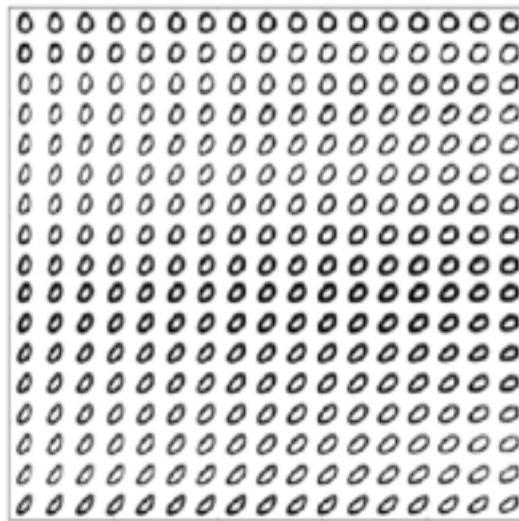
Makhzani, Alireza, Jonathon Shlens, Navdeep Jaitly, Ian Goodfellow, and Brendan Frey. "Adversarial autoencoders." *arXiv preprint arXiv:1511.05644* (2015).



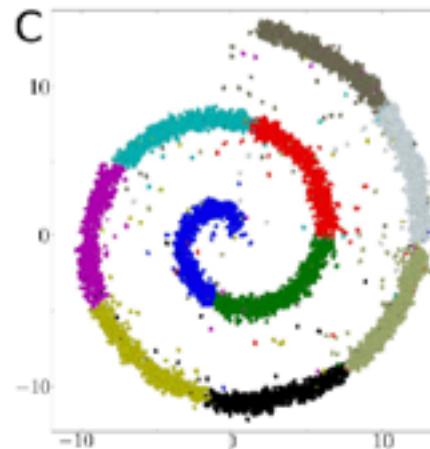
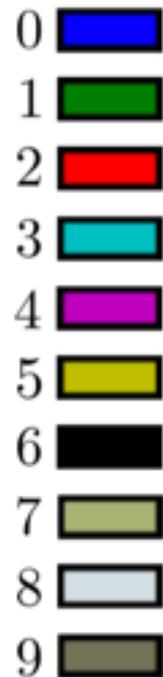
Conditional Class Latent Spaces



Sample Along Main Axis of the Gaussian Component for Each Digit



Conditional Class Latent Spaces



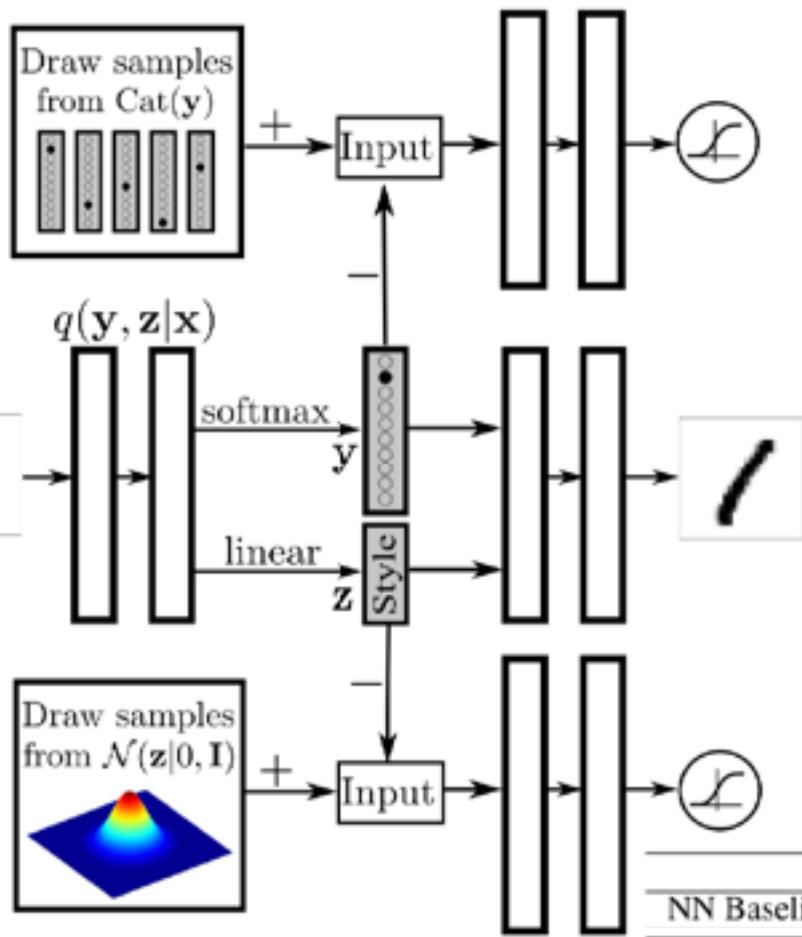
Sample Along Swiss Roll Axis



Makhzani, Alireza, Jonathon Shlens, Navdeep Jaitly, Ian Goodfellow, and Brendan Frey. "Adversarial autoencoders." *arXiv preprint arXiv:1511.05644* (2015).83



Semi-Supervised Classification



- Top Discriminator
 - Draw samples from one hot encoded labels
 - Ensures aggregated posterior matches class distributions
- Bottom Discriminator
 - Same as previous
 - Constrains latent representation
- Supervised Training
 - After GAN training:
 - Use small mini-batches on $q(y|z)$

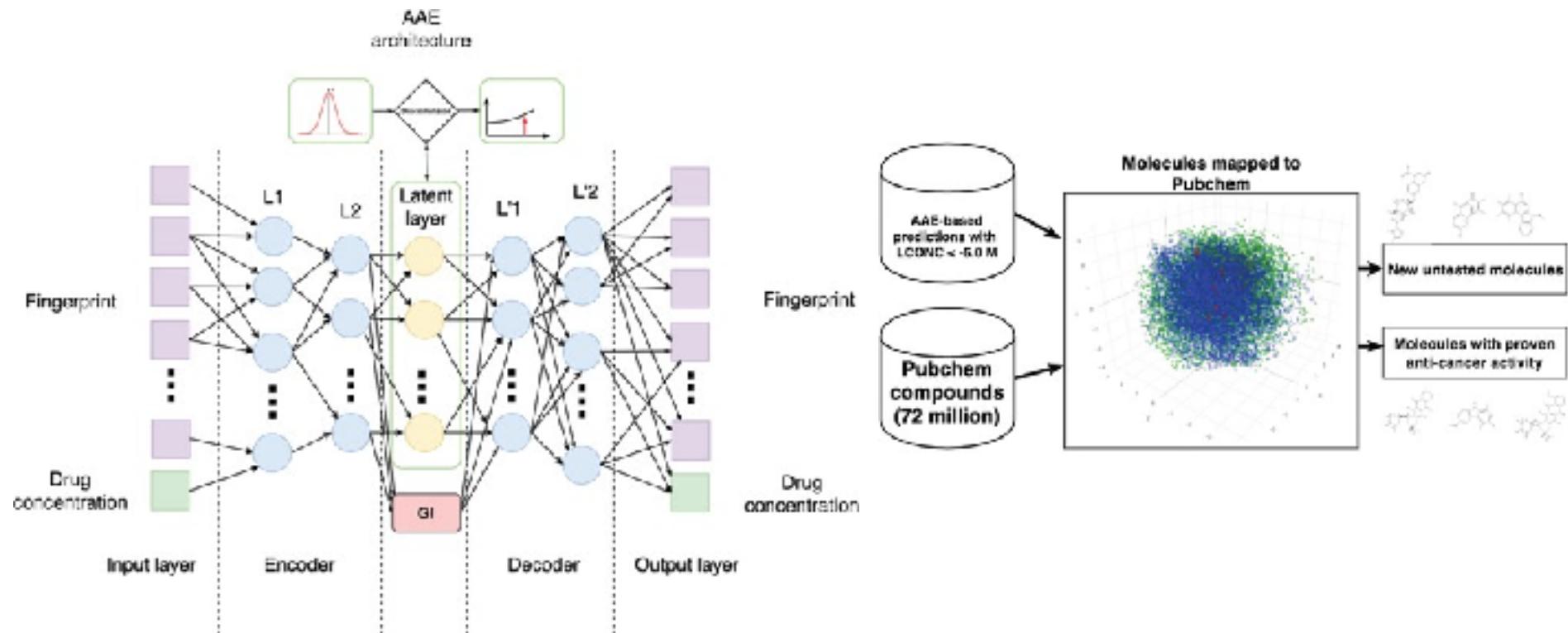
	MNIST (100)	MNIST (1000)	MNIST (All)
NN Baseline	25.80	8.73	1.25
Adversarial Autoencoders	1.90 (± 0.10)	1.60 (± 0.08)	0.85 (± 0.02)

Makhzani, Alireza, Jonathon Shlens, Navdeep Jaitly, Ian Goodfellow, and Brendan Frey. "Adversarial autoencoders." *arXiv preprint arXiv:1511.05644* (2015).84



Other Uses For AAE

- Molecular Fingerprinting



Kadurin, Artur, Alexander Aliper, Andrey Kazennov, Polina Mamoshina, Quentin Vanhaelen, Kuzma Khrabrov, and Alex Zhavoronkov. "The cornucopia of meaningful leads: Applying deep adversarial autoencoders for new molecule development in oncology." *Oncotarget* 8, no. 7 (2017): 10883.



Other Uses For AAE

- Chaos

The Newest AI-Enabled Weapon: 'Deep-Faking' Photos of the Earth

Step 1: Use AI to make undetectable changes to outdoor photos. Step 2: release them into the open-source world and enjoy the chaos.

Patrick Tucker • March 29, 2019



A Quick Aside

Meet the University Ph.D. Fellows

[Funding](#) / [Ph.D. Fellows](#) / Xinyi Ding

Xinyi Ding

Ph.D., Computer Science

Hometown: China

What is your research area?

Ubiquitous Computing, Mobile Health

What is something cool about your field?

We use mobile devices to sensor medical quantity out of clinic and build much cheaper alternatives that could change peoples' lives.

What is the best thing you've done as a graduate student at SMU so far?

We are developing an ios app that uses computer vision technologies to detect human emotions. How exciting it is if your smart phone could read your emotions!

What is your favorite thing to do in Dallas?

I enjoy the weather here.

What do you wish you'd known before starting graduate school?

Read as many papers as you can about your intended research field.

What is your favorite leisure activity?

Watching movies and playing basketball.



Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?

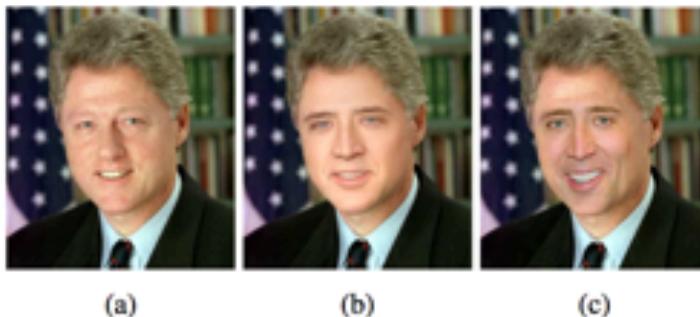


Figure 1: (a) The input image. (b) The result of face swapping with Nicolas Cage using our method. (c) The result of a manual face swap (source: <http://niccageaseeveryone.blogspot.com>).

By Robert Chesney, Danielle Citron · Wednesday, February 21, 2018, 10:00 AM

Bobby Chesney is the Charles E. Francis Professor in Law and Associate Dean for Academic Affairs at the University of Texas School of Law. He also serves as the Director of UT-Austin's interdisciplinary research center the Robert S. Strauss Center for International Security and Law. His scholarship encompasses a wide range of issues relating to national security and the law, including detention, targeting, prosecution, covert action, and the state secrets privilege; most of it is posted here. Along with Ben Wittes and Jack Goldsmith, he is one of the co-founders of the blog.

[@RobertChesney](#)

Danielle Citron is the Morton & Sophia Macht Professor of Law at the University of Maryland-Carey School of Law. She is the author of *Hate Crimes in Cyberspace* (Harvard University Press 2014).

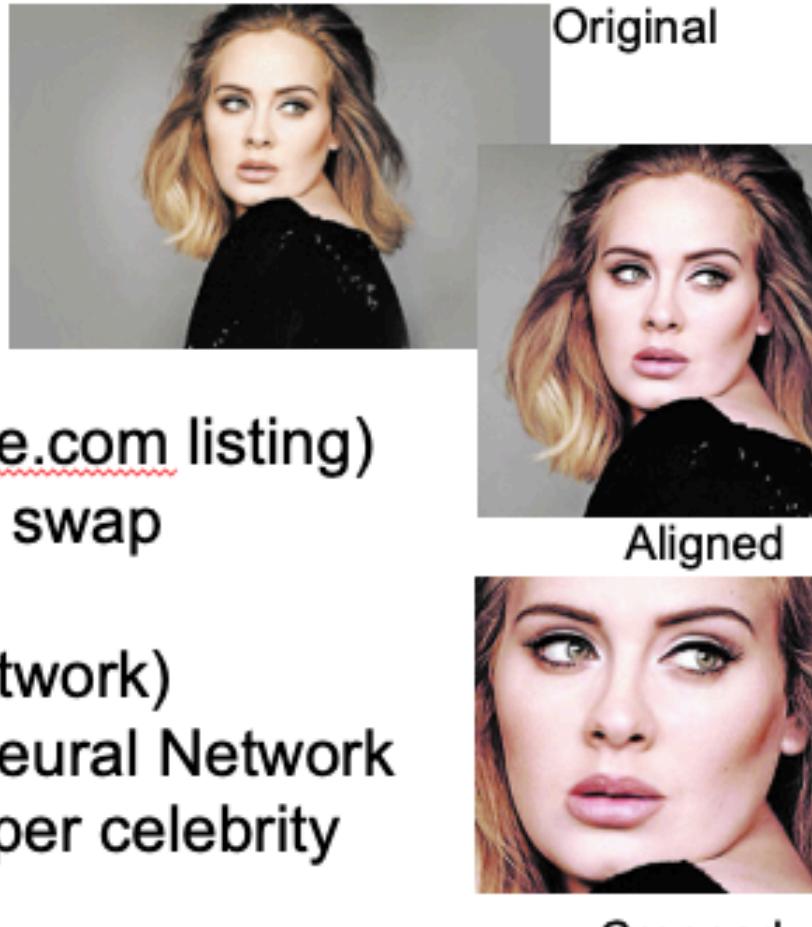
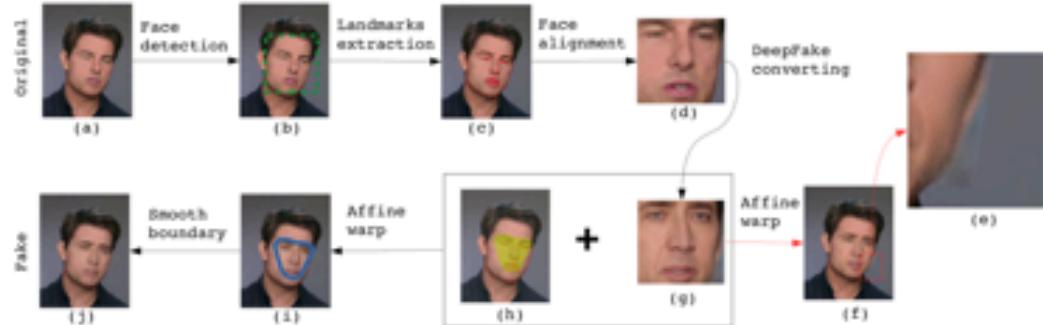
[MORE ARTICLES >](#)

Privacy Paradox: Rethinking Solitude

"As deepfake technology becomes more advanced and more accessible, it could pose a threat to United States public discourse and national security, with broad and concerning implications for offensive active measured campaigns targeting the United States."

"US lawmakers say AI Deepfakes have the potential to disrupt every facet of our society." US Congressional Letter





- 50 different celebrities (from [People.com](#) listing)
- Selected celebrity pairs of faces to swap
- Swapped Faces via:
 - Auto-Encoding (Adversarial Network)
 - Pipelining with Convolutional Neural Network
- 1000 – 3000 fake images created per celebrity pair
- 400,000 images for training and evaluation



Training Phase

Person A

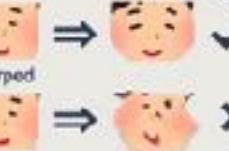


Real
face A



Warped
face A

Encoder



Decoder
A

Segmentation
mask



Masked
face A



Reconstructed
face A



Test Phase

Person B



Real
face B

Encoder

Decoder
A



Result: face B
(face A look-alike)





Rating Swapped Images

 **SMU. FaceFace** VOTE

Which of the following two faces looks
MORE FAKE to you?



faceface.lyle.smu.edu

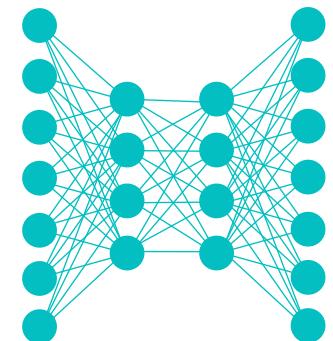
- Selected subset of 400 images to rate
- Used paired selection algorithm on website to choose most “needed” image comparison
- Collected **40,000 ratings** from ~200 unique individuals
- **Result:** Sorting of images from most fake to most real

Lecture Notes for **Neural Networks** **and Machine Learning**

Practical GANs



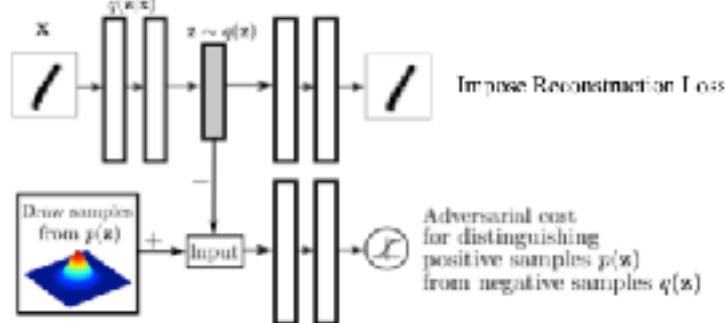
Next Time:
GAN Examples
Reading: Chollet CH8



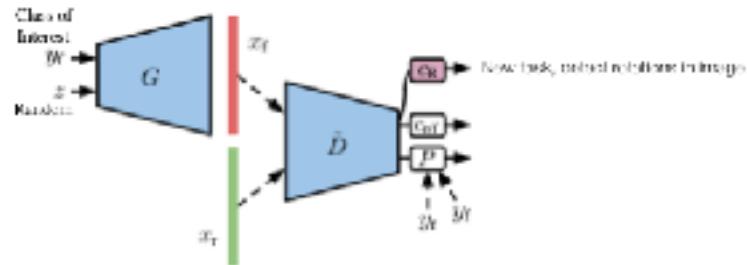


Last Time

- How can we enforce constraints on the latent space with GANs?



From: Makhzani, A., Shlens, J., Jaitly, N., Dean, J., & Ng, A.Y. (2015). Adversarial Autoencoders. arXiv preprint arXiv:1511.05644.

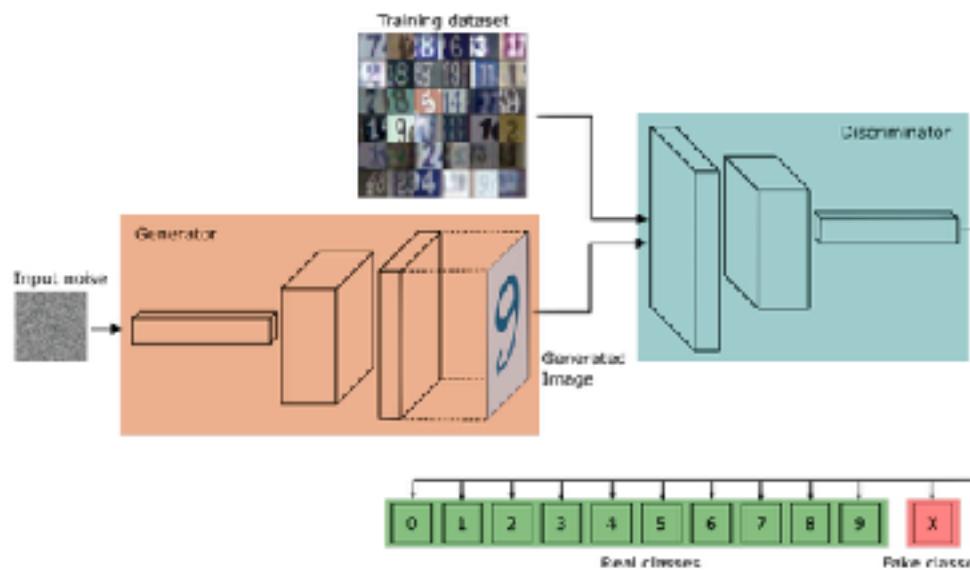


All these equations are saying is that they classify real vs fake images.

$$-\frac{\beta}{|\mathcal{R}|} \sum_{r \in \mathcal{R}} \mathbb{E}_{x \sim p_{real}(x)} [\log p(\phi_{\hat{D}}(\hat{D}(x^r)) = r)]$$

And... nothing in these equations is meaningful except α, β

$$-\frac{\alpha}{|\mathcal{R}|} \mathbb{E}_{(z,y) \sim g(z,y)} [\log p(\phi_{\hat{D}}(G(z,y)) = r)]$$





Backup slides



Title Between Topics



Example Slide





Title

Subtitle

Follow Along: Notebook Name

99

