## Generative Adversarial Networks

March 8, 2023

```
[1]: # This mounts your Google Drive to the Colab VM.
     from google.colab import drive
     drive.mount('/content/drive')
     # TODO: Enter the foldername in your Drive where you have saved the unzipped
     # assignment folder, e.g. 'cs231n/assignments/assignment3/'
     FOLDERNAME = 'cs231n/assignments/assignment3/'
     assert FOLDERNAME is not None, "[!] Enter the foldername."
     # Now that we've mounted your Drive, this ensures that
     # the Python interpreter of the Colab VM can load
     # python files from within it.
     import sys
     sys.path.append('/content/drive/My Drive/{}'.format(FOLDERNAME))
     # This downloads the COCO dataset to your Drive
     # if it doesn't already exist.
     %cd /content/drive/My\ Drive/$FOLDERNAME/cs231n/datasets/
     !bash get_datasets.sh
     %cd /content/drive/My\ Drive/$FOLDERNAME
```

Mounted at /content/drive /content/drive/My Drive/cs231n/assignments/assignment3/cs231n/datasets /content/drive/My Drive/cs231n/assignments/assignment3

### 0.1 Using GPU

Go to Runtime > Change runtime type and set Hardware accelerator to GPU. This will reset Colab. Rerun the top cell to mount your Drive again.

# 1 Generative Adversarial Networks (GANs)

So far in CS 231N, all the applications of neural networks that we have explored have been discriminative models that take an input and are trained to produce a labeled output. This has ranged from straightforward classification of image categories to sentence generation (which was still phrased as a classification problem, our labels were in vocabulary space and we had learned a recurrence to capture multi-word labels). In this notebook, we will expand our repetoire, and build

**generative models** using neural networks. Specifically, we will learn how to build models which generate novel images that resemble a set of training images.

#### 1.0.1 What is a GAN?

In 2014, Goodfellow et al. presented a method for training generative models called Generative Adversarial Networks (GANs for short). In a GAN, we build two different neural networks. Our first network is a traditional classification network, called the **discriminator**. We will train the discriminator to take images and classify them as being real (belonging to the training set) or fake (not present in the training set). Our other network, called the **generator**, will take random noise as input and transform it using a neural network to produce images. The goal of the generator is to fool the discriminator into thinking the images it produced are real.

We can think of this back and forth process of the generator (G) trying to fool the discriminator (D) and the discriminator trying to correctly classify real vs. fake as a minimax game:

$$\underset{G}{\text{minimize maximize}} \; \mathbb{E}_{x \sim p_{\text{data}}} \left[ \log D(x) \right] + \mathbb{E}_{z \sim p(z)} \left[ \log \left( 1 - D(G(z)) \right) \right]$$

where  $z \sim p(z)$  are the random noise samples, G(z) are the generated images using the neural network generator G, and D is the output of the discriminator, specifying the probability of an input being real. In Goodfellow et al., they analyze this minimax game and show how it relates to minimizing the Jensen-Shannon divergence between the training data distribution and the generated samples from G.

To optimize this minimax game, we will alternate between taking gradient descent steps on the objective for G and gradient ascent steps on the objective for D: 1. update the **generator** (G) to minimize the probability of the **discriminator making the correct choice**. 2. update the **discriminator** (D) to maximize the probability of the **discriminator making the correct choice**.

While these updates are useful for analysis, they do not perform well in practice. Instead, we will use a different objective when we update the generator: maximize the probability of the **discriminator** making the incorrect choice. This small change helps to allevaiate problems with the generator gradient vanishing when the discriminator is confident. This is the standard update used in most GAN papers and was used in the original paper from Goodfellow et al..

In this assignment, we will alternate the following updates: 1. Update the generator (G) to maximize the probability of the discriminator making the incorrect choice on generated data:

$$\underset{G}{\operatorname{maximize}} \; \mathbb{E}_{z \sim p(z)} \left[ \log D(G(z)) \right]$$

2. Update the discriminator (D), to maximize the probability of the discriminator making the correct choice on real and generated data:

$$\underset{D}{\text{maximize}} \; \mathbb{E}_{x \sim p_{\text{data}}} \left[ \log D(x) \right] + \mathbb{E}_{z \sim p(z)} \left[ \log \left( 1 - D(G(z)) \right) \right]$$

Here's an example of what your outputs from the 3 different models you're going to train should look like. Note that GANs are sometimes finicky, so your outputs might not look exactly like this. This is just meant to be a *rough* guideline of the kind of quality you can expect:

```
[3]: # Run this cell to see sample outputs.
from IPython.display import Image
Image('images/gan_outputs_pytorch.png')
```

Vanilla GAN LS-GAN DC-GAN

O 2 2 9 7 0 4 0 0 3 8 3

9 9 9 5 9

0 2 6 7 9 9 5 9

```
[2]: # Setup cell.
     import numpy as np
     import torch
     import torch.nn as nn
     from torch.nn import init
     import torchvision
     import torchvision.transforms as T
     import torch.optim as optim
     from torch.utils.data import DataLoader
     from torch.utils.data import sampler
     import torchvision.datasets as dset
     import matplotlib.pyplot as plt
     import matplotlib.gridspec as gridspec
     from cs231n.gan_pytorch import preprocess_img, deprocess_img, rel_error, u
      →count_params, ChunkSampler
     %matplotlib inline
     plt.rcParams['figure.figsize'] = (10.0, 8.0) # Set default size of plots.
     plt.rcParams['image.interpolation'] = 'nearest'
     plt.rcParams['image.cmap'] = 'gray'
     %load_ext autoreload
     %autoreload 2
     def show_images(images):
         images = np.reshape(images, [images.shape[0], -1]) # Images reshape to__
      \hookrightarrow (batch_size, D).
         sqrtn = int(np.ceil(np.sqrt(images.shape[0])))
```

```
sqrtimg = int(np.ceil(np.sqrt(images.shape[1])))

fig = plt.figure(figsize=(sqrtn, sqrtn))
gs = gridspec.GridSpec(sqrtn, sqrtn)
gs.update(wspace=0.05, hspace=0.05)

for i, img in enumerate(images):
    ax = plt.subplot(gs[i])
    plt.axis('off')
    ax.set_xticklabels([])
    ax.set_yticklabels([])
    ax.set_aspect('equal')
    plt.imshow(img.reshape([sqrtimg,sqrtimg]))
    return

answers = dict(np.load('gan-checks.npz'))
dtype = torch.cuda.FloatTensor if torch.cuda.is_available() else torch.

GFloatTensor
```

#### 1.1 Dataset

GANs are notoriously finicky with hyperparameters, and also require many training epochs. In order to make this assignment approachable, we will be working on the MNIST dataset, which is 60,000 training and 10,000 test images. Each picture contains a centered image of white digit on black background (0 through 9). This was one of the first datasets used to train convolutional neural networks and it is fairly easy – a standard CNN model can easily exceed 99% accuracy.

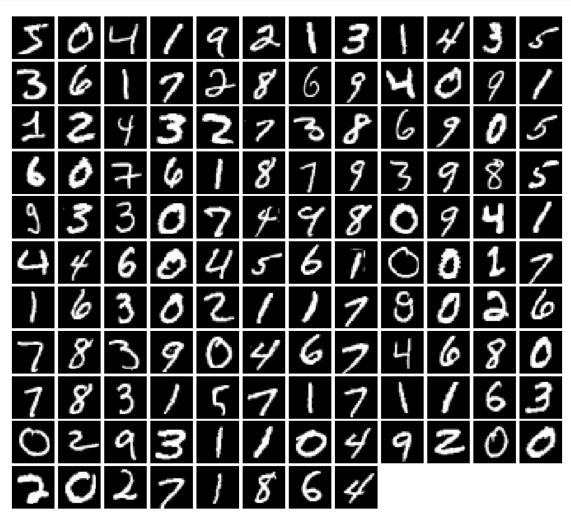
To simplify our code here, we will use the PyTorch MNIST wrapper, which downloads and loads the MNIST dataset. See the documentation for more information about the interface. The default parameters will take 5,000 of the training examples and place them into a validation dataset. The data will be saved into a folder called MNIST\_data.

```
[4]: NUM_TRAIN = 50000
NUM_VAL = 5000

NOISE_DIM = 96
batch_size = 128

mnist_train = dset.MNIST(
    './cs231n/datasets/MNIST_data',
    train=True,
    download=True,
    transform=T.ToTensor()
)
loader_train = DataLoader(
    mnist_train,
    batch_size=batch_size,
    sampler=ChunkSampler(NUM_TRAIN, 0)
```

```
mnist_val = dset.MNIST(
    './cs231n/datasets/MNIST_data',
    train=True,
    download=True,
    transform=T.ToTensor()
)
loader_val = DataLoader(
    mnist_val,
    batch_size=batch_size,
    sampler=ChunkSampler(NUM_VAL, NUM_TRAIN)
)
imgs = next(loader_train.__iter__())[0].view(batch_size, 784).numpy().squeeze()
show_images(imgs)
```



#### 1.2 Random Noise

Generate uniform noise from -1 to 1 with shape [batch\_size, dim].

Implement sample\_noise in cs231n/gan\_pytorch.py.

Hint: use torch.rand.

Make sure noise is the correct shape and type:

```
[11]: from cs231n.gan_pytorch import sample_noise

def test_sample_noise():
    batch_size = 3
    dim = 4
    torch.manual_seed(231)
    z = sample_noise(batch_size, dim)
    np_z = z.cpu().numpy()
    assert np_z.shape == (batch_size, dim)
    assert torch.is_tensor(z)
    assert np.all(np_z >= -1.0) and np.all(np_z <= 1.0)
    assert np.any(np_z < 0.0) and np.any(np_z > 0.0)
    print('All tests passed!')

test_sample_noise()
```

All tests passed!

### 1.3 Flatten

Recall our Flatten operation from previous notebooks... this time we also provide an Unflatten, which you might want to use when implementing the convolutional generator. We also provide a weight initializer (and call it for you) that uses Xavier initialization instead of PyTorch's uniform default.

```
[10]: from cs231n.gan_pytorch import Flatten, Unflatten, initialize_weights
```

### 2 Discriminator

Our first step is to build a discriminator. Fill in the architecture as part of the nn.Sequential constructor in the function below. All fully connected layers should include bias terms. The architecture is: \*Fully connected layer with input size 784 and output size 256 \* LeakyReLU with alpha 0.01 \* Fully connected layer with input\_size 256 and output size 256 \* LeakyReLU with alpha 0.01 \* Fully connected layer with input size 256 and output size 1

Recall that the Leaky ReLU nonlinearity computes  $f(x) = \max(\alpha x, x)$  for some fixed constant  $\alpha$ ; for the LeakyReLU nonlinearities in the architecture above we set  $\alpha = 0.01$ .

The output of the discriminator should have shape [batch\_size, 1], and contain real numbers corresponding to the scores that each of the batch\_size inputs is a real image.

Implement discriminator in cs231n/gan\_pytorch.py

Test to make sure the number of parameters in the discriminator is correct:

Correct number of parameters in discriminator.

### 3 Generator

Now to build the generator network: \* Fully connected layer from noise\_dim to 1024 \* ReLU \* Fully connected layer with size 1024 \* ReLU \* Fully connected layer with size 784 \* TanH (to clip the image to be in the range of [-1,1])

Implement generator in cs231n/gan\_pytorch.py

Test to make sure the number of parameters in the generator is correct:

Correct number of parameters in generator.

### 4 GAN Loss

Compute the generator and discriminator loss. The generator loss is:

$$\ell_G = -\mathbb{E}_{z \sim p(z)} \left[ \log D(G(z)) \right]$$

and the discriminator loss is:

$$\ell_D = -\mathbb{E}_{x \sim p_{\text{data}}} \left[ \log D(x) \right] - \mathbb{E}_{z \sim p(z)} \left[ \log \left( 1 - D(G(z)) \right) \right]$$

Note that these are negated from the equations presented earlier as we will be *minimizing* these losses.

**HINTS**: You should use the bce\_loss function defined below to compute the binary cross entropy loss which is needed to compute the log probability of the true label given the logits output from the discriminator. Given a score  $s \in \mathbb{R}$  and a label  $y \in \{0,1\}$ , the binary cross entropy loss is

$$bce(s, y) = -y * \log(s) - (1 - y) * \log(1 - s)$$

A naive implementation of this formula can be numerically unstable, so we have provided a numerically stable implementation that relies on PyTorch's nn.BCEWithLogitsLoss.

You will also need to compute labels corresponding to real or fake and use the logit arguments to determine their size. Make sure you cast these labels to the correct data type using the global dtype variable, for example:

```
true_labels = torch.ones(size).type(dtype)
```

Instead of computing the expectation of  $\log D(G(z))$ ,  $\log D(x)$  and  $\log (1 - D(G(z)))$ , we will be averaging over elements of the minibatch. This is taken care of in bce\_loss which combines the loss by averaging.

Implement discriminator\_loss and generator\_loss in cs231n/gan\_pytorch.py

Test your generator and discriminator loss. You should see errors < 1e-7.

Maximum error in d\_loss: 2.83811e-08

```
[22]: def test_generator_loss(logits_fake, g_loss_true):
        g_loss = generator_loss(torch.Tensor(logits_fake).type(dtype)).cpu().numpy()
        print("Maximum error in g_loss: %g"%rel_error(g_loss_true, g_loss))

test_generator_loss(
```

```
answers['logits_fake'],
answers['g_loss_true']
)
```

Maximum error in g\_loss: 4.4518e-09

### 5 Optimizing our Loss

Make a function that returns an optim.Adam optimizer for the given model with a 1e-3 learning rate, beta1=0.5, beta2=0.999. You'll use this to construct optimizers for the generators and discriminators for the rest of the notebook.

Implement get\_optimizer in cs231n/gan\_pytorch.py

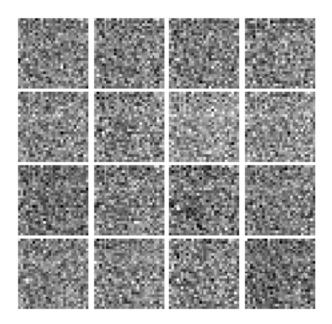
## 6 Training a GAN!

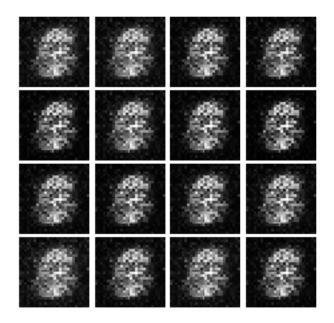
We provide you the main training loop. You won't need to change run\_a\_gan in cs231n/gan\_pytorch.py, but we encourage you to read through it for your own understanding.

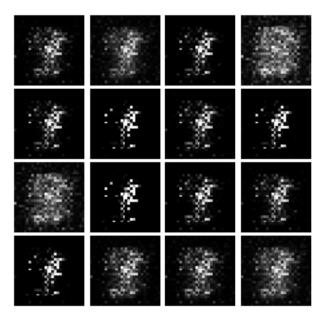
```
[15]: from cs231n.gan_pytorch import get_optimizer, run_a_gan
      # Make the discriminator
      D = discriminator().type(dtype)
      # Make the generator
      G = generator().type(dtype)
      # Use the function you wrote earlier to get optimizers for the Discriminator
       ⇔and the Generator
      D_solver = get_optimizer(D)
      G_solver = get_optimizer(G)
      # Run it!
      images = run_a_gan(
          D.
          G,
          D_solver,
          G_solver,
          discriminator_loss,
          generator_loss,
          loader_train
      )
```

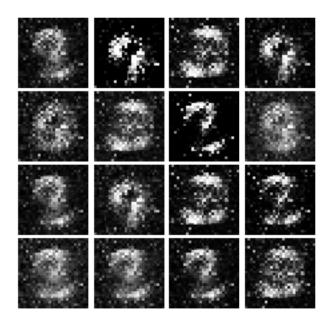
Run the cell below to show the generated images.

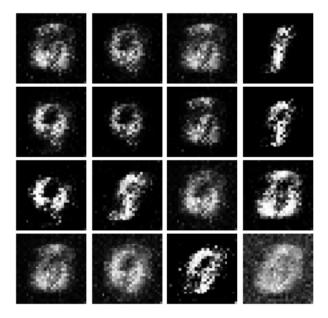
```
[24]: numIter = 0
for img in images:
    print("Iter: {}".format(numIter))
    show_images(img)
    plt.show()
    numIter += 250
    print()
```

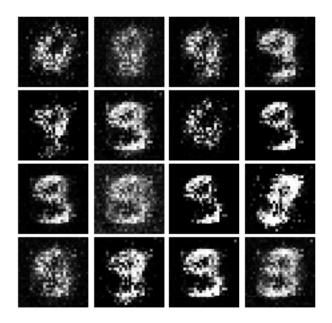


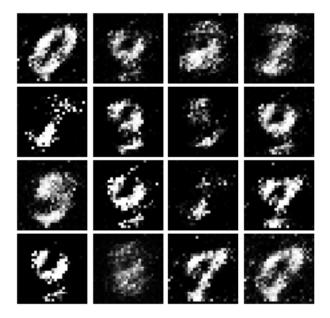


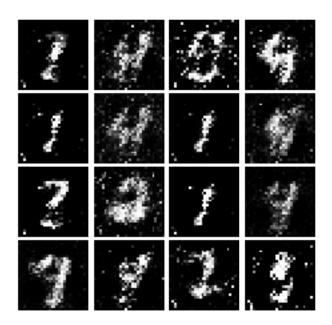


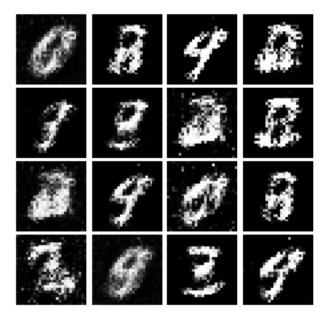


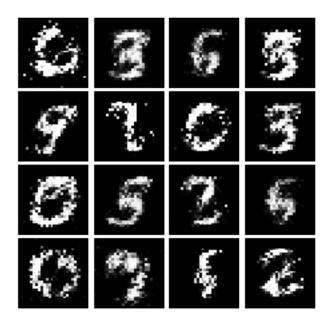


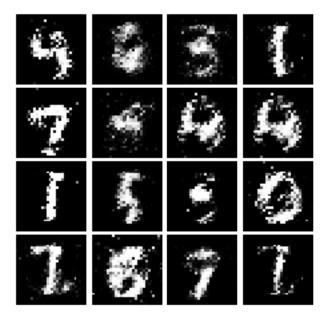


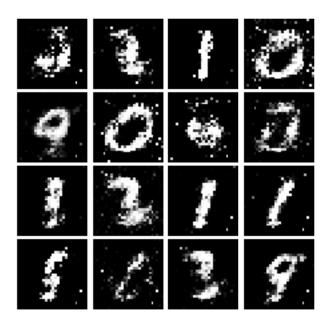


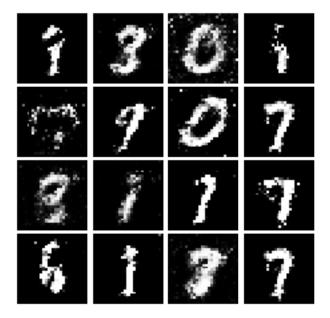


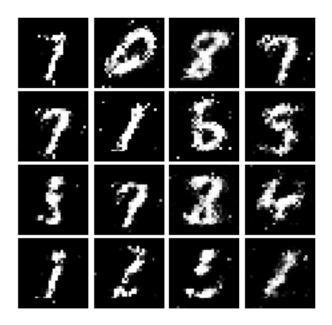


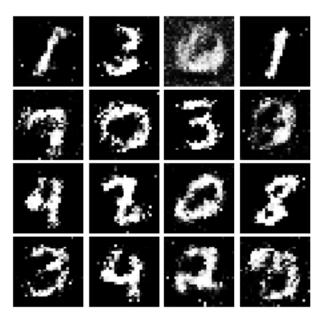


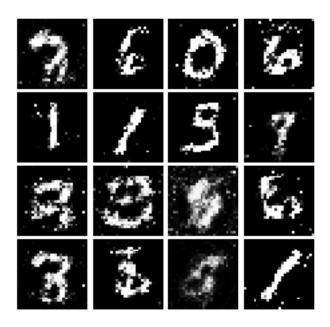












## 6.1 Inline Question 1

What does your final vanilla GAN image look like?

```
[25]: # This output is your answer.
print("Vanilla GAN final image:")
show_images(images[-1])
plt.show()
```

Vanilla GAN final image:



Well that wasn't so hard, was it? In the iterations in the low 100s you should see black backgrounds, fuzzy shapes as you approach iteration 1000, and decent shapes, about half of which will be sharp and clearly recognizable as we pass 3000.

# 7 Least Squares GAN

We'll now look at Least Squares GAN, a newer, more stable alernative to the original GAN loss function. For this part, all we have to do is change the loss function and retrain the model. We'll implement equation (9) in the paper, with the generator loss:

$$\ell_G = \frac{1}{2}\mathbb{E}_{z \sim p(z)}\left[\left(D(G(z)) - 1\right)^2\right]$$

and the discriminator loss:

$$\ell_D = \frac{1}{2}\mathbb{E}_{x \sim p_{\text{data}}}\left[\left(D(x) - 1\right)^2\right] + \frac{1}{2}\mathbb{E}_{z \sim p(z)}\left[\left(D(G(z))\right)^2\right]$$

**HINTS**: Instead of computing the expectation, we will be averaging over elements of the minibatch, so make sure to combine the loss by averaging instead of summing. When plugging in for D(x) and D(G(z)) use the direct output from the discriminator (scores\_real and scores\_fake).

Implement ls\_discriminator\_loss, ls\_generator\_loss in cs231n/gan\_pytorch.py

Before running a GAN with our new loss function, let's check it:

```
[6]: from cs231n.gan_pytorch import ls_discriminator_loss, ls_generator_loss

def test_lsgan_loss(score_real, score_fake, d_loss_true, g_loss_true):
    score_real = torch.Tensor(score_real).type(dtype)
```

```
score_fake = torch.Tensor(score_fake).type(dtype)
d_loss = ls_discriminator_loss(score_real, score_fake).cpu().numpy()
g_loss = ls_generator_loss(score_fake).cpu().numpy()
print("Maximum error in d_loss: %g"%rel_error(d_loss_true, d_loss))
print("Maximum error in g_loss: %g"%rel_error(g_loss_true, g_loss))

test_lsgan_loss(
    answers['logits_real'],
    answers['logits_fake'],
    answers['d_loss_lsgan_true'],
    answers['g_loss_lsgan_true'])
```

Maximum error in d\_loss: 1.53171e-08 Maximum error in g\_loss: 2.7837e-09

Run the following cell to train your model!

```
Iter: 0, D: 0.3267, G:0.4508

Iter: 250, D: 0.1226, G:0.2369

Iter: 500, D: 0.1477, G:0.3876

Iter: 750, D: 0.1706, G:0.2707

Iter: 1000, D: 0.1516, G:0.2556

Iter: 1250, D: 0.19, G:0.4825

Iter: 1500, D: 0.2088, G:0.2529

Iter: 1750, D: 0.1985, G:0.1753

Iter: 2000, D: 0.2329, G:0.1823

Iter: 2250, D: 0.2435, G:0.142

Iter: 2500, D: 0.2055, G:0.1801

Iter: 2750, D: 0.234, G:0.169

Iter: 3000, D: 0.2296, G:0.1678

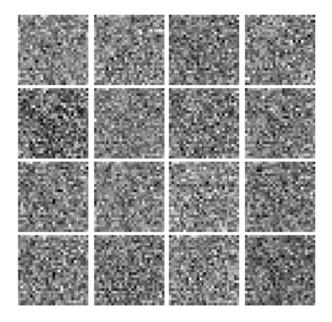
Iter: 3250, D: 0.2126, G:0.1895
```

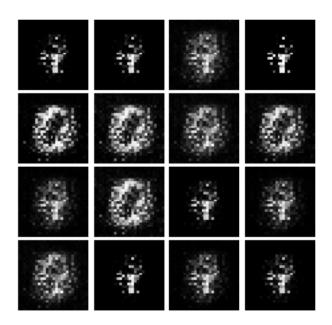
Iter: 3500, D: 0.2173, G:0.1624 Iter: 3750, D: 0.2323, G:0.1826

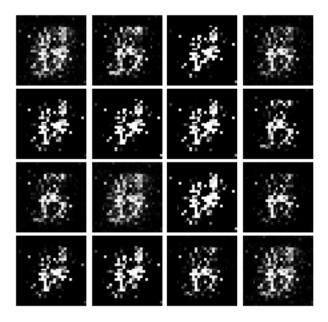
Run the cell below to show generated images.

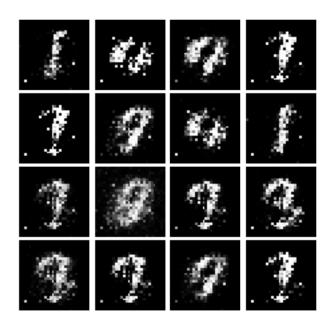
```
[17]: numIter = 0
    for img in images:
        print("Iter: {}".format(numIter))
        show_images(img)
        plt.show()
        numIter += 250
        print()
```

Iter: 0



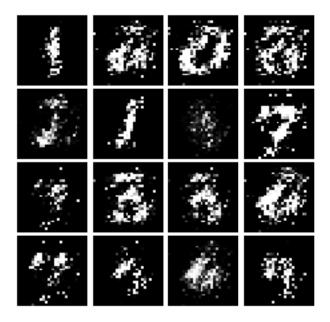


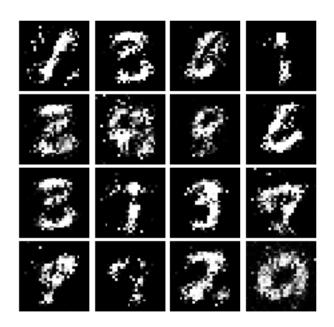


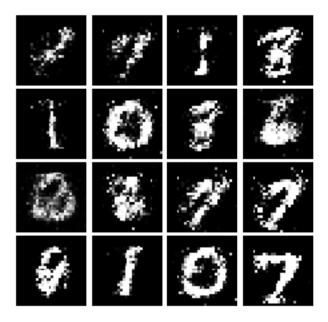








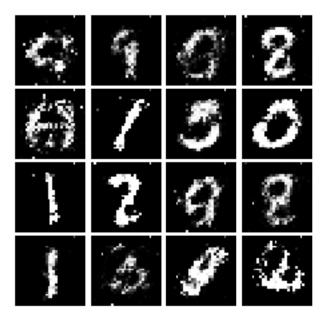




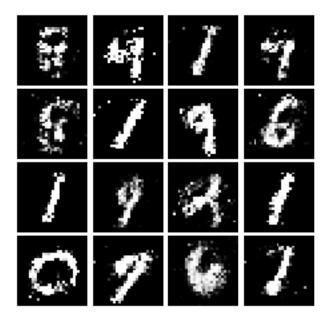












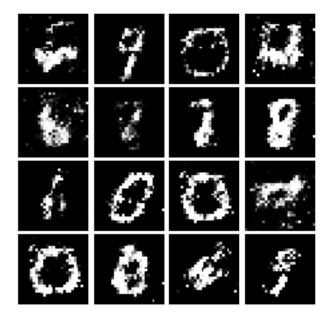


## 7.1 Inline Question 2

What does your final LSGAN image look like?

```
[18]: # This output is your answer.
print("LSGAN final image:")
show_images(images[-1])
plt.show()
```

LSGAN final image:



### 8 Deeply Convolutional GANs

In the first part of the notebook, we implemented an almost direct copy of the original GAN network from Ian Goodfellow. However, this network architecture allows no real spatial reasoning. It is unable to reason about things like "sharp edges" in general because it lacks any convolutional layers. Thus, in this section, we will implement some of the ideas from DCGAN, where we use convolutional networks

**Discriminator** We will use a discriminator inspired by the TensorFlow MNIST classification tutorial, which is able to get above 99% accuracy on the MNIST dataset fairly quickly. \* Conv2D: 32 Filters, 5x5, Stride 1 \* Leaky ReLU(alpha=0.01) \* Max Pool 2x2, Stride 2 \* Conv2D: 64 Filters, 5x5, Stride 1 \* Leaky ReLU(alpha=0.01) \* Max Pool 2x2, Stride 2 \* Flatten \* Fully Connected with output size 4 x 4 x 64 \* Leaky ReLU(alpha=0.01) \* Fully Connected with output size 1

Implement build\_dc\_classifier in cs231n/gan\_pytorch.py

```
[25]: from cs231n.gan_pytorch import build_dc_classifier

data = next(enumerate(loader_train))[-1][0].type(dtype)
b = build_dc_classifier(batch_size).type(dtype)
out = b(data)
print(out.size())
print(data.shape)
```

```
torch.Size([128, 1])
torch.Size([128, 1, 28, 28])
```

Check the number of parameters in your classifier as a sanity check:

Correct number of parameters in classifier.

Generator For the generator, we will copy the architecture exactly from the InfoGAN paper. See Appendix C.1 MNIST. See the documentation for nn.ConvTranspose2d. We are always "training" in GAN mode. \* Fully connected with output size 1024 \* ReLU \* BatchNorm \* Fully connected with output size 7 x 7 x 128 \* ReLU \* BatchNorm \* Use Unflatten() to reshape into Image Tensor of shape 7, 7, 128 \* ConvTranspose2d: 64 filters of 4x4, stride 2, 'same' padding (use padding=1) \* ReLU \* BatchNorm \* ConvTranspose2d: 1 filter of 4x4, stride 2, 'same' padding (use padding=1) \* TanH \* Should have a 28x28x1 image, reshape back into 784 vector (using Flatten())

Implement build\_dc\_generator in cs231n/gan\_pytorch.py

```
[31]: from cs231n.gan_pytorch import build_dc_generator

test_g_gan = build_dc_generator().type(dtype)
test_g_gan.apply(initialize_weights)

fake_seed = torch.randn(batch_size, NOISE_DIM).type(dtype)
fake_images = test_g_gan.forward(fake_seed)
fake_images.size()
```

[31]: torch.Size([128, 784])

Check the number of parameters in your generator as a sanity check:

Correct number of parameters in generator.

```
[33]: D_DC = build_dc_classifier(batch_size).type(dtype)
      D_DC.apply(initialize_weights)
      G_DC = build_dc_generator().type(dtype)
      G_DC.apply(initialize_weights)
      D_DC_solver = get_optimizer(D_DC)
      G_DC_solver = get_optimizer(G_DC)
      images = run_a_gan(
          D_DC,
          G DC,
          D_DC_solver,
          G_DC_solver,
          discriminator_loss,
          generator_loss,
          loader_train,
          num_epochs=5
      )
```

```
Iter: 0, D: 1.468, G:1.793

Iter: 250, D: 1.267, G:0.6475

Iter: 500, D: 1.221, G:0.9303

Iter: 750, D: 1.169, G:0.9745

Iter: 1000, D: 1.282, G:1.072

Iter: 1250, D: 1.222, G:0.8577

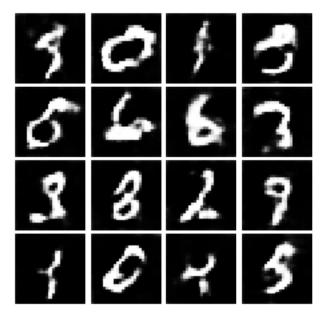
Iter: 1500, D: 1.216, G:0.995

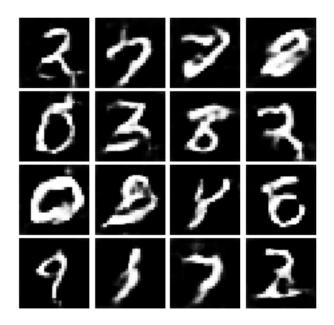
Iter: 1750, D: 1.215, G:0.7586
```

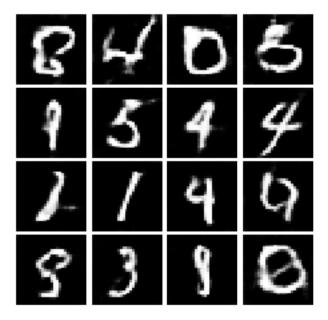
Run the cell below to show generated images.

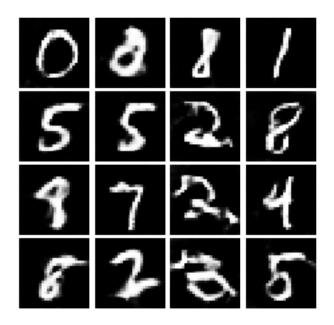
```
[34]: numIter = 0
for img in images:
    print("Iter: {}".format(numIter))
    show_images(img)
    plt.show()
    numIter += 250
    print()
```

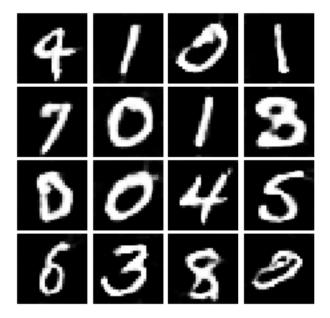


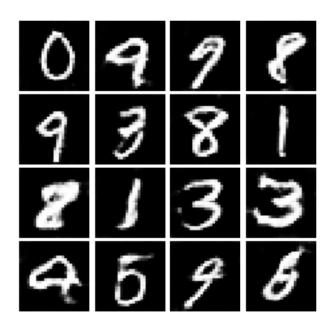


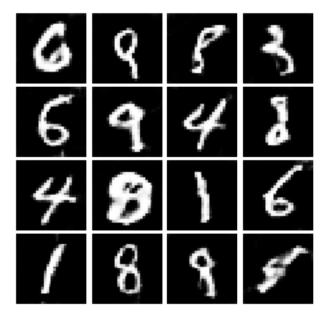










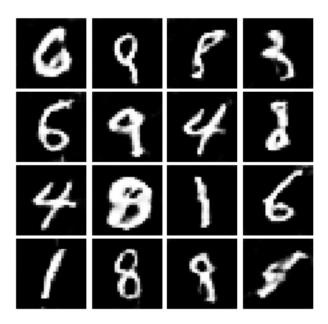


## 8.1 Inline Question 3

What does your final DCGAN image look like?

```
[35]: # This output is your answer.
print("DCGAN final image:")
show_images(images[-1])
plt.show()
```

DCGAN final image:



### 8.2 Inline Question 4

We will look at an example to see why alternating minimization of the same objective (like in a GAN) can be tricky business.

Consider f(x,y) = xy. What does  $\min_x \max_y f(x,y)$  evaluate to? (Hint: minmax tries to minimize the maximum value achievable.)

Now try to evaluate this function numerically for 6 steps, starting at the point (1,1), by using alternating gradient (first updating y, then updating x using that updated y) with step size 1. Here step size is the learning\_rate, and steps will be learning\_rate \* gradient. You'll find that writing out the update step in terms of  $x_t, y_t, x_{t+1}, y_{t+1}$  will be useful.

Breifly explain what  $\min_x \max_y f(x, y)$  evaluates to and record the six pairs of explicit values for  $(x_t, y_t)$  in the table below.

#### 8.2.1 Your answer:

$y_0$	$y_1$	$y_2$	$y_3$	$y_4$	$y_5$	$y_6$
1	2	1	-1	-2	-1	1
$x_0$	$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	$x_6$

$y_0$	$y_1$	$y_2$	$y_3$	$y_4$	$y_5$	$y_6$
1	-1	-2	-1	1	2	1

### 8.3 Inline Question 5

Using this method, will we ever reach the optimal value? Why or why not?

#### 8.3.1 Your answer:

No. In this example, every 6 steps the (x, y) value would come back to (1, 1).

### 8.4 Inline Question 6

If the generator loss decreases during training while the discriminator loss stays at a constant high value from the start, is this a good sign? Why or why not? A qualitative answer is sufficient.

### 8.4.1 Your answer:

No. Because this phenomenon would only indicate that the discriminator tend to "think" the generator's output is true image but no real iteration exists.