RNN_Captioning

May 25, 2022

```
[]: # 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 = 'Colab_Notebooks/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/Colab_Notebooks/cs231n/assignments/assignment3/cs231n/datasets /content/drive/My Drive/Colab Notebooks/cs231n/assignments/assignment3

1 Image Captioning with RNNs

In this exercise, you will implement vanilla Recurrent Neural Networks and use them to train a model that can generate novel captions for images.

```
[]: # Setup cell.
import time, os, json
import numpy as np
import matplotlib.pyplot as plt
```

```
from cs231n.gradient_check import eval_numerical_gradient, __
→eval_numerical_gradient_array
from cs231n.rnn_layers import *
from cs231n.captioning solver import CaptioningSolver
from cs231n.classifiers.rnn import CaptioningRNN
from cs231n.coco utils import load coco data, sample coco minibatch,
→decode captions
from cs231n.image_utils import image_from_url
%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 rel_error(x, y):
    """ returns relative error """
   return np.max(np.abs(x - y) / (np.maximum(1e-8, np.abs(x) + np.abs(y))))
```

2 COCO Dataset

For this exercise, we will use the 2014 release of the COCO dataset, a standard testbed for image captioning. The dataset consists of 80,000 training images and 40,000 validation images, each annotated with 5 captions written by workers on Amazon Mechanical Turk.

Image features. We have preprocessed the data and extracted features for you already. For all images, we have extracted features from the fc7 layer of the VGG-16 network pretrained on ImageNet, and these features are stored in the files train2014_vgg16_fc7.h5 and val2014_vgg16_fc7.h5. To cut down on processing time and memory requirements, we have reduced the dimensionality of the features from 4096 to 512 using Principal Component Analysis (PCA), and these features are stored in the files train2014_vgg16_fc7_pca.h5 and val2014_vgg16_fc7_pca.h5. The raw images take up nearly 20GB of space so we have not included them in the download. Since all images are taken from Flickr, we have stored the URLs of the training and validation images in the files train2014_urls.txt and val2014_urls.txt. This allows you to download images on-the-fly for visualization.

Captions. Dealing with strings is inefficient, so we will work with an encoded version of the captions. Each word is assigned an integer ID, allowing us to represent a caption by a sequence of integers. The mapping between integer IDs and words is in the file coco2014_vocab.json, and you can use the function decode_captions from the file cs231n/coco_utils.py to convert NumPy arrays of integer IDs back into strings.

Tokens. There are a couple special tokens that we add to the vocabulary, and we have taken care of all implementation details around special tokens for you. We prepend a special <START> token and append an <END> token to the beginning and end of each caption respectively. Rare words

are replaced with a special <UNK> token (for "unknown"). In addition, since we want to train with minibatches containing captions of different lengths, we pad short captions with a special <NULL> token after the <END> token and don't compute loss or gradient for <NULL> tokens.

You can load all of the COCO data (captions, features, URLs, and vocabulary) using the load_coco_data function from the file cs231n/coco_utils.py. Run the following cell to do so:

```
base dir /content/drive/My Drive/Colab_Notebooks/cs231n/assignments/
/cs231n/datasets/coco_captioning
train_captions <class 'numpy.ndarray'> (400135, 17) int32
train_image_idxs <class 'numpy.ndarray'> (400135,) int32
val_captions <class 'numpy.ndarray'> (195954, 17) int32
val_image_idxs <class 'numpy.ndarray'> (195954,) int32
train_features <class 'numpy.ndarray'> (82783, 512) float32
val_features <class 'numpy.ndarray'> (40504, 512) float32
idx_to_word <class 'list'> 1004
word_to_idx <class 'dict'> 1004
train_urls <class 'numpy.ndarray'> (82783,) <U63
val_urls <class 'numpy.ndarray'> (40504,) <U63</pre>
```

2.1 Inspect the Data

It is always a good idea to look at examples from the dataset before working with it.

You can use the sample_coco_minibatch function from the file cs231n/coco_utils.py to sample minibatches of data from the data structure returned from load_coco_data. Run the following to sample a small minibatch of training data and show the images and their captions. Running it multiple times and looking at the results helps you to get a sense of the dataset.

```
[]: # Sample a minibatch and show the images and captions.
# If you get an error, the URL just no longer exists, so don't worry!
# You can re-sample as many times as you want.
batch_size = 3
```

```
captions, features, urls = sample_coco_minibatch(data, batch_size=batch_size)
for i, (caption, url) in enumerate(zip(captions, urls)):
    plt.imshow(image_from_url(url))
    plt.axis('off')
    caption_str = decode_captions(caption, data['idx_to_word'])
    plt.title(caption_str)
    plt.show()
```

<START> a walkway <UNK> a train which appears to be stopped at the station <END>



<START> a farm yard with grazing animals next to a <UNK> <END>



<START> a man holds a box as he smiles <END>

Recurrent Neural Network

As discussed in lecture, we will use Recurrent Neural Network (RNN) language models for image captioning. The file cs231n/rnn_layers.py contains implementations of different layer types that are needed for recurrent neural networks, and the file cs231n/classifiers/rnn.py uses these layers to implement an image captioning model.

We will first implement different types of RNN layers in cs231n/rnn_layers.py.

NOTE: The Long-Short Term Memory (LSTM) RNN is a common variant of the vanilla RNN. LSTM_Captioning.ipynb is optional extra credit, so don't worry about references to LSTM in cs231n/classifiers/rnn.py and cs231n/rnn_layers.py for now.

4 Vanilla RNN: Step Forward

Open the file cs231n/rnn_layers.py. This file implements the forward and backward passes for different types of layers that are commonly used in recurrent neural networks.

First implement the function rnn_step_forward which implements the forward pass for a single timestep of a vanilla recurrent neural network. After doing so run the following to check your implementation. You should see errors on the order of e-8 or less.

```
[]: N, D, H = 3, 10, 4

x = np.linspace(-0.4, 0.7, num=N*D).reshape(N, D)
prev_h = np.linspace(-0.2, 0.5, num=N*H).reshape(N, H)
Wx = np.linspace(-0.1, 0.9, num=D*H).reshape(D, H)
Wh = np.linspace(-0.3, 0.7, num=H*H).reshape(H, H)
b = np.linspace(-0.2, 0.4, num=H)

next_h, _ = rnn_step_forward(x, prev_h, Wx, Wh, b)
expected_next_h = np.asarray([
    [-0.58172089, -0.50182032, -0.41232771, -0.31410098],
    [ 0.66854692, 0.79562378, 0.87755553, 0.92795967],
    [ 0.97934501, 0.99144213, 0.99646691, 0.99854353]])

print('next_h error: ', rel_error(expected_next_h, next_h))
```

next h error: 6.292421426471037e-09

5 Vanilla RNN: Step Backward

In the file cs231n/rnn_layers.py implement the rnn_step_backward function. After doing so run the following to numerically gradient check your implementation. You should see errors on the order of e-8 or less.

```
[]: from cs231n.rnn_layers import rnn_step_forward, rnn_step_backward
    np.random.seed(231)
    N, D, H = 4, 5, 6
    x = np.random.randn(N, D)
    h = np.random.randn(N, H)
    Wx = np.random.randn(D, H)
    Wh = np.random.randn(H, H)
    b = np.random.randn(H)
```

```
out, cache = rnn_step_forward(x, h, Wx, Wh, b)
dnext_h = np.random.randn(*out.shape)
fx = lambda x: rnn_step_forward(x, h, Wx, Wh, b)[0]
fh = lambda prev_h: rnn_step_forward(x, h, Wx, Wh, b)[0]
fWx = lambda Wx: rnn_step_forward(x, h, Wx, Wh, b)[0]
fWh = lambda Wh: rnn_step_forward(x, h, Wx, Wh, b)[0]
fb = lambda b: rnn step forward(x, h, Wx, Wh, b)[0]
dx num = eval numerical gradient array(fx, x, dnext h)
dprev_h_num = eval_numerical_gradient_array(fh, h, dnext_h)
dWx_num = eval_numerical_gradient_array(fWx, Wx, dnext_h)
dWh_num = eval_numerical_gradient_array(fWh, Wh, dnext_h)
db_num = eval_numerical_gradient_array(fb, b, dnext_h)
dx, dprev_h, dWx, dWh, db = rnn_step_backward(dnext_h, cache)
print('dx error: ', rel_error(dx_num, dx))
print('dprev_h error: ', rel_error(dprev_h_num, dprev_h))
print('dWx error: ', rel_error(dWx_num, dWx))
print('dWh error: ', rel_error(dWh_num, dWh))
print('db error: ', rel_error(db_num, db))
```

dx error: 4.0192769090159184e-10
dprev_h error: 2.5632975303201374e-10
dWx error: 8.820222259148609e-10
dWh error: 4.703287554560559e-10
db error: 7.30162216654e-11

6 Vanilla RNN: Forward

Now that you have implemented the forward and backward passes for a single timestep of a vanilla RNN, you will combine these pieces to implement a RNN that processes an entire sequence of data.

In the file cs231n/rnn_layers.py, implement the function rnn_forward. This should be implemented using the rnn_step_forward function that you defined above. After doing so run the following to check your implementation. You should see errors on the order of e-7 or less.

```
[]: N, T, D, H = 2, 3, 4, 5

x = np.linspace(-0.1, 0.3, num=N*T*D).reshape(N, T, D)
h0 = np.linspace(-0.3, 0.1, num=N*H).reshape(N, H)
Wx = np.linspace(-0.2, 0.4, num=D*H).reshape(D, H)
Wh = np.linspace(-0.4, 0.1, num=H*H).reshape(H, H)
b = np.linspace(-0.7, 0.1, num=H)
```

h error: 7.728466158305164e-08

7 Vanilla RNN: Backward

In the file cs231n/rnn_layers.py, implement the backward pass for a vanilla RNN in the function rnn_backward. This should run back-propagation over the entire sequence, making calls to the rnn_step_backward function that you defined earlier. You should see errors on the order of e-6 or less.

```
[]: np.random.seed(231)
     N, D, T, H = 2, 3, 10, 5
     x = np.random.randn(N, T, D)
     h0 = np.random.randn(N, H)
     Wx = np.random.randn(D, H)
     Wh = np.random.randn(H, H)
     b = np.random.randn(H)
     out, cache = rnn_forward(x, h0, Wx, Wh, b)
     dout = np.random.randn(*out.shape)
     dx, dh0, dWx, dWh, db = rnn_backward(dout, cache)
     fx = lambda x: rnn_forward(x, h0, Wx, Wh, b)[0]
     fh0 = lambda h0: rnn_forward(x, h0, Wx, Wh, b)[0]
     fWx = lambda Wx: rnn_forward(x, h0, Wx, Wh, b)[0]
     fWh = lambda Wh: rnn forward(x, h0, Wx, Wh, b)[0]
     fb = lambda b: rnn_forward(x, h0, Wx, Wh, b)[0]
     dx_num = eval_numerical_gradient_array(fx, x, dout)
```

```
dh0_num = eval_numerical_gradient_array(fh0, h0, dout)
dWx_num = eval_numerical_gradient_array(fWx, Wx, dout)
dWh_num = eval_numerical_gradient_array(fWh, Wh, dout)
db_num = eval_numerical_gradient_array(fb, b, dout)

print('dx error: ', rel_error(dx_num, dx))
print('dh0 error: ', rel_error(dh0_num, dh0))
print('dWx error: ', rel_error(dWx_num, dWx))
print('dWh error: ', rel_error(dWh_num, dWh))
print('db error: ', rel_error(db_num, db))
```

dx error: 1.5382468491701097e-09
dh0 error: 3.3839681556240896e-09
dWx error: 7.150535245339328e-09
dWh error: 1.297338408201546e-07
db error: 1.4889022954777414e-10

8 Word Embedding: Forward

In deep learning systems, we commonly represent words using vectors. Each word of the vocabulary will be associated with a vector, and these vectors will be learned jointly with the rest of the system.

In the file cs231n/rnn_layers.py, implement the function word_embedding_forward to convert words (represented by integers) into vectors. Run the following to check your implementation. You should see an error on the order of e-8 or less.

out error: 1.000000094736443e-08

9 Word Embedding: Backward

Implement the backward pass for the word embedding function in the function word_embedding_backward. After doing so run the following to numerically gradient check your implementation. You should see an error on the order of e-11 or less.

```
[]: np.random.seed(231)

N, T, V, D = 50, 3, 5, 6
x = np.random.randint(V, size=(N, T))
W = np.random.randn(V, D)

out, cache = word_embedding_forward(x, W)
dout = np.random.randn(*out.shape)
dW = word_embedding_backward(dout, cache)

f = lambda W: word_embedding_forward(x, W)[0]
dW_num = eval_numerical_gradient_array(f, W, dout)

print('dW error: ', rel_error(dW, dW_num))
```

dW error: 3.2760093562196586e-12

10 Temporal Affine Layer

At every timestep we use an affine function to transform the RNN hidden vector at that timestep into scores for each word in the vocabulary. Because this is very similar to the affine layer that you implemented in assignment 2, we have provided this function for you in the temporal_affine_forward and temporal_affine_backward functions in the file cs231n/rnn_layers.py. Run the following to perform numeric gradient checking on the implementation. You should see errors on the order of e-9 or less.

```
[]: np.random.seed(231)

# Gradient check for temporal affine layer
N, T, D, M = 2, 3, 4, 5
x = np.random.randn(N, T, D)
w = np.random.randn(D, M)
b = np.random.randn(M)

out, cache = temporal_affine_forward(x, w, b)

dout = np.random.randn(*out.shape)

fx = lambda x: temporal_affine_forward(x, w, b)[0]
fw = lambda w: temporal_affine_forward(x, w, b)[0]
```

```
fb = lambda b: temporal_affine_forward(x, w, b)[0]

dx_num = eval_numerical_gradient_array(fx, x, dout)
dw_num = eval_numerical_gradient_array(fw, w, dout)
db_num = eval_numerical_gradient_array(fb, b, dout)

dx, dw, db = temporal_affine_backward(dout, cache)

print('dx error: ', rel_error(dx_num, dx))
print('dw error: ', rel_error(dw_num, dw))
print('db error: ', rel_error(db_num, db))
```

dx error: 2.9215945034030545e-10
dw error: 1.5772088618663602e-10
db error: 3.252200556967514e-11

11 Temporal Softmax Loss

In an RNN language model, at every timestep we produce a score for each word in the vocabulary. We know the ground-truth word at each timestep, so we use a softmax loss function to compute loss and gradient at each timestep. We sum the losses over time and average them over the minibatch.

However there is one wrinkle: since we operate over minibatches and different captions may have different lengths, we append <NULL> tokens to the end of each caption so they all have the same length. We don't want these <NULL> tokens to count toward the loss or gradient, so in addition to scores and ground-truth labels our loss function also accepts a mask array that tells it which elements of the scores count towards the loss.

Since this is very similar to the softmax loss function you implemented in assignment 1, we have implemented this loss function for you; look at the temporal_softmax_loss function in the file cs231n/rnn_layers.py.

Run the following cell to sanity check the loss and perform numeric gradient checking on the function. You should see an error for dx on the order of e-7 or less.

```
[]: # Sanity check for temporal softmax loss
from cs231n.rnn_layers import temporal_softmax_loss

N, T, V = 100, 1, 10

def check_loss(N, T, V, p):
    x = 0.001 * np.random.randn(N, T, V)
    y = np.random.randint(V, size=(N, T))
    mask = np.random.rand(N, T) <= p
    print(temporal_softmax_loss(x, y, mask)[0])

check_loss(100, 1, 10, 1.0) # Should be about 2.3
check_loss(100, 10, 10, 1.0) # Should be about 23</pre>
```

```
check_loss(5000, 10, 10, 0.1) # Should be within 2.2-2.4

# Gradient check for temporal softmax loss
N, T, V = 7, 8, 9

x = np.random.randn(N, T, V)
y = np.random.randint(V, size=(N, T))
mask = (np.random.rand(N, T) > 0.5)

loss, dx = temporal_softmax_loss(x, y, mask, verbose=False)

dx_num = eval_numerical_gradient(lambda x: temporal_softmax_loss(x, y, mask) [0], x, verbose=False)

print('dx error: ', rel_error(dx, dx_num))
```

2.3027781774290146 23.025985953127226 2.2643611790293394 dx error: 2.583585303524283e-08

12 RNN for Image Captioning

Now that you have implemented the necessary layers, you can combine them to build an image captioning model. Open the file cs231n/classifiers/rnn.py and look at the CaptioningRNN class.

Implement the forward and backward pass of the model in the loss function. For now you only need to implement the case where cell_type='rnn' for vanilla RNNs; you will implement the LSTM case later. After doing so, run the following to check your forward pass using a small test case; you should see error on the order of e-10 or less.

```
[]: N, D, W, H = 10, 20, 30, 40
word_to_idx = {'<NULL>': 0, 'cat': 2, 'dog': 3}
V = len(word_to_idx)
T = 13

model = CaptioningRNN(
    word_to_idx,
    input_dim=D,
    wordvec_dim=W,
    hidden_dim=H,
    cell_type='rnn',
    dtype=np.float64
)
```

```
# Set all model parameters to fixed values
for k, v in model.params.items():
    model.params[k] = np.linspace(-1.4, 1.3, num=v.size).reshape(*v.shape)

features = np.linspace(-1.5, 0.3, num=(N * D)).reshape(N, D)
captions = (np.arange(N * T) % V).reshape(N, T)

loss, grads = model.loss(features, captions)
expected_loss = 9.83235591003

print('loss: ', loss)
print('expected loss: ', expected_loss)
print('difference: ', abs(loss - expected_loss))
```

loss: 9.832355910027387 expected loss: 9.83235591003 difference: 2.6130209107577684e-12

Run the following cell to perform numeric gradient checking on the CaptioningRNN class; you should see errors around the order of e-6 or less.

```
[]: np.random.seed(231)
     batch_size = 2
     timesteps = 3
     input_dim = 4
     wordvec_dim = 5
     hidden_dim = 6
     word_to_idx = {'<NULL>': 0, 'cat': 2, 'dog': 3}
     vocab_size = len(word_to_idx)
     captions = np.random.randint(vocab_size, size=(batch_size, timesteps))
     features = np.random.randn(batch size, input dim)
     model = CaptioningRNN(
         word_to_idx,
         input_dim=input_dim,
         wordvec_dim=wordvec_dim,
         hidden_dim=hidden_dim,
         cell_type='rnn',
         dtype=np.float64,
     loss, grads = model.loss(features, captions)
     for param name in sorted(grads):
         f = lambda _: model.loss(features, captions)[0]
```

W_embed relative error: 2.331070e-09
W_proj relative error: 1.112417e-08
W_vocab relative error: 4.274379e-09
Wh relative error: 5.858117e-09
Wx relative error: 1.590657e-06
b relative error: 9.727211e-10
b_proj relative error: 1.934807e-08
b_vocab relative error: 7.087097e-11

13 Overfit RNN Captioning Model on Small Data

Similar to the Solver class that we used to train image classification models on the previous assignment, on this assignment we use a CaptioningSolver class to train image captioning models. Open the file cs231n/captioning_solver.py and read through the CaptioningSolver class; it should look very familiar.

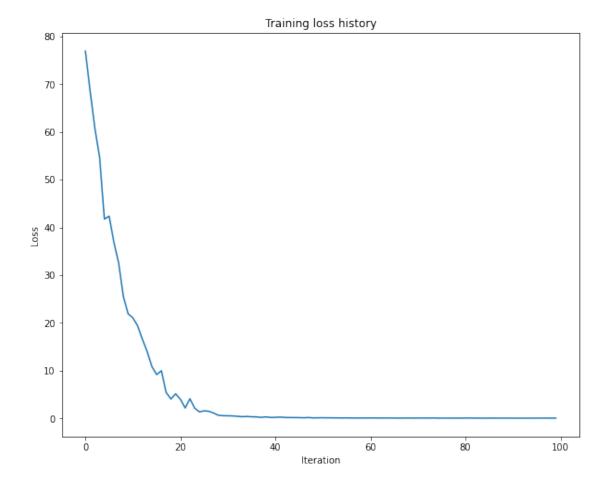
Once you have familiarized yourself with the API, run the following to make sure your model overfits a small sample of 100 training examples. You should see a final loss of less than 0.1.

```
[]: np.random.seed(231)
     small_data = load_coco_data(max_train=50)
     small_rnn_model = CaptioningRNN(
         cell_type='rnn',
         word_to_idx=data['word_to_idx'],
         input_dim=data['train_features'].shape[1],
         hidden_dim=512,
         wordvec_dim=256,
     )
     small_rnn_solver = CaptioningSolver(
         small_rnn_model, small_data,
         update_rule='adam',
         num epochs=50,
         batch_size=25,
         optim config={
          'learning_rate': 5e-3,
         },
         lr_decay=0.95,
         verbose=True, print_every=10,
```

```
small_rnn_solver.train()

# Plot the training losses.
plt.plot(small_rnn_solver.loss_history)
plt.xlabel('Iteration')
plt.ylabel('Loss')
plt.title('Training loss history')
plt.show()
```

base dir /content/drive/My Drive/Colab_Notebooks/cs231n/assignments/assignment3
/cs231n/datasets/coco_captioning
(Iteration 1 / 100) loss: 76.913487
(Iteration 11 / 100) loss: 21.062675
(Iteration 21 / 100) loss: 4.016271
(Iteration 31 / 100) loss: 0.567217
(Iteration 41 / 100) loss: 0.239402
(Iteration 51 / 100) loss: 0.161974
(Iteration 61 / 100) loss: 0.111526
(Iteration 71 / 100) loss: 0.097580
(Iteration 81 / 100) loss: 0.099062
(Iteration 91 / 100) loss: 0.073966



Print final training loss. You should see a final loss of less than 0.1.

```
[]: print('Final loss: ', small_rnn_solver.loss_history[-1])
```

Final loss: 0.08207057489049083

14 RNN Sampling at Test Time

Unlike classification models, image captioning models behave very differently at training time vs. at test time. At training time, we have access to the ground-truth caption, so we feed ground-truth words as input to the RNN at each timestep. At test time, we sample from the distribution over the vocabulary at each timestep and feed the sample as input to the RNN at the next timestep.

In the file cs231n/classifiers/rnn.py, implement the sample method for test-time sampling. After doing so, run the following to sample from your overfitted model on both training and validation data. The samples on training data should be very good. The samples on validation data, however, probably won't make sense.

```
[]: # If you get an error, the URL just no longer exists, so don't worry!
     # You can re-sample as many times as you want.
     for split in ['train', 'val']:
        minibatch = sample_coco_minibatch(small_data, split=split, batch_size=2)
        gt_captions, features, urls = minibatch
        gt_captions = decode_captions(gt_captions, data['idx_to_word'])
         sample_captions = small_rnn_model.sample(features)
         sample_captions = decode_captions(sample_captions, data['idx_to_word'])
        for gt_caption, sample_caption, url in zip(gt_captions, sample_captions,
     →urls):
            img = image_from_url(url)
             # Skip missing URLs.
            if img is None: continue
            plt.imshow(img)
            plt.title('%s\n%s\nGT:%s' % (split, sample_caption, gt_caption))
            plt.axis('off')
            plt.show()
```

train
a man posing with his skiing gear in room <UNK> with wood <END>
GT:<START> a man posing with his skiing gear in room <UNK> with wood <END>



URL Error: Not Found

http://farm3.staticflickr.com/2156/2322375142_d473bec018_z.jpg

val two of <UNK> woman of a while in sun <UNK> <END> GT:<START> a red and white light tower on a hill near the ocean <END>



val to tracks with out of a <END> GT:<START> a table filled with many assorted food items <END>



15 Inline Question 1

In our current image captioning setup, our RNN language model produces a word at every timestep as its output. However, an alternate way to pose the problem is to train the network to operate over *characters* (e.g. 'a', 'b', etc.) as opposed to words, so that at it every timestep, it receives the previous character as input and tries to predict the next character in the sequence. For example, the network might generate a caption like

Can you describe one advantage of an image-captioning model that uses a character-level RNN? Can you also describe one disadvantage? HINT: there are several valid answers, but it might be useful to compare the parameter space of word-level and character-level models.

Your Answer:

Disdvantage:

From parameter space perspective, embeddings for character level model (limited to 26 characters

in english) will not be as diverse and expressive as compared to word level model. Hence, model trained on character level will not have semantic meaning associated which exists in word level model. Also, on the other side, it would be harder to predict the exact combination and sequence of words, since the number of permutation is much higher.

Advantages

Character level model will be faster to train as compared to word level model because there will not be complex representations to be learnt. However this faster model training will suffer from the lower validation accuracy as compared to word level model. In addition, embeddings of the characters would be fairly simpler than that of word level model since the number of characters are limited as opposed to large number of words possible so less tokens.

Transformer Captioning

May 25, 2022

```
[]: # 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 = 'Colab_Notebooks/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/Colab_Notebooks/cs231n/assignments/assignment3/cs231n/datasets /content/drive/My Drive/Colab Notebooks/cs231n/assignments/assignment3

1 Image Captioning with Transformers

You have now implemented a vanilla RNN and for the task of image captioning. In this notebook you will implement key pieces of a transformer decoder to accomplish the same task.

NOTE: This notebook will be primarily written in PyTorch rather than NumPy, unlike the RNN notebook.

```
[]: # Setup cell.
import time, os, json
import numpy as np
```

```
import matplotlib.pyplot as plt
from cs231n.gradient_check import eval_numerical_gradient,_
→eval_numerical_gradient_array
from cs231n.transformer_layers import *
from cs231n.captioning solver transformer import CaptioningSolverTransformer
from cs231n.classifiers.transformer import CaptioningTransformer
from cs231n.coco_utils import load_coco_data, sample_coco_minibatch, u
→decode_captions
from cs231n.image_utils import image_from_url
%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 rel_error(x, y):
    """ returns relative error """
   return np.max(np.abs(x - y) / (np.maximum(1e-8, np.abs(x) + np.abs(y))))
```

2 COCO Dataset

As in the previous notebooks, we will use the COCO dataset for captioning.

```
[]: # Load COCO data from disk into a dictionary.
data = load_coco_data(pca_features=True)

# Print out all the keys and values from the data dictionary.
for k, v in data.items():
    if type(v) == np.ndarray:
        print(k, type(v), v.shape, v.dtype)
    else:
        print(k, type(v), len(v))
```

```
base dir /content/drive/My Drive/Colab_Notebooks/cs231n/assignments/assignment3 /cs231n/datasets/coco_captioning train_captions <class 'numpy.ndarray'> (400135, 17) int32 train_image_idxs <class 'numpy.ndarray'> (400135,) int32 val_captions <class 'numpy.ndarray'> (195954, 17) int32 val_image_idxs <class 'numpy.ndarray'> (195954,) int32 train_features <class 'numpy.ndarray'> (82783, 512) float32 val_features <class 'numpy.ndarray'> (40504, 512) float32 idx_to_word <class 'list'> 1004
```

```
word_to_idx <class 'dict'> 1004
train_urls <class 'numpy.ndarray'> (82783,) <U63
val_urls <class 'numpy.ndarray'> (40504,) <U63</pre>
```

3 Transformer

As you have seen, RNNs are incredibly powerful but often slow to train. Further, RNNs struggle to encode long-range dependencies (though LSTMs are one way of mitigating the issue). In 2017, Vaswani et al introduced the Transformer in their paper "Attention Is All You Need" to a) introduce parallelism and b) allow models to learn long-range dependencies. The paper not only led to famous models like BERT and GPT in the natural language processing community, but also an explosion of interest across fields, including vision. While here we introduce the model in the context of image captioning, the idea of attention itself is much more general.

4 Transformer: Multi-Headed Attention

4.0.1 Dot-Product Attention

Recall that attention can be viewed as an operation on a query $q \in \mathbb{R}^d$, a set of value vectors $\{v_1, \ldots, v_n\}, v_i \in \mathbb{R}^d$, and a set of key vectors $\{k_1, \ldots, k_n\}, k_i \in \mathbb{R}^d$, specified as

$$c = \sum_{i=1}^{n} v_i \alpha_i \alpha_i = \frac{\exp(k_i^\top q)}{\sum_{j=1}^{n} \exp(k_j^\top q)}$$
 (1)

(2)

where α_i are frequently called the "attention weights", and the output $c \in \mathbb{R}^d$ is a correspondingly weighted average over the value vectors.

4.0.2 Self-Attention

In Transformers, we perform self-attention, which means that the values, keys and query are derived from the input $X \in \mathbb{R}^{\ell \times d}$, where ℓ is our sequence length. Specifically, we learn parameter matrices $V, K, Q \in \mathbb{R}^{d \times d}$ to map our input X as follows:

$$v_i = Vx_i \quad i \in \{1, \dots, \ell\} \tag{3}$$

$$k_i = Kx_i \quad i \in \{1, \dots, \ell\} \tag{4}$$

$$q_i = Qx_i \quad i \in \{1, \dots, \ell\} \tag{5}$$

4.0.3 Multi-Headed Scaled Dot-Product Attention

In the case of multi-headed attention, we learn a parameter matrix for each head, which gives the model more expressivity to attend to different parts of the input. Let h be number of heads, and Y_i be the attention output of head i. Thus we learn individual matrices Q_i , K_i and V_i . To keep our overall computation the same as the single-headed case, we choose $Q_i \in \mathbb{R}^{d \times d/h}$, $K_i \in \mathbb{R}^{d \times d/h}$ and $V_i \in \mathbb{R}^{d \times d/h}$. Adding in a scaling term $\frac{1}{\sqrt{d/h}}$ to our simple dot-product attention above, we have

$$Y_i = \operatorname{softmax}\left(\frac{(XQ_i)(XK_i)^{\top}}{\sqrt{d/h}}\right)(XV_i)$$
(6)

where $Y_i \in \mathbb{R}^{\ell \times d/h}$, where ℓ is our sequence length.

In our implementation, we then apply dropout here (though in practice it could be used at any step):

$$Y_i = dropout(Y_i)$$

Finally, then the output of the self-attention is a linear transformation of the concatenation of the heads:

$$Y = [Y_1; \dots; Y_h]A \tag{7}$$

were $A \in \mathbb{R}^{d \times d}$ and $[Y_1; \dots; Y_h] \in \mathbb{R}^{\ell \times d}$.

Implement multi-headed scaled dot-product attention in the MultiHeadAttention class in the file cs231n/transformer_layers.py. The code below will check your implementation. The relative error should be less than e-3.

```
other_data = torch.randn(batch_size, sequence_length, embed_dim)
attn_output = attn(query=data, key=other_data, value=other_data)
expected_self_attn_output = np.asarray([[
[-0.2494, 0.1396, 0.4323, -0.2411, -0.1547, 0.2329, -0.1936,
         -0.1444],
         [-0.1997, 0.1746, 0.7377, -0.3549, -0.2657, 0.2693, -0.2541,
         -0.2476],
         [-0.0625, 0.1503, 0.7572, -0.3974, -0.1681, 0.2168, -0.2478,
         -0.3038]]])
expected_masked_self_attn_output = np.asarray([[
[-0.1347, 0.1934, 0.8628, -0.4903, -0.2614, 0.2798, -0.2586,
         -0.3019],
         [-0.1013, 0.3111, 0.5783, -0.3248, -0.3842, 0.1482, -0.3628,
         -0.1496],
         [-0.2071, 0.1669, 0.7097, -0.3152, -0.3136, 0.2520, -0.2774,
         -0.2208]]])
expected_attn_output = np.asarray([[
[-0.1980, 0.4083, 0.1968, -0.3477, 0.0321, 0.4258, -0.8972,
          -0.2744],
         [-0.1603, 0.4155, 0.2295, -0.3485, -0.0341, 0.3929, -0.8248,
         -0.2767].
         [-0.0908, 0.4113, 0.3017, -0.3539, -0.1020, 0.3784, -0.7189,
         -0.2912]]])
print('self_attn_output error: ', rel_error(expected_self_attn_output,__
⇒self_attn_output.detach().numpy()))
print('masked_self_attn_output error: ', __
→rel error(expected masked self_attn_output, masked_self_attn_output.detach().
print('attn_output error: ', rel_error(expected_attn_output, attn_output.
 →detach().numpy()))
```

```
self_attn_output error: 0.0003775124598178026
masked_self_attn_output error: 0.0001526367643724865
attn_output error: 0.0003527921483788199
```

5 Positional Encoding

While transformers are able to easily attend to any part of their input, the attention mechanism has no concept of token order. However, for many tasks (especially natural language processing), relative token order is very important. To recover this, the authors add a positional encoding to the embeddings of individual word tokens.

Let us define a matrix $P \in \mathbb{R}^{l \times d}$, where $P_{ij} =$

$$\begin{cases} \sin\left(i \cdot 10000^{-\frac{j}{d}}\right) & \text{if j is even} \\ \cos\left(i \cdot 10000^{-\frac{(j-1)}{d}}\right) & \text{otherwise} \end{cases}$$

Rather than directly passing an input $X \in \mathbb{R}^{l \times d}$ to our network, we instead pass X + P.

Implement this layer in PositionalEncoding in cs231n/transformer_layers.py. Once you are done, run the following to perform a simple test of your implementation. You should see errors on the order of e-3 or less.

pe_output error: 0.00010421011374914356

6 Inline Question 1

Several key design decisions were made in designing the scaled dot product attention we introduced above. Explain why the following choices were beneficial: 1. Using multiple attention heads as opposed to one. 2. Dividing by $\sqrt{d/h}$ before applying the softmax function. Recall that d is the feature dimension and h is the number of heads. 3. Adding a linear transformation to the output of the attention operation.

Only one or two sentences per choice is necessary, but be sure to be specific in addressing what would have happened without each given implementation detail, why such a situation would be suboptimal, and how the proposed implementation improves the situation.

Your Answer: 1. Individual attentions learn different features from the word embeddings (eg. noun, verb, adjectives, pronouns etc.). With multiple attention heads, model will be able to learn different features from word embeddings and improve model's expressivity and provides training stability. If multiple attention heads are not used, model will not be able to learn different feature

from word embeddings. Multiple head also helps in reducing the depth of the model. A corollary could be thought of between filters in CNN and attention heads in transformers.

- 2. Dividign by $\sqrt{d/h}$ is a way of performing self normalization (increases model's robustness) which helps avoid output of softmax to be concentrated to either 0 or 1 (i.e. prevents vanishing/exploding gradients). This in turn helps avoid saturation condition and ensures good gradient flow.
- 3. The linear transformation on the output to the attention operation helps in giving adequate weightage to each of the heads to prioritize over the most important features to help in training.

7 Transformer for Image Captioning

Now that you have implemented the previous layers, you can combine them to build a Transformer-based image captioning model. Open the file cs231n/classifiers/transformer.py and look at the CaptioningTransformer class.

Implement the forward function of the class. After doing so, run the following to check your forward pass using a small test case; you should see error on the order of e-5 or less.

```
[]: torch.manual_seed(231)
     np.random.seed(231)
     N, D, W = 4, 20, 30
     word_to_idx = {'<NULL>': 0, 'cat': 2, 'dog': 3}
     V = len(word_to_idx)
     T = 3
     transformer = CaptioningTransformer(
         word_to_idx,
         input_dim=D,
         wordvec_dim=W,
         num_heads=2,
         num_layers=2,
         max_length=30
     # Set all model parameters to fixed values
     for p in transformer.parameters():
         p.data = torch.tensor(np.linspace(-1.4, 1.3, num=p.numel()).reshape(*p.
     →shape))
     features = torch.tensor(np.linspace(-1.5, 0.3, num=(N * D)).reshape(N, D))
     captions = torch.tensor((np.arange(N * T) % V).reshape(N, T))
     scores = transformer(features, captions)
     expected_scores = np.asarray([[[-16.9532,
                                                 4.8261, 26.6054],
```

```
[-17.1033, 4.6906, 26.4844],
[-15.0708, 4.1108, 23.2924]],
[[-17.1767, 4.5897, 26.3562],
[-15.6017, 4.8693, 25.3403],
[-15.1028, 4.6905, 24.4839]],
[[-17.2172, 4.7701, 26.7574],
[-16.6755, 4.8500, 26.3754],
[-17.2172, 4.7701, 26.7574]],
[[-16.3669, 4.1602, 24.6872],
[-16.7897, 4.3467, 25.4831],
[-17.0103, 4.7775, 26.5652]]])
print('scores error: ', rel_error(expected_scores, scores.detach().numpy()))
```

scores error: 5.0561688361043265e-06

8 Overfit Transformer Captioning Model on Small Data

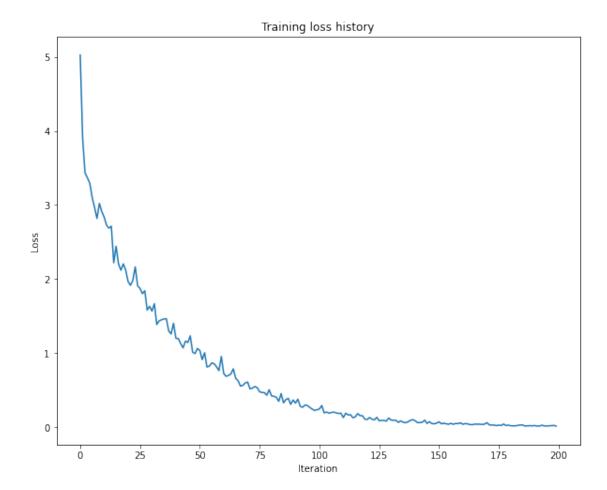
Run the following to overfit the Transformer-based captioning model on the same small dataset as we used for the RNN previously.

```
[]: torch.manual_seed(231)
    np.random.seed(231)
    data = load_coco_data(max_train=50)
    transformer = CaptioningTransformer(
              word_to_idx=data['word_to_idx'],
              input_dim=data['train_features'].shape[1],
              wordvec_dim=256,
              num heads=2,
              num_layers=2,
              max_length=30
    transformer_solver = CaptioningSolverTransformer(transformer, data,_
     num_epochs=100,
               batch_size=25,
               learning_rate=0.001,
               verbose=True, print_every=10,
             )
    transformer solver.train()
    # Plot the training losses.
```

```
plt.plot(transformer_solver.loss_history)
plt.xlabel('Iteration')
plt.ylabel('Loss')
plt.title('Training loss history')
plt.show()
```

base dir /content/drive/My Drive/Colab_Notebooks/cs231n/assignments/assignment3
/cs231n/datasets/coco_captioning

```
(Iteration 1 / 200) loss: 5.023293
(Iteration 11 / 200) loss: 2.836593
(Iteration 21 / 200) loss: 1.968886
(Iteration 31 / 200) loss: 1.569382
(Iteration 41 / 200) loss: 1.202124
(Iteration 51 / 200) loss: 1.039567
(Iteration 61 / 200) loss: 0.726249
(Iteration 71 / 200) loss: 0.610638
(Iteration 81 / 200) loss: 0.424673
(Iteration 91 / 200) loss: 0.327660
(Iteration 101 / 200) loss: 0.247739
(Iteration 111 / 200) loss: 0.131435
(Iteration 121 / 200) loss: 0.106064
(Iteration 131 / 200) loss: 0.097680
(Iteration 141 / 200) loss: 0.090001
(Iteration 151 / 200) loss: 0.075100
(Iteration 161 / 200) loss: 0.041143
(Iteration 171 / 200) loss: 0.064028
(Iteration 181 / 200) loss: 0.021940
(Iteration 191 / 200) loss: 0.024916
```



Print final training loss. You should see a final loss of less than 0.03.

```
[]: print('Final loss: ', transformer_solver.loss_history[-1])
```

Final loss: 0.017378977

9 Transformer Sampling at Test Time

The sampling code has been written for you. You can simply run the following to compare with the previous results with the RNN. As before the training results should be much better than the validation set results, given how little data we trained on.

```
[]: # If you get an error, the URL just no longer exists, so don't worry!
# You can re-sample as many times as you want.
for split in ['train', 'val']:
    minibatch = sample_coco_minibatch(data, split=split, batch_size=2)
    gt_captions, features, urls = minibatch
    gt_captions = decode_captions(gt_captions, data['idx_to_word'])
```

```
sample_captions = transformer.sample(features, max_length=30)
sample_captions = decode_captions(sample_captions, data['idx_to_word'])

for gt_caption, sample_caption, url in zip(gt_captions, sample_captions, urls):
    img = image_from_url(url)
    # Skip missing URLs.
    if img is None: continue
    plt.imshow(img)
    plt.title('%s\n%s\nGT:%s' % (split, sample_caption, gt_caption))
    plt.axis('off')
    plt.show()
```

URL Error: Gone http://farm1.staticflickr.com/202/487987371_489a65d670_z.jpg

train
a <UNK> decorated living room with a big tv in it <END>
GT:<START> a <UNK> decorated living room with a big tv in it <END>



val
red and with cement a some bottles curtain pizza <END>
GT:<START> a bedroom with a bed desk and <UNK> <UNK> <END>



val man man dog smiling a <UNK> office his food <UNK> having his picture taken <END> GT:<START> a group of people <UNK> outside by a wall <END>



Generative Adversarial Networks

May 25, 2022

```
[]: # 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 = 'Colab_Notebooks/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/Colab_Notebooks/cs231n/assignments/assignment3/cs231n/datasets /content/drive/My Drive/Colab_Notebooks/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:

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

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:

```
[]: # 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 0 2 9 1 0 4 0 0 3 8 3

9 9 9 5 9 9 5 9

0 5 0 6 9 9 5 9

```
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, __
     %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.
 →FloatTensor
```

The autoreload extension is already loaded. To reload it, use: %reload_ext autoreload

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.

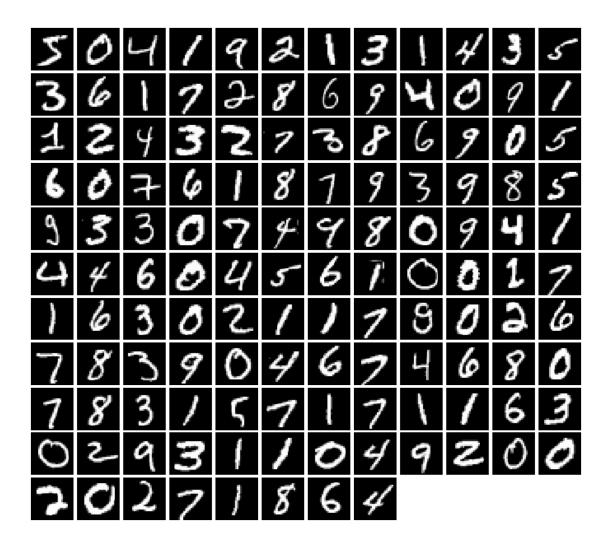
To simplify our code here, we will use the PyTorch MNIST wrapper, which downloads and loads the MNIST dataset. See the documentation for more information about the interface. The default parameters will take 5,000 of the training examples and place them into a validation dataset. The data will be saved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

```
[]: 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 = loader_train.__iter__().next()[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:

```
[]: 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.

```
[]: 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 α ; 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:

```
[]: from cs231n.gan_pytorch import discriminator

def test_discriminator(true_count=267009):
    model = discriminator()
    cur_count = count_params(model)
    if cur_count != true_count:
```

```
print('Incorrect number of parameters in discriminator. Check your

→achitecture.')
else:
    print('Correct number of parameters in discriminator.')

test_discriminator()
```

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:

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

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: 3.97058e-09

```
[]: 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']
)
```

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.

```
[]: 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_{\sqcup}
      \rightarrow 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
     )
```

```
Iter: 0, D: 1.328, G:0.7202

Iter: 250, D: 1.108, G:1.37

Iter: 500, D: 1.092, G:1.978

Iter: 750, D: 1.224, G:1.104

Iter: 1000, D: 1.299, G:0.9583

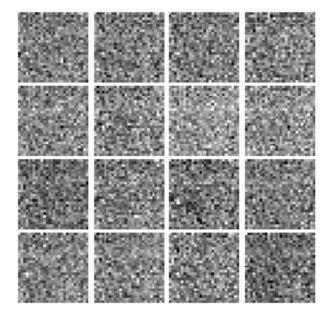
Iter: 1250, D: 1.0, G:1.306
```

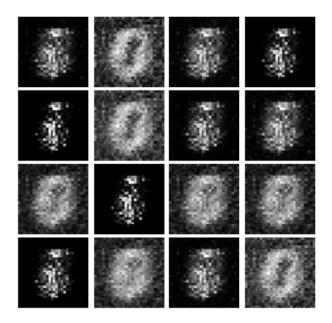
```
Iter: 1500, D: 1.27, G:1.206
Iter: 1750, D: 1.141, G:0.9829
Iter: 2000, D: 1.334, G:1.065
Iter: 2250, D: 1.295, G:0.8569
Iter: 2500, D: 1.2, G:0.9099
Iter: 2750, D: 1.27, G:0.8721
Iter: 3000, D: 1.391, G:0.7718
Iter: 3250, D: 1.363, G:0.8724
Iter: 3500, D: 1.364, G:0.8553
Iter: 3750, D: 1.416, G:0.812
```

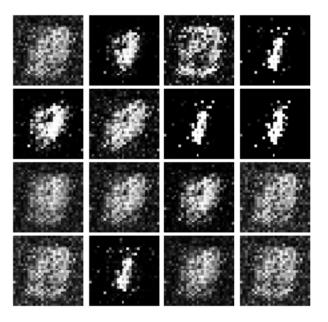
Run the cell below to show the generated images.

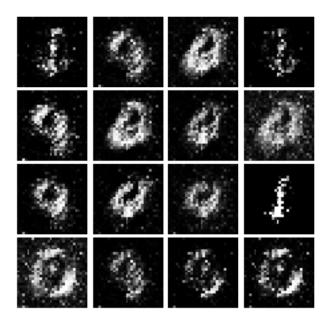
```
[]: numIter = 0
for img in images:
    print("Iter: {}".format(numIter))
    show_images(img)
    plt.show()
    numIter += 250
    print()
```

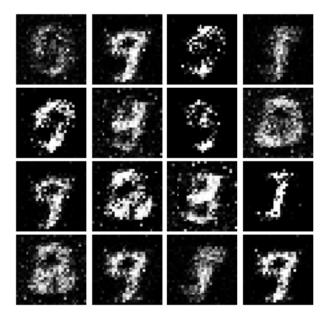
Iter: 0

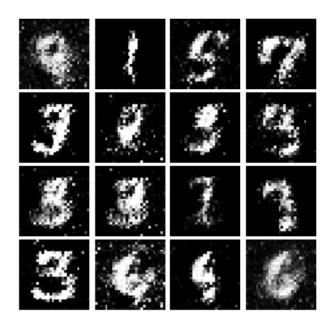


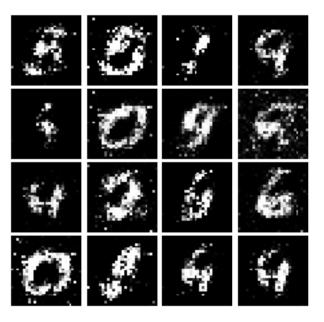


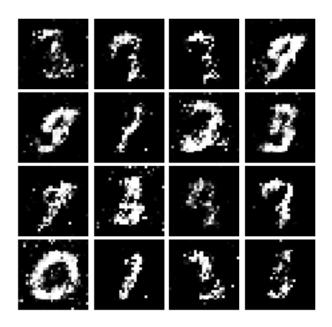


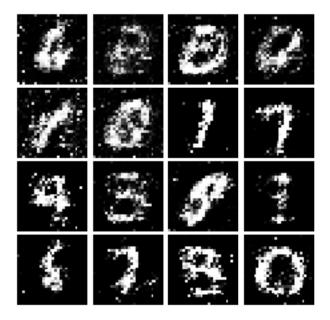


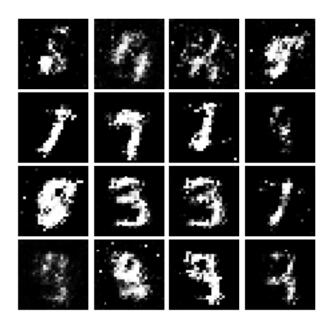








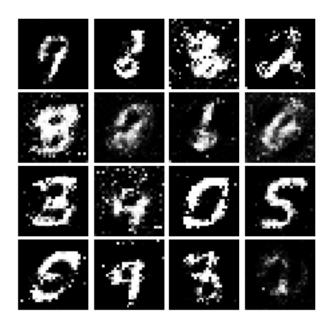
















6.1 Inline Question 1

What does your final vanilla GAN image look like?

Answer:

Vanilla GAN image looks a bit blurry, some numbers are not clearly legible. For instance digits like 2, 5, 8 are not very clear.

```
[]: # 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:

```
[]: 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: 1.64377e-08 Maximum error in g_loss: 2.7837e-09

/usr/local/lib/python3.7/dist-packages/torch/nn/modules/loss.py:529: UserWarning: Using a target size (torch.Size([10])) that is different to the input size (torch.Size([10, 1])). This will likely lead to incorrect results due to broadcasting. Please ensure they have the same size.

return F.mse_loss(input, target, reduction=self.reduction)

Run the following cell to train your model!

```
[]: D_LS = discriminator().type(dtype)

G_LS = generator().type(dtype)

D_LS_solver = get_optimizer(D_LS)

G_LS_solver = get_optimizer(G_LS)

images = run_a_gan(
    D_LS,
    G_LS,
    D_LS_solver,
    G_LS_solver,
    ls_discriminator_loss,
    ls_generator_loss,
    loader_train
)
```

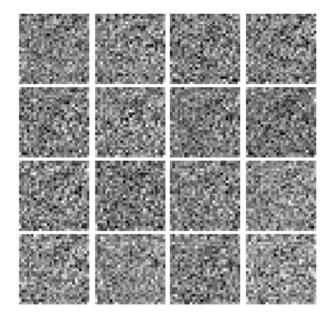
/usr/local/lib/python3.7/dist-packages/torch/nn/modules/loss.py:529: UserWarning: Using a target size (torch.Size([128])) that is different to the input size (torch.Size([128, 1])). This will likely lead to incorrect results due to broadcasting. Please ensure they have the same size.

return F.mse_loss(input, target, reduction=self.reduction)

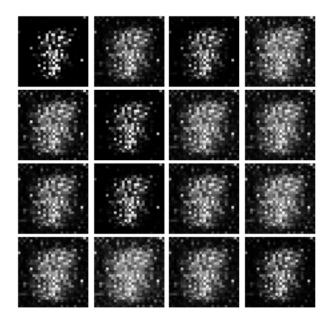
```
Iter: 0, D: 0.5689, G:0.51
Iter: 250, D: 0.1487, G:0.2958
Iter: 500, D: 0.1049, G:0.3745
Iter: 750, D: 0.128, G:0.3359
Iter: 1000, D: 0.1822, G:0.245
Iter: 1250, D: 0.1767, G:0.322
Iter: 1500, D: 0.1581, G:0.2521
Iter: 1750, D: 0.2078, G:0.1941
Iter: 2000, D: 0.2077, G:0.417
Iter: 2250, D: 0.2365, G:0.1838
Iter: 2500, D: 0.229, G:0.1851
Iter: 2750, D: 0.2349, G:0.1661
Iter: 3000, D: 0.2128, G:0.1637
Iter: 3250, D: 0.2352, G:0.1756
Iter: 3500, D: 0.2188, G:0.1699
Iter: 3750, D: 0.2383, G:0.1455
```

Run the cell below to show generated images.

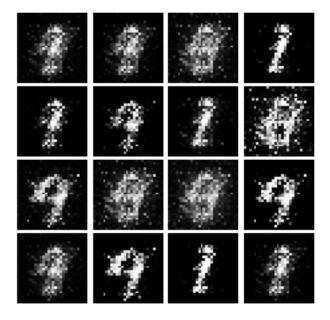
```
[]: numIter = 0
for img in images:
    print("Iter: {}".format(numIter))
    show_images(img)
    plt.show()
    numIter += 250
    print()
```

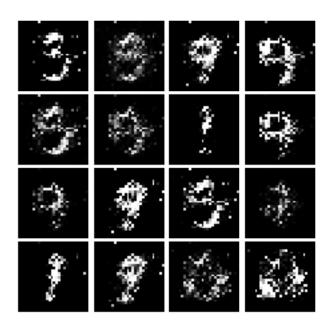


Iter: 250



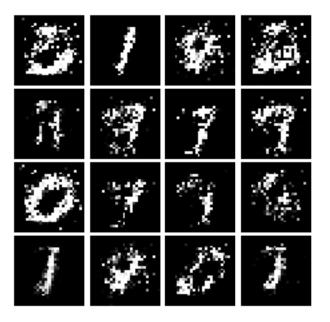
Iter: 500





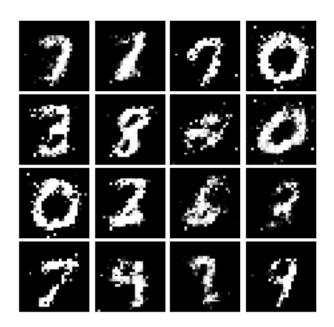




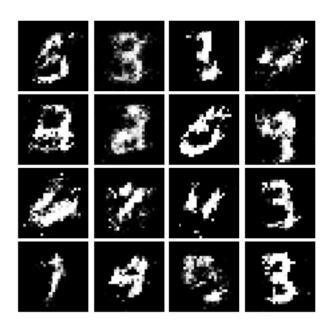




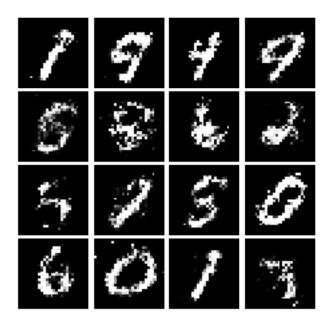


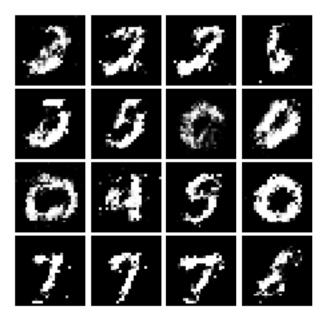


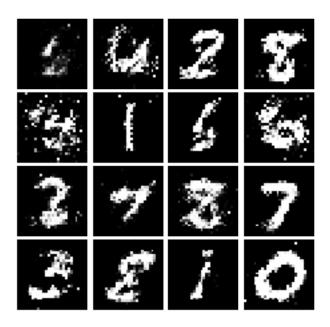












7.1 Inline Question 2

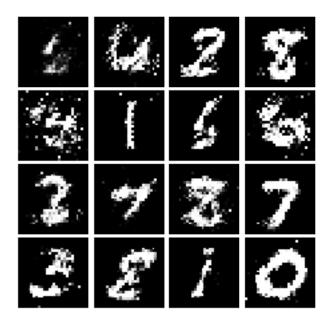
What does your final LSGAN image look like?

Answer:

Least square GAN has better final image as compared to vanilla GAN, because the loss function of least square helps reduce loss better than vanilla GAN.

```
[]: # 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

```
[]: 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())
```

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

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

```
[]: def test_dc_classifer(true_count=1102721):
    model = build_dc_classifier(batch_size)
    cur_count = count_params(model)
    if cur_count != true_count:
        print('Incorrect number of parameters in classifier. Check your_
    →achitecture.')
    else:
        print('Correct number of parameters in classifier.')

test_dc_classifer()
```

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

```
[]: 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()
```

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

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

```
[]: def test_dc_generator(true_count=6580801):
    model = build_dc_generator(4)
    cur_count = count_params(model)
    if cur_count != true_count:
        print('Incorrect number of parameters in generator. Check your_
    →achitecture.')
```

```
else:
    print('Correct number of parameters in generator.')

test_dc_generator()
```

Correct number of parameters in generator.

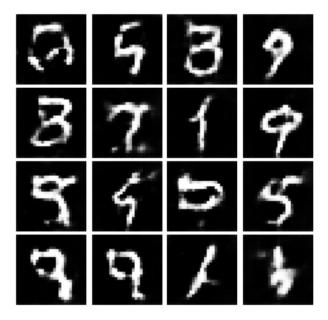
```
[]: D_DC = build_dc_classifier(batch_size).type(dtype)
     D_DC.apply(initialize_weights)
     G_DC = build_dc_generator().type(dtype)
     G_DC.apply(initialize_weights)
     D_DC_solver = get_optimizer(D_DC)
     G_DC_solver = get_optimizer(G_DC)
     images = run_a_gan(
         D_DC,
      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

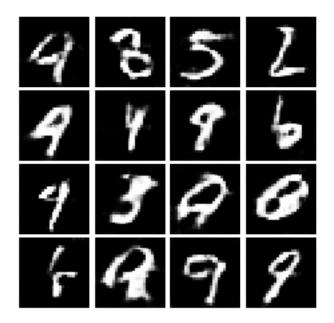
```
Iter: 0, D: 1.403, G:1.433
Iter: 250, D: 1.27, G:0.8093
Iter: 500, D: 1.216, G:1.344
Iter: 750, D: 1.103, G:1.03
Iter: 1000, D: 1.198, G:0.9077
Iter: 1250, D: 1.197, G:1.142
Iter: 1500, D: 1.043, G:1.089
Iter: 1750, D: 0.9696, G:1.024
```

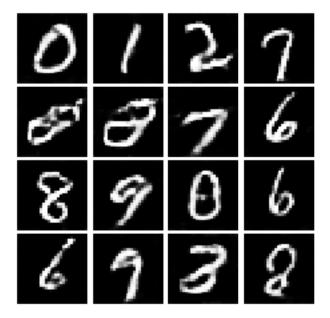
Run the cell below to show generated images.

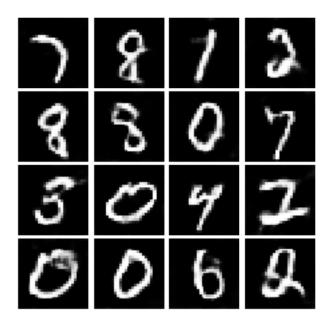
```
[]: numIter = 0
for img in images:
    print("Iter: {}".format(numIter))
    show_images(img)
    plt.show()
    numIter += 250
    print()
```

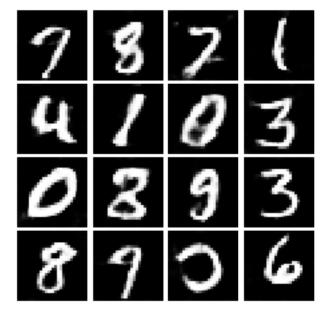


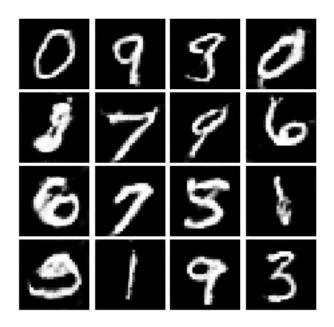


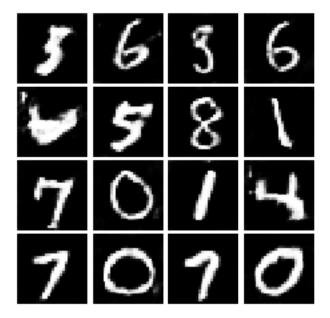












8.1 Inline Question 3

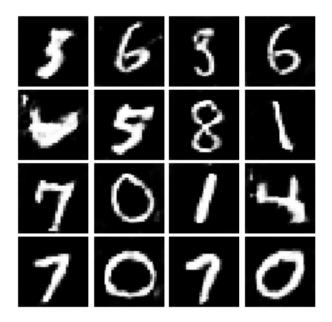
What does your final DCGAN image look like?

Answer:

Deep Convolution GAN produces clearly legible image than LSGAN, because CNN learn image features (i.e. digits) locally and hence clear representation of digits are learnt.

```
[]: # 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
		<i>x</i> ₂ -2				

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, we will never reach the optimal because of the competing objectives of minimization over x and maximization over y using gradient descent and ascent, respectively. It will keep on oscillating with a period of 6.

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:

It is not a good sign because although the generator is improving its performance owing to the decrease in the loss, the discriminator's performance is below par owing to constant high value of the loss but we want superior performance of both the generator and the discriminator for a good GAN.