Computing Quiz 2 Q3

April 26, 2024

3. MCMC to decode an encrypted text

[ ]:
```
import numpy as np
import random
from random import shuffle
import string
import math
import matplotlib.pyplot as plt
```

[ ]:
```
# Convert cipher to string
def cipher_string(cipher):
    cipher_st = ''
    for key in alphabet:
        if key in cipher:
            cipher_st = cipher_st + cipher[key]
    return cipher_st

# Use cipher to decode text
def string_cipher(in_string):
    cipher = {}
    for i in range(len(in_string)):
        cipher[list_alphabet[i]] = in_string[i]
    return cipher

# Create random cipher
def random_cipher():
    cipher = {}
    random_index = [[i] for i in range(len(alphabet))]
    shuffle(random_index)
    for i in range(len(alphabet)-1):
        cipher[list_alphabet[i]] = list_alphabet[random_index[i][0]]
    return cipher

# Encode text
def apply_cipher(text,ci):
    text = list(text)
    new_text = ''
    for char in text:
```

```
        if char.upper() in ci:
            new_text +=ci[char.upper()]
        else:
            new_text += char
    return new_text

# Counts the number of times each character appears in text
def create_single_count_dict(text):
    single_count = {}
    data = list(text.strip())
    for i in range(len(data) - 1):
        char = data[i].upper()
        if char not in alphabet_list and char != " ":
            char = " "
        if char in single_count:
            single_count[char] += 1
        else:
            single_count[char] = 1
    return single_count

# Counts the number of times a pair appears in text
def create_pair_count_dict(text):
    pair_count = {}
    data = list(text.strip())
    for i in range(len(data) - 1):
        char_1 = data[i].upper()
        char_2 = data[i + 1].upper()
        key = char_1 + char_2
        if char_1 not in alphabet_list and char_1 != " ":
            char_1 = " "
        if key in pair_count:
            pair_count[key] += 1
        else:
            pair_count[key] = 1
    return pair_count

# Create conditional prob dict
def create_pair_frequency_dict(text):
    frequency_dict = {}
    text_pair = create_pair_count_dict(text)
    text_single = create_single_count_dict(text)
    for i in range(len(list(text_pair.keys())) - 1):
        key = list(text_pair.keys())[i]
        if key[0] in text_single:
            frequency_dict[key] = text_pair[key]/text_single[key[0]]
    return frequency_dict
```

```
# Find log frequency
def create_pair_log_frequency_dict(text):
    frequency_dict = {}
    text_pair = create_pair_count_dict(text)
    text_single = create_single_count_dict(text)
    for i in range(len(list(text_pair.keys())) - 1):
        key = list(text_pair.keys())[i]
        if key[0] in text_single: #if char in text
            frequency_dict[key] = math.log(text_pair[key]) - math.
 ↪log(text_single[key[0]])
    return frequency_dict

# Find log likelihood of a given cipher
def get_cipher_log_likelihood(text, in_cipher):
    decrypted_text = apply_cipher(text, in_cipher)
    likelihood = 0
    # Loop through text pairs
    for i in range(len(decrypted_text)-1):
        char_1 = decrypted_text[i]
        char_2 = decrypted_text[i + 1]
        key = char_1 + char_2
        if key in likelihood_table: # in reference text
            likelihood = likelihood + likelihood_table[key] # adds the␣
 ↪conditional probabilities
        else: # doesn't appear in reference text
            likelihood = likelihood - 25 #decrease likelihood because this␣
 ↪pairing doesn't exist in reference
    return likelihood

# Generate proposal codebook
def generate_swap(cipher):
    pos1 = random.randint(0, len(list(cipher)) - 1)
    pos2 = random.randint(0, len(list(cipher)) - 1)
    if pos1 == pos2: # same codebook
        return generate_swap(cipher)
    else: # switch the letters in the substitution cipher
        cipher = list(cipher)
        pos1_alpha = cipher[pos1]
        pos2_alpha = cipher[pos2]
        cipher[pos1] = pos2_alpha
        cipher[pos2] = pos1_alpha
        return "".join(cipher)


def MCMC_sample_cipher(text, steps, log_likelihood):
    current_cipher_st = string.ascii_uppercase
    best_state = '' # holds the string of the best cipher
```

```
    switched = 0
    score = -1000000 #starts with a poor score because it is encoded
    for i in range(steps):
        proposed_cipher_st = generate_swap(current_cipher_st) #creates proposal␣
 ↪codebook
        # Convert ciphers to string
        current_cipher = string_cipher(current_cipher_st)
        proposed_cipher = string_cipher(proposed_cipher_st)
        # Find scores of current and proposal for acceptance
        score_current_cipher = get_cipher_log_likelihood(text, current_cipher)
        log_likelihood.append(score_current_cipher)
        score_proposed_cipher = get_cipher_log_likelihood(text, proposed_cipher)
        # Acceptance stage:
        acceptance_prob = score_proposed_cipher - score_current_cipher
        # Switch if uniform random variable is less than the acceptance prob
        if math.log(np.random.uniform(low=0,high=1,size=1)) <  acceptance_prob:
            current_cipher_st = proposed_cipher_st
            switched +=1
        # Don't switch because the current is better
        if score_current_cipher > score:
            best_state = current_cipher_st
            score = score_current_cipher
    #return best substitution (cipher that decodes best)
    return best_state, log_likelihood

# Load reference text
with open('/home/dknox/math231/Quizzes/walden.txt', 'r') as reference:
   reference_text=reference.read().replace('\n', '')

alphabet = string.ascii_uppercase
list_alphabet = list(alphabet)
alphabet_list = list_alphabet

reference_pair = create_pair_frequency_dict(reference_text)
likelihood_table = create_pair_log_frequency_dict(reference_text) # Create log␣
 ↪frequency table

# Load encoded text
directory="/home/dknox/math231/Quizzes/"
file_tag = open(directory+"encoded.txt", "r") # read in encoded message
text=file_tag.read()
file_tag.close()

# Create random cipher
random_cipher_list = list(string.ascii_uppercase)
random.shuffle(random_cipher_list)
test_cipher_st = "".join(random_cipher_list)
```

```
test_cipher = string_cipher(test_cipher_st)
inverse_test_cipher = {v: k for k, v in test_cipher.items()}
encrypted_text = apply_cipher(text,test_cipher)

# Track log-likelihood
log_likelihood = []

# Run MCMC
runs = 3000
MCMC, log_likelihood = MCMC_sample_cipher(encrypted_text,runs,log_likelihood) #␣
 ↪Motropolis-Hastings MCMC
print('The decrypted text is:')
print(apply_cipher(encrypted_text,string_cipher(MCMC)))
print('The best cipher found is:')
print(MCMC + '.')

plt.figure()
x_value = np.linspace(1,3000,3000)
plt.plot(x_value, log_likelihood)
plt.title('Log-Likelihood vs Step #')
plt.xlabel('Step')
plt.ylabel('Log-Likelihood')
plt.grid(True)
plt.show()
```

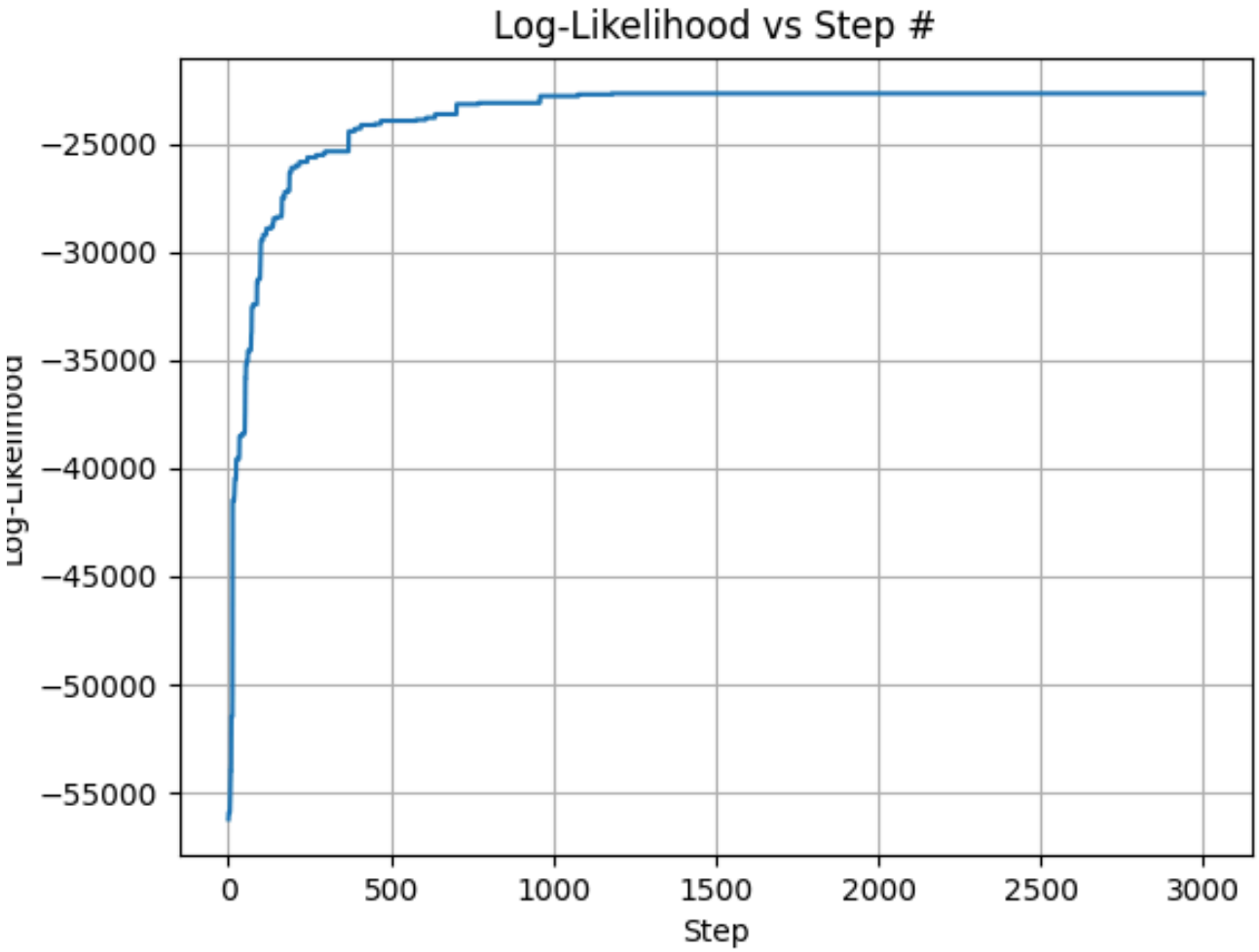
Output of code above is on the following page since it was not run locally in this notebook

The decrypted text is:
WHEN IN THE COURSE OF HUMAN EVENTS IT BECOMES NECESSARY FOR ONE PEOPLE TO DISSOLVE THE POLITICAL BANDS WHICH HAVE CONNECTED THEM WITH ANOTHER AND TO ASSUME AMONG THE POWERS OF THE EARTH THE SEPARATE AND EQUAL STATION TO WHICH THE LAWS OF NATURE AND OF NATURES GOD ENTITLE THEM A DECENT RESPECT TO THE OPINIONS OF MANKIND REQUIRES THAT THEY SHOULD DECLARE THE CAUSES WHICH IMPEL THEM TO THE SEPARATION WE HOLD THESE TRUTHS TO BE SELFEVIDENT THAT ALL MEN ARE CREATED EQUAL THAT THEY ARE ENDOWED BY THEIR CREATOR WITH CERTAIN UNALIENABLE RIGHTS THAT AMONG THESE ARE LIFE LIBERTY AND THE PURSUIT OF HAPPINESS THAT TO SECURE THESE RIGHTS GOVERNMENTS ARE INSTITUTED AMONG MEN DERIVING THEIR JUST POWERS FROM THE CONSENT OF THE GOVERNED THAT WHENEVER ANY FORM OF GOVERNMENT BECOMES DESTRUCTIVE OF THESE ENDS IT IS THE RIGHT OF THE PEOPLE TO ALTER OR TO ABOLISH IT AND TO INSTITUTE NEW GOVERNMENT LAYING ITS FOUNDATION ON SUCH PRINCIPLES AND ORGANIZING ITS POWERS IN SUCH FORM AS TO THEM SHALL SEEM MOST LIKELY TO EFFECT THEIR SAFETY AND HAPPINESS PRUDENCE INDEED WILL DICTATE THAT GOVERNMENTS LONG ESTABLISHED SHOULD NOT BE CHANGED FOR LIGHT AND TRANSIENT CAUSES AND ACCORDINGLY ALL EXPERIENCE HATH SHOWN THAT MANKIND ARE MORE DISPOSED TO SUFFER WHILE EVILS ARE SUFFERABLE THAN TO RIGHT THEMSELVES BY ABOLISHING THE FORMS TO WHICH THEY ARE ACCUSTOMED BUT WHEN A LONG TRAIN OF ABUSES AND USURPATIONS PURSUING INVARIABLY THE SAME OBJECT EVINCES A DESIGN TO REDUCE THEM UNDER ABSOLUTE DESPOTISM IT IS THEIR RIGHT IT IS THEIR DUTY TO THROW OFF SUCH GOVERNMENT AND TO PROVIDE NEW GUARDS FOR THEIR FUTURE SECURITY SUCH HAS BEEN THE PATIENT SUFFERANCE OF THESE COLONIES AND SUCH IS NOW THE NECESSITY WHICH CONSTRAINS THEM TO ALTER THEIR FORMER SYSTEMS OF GOVERNMENT THE HISTORY OF THE PRESENT KING OF GREAT BRITAIN IS A HISTORY OF REPEATED INJURIES AND USURPATIONS ALL HAVING IN DIRECT OBJECT THE ESTABLISHMENT OF AN ABSOLUTE TYRANNY OVER THESE STATES TO PROVE THIS LET FACTS BE SUBMITTED TO A CANDID WORLD HE HAS REFUSED HIS ASSENT TO LAWS THE MOST WHOLESOME AND NECESSARY FOR THE PUBLIC GOOD HE HAS FORBIDDEN HIS GOVERNORS TO PASS LAWS OF IMMEDIATE AND PRESSING IMPORTANCE UNLESS SUSPENDED IN THEIR OPERATIONS TILL HIS ASSENT SHOULD BE OBTAINED AND WHEN SO SUSPENDED HE HAS UTTERLY NEGLECTED TO ATTEND TO THEM HE HAS REFUSED TO PASS OTHER LAWS FOR THE ACCOMMODATION OF LARGE DISTRICTS OF PEOPLE UNLESS THOSE PEOPLE WOULD RELINQUISH THE RIGHT OF REPRESENTATION IN THE LEGISLATURE A RIGHT INESTIMABLE TO THEM AND FORMIDABLE TO TYRANTS ONLY HE HAS CALLED TOGETHER LEGISLATIVE BODIES AT PLACES UNUSUAL UNCOMFORTABLE AND DISTANT FROM THE DEPOSITORY OF THEIR PUBLIC RECORDS FOR THE SOLE PURPOSE OF FATIGUING THEM INTO COMPLIANCE WITH HIS MEASURES HE HAS DISSOLVED REPRESENTATIVE HOUSES REPEATEDLY FOR OPPOSING WITH MANLY FIRMNESS HIS INVASIONS ON THE RIGHTS OF THE PEOPLE HE HAS REFUSED FOR A LONG TIME AFTER SUCH DISSOLUTIONS TO CAUSE OTHERS TO BE ELECTED

WHEREBY THE LEGISLATIVE POWERS INCAPABLE OF ANNIHILATION HAVE RETURNED TO THE PEOPLE AT LARGE FOR THEIR EXERCISE THE STATE REMAINING IN THE MEANTIME EXPOSED TO ALL THE DANGERS OF INVASION FROM WITHOUT AND CONVULSIONS WITHIN HE HAS ENDEAVORED TO PREVENT THE POPULATION OF THESE STATES FOR THAT PURPOSE OBSTRUCTING THE LAWS FOR NATURALIZATION OF FOREIGNERS REFUSING TO PASS OTHERS TO ENCOURAGE THEIR MIGRATIONS HITHER AND RAISING THE CONDITIONS OF NEW APPROPRIATIONS OF LANDS HE HAS OBSTRUCTED THE ADMINISTRATION OF JUSTICE BY REFUSING HIS ASSENT TO LAWS FOR ESTABLISHING JUDICIARY POWERS HE HAS MADE JUDGES DEPENDENT ON HIS WILL ALONE FOR THE TENURE OF THEIR OFFICES AND THE AMOUNT AND PAYMENT OF THEIR SALARIES HE HAS ERECTED A MULTITUDE OF NEW OFFICES AND SENT HITHER SWARMS OF OFFICERS TO HARASS OUR PEOPLE AND EAT OUT THEIR SUBSTANCE HE HAS KEPT AMONG US IN TIMES OF PEACE STANDING ARMIES WITHOUT THE CONSENT OF OUR LEGISLATURES HE HAS AFFECTED TO RENDER THE MILITARY INDEPENDENT OF AND SUPERIOR TO THE CIVIL POWER HE HAS COMBINED WITH OTHERS TO SUBJECT US TO A JURISDICTION FOREIGN TO OUR CONSTITUTION AND UNACKNOWLEDGED BY OUR LAWS GIVING HIS ASSENT TO THEIR ACTS OF PRETENDED LEGISLATION FOR QUARTERING LARGE BODIES OF ARMED TROOPS AMONG US FOR PROTECTING THEM BY A MOCK TRIAL FROM PUNISHMENT FOR ANY MURDERS WHICH THEY SHOULD COMMIT ON THE INHABITANTS OF THESE STATES FOR CUTTING OFF OUR TRADE WITH ALL PARTS OF THE WORLD FOR IMPOSING TAXES ON US WITHOUT OUR CONSENT FOR DEPRIVING US IN MANY CASES OF THE BENEFITS OF TRIAL BY JURY FOR TRANSPORTING US BEYOND SEAS TO BE TRIED FOR PRETENDED OFFENCES FOR ABOLISHING THE FREE SYSTEM OF ENGLISH LAWS IN A NEIGHBORING PROVINCE ESTABLISHING THEREIN AN ARBITRARY GOVERNMENT AND ENLARGING ITS BOUNDARIES SO AS TO RENDER IT AT ONCE AN EXAMPLE AND FIT INSTRUMENT FOR INTRODUCING THE SAME ABSOLUTE RULE INTO THESE COLONIES FOR TAKING AWAY OUR CHARTERS ABOLISHING OUR MOST VALUABLE LAWS AND ALTERING FUNDAMENTALLY THE FORMS OF OUR GOVERNMENTS FOR SUSPENDING OUR OWN LEGISLATURES AND DECLARING THEMSELVES INVESTED WITH POWER TO LEGISLATE FOR US IN ALL CASES WHATSOEVER HE HAS ABDICATED GOVERNMENT HERE BY DECLARING US OUT OF HIS PROTECTION AND WAGING WAR AGAINST US HE HAS PLUNDERED OUR SEAS RAVAGED OUR COASTS BURNT OUR TOWNS AND DESTROYED THE LIVES OF OUR PEOPLE HE IS AT THIS TIME TRANSPORTING LARGE ARMIES OF FOREIGN MERCENARIES TO COMPLETE THE WORKS OF DEATH DESOLATION AND TYRANNY ALREADY BEGUN WITH CIRCUMSTANCES OF CRUELTY AND PERFIDY SCARCELY PARALLELED IN THE MOST BARBAROUS AGES AND TOTALLY UNWORTHY THE HEAD OF A CIVILIZED NATION HE HAS CONSTRAINED OUR FELLOWCITIZENS TAKEN CAPTIVE ON THE HIGH SEAS TO BEAR ARMS AGAINST THEIR COUNTRY TO BECOME THE EXECUTIONERS OF THEIR FRIENDS AND BRETHREN OR TO FALL THEMSELVES BY THEIR HANDS HE HAS EXCITED DOMESTIC INSURRECTIONS AMONGST US AND HAS ENDEAVORED TO BRING ON THE INHABITANTS OF OUR FRONTIERS THE MERCILESS INDIAN SAVAGES WHOSE KNOWN RULE OF WARFARE IS AN UNDISTINGUISHED DESTRUCTION OF ALL AGES

SEXES AND CONDITIONS IN EVERY STAGE OF THESE OPPRESSIONS WE HAVE PETITIONED FOR REDRESS IN THE MOST HUMBLE TERMS OUR REPEATED PETITIONS HAVE BEEN ANSWERED ONLY BY REPEATED INJURY A PRINCE WHOSE CHARACTER IS THUS MARKED BY EVERY ACT WHICH MAY DEFINE A TYRANT IS UNFIT TO BE THE RULER OF A FREE PEOPLE NOR HAVE WE BEEN WANTING IN ATTENTIONS TO OUR BRITISH BRETHREN WE HAVE WARNED THEM FROM TIME TO TIME OF ATTEMPTS BY THEIR LEGISLATURE TO EXTEND AN UNWARRANTABLE JURISDICTION OVER US WE HAVE REMINDED THEM OF THE CIRCUMSTANCES OF OUR EMIGRATION AND SETTLEMENT HERE WE HAVE APPEALED TO THEIR NATIVE JUSTICE AND MAGNANIMITY AND WE HAVE CONJURED THEM BY THE TIES OF OUR COMMON KINDRED TO DISAVOW THESE USURPATIONS WHICH WOULD INEVITABLY INTERRUPT OUR CONNECTIONS AND CORRESPONDENCE THEY TOO HAVE BEEN DEAF TO THE VOICE OF JUSTICE AND OF CONSANGUINITY WE MUST THEREFORE ACQUIESCE IN THE NECESSITY WHICH DENOUNCES OUR SEPARATION AND HOLD THEM AS WE HOLD THE REST OF MANKIND ENEMIES IN WAR IN PEACE FRIENDS WE THEREFORE THE REPRESENTATIVES OF THE UNITED STATES OF AMERICA IN GENERAL CONGRESS ASSEMBLED APPEALING TO THE SUPREME JUDGE OF THE WORLD FOR THE RECTITUDE OF OUR INTENTIONS DO IN THE NAME AND BY THE AUTHORITY OF THE GOOD PEOPLE OF THESE COLONIES SOLEMNLY PUBLISH AND DECLARE THAT THESE UNITED COLONIES ARE AND OF RIGHT OUGHT TO BE FREE AND INDEPENDENT STATES THAT THEY ARE ABSOLVED FROM ALL ALLEGIANCE TO THE BRITISH CROWN AND THAT ALL POLITICAL CONNECTION BETWEEN THEM AND THE STATE OF GREAT BRITAIN IS AND OUGHT TO BE TOTALLY DISSOLVED AND THAT AS FREE AND INDEPENDENT STATES THEY HAVE FULL POWER TO LEVY WAR CONCLUDE PEACE CONTRACT ALLIANCES ESTABLISH COMMERCE AND TO DO ALL OTHER ACTS AND THINGS WHICH INDEPENDENT STATES MAY OF RIGHT DO AND FOR THE SUPPORT OF THIS DECLARATION WITH A FIRM RELIANCE ON THE PROTECTION OF DIVINE PROVIDENCE WE MUTUALLY PLEDGE TO EACH OTHER OUR LIVES OUR FORTUNES AND OUR SACRED HONOUR

The best cipher found is:
KXZWOBAFPYHTDCEGQVRMUNILSJ.


Log-Likelihood vs Step #
−25000
−30000
−35000
−40000
−45000
−50000
−55000
Log-Likelihood
0
500
1000
1500
2000
2500
3000
Step