Untitled2

April 27, 2022

[2]:
```
import numpy as np
from sage.matrix.berlekamp_massey import berlekamp_massey as bm
import matplotlib.pyplot as plt
```

[3]:
```
p = 4999  # 13-bit prime
F = GF(p, 'zeta', modulus='primitive')
zeta = F.gen()    # value of zeta
k = 2^(int(np.log2(p)) + 1)
ks = [2*k]
zeta
```

[3]: 3

[4]:
```
num_elems = 0  # number of new primitive elements found
elems = [zeta]
while (num_elems<2):
    power_prime = np.random.randint(100, p-1)
    new_elem = zeta^power_prime     # generating a new element of the␣
 ↪multiplicative group
    if new_elem.is_primitive_root():  # checking if the new element is a␣
 ↪primitive root
        num_elems = num_elems + 1
        elems.append(new_elem)
elems
```

[4]: [3, 4137, 4364]

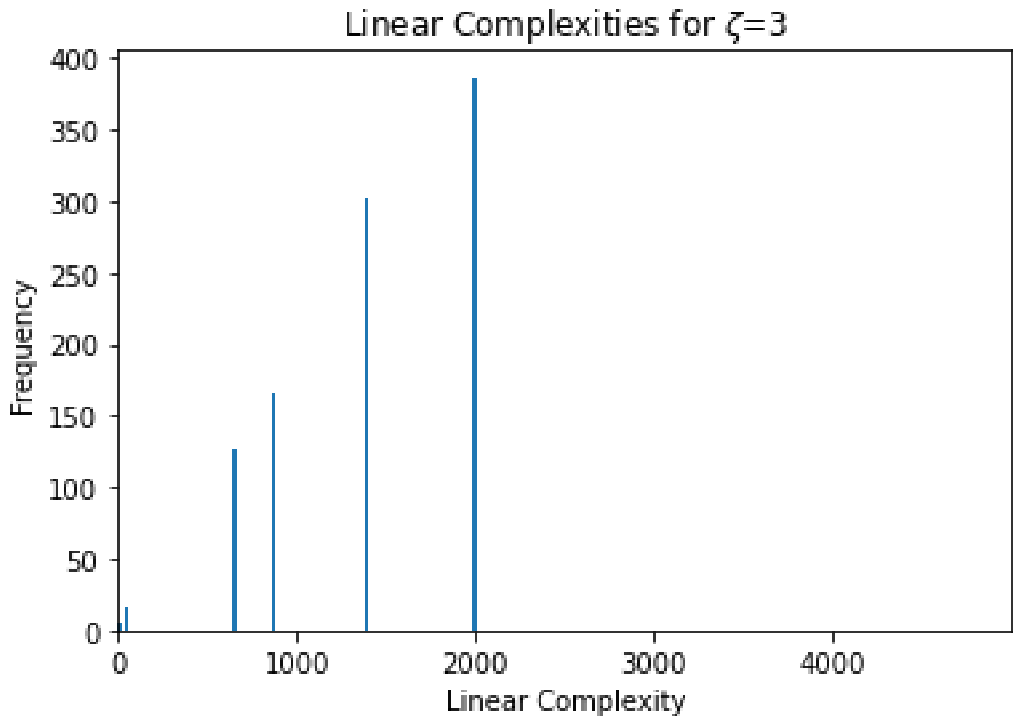
[5]:
```
complexities = np.zeros((3, 1000)) # initializing the array to store linear␣
 ↪complexity values
points = np.random.randint(0, p, (3, 1000))
```

[6]:
```
for i_zeta in range(3):
    zeta_iteration = elems[i_zeta]
    for i_point in range(1000):
        seq = [0]*ks[0]
        point = points[i_zeta, i_point]
        seq[0] = zeta^point
        if (i_point%100 == 0):
```

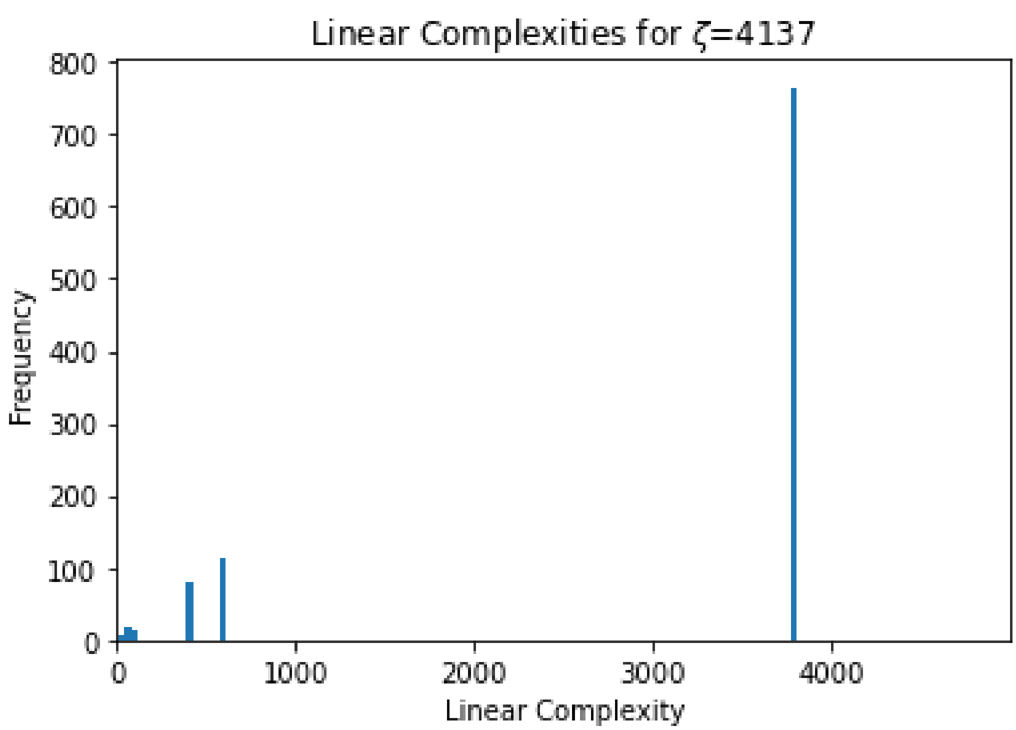
```
            print(i_zeta, i_point)  # print the value of i_zeta and i_point
        for i in range(1, ks[0]):
            seq[i] = zeta_iteration^seq[i-1]
        minimal_poly = bm(seq)          # minimal polynomial
        lin_complexity = int(minimal_poly.degree())  # linear complexity
        complexities[i_zeta, i_point] = lin_complexity
```

```
0 0
0 100
0 200
0 300
0 400
0 500
0 600
0 700
0 800
0 900
1 0
1 100
1 200
1 300
1 400
1 500
1 600
1 700
1 800
1 900
2 0
2 100
2 200
2 300
2 400
2 500
2 600
2 700
2 800
2 900
```

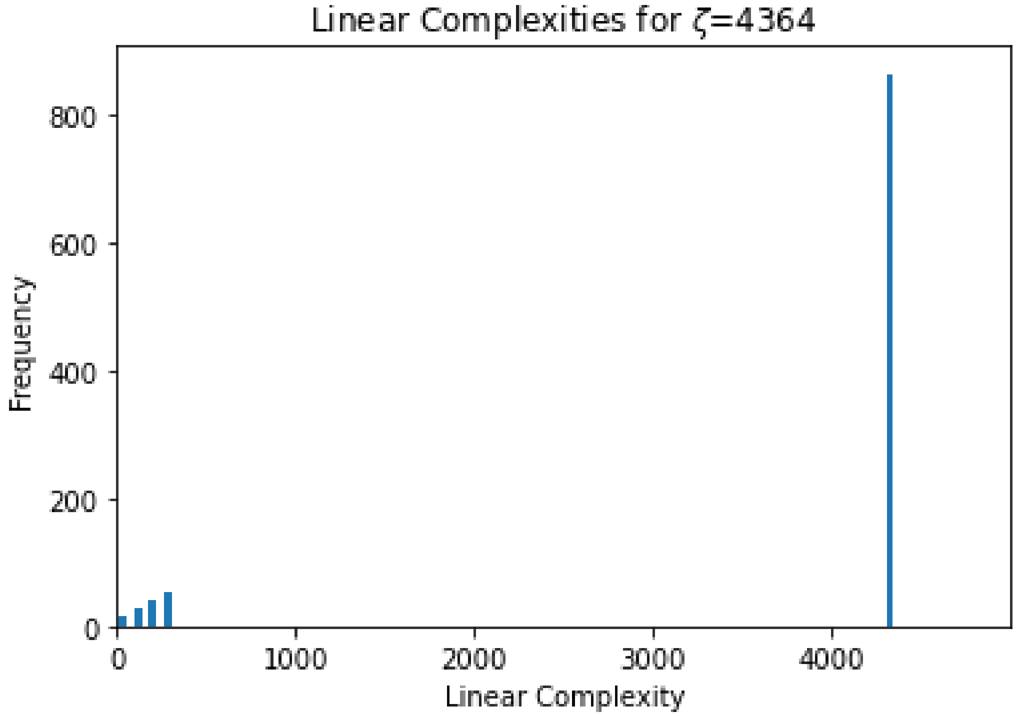
[7]:
```
for i_zeta in range(3):
    plt.figure
    plt.hist(complexities[i_zeta], bins=100, rwidth = 4000)
    plt.xlabel('Linear Complexity')
    plt.ylabel('Frequency')
    plt.title(r"Linear Complexities for $\zeta$=" + str(elems[i_zeta]))
    plt.xlim([0, p])
    plt.show()
```



Linear Complexities for ζ=3
Frequency
0
50
100
150
200
250
300
350
400
0
1000
2000
3000
4000
Linear Complexity



Linear Complexities for ζ=4137
Frequency
0
100
200
300
400
500
600
700
800
0
1000
2000
3000
4000
Linear Complexity



Linear Complexities for ζ=4364
Frequency
Linear Complexity
800
600
400
200
0
0
1000
2000
3000
4000