レポートタイトル

学科　学籍番号　氏名

2023 年?? 月?? 日

1　はじめに

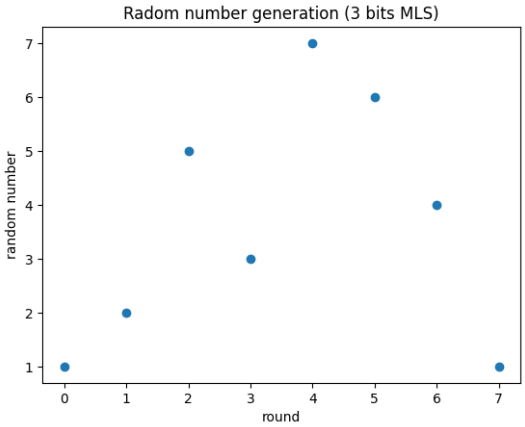


図1　図の貼り方

2　実験 1-5

2.1　目的

これからランダムウォーク実験を行うにあたって、ランダムな数を生成することが必要であるが、パソコンはランダムな数を生成できない。そこでコンピューター上では数式を用いて擬似乱数列ー乱数のように思えるが、初期状態が決定すれば未来の数列が決定してしまうので真にランダムではない数列ーを生成するのだが、このとき C 言語における srand(time(NULL)) や、python における rand() のようないわゆる組み込み関数を用いずに擬似乱数列を生成するのが今回の実験の目的である。

2.2　理論

擬似乱数列の生成を行う。このとき LFSR 法を用いた。LFSR とは次の数を直前の数に基づきシフト演算を使って漸化式的に決定した数列 (次の数が直前の数の線形写像になっているシフトレジスタ) のことで、このとき直前の数から次の数を求める漸化式をうまく設定することで、全ビットが 0 という状態以外のすべての

取る整数列を作ることができることが分かっており、これを最長 LFSR と呼ぶ。今回はこの最長 LSFR を作ることで擬似乱数列を生成した。

ここで、最長 LSFR を生成できる漸化式を次に示す。このとき、下に示す漸化式は 2 進数である

$$a_{n+1} = b_{n+1} + c_{n+1}\&1$$

但し

$$b_{n+1} = (a_n << 1)\&(10^{bit} - 1)$$

(しつこいようだが、10 はいわゆる 2 進数の 10 であり、つまり 10 進数における 2 である)

$$c_{n+1} = \sum_k (a_n >> k)$$

このとき、c_{n+1} を以下のように設定することで、最長 LFSR を計算することができる:

n	XNOR from	n	XNOR from	n	XNOR from	n	XNOR from
3	3,2	45	45,44,42,41	87	87,74	129	129,124
4	4,3	46	46,45,26,25	88	88,87,17,16	130	130,127
5	5,3	47	47,42	89	89,51	131	131,130,84,83
6	6,5	48	48,47,21,20	90	90,89,72,71	132	132,103
7	7,6	49	49,40	91	91,90,8,7	133	133,132,82,81
8	8,6,5,4	50	50,49,24,23	92	92,91,80,79	134	134,77
9	9,5	51	51,50,36,35	93	93,91	135	135,124
10	10,7	52	52,49	94	94,73	136	136,135,11,10
11	11,9	53	53,52,38,37	95	95,84	137	137,116
12	12,6,4,1	54	54,53,18,17	96	96,94,49,47	138	138,137,131,130
13	13,4,3,1	55	55,31	97	97,91	139	139,136,134,131
14	14,5,3,1	56	56,55,35,34	98	98,87	140	140,111
15	15,14	57	57,50	99	99,97,54,52	141	141,140,110,109
16	16,15,13,4	58	58,39	100	100,63	142	142,121
17	17,14	59	59,58,38,37	101	101,100,95,94	143	143,142,123,122
18	18,11	60	60,59	102	102,101,36,35	144	144,143,75,74
19	19,6,2,1	61	61,60,46,45	103	103,94	145	145,93
20	20,17	62	62,61,6,5	104	104,103,94,93	146	146,145,87,86
21	21,19	63	63,62	105	105,89	147	147,146,110,109
22	22,21	64	64,63,61,60	106	106,91	148	148,121
23	23,18	65	65,47	107	107,105,44,42	149	149,148,40,39
24	24,23,22,17	66	66,65,57,56	108	108,77	150	150,97
25	25,22	67	67,66,58,57	109	109,108,103,102	151	151,148
26	26,6,2,1	68	68,59	110	110,109,98,97	152	152,151,87,86
27	27,5,2,1	69	69,67,42,40	111	111,101	153	153,152
28	28,25	70	70,69,55,54	112	112,110,69,67	154	154,152,27,25
29	29,27	71	71,65	113	113,104	155	155,154,124,123
30	30,6,4,1	72	72,66,25,19	114	114,113,33,32	156	156,155,41,40
31	31,28	73	73,48	115	115,114,101,100	157	157,156,131,130
32	32,22,2,1	74	74,73,59,58	116	116,115,46,45	158	158,157,132,131
33	33,20	75	75,74,65,64	117	117,115,99,97	159	159,128
34	34,27,2,1	76	76,75,41,40	118	118,85	160	160,159,142,141
35	35,33	77	77,76,47,46	119	119,111	161	161,143
36	36,25	78	78,77,59,58	120	120,113,9,2	162	162,161,75,74
37	37,5,4,3,2,1	79	79,70	121	121,103	163	163,162,104,103
38	38,6,5,1	80	80,79,43,42	122	122,121,63,62	164	164,163,151,150
39	39,35	81	81,77	123	123,121	165	165,164,135,134
40	40,38,21,19	82	82,79,47,44	124	124,87	166	166,165,128,127
41	41,38	83	83,82,38,37	125	125,124,18,17	167	167,161
42	42,41,20,19	84	84,71	126	126,125,90,89	168	168,166,153,151
43	43,42,38,37	85	85,84,58,57	127	127,126		
44	44,43,18,17	86	86,85,74,73	128	128,126,101,99		

但し、表中の n を bit、XNOR from を k と読み替えて漸化式に適用すること

2.3 実験方法

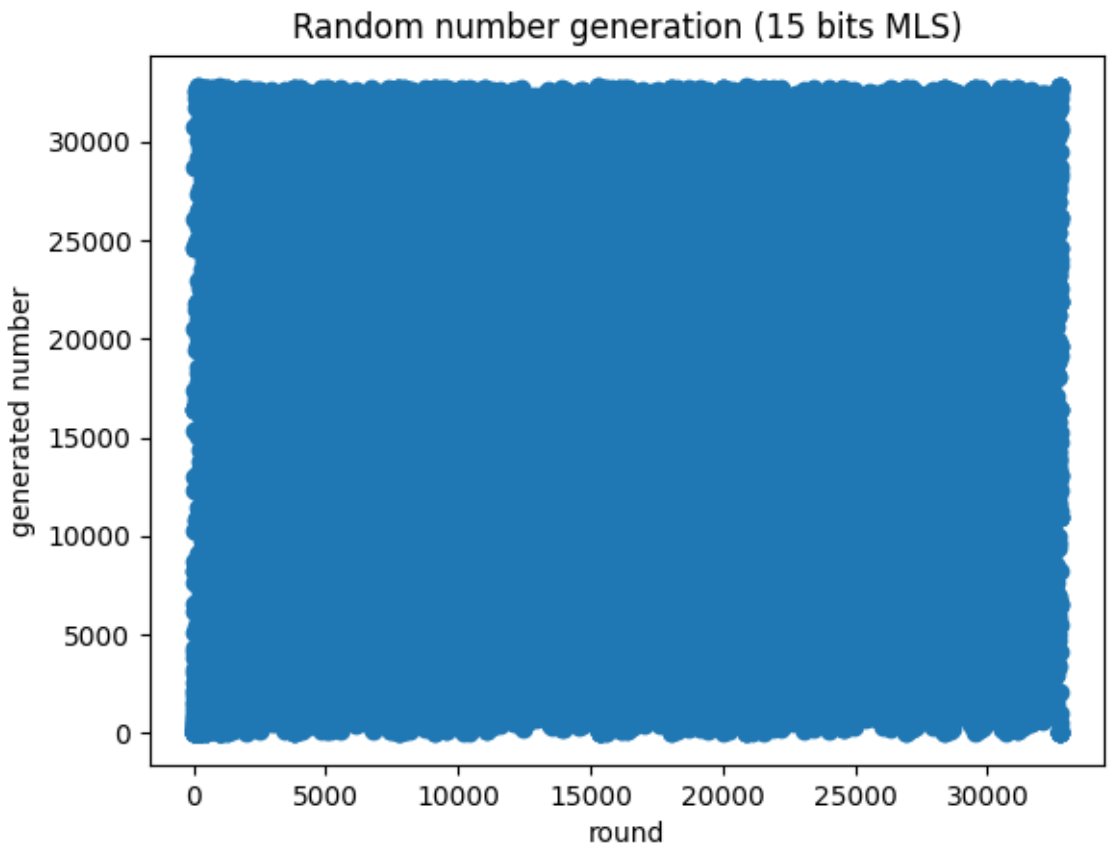
実験に用いた python プログラムを次に示す

Listing 1　キャプション 2

```
import matplotlib.pyplot as plt

feedbacks = [[],[],[],[3,2],[4,3],
             [5,3],[6,5],[7,6],[8,6,5,4],[9,5],
             [10,7],[11,9],[12,11,10,4],[13,12,11,8],[14,13,12,2],
             [15,14],[16,14,13,11],[17,14],[18,11],[19,18,17,14],
             [20,17],[21,19],[22,21],[23,18],[24,23,22,17]
            ]

def calculate_lfsr(initNumber, bits):
    num = initNumber # initial number
    maxrounds = 2**bits
    formater = "0" + str(bits) + "b"

    rands = []

    for i in range(maxrounds):
        # print(num, "(" , format(num, formater), ")")
        rands.append(num)

        a = (num << 1) & (maxrounds-1)

        #seems both acceptable, but b=1 would become more complex and difficult to estimate
        # b = 1
        b = 0

        for j in range(len(feedbacks[bits])):
            target = feedbacks[bits][j] - 1
            b = ((b & 1) ^ (num >> target) & 1) & 1

        num = a+(b&1)

    return rands

def plot_results_a(rands, bits):
    nums = range(2**bits)
    title_str = "Random number generation ({:d} bits MLS)".format(bits)
    plt.scatter(nums, rands)
    plt.title(title_str)
    plt.xlabel("round")
    plt.ylabel("generated number")
    plt.show()

def plot_results_b(rands, bits):
    title_str = "Random number generation ({:d} bits MLS)".format(bits)
    plt.figure()
    plt.hist(rands, bins=2**bits, range=[0,2**bits])
    plt.title(title_str)
    plt.xlabel("random_number")
    plt.ylabel("counts/bin")
    plt.show()

def main():
    init = 3 # change variants here
    bits = 9 # change variants here
    # this program can calculate from 3 bits to 24 bits, but calculating 24 bits never finishes ! (due to
        the amount of calculation)
    local_rands = calculate_lfsr(init, bits)
    plot_results_a(local_rands, bits)
    plot_results_b(local_rands, bits)

if __name__ == "__main__":
    main()
```

2.4 実験結果

このプログラムを 15bit で実行した結果を次に示す



ここに示したヒストグラムのように、初期値である 3 (ソースコード 1.py の 54 行目で指定した) を除いた全ての数が 1 から 2^{15} まで 1 回ずつのみ現れ、3 のみ 2 回現れている。

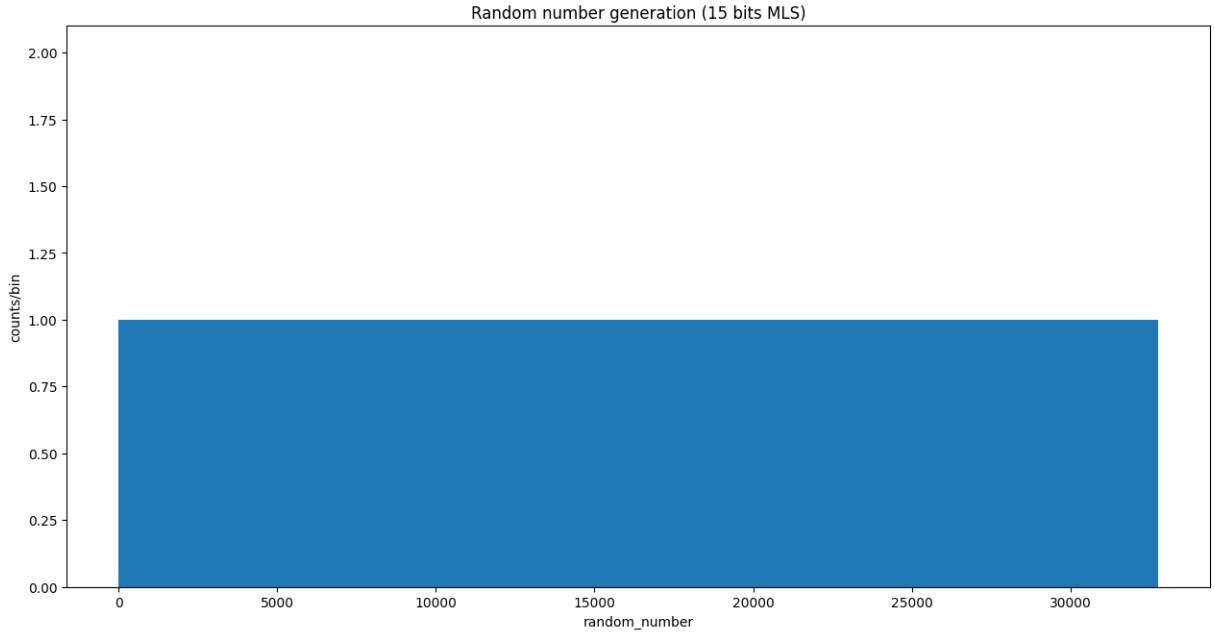
3 実験 2-1

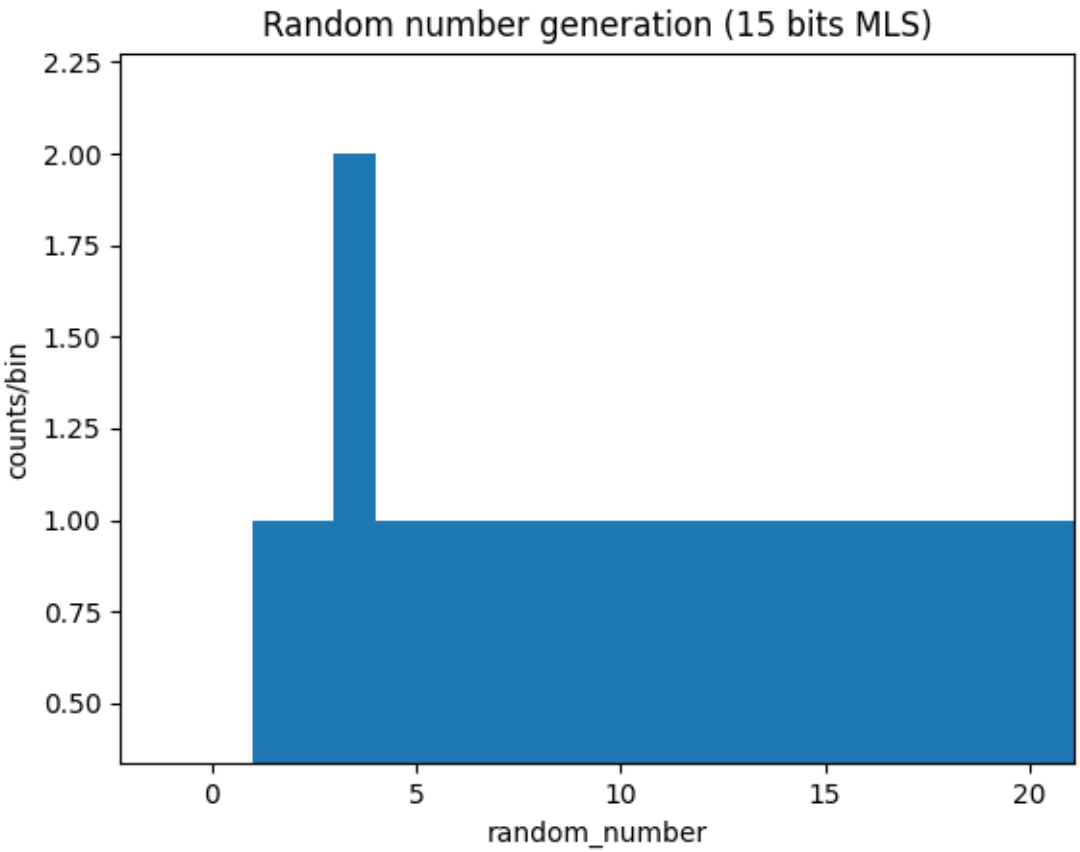
3.1 目的

3.2 理論

3.3 実験方法

3.4 実験結果


Random number generation (15 bits MLS)
counts/bin
random_number
0.00
0.25
0.50
0.75
1.00
1.25
1.50
1.75
2.00
0
5000
10000
15000
20000
25000
30000


Random number generation (15 bits MLS)
2.25
2.00
1.75
1.50
1.25
1.00
0.75
0.50
counts/bin
0
5
10
15
20
random_number