

```

1 import time
2 import matplotlib.pyplot as plt # Adicionado para gerar o gráfico
3
4 def lfsr_galois(bits):
5     # Estado inicial com um número grande (dependendo do número de bits)
6     estado_inicial = 0xACE1
7     lfsr = estado_inicial
8     periodo = 0
9     numero_gerado = 0
10
11     # Gerar o número pseudo-aleatório com o tamanho desejado
12     for i in range(bits):
13         lsb = lfsr & 1 # Obtém o bit menos significativo (bit de saída)
14         lfsr >>= 1      # Desloca o registrador para a direita
15
16         if lsb == 1:    # Se o bit de saída for 1
17             lfsr ^= 0xB400 # Aplica a máscara de realimentação (tap positions)
18
19         # Adiciona o bit gerado ao número final
20         numero_gerado = (numero_gerado << 1) | lsb
21
22     return numero_gerado
23
24 # Função para medir o tempo de execução
25 def medir_tempo_lfsr(bits, tentativas=10):
26     tempos = []
27     for _ in range(tentativas):
28         inicio = time.time()
29         lfsr_galois(bits)
30         fim = time.time()
31         tempos.append(fim - inicio)
32
33     tempo_medio = sum(tempos) / len(tempos)
34     return tempo_medio
35
36 # Testando para diferentes tamanhos de números
37 tamanhos = [40, 56, 80, 128, 168, 224, 256]
38 resultados = []
39
40 for tamanho in tamanhos:
41     tempo_medio = medir_tempo_lfsr(tamanho)
42     resultados.append((tamanho, tempo_medio))
43
44 # Exibir os resultados em uma tabela
45 print("Tabela de Resultados LFSR (configuração Galois)")
46 print("Tamanho do Número (bits) | Tempo Médio (segundos)")
47 for tamanho, tempo in resultados:
48     print(f"{tamanho} | {tempo:.6f} segundos")
49
50 ##### Explicação do Código #####
51
52 # Este código implementa um Registrador de Deslocamento com Realimentação Linear
53 # (LFSR) utilizando a configuração Galois, capaz de gerar números pseudo-aleatórios de
54 # tamanhos variados.
55
56 ### Valor inicial (estado_inicial = 0xACE1) ###
57 # O registrador é inicializado com o valor hexadecimal 0xACE1, equivalente a 44257 em
58 # decimal e 1010110011100001 em binário. Este valor deve ser diferente de zero para
59 # garantir que o LFSR não entre em um estado estático.

```

```

57 ### Máscara de realimentação (feedback mask = 0xB400) ###
58 # A máscara 0xB400 determina as posições dos bits (taps) que serão utilizadas no
    processo de realimentação. Essa escolha de máscara é típica para LFSRs de 16 bits,
    garantindo boas propriedades pseudo-aleatórias.
59
60 ### Processo de geração ###
61 # A cada iteração, o bit menos significativo (LSB) é extraído.
62 # O registrador é deslocado uma posição para a direita.
63 # Caso o bit de saída seja 1, a máscara de realimentação é aplicada via operação XOR.
64 # O bit gerado é adicionado à esquerda do número pseudo-aleatório final
    (numero_gerado).
65
66 ### Função de medição de tempo ###
67 # A função medir_tempo_lfsr avalia o tempo médio necessário para gerar números de
    diferentes tamanhos em bits. Para cada tamanho, são realizadas 10 execuções para
    calcular o tempo médio de geração.
68
69 ### Tamanhos testados ###
70 # O algoritmo foi testado para números de 40, 56, 80, 128, 168, 224 e 256 bits.
    Tamanhos superiores (como 512, 1024, 2048 e 4096 bits) não foram incluídos devido à
    limitação da largura do estado do LFSR implementado (16 bits), o que impossibilita
    gerar sequências suficientemente longas sem repetição ou colapsos.
71
72 ##### Referências Algoritmo #####
73 # Adapted from:
74 # https://en.wikipedia.org/wiki/Linear-feedback\_shift\_register
75 # All credits to the authors.
76
77 ##### Geração de Gráfico #####
78 # Visualização da relação entre o tamanho do número (bits) e o tempo médio de
    execução.
79
80 # Extraíndo dados para o gráfico
81 tamanhos_bits = [r[0] for r in resultados]
82 tempos_execucao = [r[1] for r in resultados]
83
84 # Criando o gráfico
85 plt.figure(figsize=(10,6))
86 plt.plot(tamanhos_bits, tempos_execucao, marker='o', linestyle='-', color='g')
87 plt.title('Tempo de Execução para Geração com LFSR (Configuração Galois)')
88 plt.xlabel('Tamanho do Número (bits)')
89 plt.ylabel('Tempo Médio de Execução (segundos)')
90 plt.grid(True)
91 plt.xticks(tamanhos_bits)
92 plt.tight_layout()
93 plt.show()
94

```