Exercício
LFSR em Assembly

- **Pesquise sobre a geração de pseudos-aleatórios com registrador de deslocamento.**
  - **Na literatura especializada essa abordagem é conhecida como linear feedback shift register (LFSR)**
  - **Implemente um gerador baseado em registrador de deslocamento de 16 bits.**
    - **a) Nesse módulo, use programa Assembly NASM**
    - **b) Alternativamente, implemente um programa em C**
  - **Gere 64k pseudos-aleatórios (0..65535)**
    - **Divida-os em 64 intervalos e calcule a freqüência em cada.**
      - **Aplique o teste chi-quadrado e verifiquem se de fato os números são aleatórios ou não, ao nível de significância de 5%.**
        - **Nesse módulo, use linguagem C.**
  - Compare os tempos de execução em C e em ASM

LFSR em Assembly
Documentação de programa

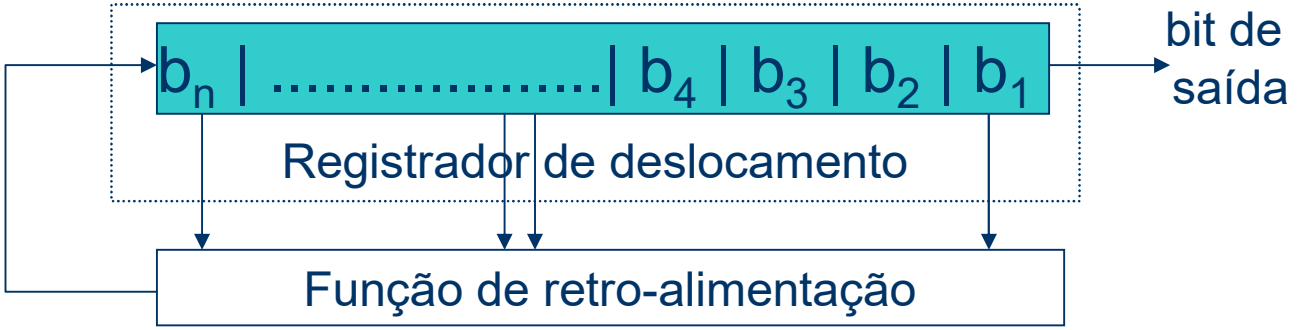
- Divida os 64k números em cada algoritmo em 64 classes, a primeira de (0, 1k), etc. Para cada classe calcule a freqüência observada, fo, e a esperada, fe (se os números seguissem a distribuição uniforme).

  $\text{chi-quadrado}_{k-1,\alpha} = \sum_k (fo_k - fe_k)^2 \ / \ fe_k$

  - A semente inicial não pode ser zero
- O trabalho é em grupo, o mesmo do exercício de C. Use o padrão C ISO. Entregue o código fonte e o código executável. Informe qual foi a semente que utilizou. O programa deve emitir um relatório com as freqüências observadas e esperadas e o valor da estatística do chi-quadrado.
- Documentação requerida: número do grupo, matriculas e nomes dos componentes, nome do programa, função do programa e descrição das principais estruturas de dados utilizadas. Se o programa tiver módulos, apresente também um diagrama mostrando o relacionamento entre eles.
- Os nomes dos arquivos do programa devem iniciar com o número do grupo, traço, dois dígitos seqüenciais indicando o número do programa (nesse caso deve ser 02), traço, mnemônico para indicar a função do programa.

Técnica de Pesos Adaptativos de Operadores LFSR de n Bits

- **Estrutura geral**



  - **Período**
    - **Máximo 2^n-1.**
    - **Depende da função de retro-alimentação e do valor inicial (que deve ser não nulo)**

A concatenação de n bits de saída gera um número pseudo-aleatório.

Técnica de Pesos Adaptativos de Operadores LFSR de n Bits

- **Função de retro-alimentação**

  XOR – representa um polinômio com coeficientes dados pela seqüência de captura (TAP).

- **Período**
  - Máximo se as posições de captura representam um polinômio primitivo módulo 2, isto é, as posições do LFSR com $b_i = 1$ apenas nas posições de TAP representam esse polinômio.
  - Exemplo de LFSR de 32 bits

    TAP = (32, 7, 6, 2)

    Representa o polinômio $p(x) = x^{32} \oplus x^7 \oplus x^6 \oplus x^2 \oplus 1$, com período de $2^{32} - 1$ (máximo).