PCS 3115 – Sistemas Digitais I

Circuitos Sequenciais:
Registradores De Deslocamento

EAD – Ensino A Distância

Parte II:
Linear Feedback Shift Registers – LFSRs.

Aula: 23 – Data: 10/06 (Q)

Prof. Dr. Marco Túlio Carvalho de Andrade

versão: 2.0 (Maio/2020)

Linear Feedback Shift Register – LFSR

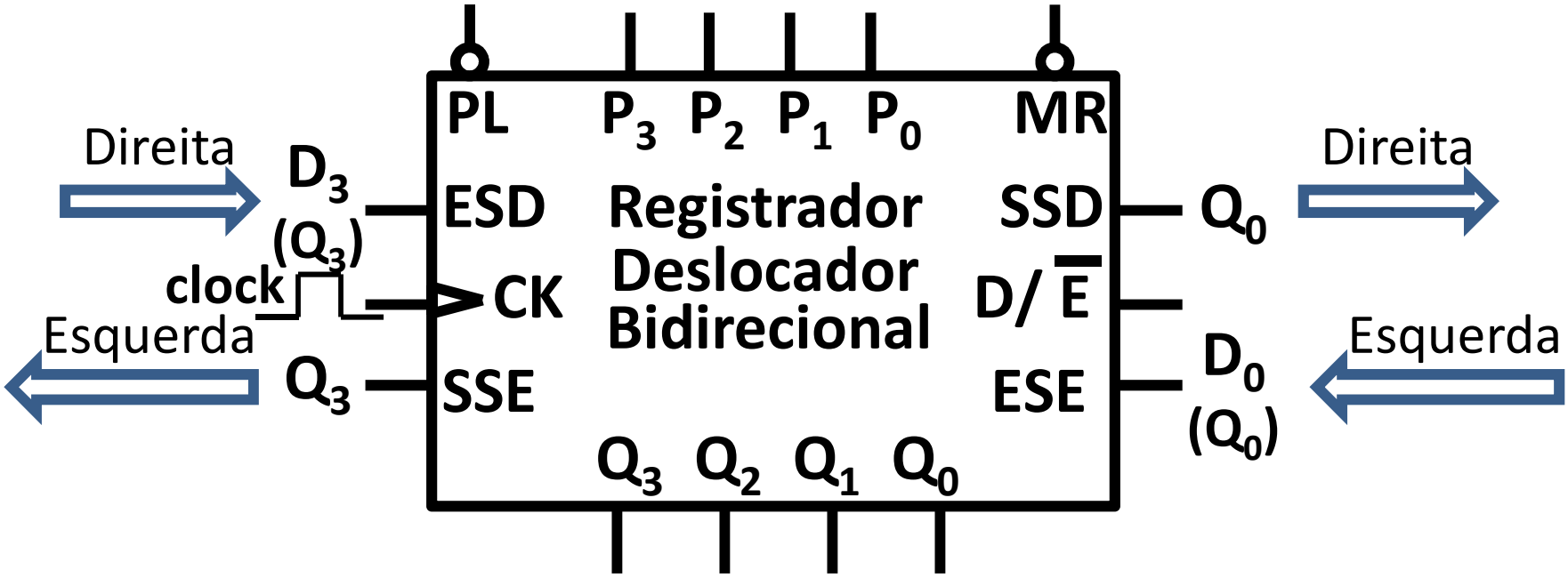
- *Linear Feedback Shift Register* (LFSR) – Um LFSR é um **Registrador com Realimentação Linear**, ou seja, realimenta uma Função Linear das saídas para a Entrada Série.
- Sabe-se da Teoria de Corpos [Evariste Galois – 1.832] que quando a função de realimentação é uma Função Booleana que só utiliza operadores OU-EXCLUSIVO, se a função for escolhida de maneira apropriada, o contador LFSR resultante terá uma sequência principal de $2^n - 1$ Estados (onde n = número de Flip-Flop's).

Linear Feedback Shift Register – LFSR

- Teoria de Corpos – Qualquer que seja n, existe pelo menos uma equação de realimentação linear que faz o contador passar por uma sequência de $2^n - 1$ (sequência de máximo comprimento) estados diferentes de ZERO, antes de repetir algum Estado.
- Aplicações – Códigos para transmissão de dados, criptografia, geração de sequências pseudo-aleatórias semelhante a um embaralhamento das palavras de código (*Scrambler*), detecção de erros na recepção de códigos.

Linear Feedback Shift Register – Convenções

- Diagrama do Bloco Básico genérico do registrador deslocador a ser utilizado:



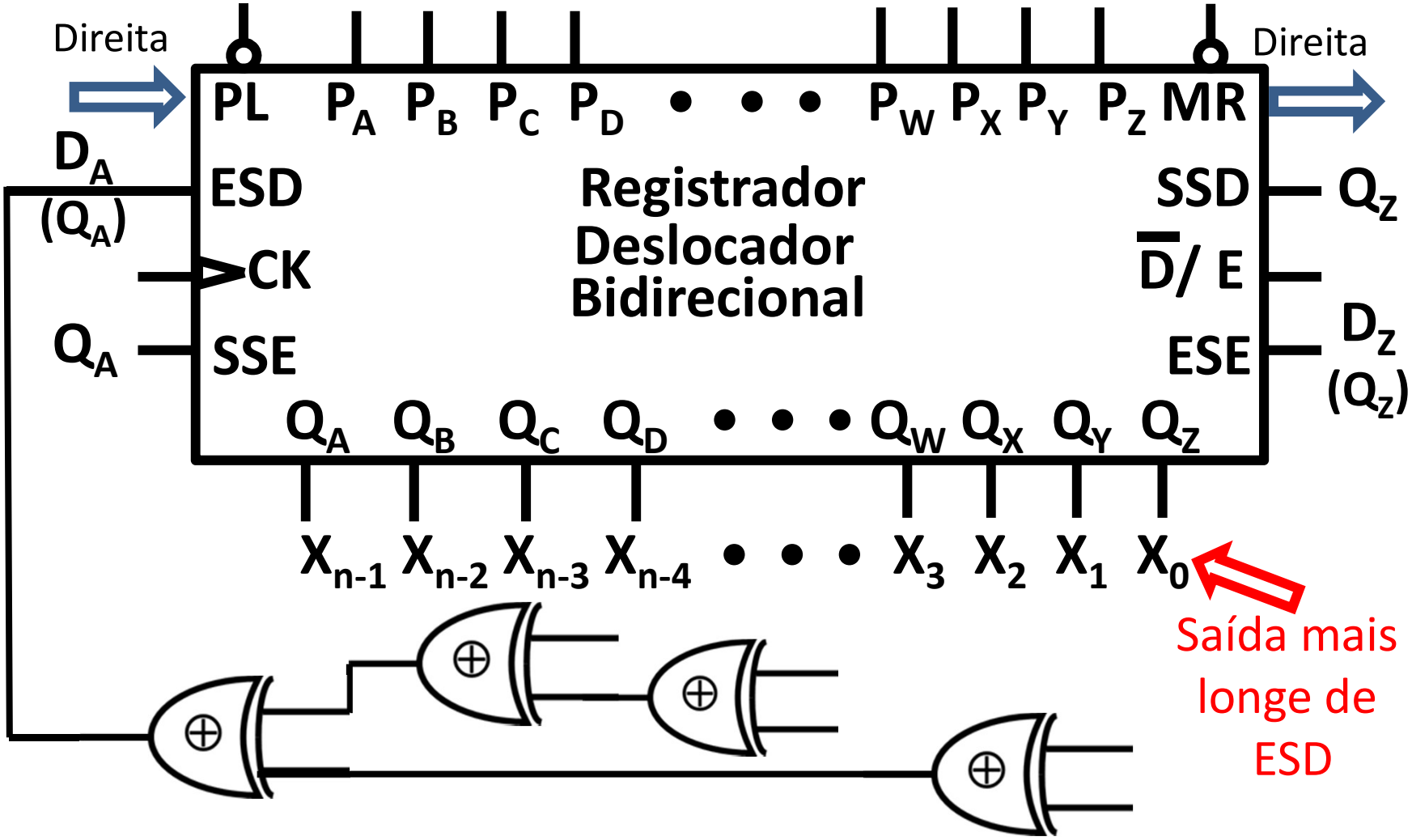
Linear Feedback Shift Register – LFSR

- *Linear Feedback Shift Register* (LFSR) – Funções lineares (só usam "X-OR") com $2^n - 1$ estados na única sequência principal. Onde: "n" é o número de Flip-Flops e "⊕" a operação "X-OR".

n	Função	n	Função
2:	$X_2 = X_1 \oplus X_0$	6:	$X_6 = X_1 \oplus X_0$
3:	$X_3 = X_1 \oplus X_0$	7:	$X_7 = X_3 \oplus X_0$
4:	$X_4 = X_1 \oplus X_0$	8:	$X_8 = X_4 \oplus X_3 \oplus X_2 \oplus X_0$
5:	$X_5 = X_2 \oplus X_0$	12:	$X_{12} = X_6 \oplus X_4 \oplus X_1 \oplus X_0$

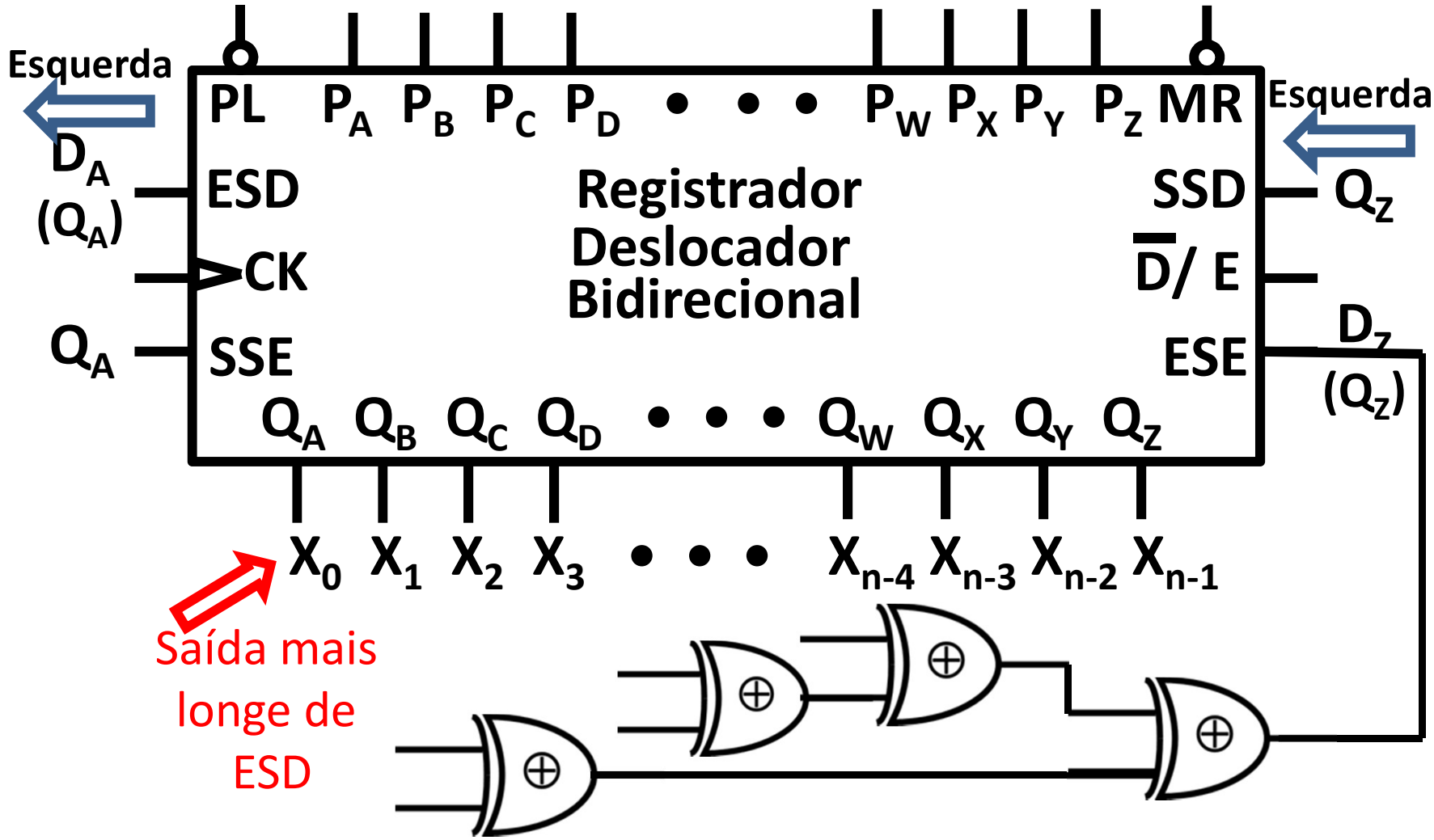
Linear Feedback Shift Register – Convenções

- Estrutura de um LFSR de n bits, genérico:



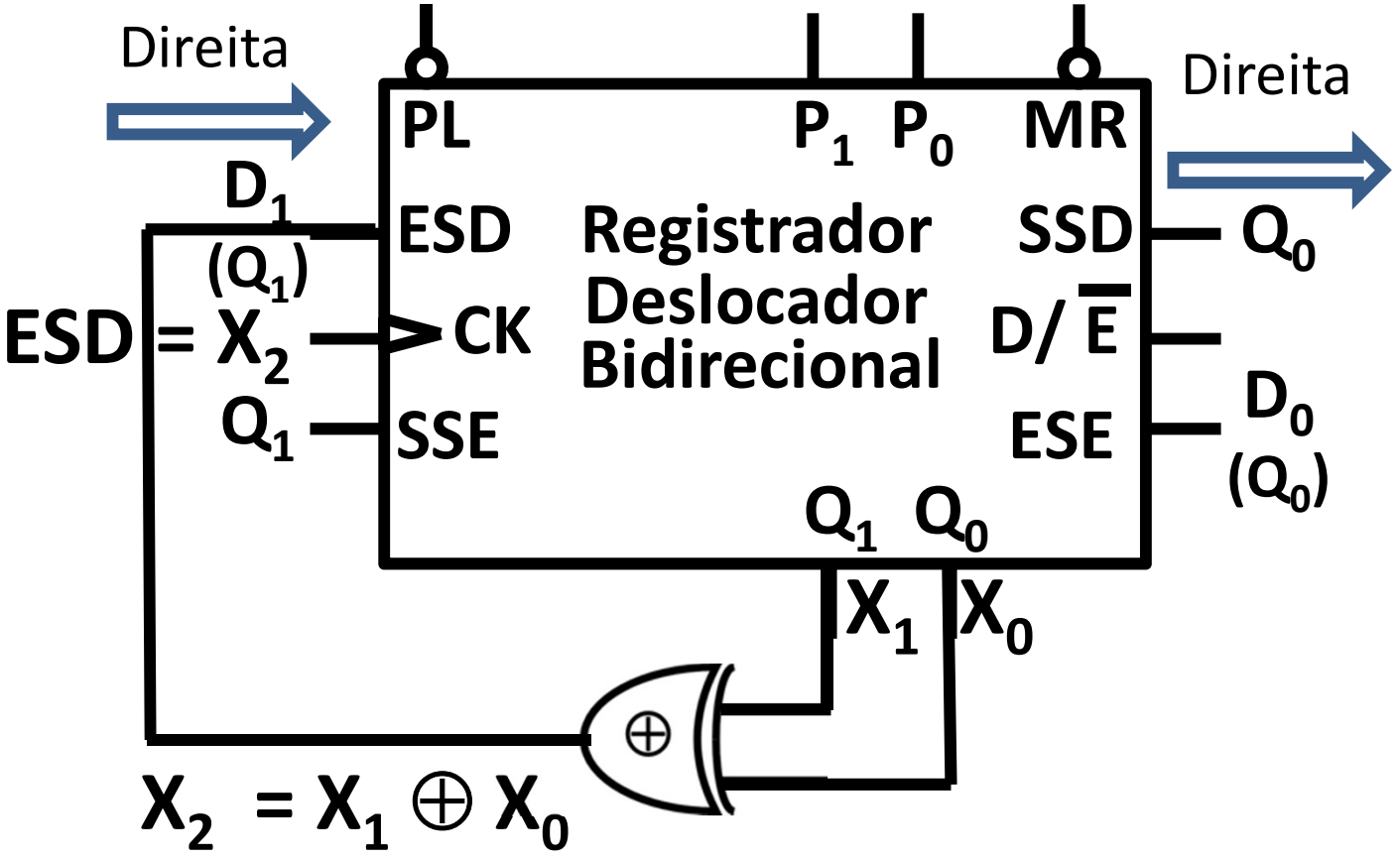
Linear Feedback Shift Register – Convenções

- Estrutura de um LFSR de n bits, genérico:



Linear Feedback Shift Register – Convenções

- Estrutura de LFSR, n = 2 bits – Função linear com $2^2 - 1$ estados na sequência principal:

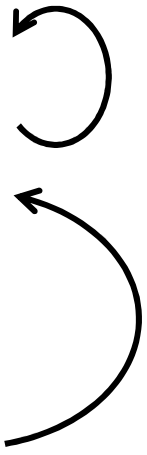


Linear Feedback Shift Register – LFSR

- *Linear Feedback Shift Register* (LFSR) – Sequência principal de $2^2 - 1$ estados:

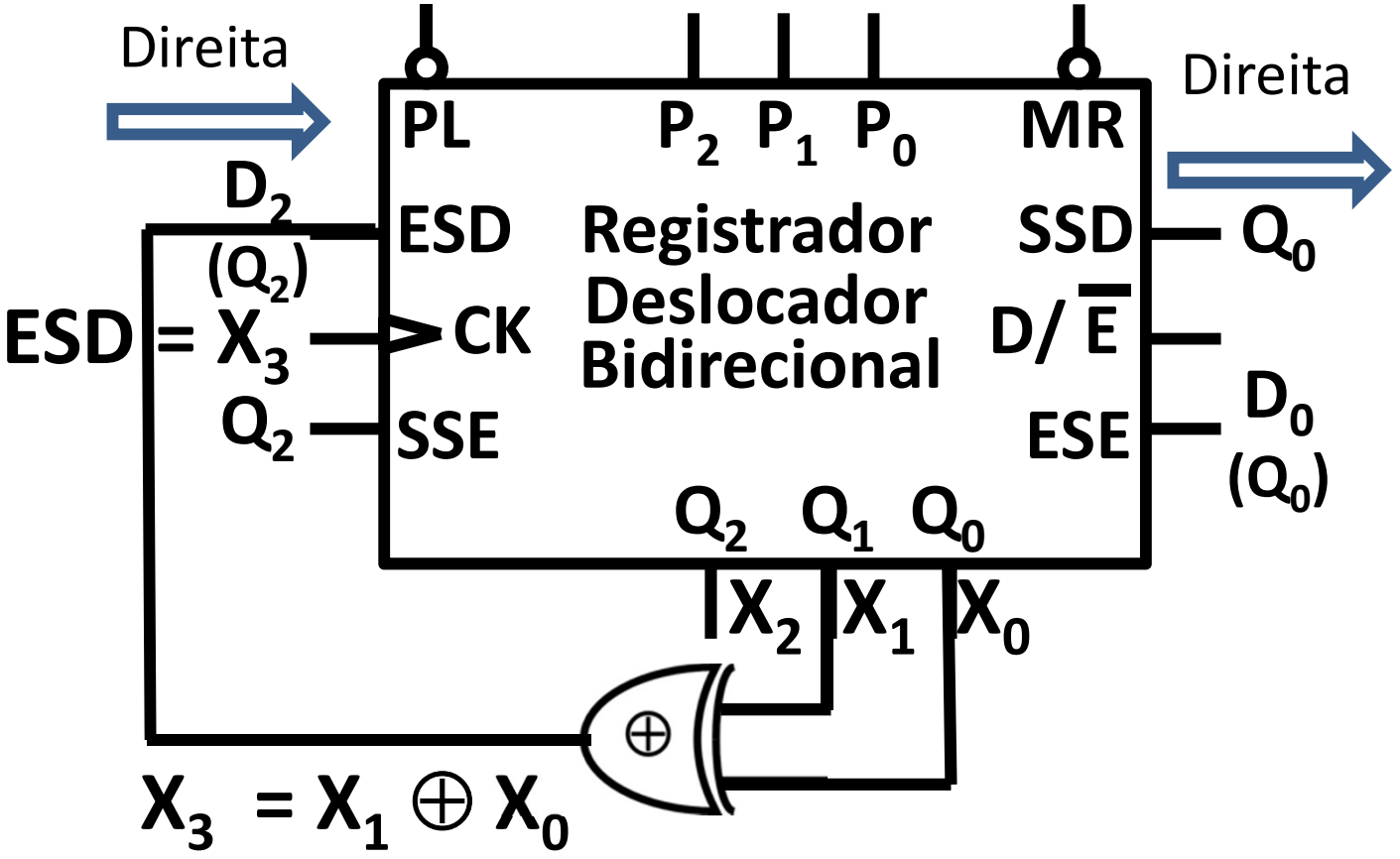
n = 2; Função $X_1 \oplus X_0$

	Q_1	Q_0
	0	**0**
1	**0**	**1**
2	**1**	**0**
3	**1**	**1**



Linear Feedback Shift Register – LFSR

- Estrutura de LFSR, n = 3 bits – Função linear com $2^3 - 1$ estados na sequência principal:

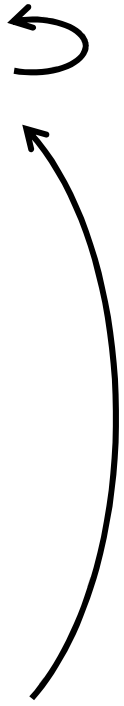


Linear Feedback Shift Register – LFSR

- *Linear Feedback Shift Register* (LFSR) – Sequência principal de $2^3 - 1$ estados:

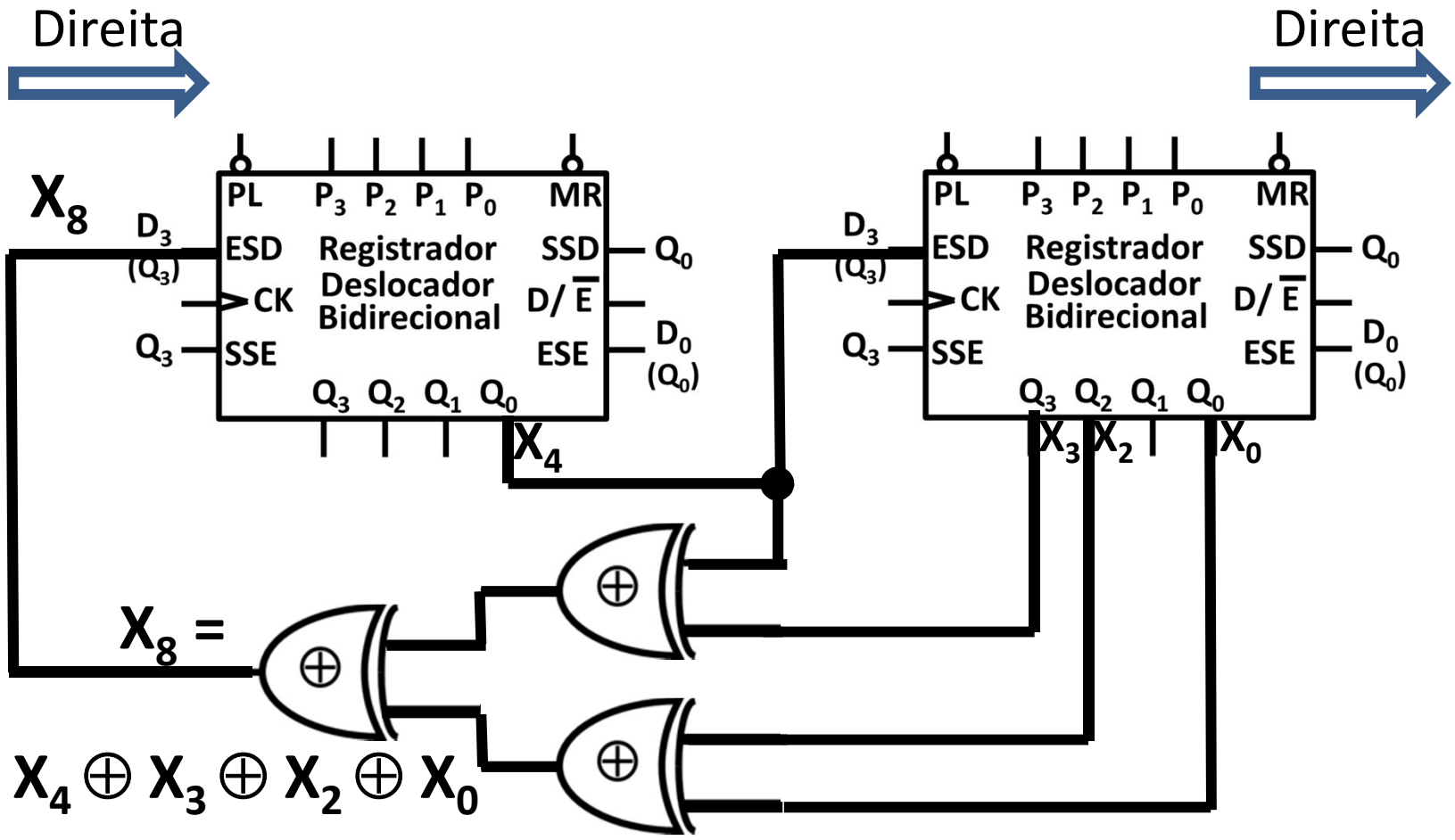
n = 3; Função $X_1 \oplus X_0$

	Q_2	Q_1	Q_0
	0	0	0
1	0	0	1
2	1	0	0
3	0	1	0
4	1	0	1
5	1	1	0
6	1	1	1
7	0	1	1



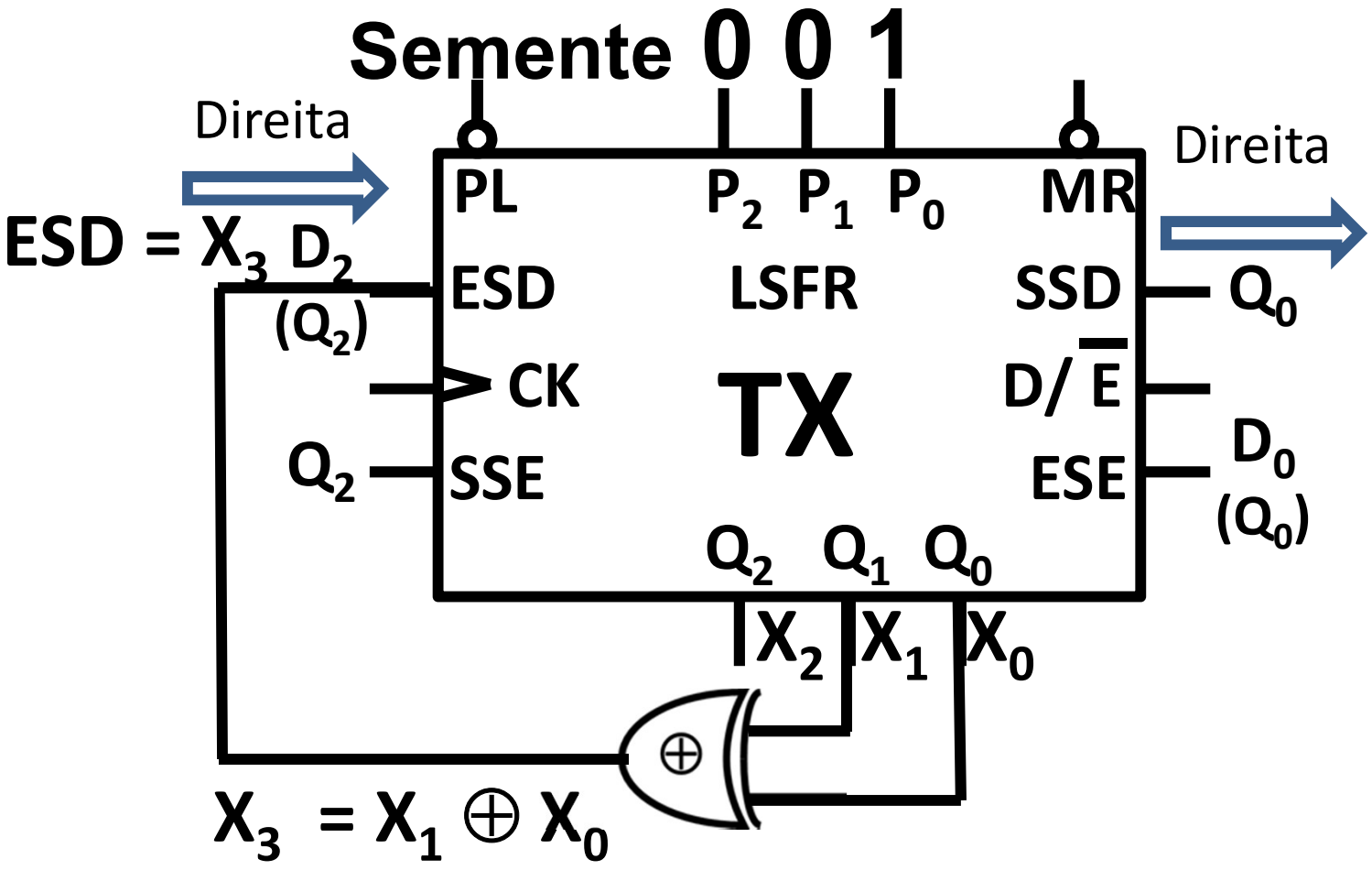
Linear Feedback Shift Register – LFSR

- Estrutura de um LFSR de 8 bits:



Linear Feedback Shift Register – Aplicações

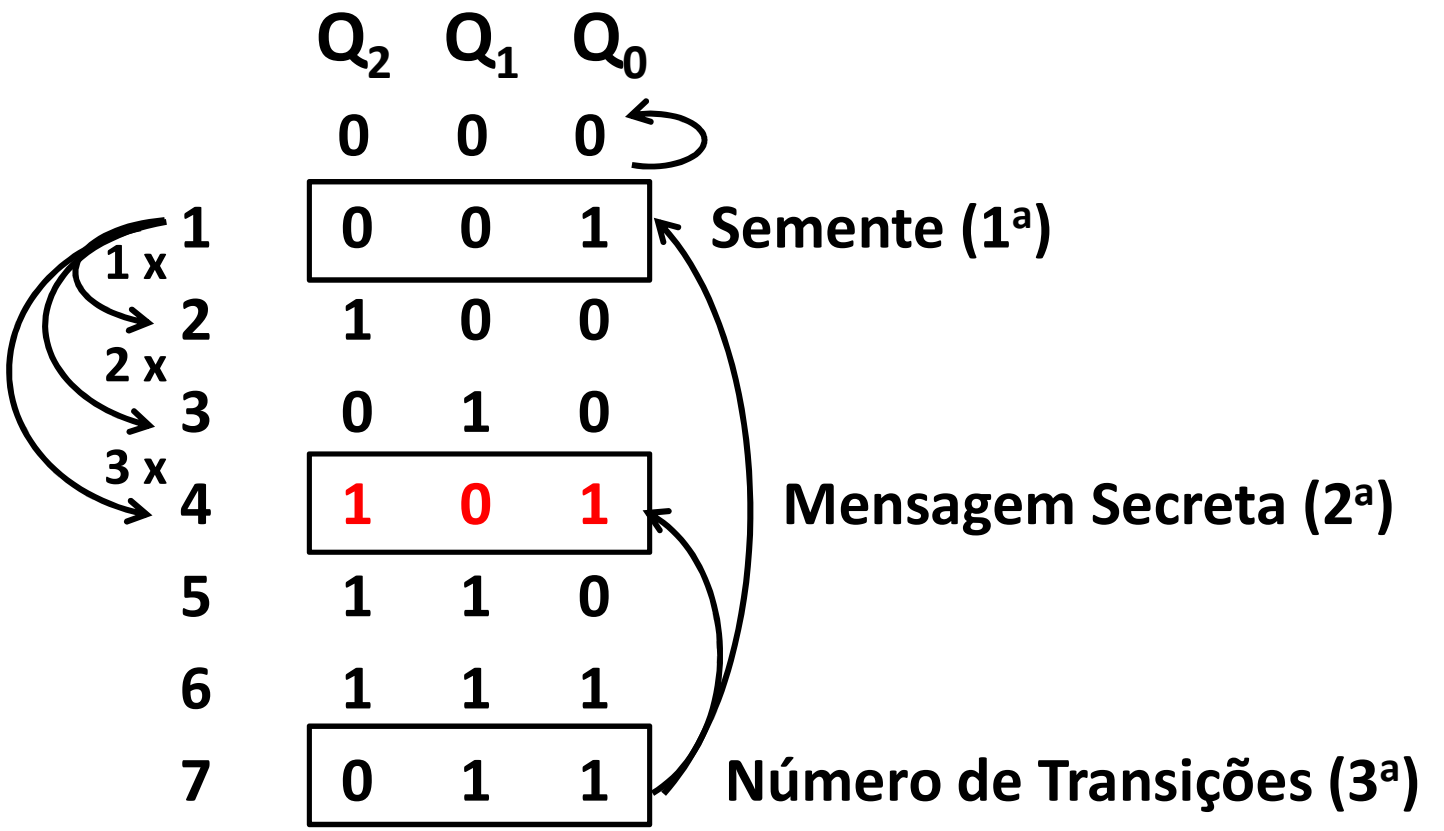
- TX codificada (“embaralhada”) – Pré-definidos: Polinômio gerador “$X_1 \oplus X_0$” e **semente** = “001”.



Linear Feedback Shift Register – LFSR

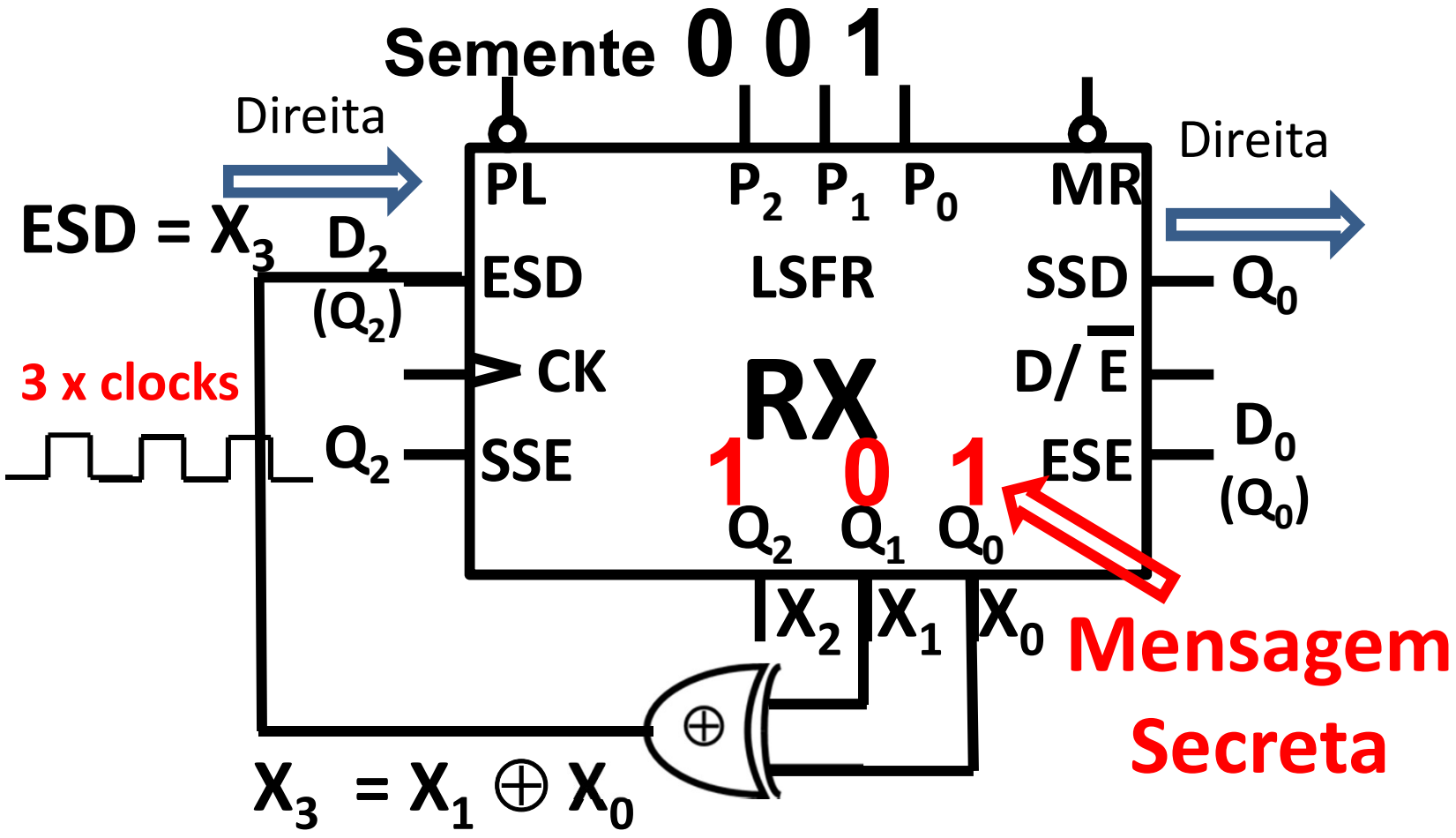
TX e RX: Função $X_1 \oplus X_0$; Semente = "001";

TX: Mensagem Secreta = "101".



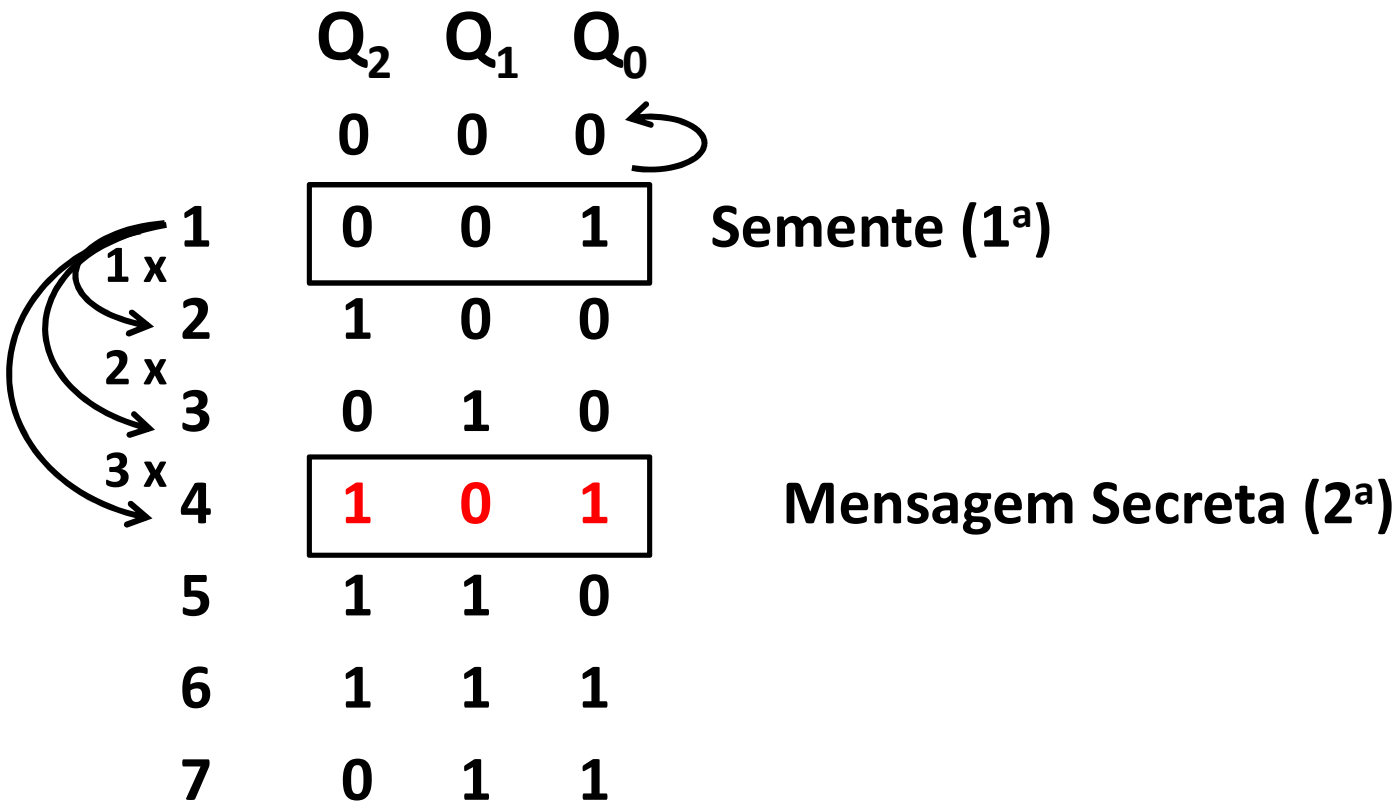
Linear Feedback Shift Register – Aplicações

- **RX – Ações**: Carrega a **semente** = $(001)_2$; faz pulsar o clock $(011)_2$ vezes.



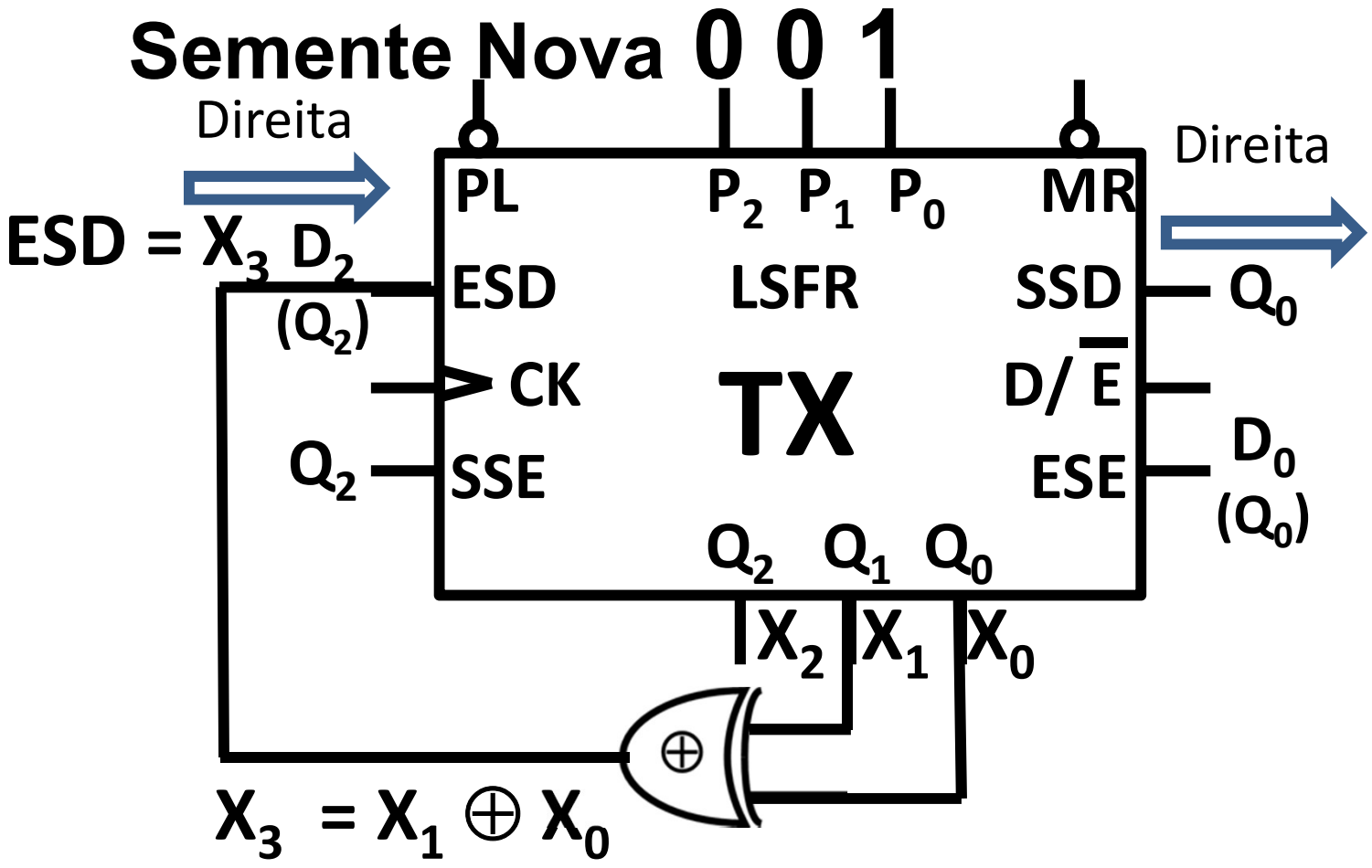
Linear Feedback Shift Register – LFSR

RX – Ações: Carrega a **semente** = $(001)_2$; faz pulsar o clock $(011)_2$ vezes.



Linear Feedback Shift Register – Aplicações

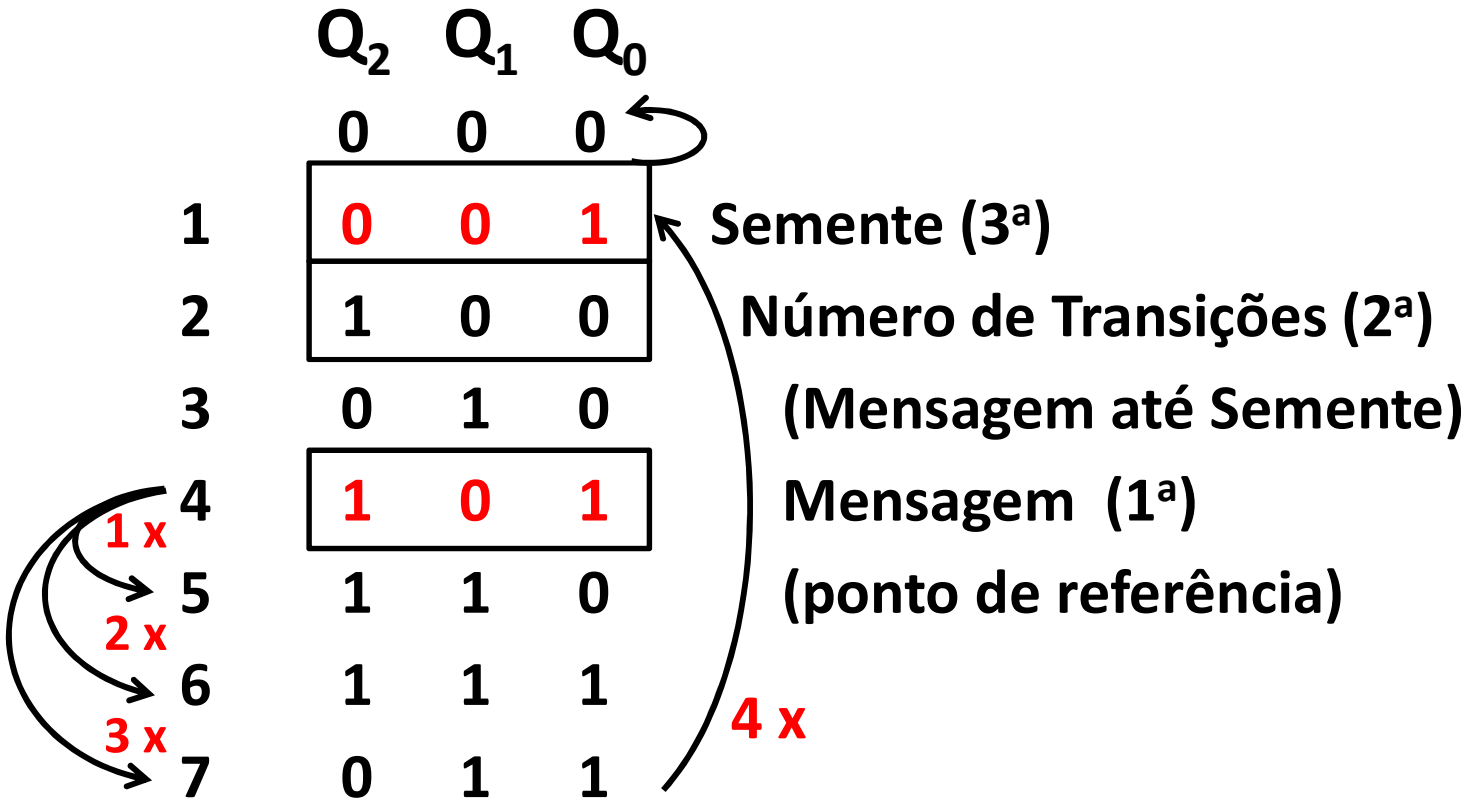
- **TX** propõe **Troca de Semente** – Pré-definidos: Polinômio gerador "$X_1 \oplus X_0$" e **procedimento**.



Linear Feedback Shift Register – LFSR

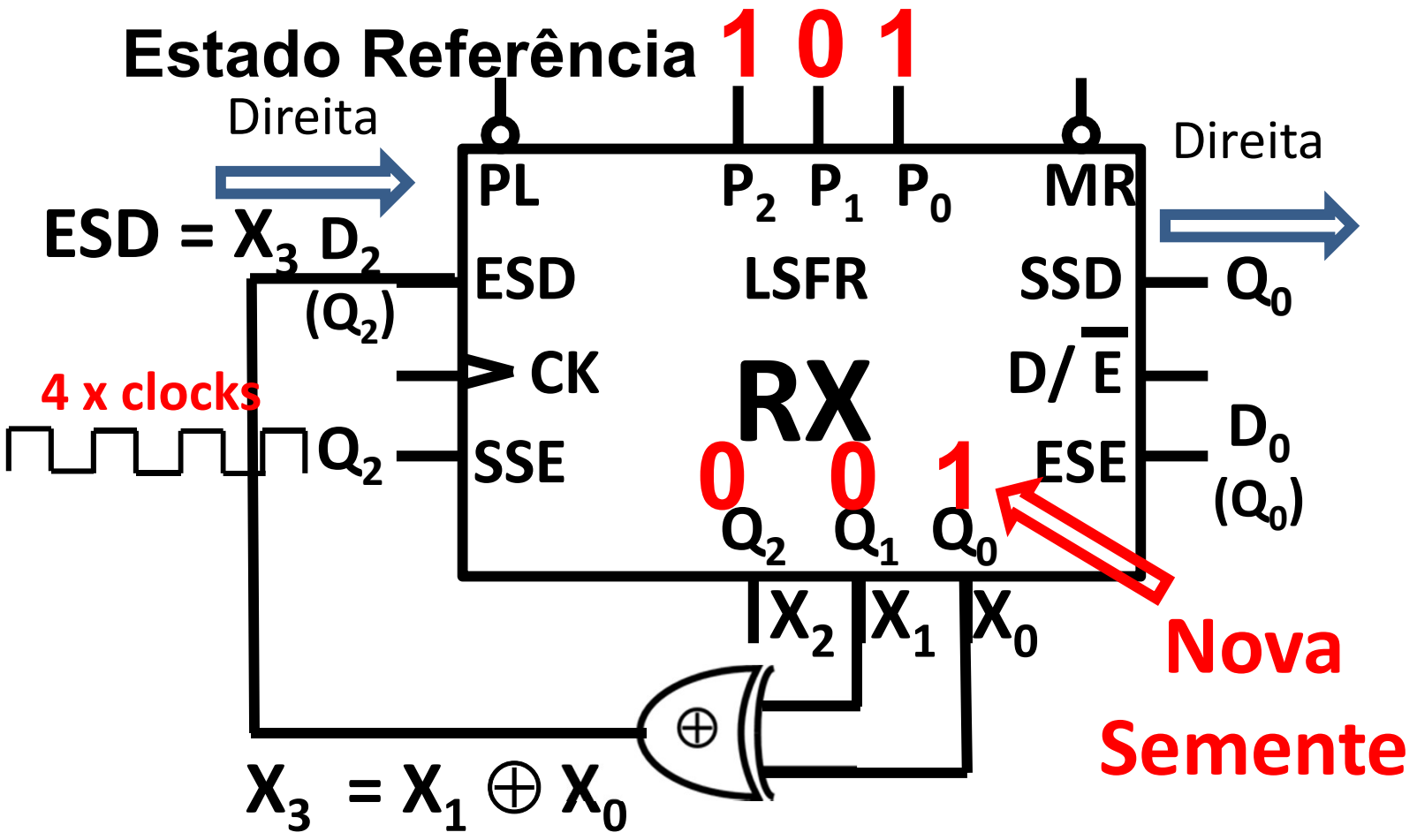
TX e RX: Função $X_1 \oplus X_0$; Troca de Semente;

TX: Definição do Estado Referência = "101".



Linear Feedback Shift Register – Aplicações

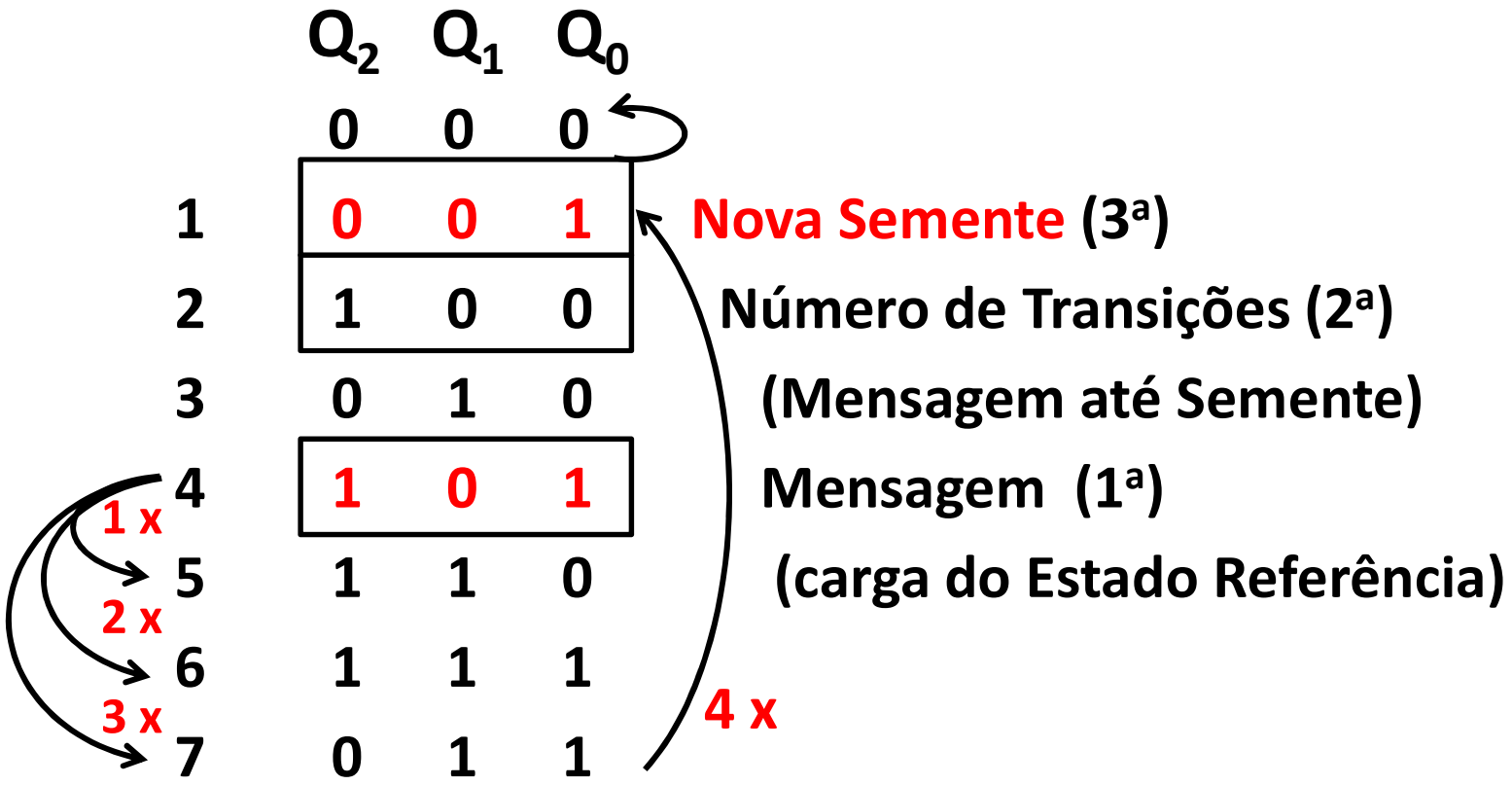
- **RX** processa **Troca de Semente** – Pré-definidos: Polinômio gerador "$X_1 \oplus X_0$" e **procedimento**.



Linear Feedback Shift Register – LFSR

TX e RX: Função $X_1 \oplus X_0$; Troca de Semente;

RX: Carregar o Estado Referência = "101".



Houston ...

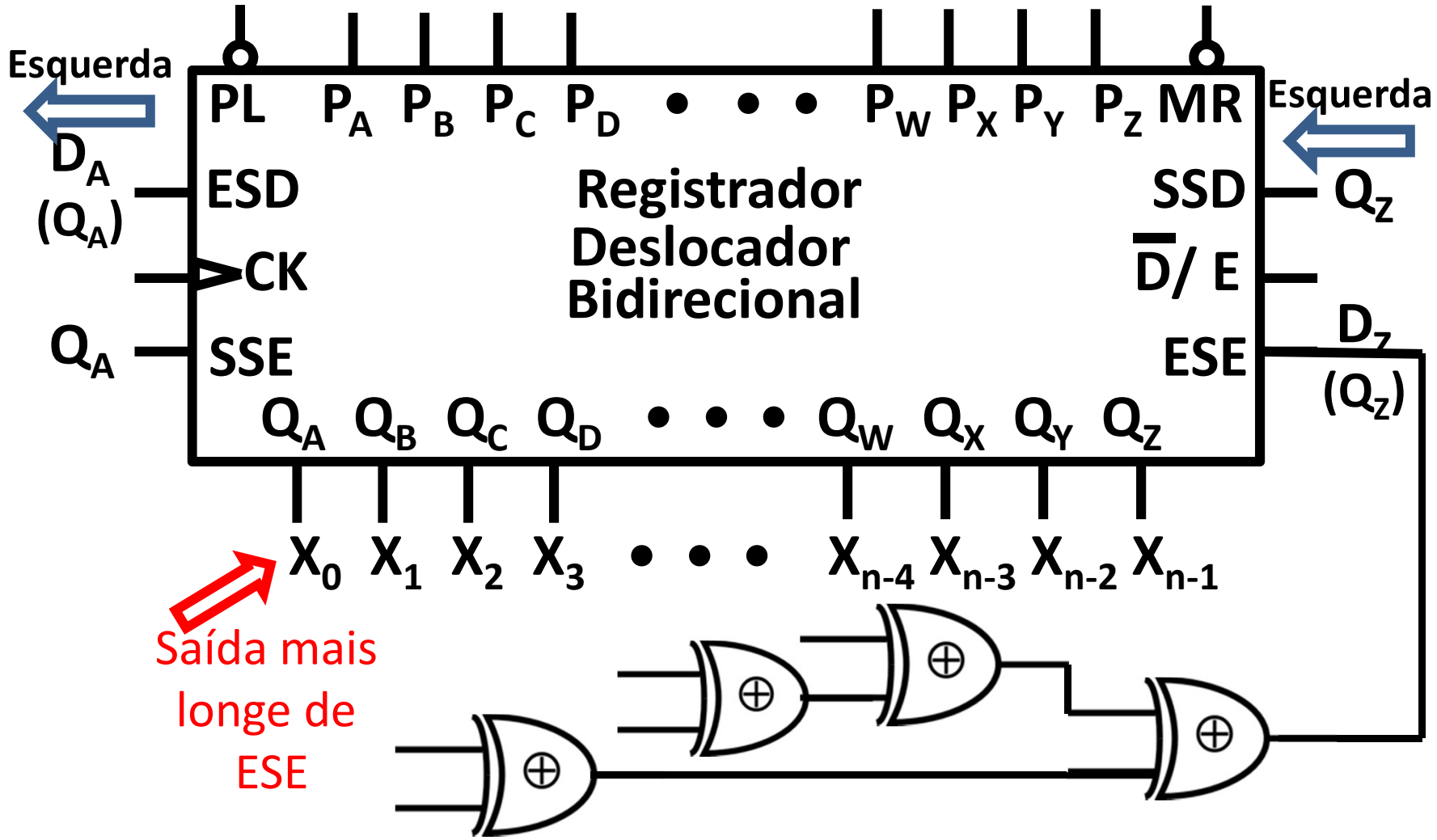
We have a problem!!!!

Em RX o LFSR no modo deslocador à direita não funciona!

- Mas no modo deslocador à esquerda funciona!
- Podemos resolver o problema com este recurso?
- Se sim, usa-se a mesma função de realimentação?
- Utiliza-se o mesmo procedimento de decifração?
- Lembrar que em TX e RX, aplicando o procedimento de geração e decifração das mensagens, percorremos os Estados no mesmo sentido ("embaralhando" os dados) com deslocamento à direita!
- E se em RX usarmos um procedimento de decifração das mensagens percorrendo os Estados no sentido contrário ("desembaralhando" os dados) com deslocamento à esquerda?

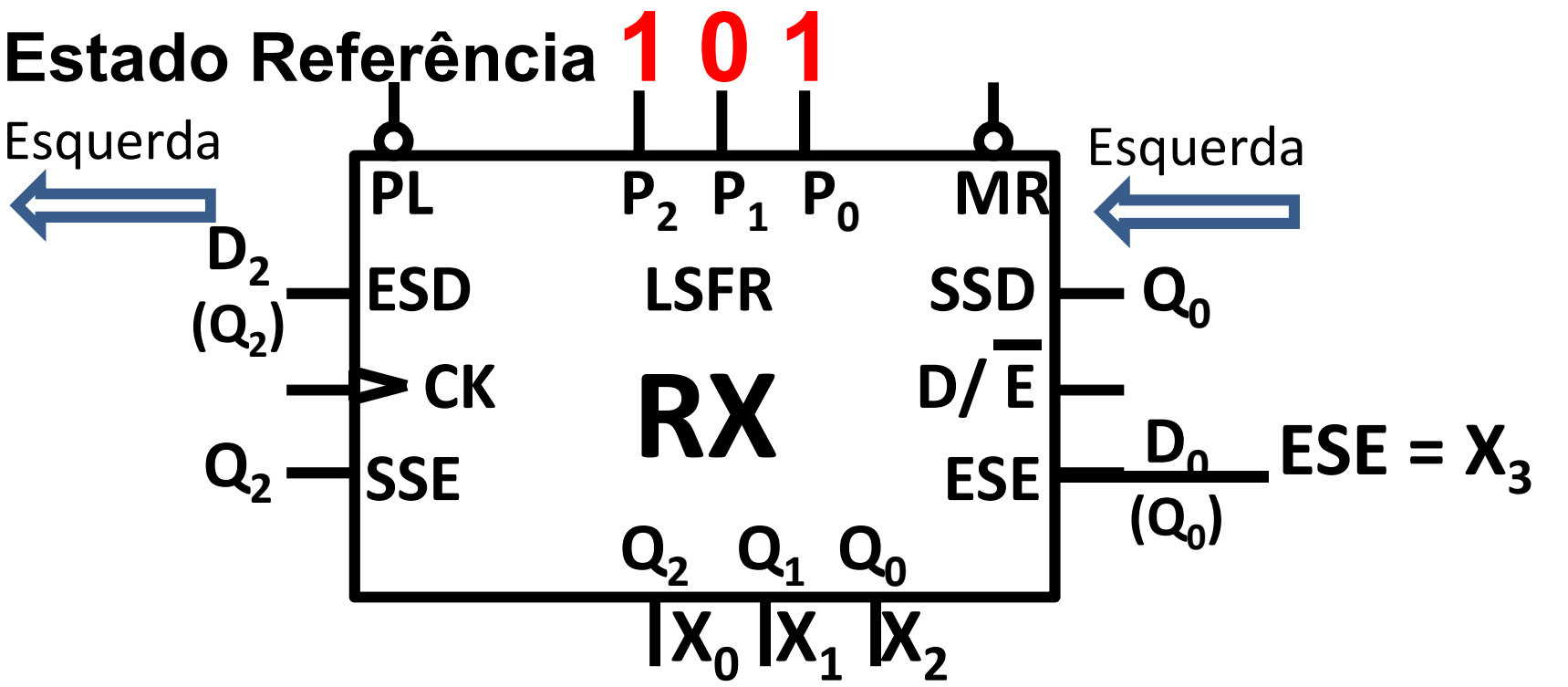
Linear Feedback Shift Register – Convenções

- LFSR de n bits, deslocamento à esquerda:



Linear Feedback Shift Register – Aplicações

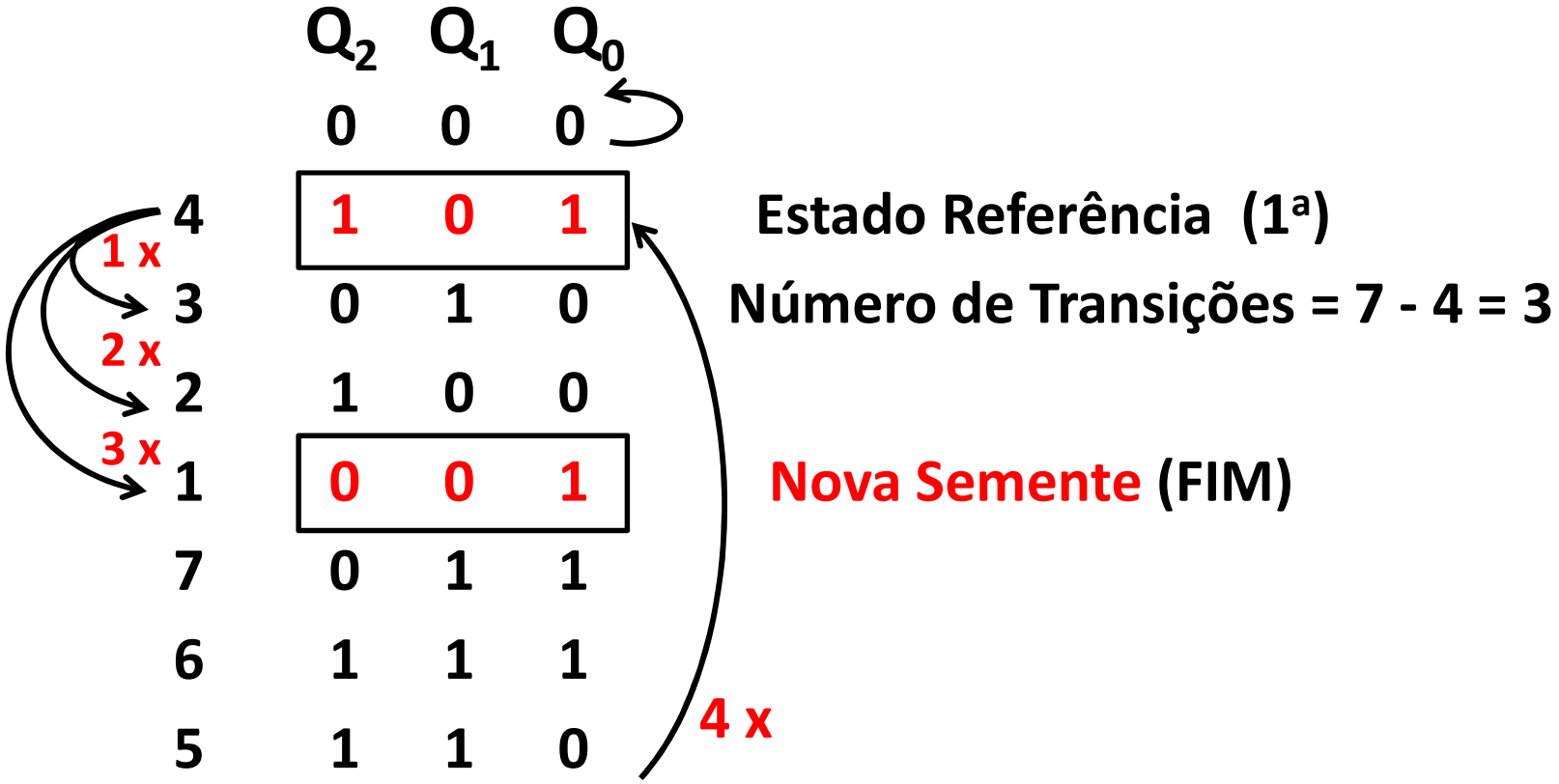
- **RX**, **Troca de Semente** – **Plano B**: Adaptação para deslocamento à esquerda!



$$ESE = X_3 = F(X_2, X_1, X_0)$$

Linear Feedback Shift Register – LFSR

RX: Plano B: Adaptação para deslocamento à esquerda!



Linear Feedback Shift Register – LFSR

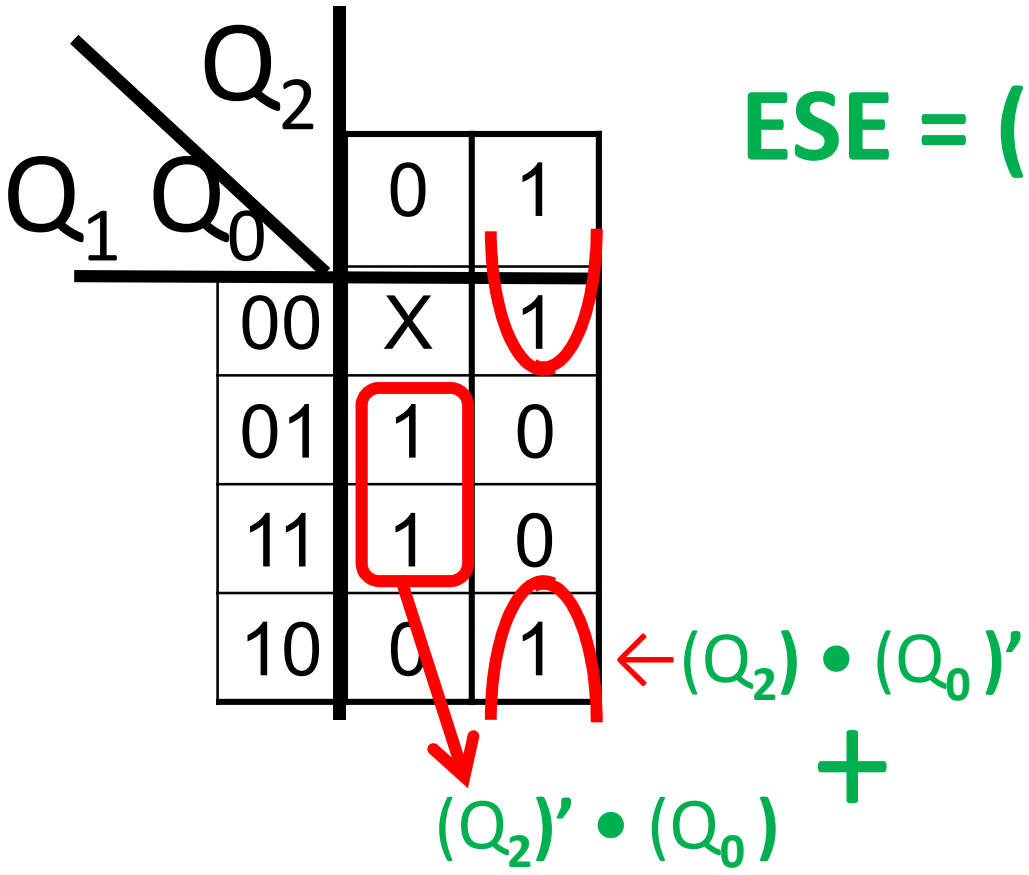
Tabela de Transição de Estados para deslocamento à esquerda!

	Q_2	Q_1	Q_0	Q_2^*	Q_1^*	Q_0^* = ESE
0	0	0	0	0	0	X
4	1	0	1	0	1	0
3	0	1	0	1	0	0
2	1	0	0	0	0	1
1	0	0	1	0	1	1
7	0	1	1	1	1	1
6	1	1	1	1	1	0
5	1	1	0	1	0	1

LFSRs – RX

✓ Mapas de *karnaugh*.

ESE



ESE = $(Q_2 \oplus Q_0)$

Linear Feedback Shift Register – Aplicações

- **RX**, **Troca de Semente** – **Plano B**: Adaptação para deslocamento à esquerda!