## Implementação de encoder/checker CRC-8



André Almeida 88960, Rui Santos 89293, T3G7

Solução para proteger a integridade de uma mensagem, implementado com um cyclic redundancy check, com o polinómio  $b(x) = x^8 + x^5 + x^3 + x^2 + x + 1$ .

A mensagem e o resultado do resto da divisão pelo polinómio em cima são enviados juntos pelo encoder, aquando do envio da mensagem, para quando esta for recebida, o checker realiza de novo o resto e compara-o com o recebido.

Se estes forem iguais, a mensagem não foi corrompida durante a "viagem" até ao recetor.

```
54_7 \le a(4) \times a(7);

50_3 \le a(0) \times a(3);
50_5 <= a(12) XOR a(15);

512_15 <= a(12) XOR a(9);

57_9 <= a(7) XOR a(9);

55_13 <= a(5) XOR a(13);
   s1_8 <= a(1) XOR a(8);
s5_10 <= a(5) XOR a(10);
    --level2
   s10_11_12_15 <= s10_11 XOR s12_15;
    s0_4_2_9 \le s0_4 \times R s2_9;
50, 45, 8 < 56, 75, 8 < 56, 75, 8 < 56, 75, 8 < 55, 70, 85, 8; 5.1, 8.13 <= $1.8 \text{ xor a(13);} $5, 0.35, 8 <= $0.3 \text{ xor s(3);} $5, 0.46, 7 <= $0.4 \text{ xor s(6);} $1.35, 13 <= $1.3 \text{ xor s(6);} $1.35, 13 <= $1.3 \text{ xor s(6);} $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.35, 14 <= $1.
 s1_3_6_14 <= s1_3 XOR s6_14;
s1_3_2_9 <= s1_3 XOR s2_9;
s5_10_14 <= s5_10 XOR a(14);
   s9_10_13 <= s9_10 XOR a(13);
 s4_7_8 <= s4_7 XOR a(8);
s2_9_10_11 <= s2_9 XOR s10_11;
    --level3
   s7_9_10_11_12_15 <= s7_9 xor s10_11_12_15;
s1_3_5_13_15 <= s1_3_5_13 xor a(15);
$1_3_5_13_1$ <= $1_3_5_1$ xor a(15);

$10_11_12_15_1_3_6_14 <= $10_11_12_1$ xor $1_3_6_14;

$6_7_5_8_12 <= $6_7_5_8$ xor a(12);

$1_3_6_7_5_8 <= $1_3$ xor $6_7_5_8;

$6_14_4_7_8 <= $6_14$ xor $4_7_8;

$7(3) <= $0_4_2_9$ xor $5_1_8_13;

$7(4) <= $1_3_2_9$ xor $5_1_0_14;
                                    Vel4

= $_0_3_5_8 XOR $7_9_10_11_12_15;

<= $0.4.6_7 XOR $1_3.5_13_15;

<= $0.4.2_9 XOR $10_11_12_15_1_3_6_14;

<= $0.4.2_9 XOR $6_7_5_8_12;

<= $0.4.2_9 XOR $6_7_5_8_12;

<= $1_3_6_7_5_8 XOR $9_10_13;

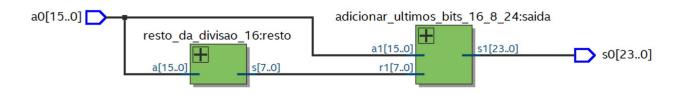
<= $2_9_10_11 XOR $6_14_4_7_8;
```

## Encoder - Versão Paralela

O resto foi calculado utilizando as suas propriedades

**XORs: 42** 

Atraso Máximo: 4



		Name	Value at	0 ps	80.0 ns	160,0 ns	240.0 ns	320 <sub>.</sub> 0 ns	400.0 ns	480.0 ns	560.0 ns	640.0 ns	720.0 ns	800,0 ns	880 <mark>.0 ns</mark>	960.0 ns
		Name	0 ps	0 ps												
ì		> a0	В 11111111		11111111	11111110		11100111	01110001		000110101	0101110	X	1111000	000000110	
-	*	> s0	В 11111111	11	111111111	11101101010	01 11	1001110111	00010000110	000	1101010101	11001111000	) X 1	11110000000	0011000011	110

## Checker - Versão Paralela

É calculado o resto dos primeiros 16 bits de entrada (usando o mesmo módulo do encoder) e é comparado com os últimos 8 bits de entrada que correspondem ao resto enviado. O comparador envia 1 no caso das entradas serem diferentes e 0 no caso contrário. Para isso, usa 8 XORs e 7 ORs.

