Arquitectura de Computadores Avançada

CRC Design

António Rui Borges

Application areas

Two basic application areas are considered

- message transmission
  - bit serial transmission
- data storage
  - parallel access.

Engineering problem to be dealt with

- how confidant can one be that the received message, or the retrieved data, is the same as the one that was transmitted, or stored?

Solution to be pursued

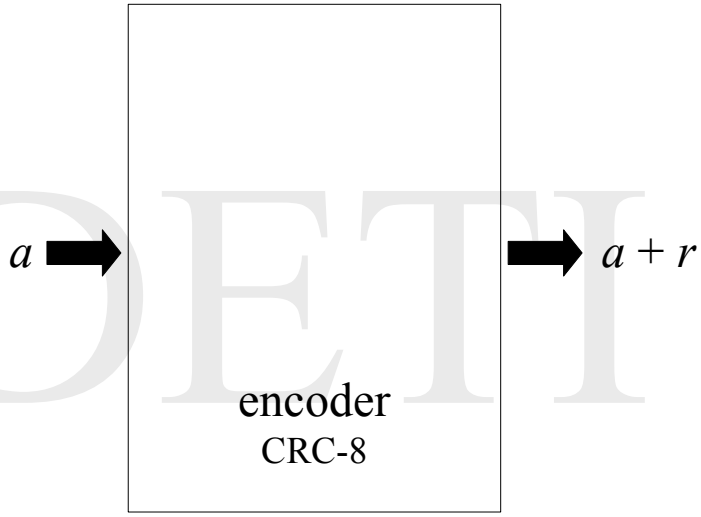
The message, or data, bits will be thought of to represent the coefficients of a polynomial to be operated in the Galois Field F_2.

The remainder $r(x)$, Cyclic Redundancy Checksum (CRC), of the polynomial division of $a(x) \times 10^8$ by $b(x) = x^8 + x^5 + x^3 + x^2 + x + 1$ is to be computed and attached to the message before transmission, or to the data before storage.

Upon message reception, or data retrieval, the polynomial $a(x) \times 10^8 + r(x)$ is to be divided again by $b(x)$ and, if the remainder is not zero, an error should be signaled.

Requirements - 1

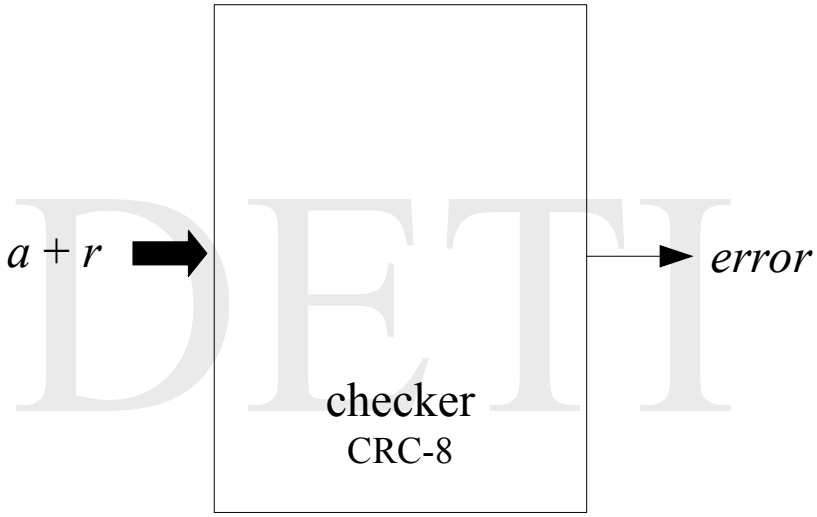
Parallel version



a – 16 bit word
r – 8 bit word

Requirements - 2

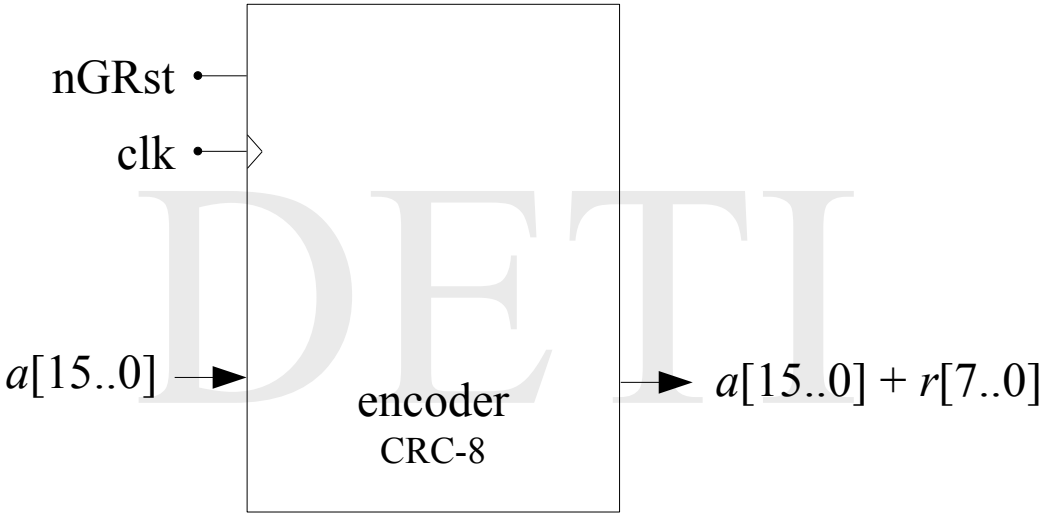
Parallel version



a – 16 bit word
r – 8 bit word
error – 1 bit word

Requirements - 3

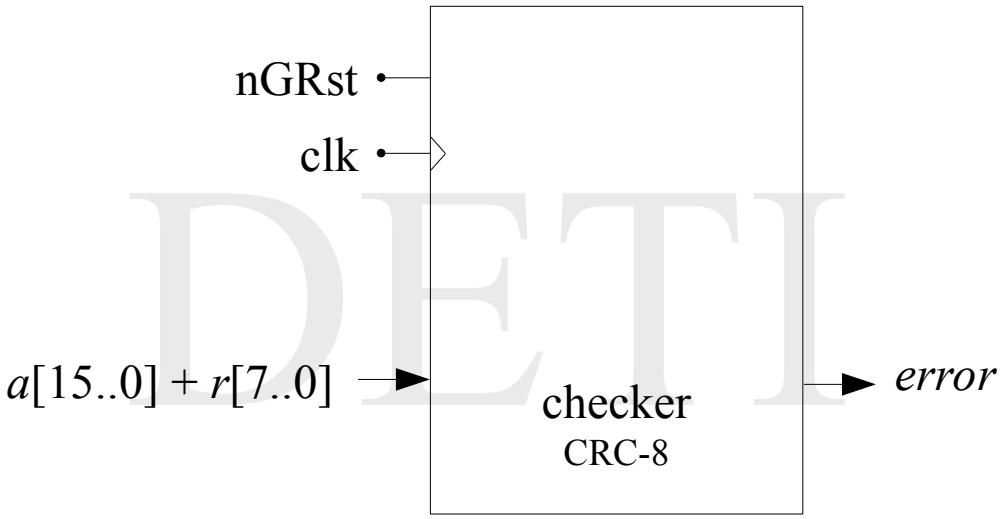
Bit serial version



a – msb is inputted / outputted first
r – msb is outputted first

Requirements - 4

Bit serial version



a – msb is inputted first
r – msb is inputted first

Basic approaches

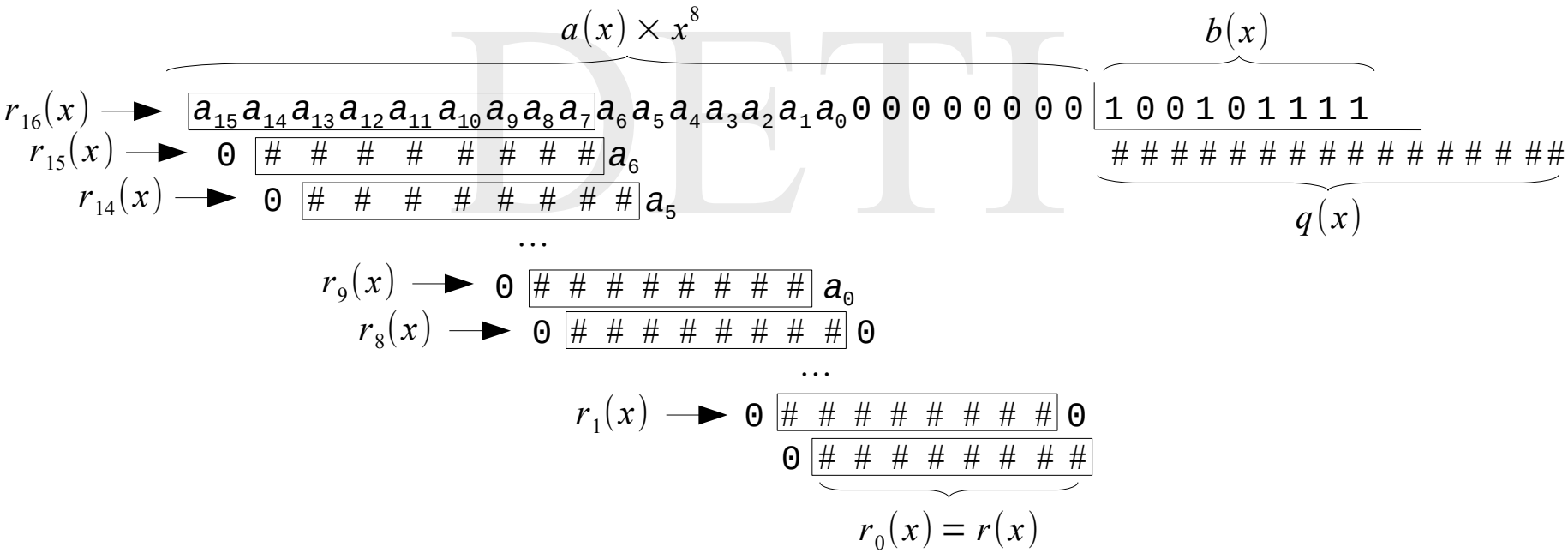
The design may be approached through different methods, such as

- the division algorithm
- properties of the remainder.

Division Algorithm - 1

$$a(x) \times x^8 = q(x) \times b(x) + r(x)$$

where $b(x) = x^8 + x^5 + x^3 + x^2 + x + 1$ $\left(\text{CRC}-8\ \text{AutoSar}\right)$



Division Algorithm - 2

The computation can be simplified if we take into consideration that

- only the polynomial $r(x)$ is required
- the last 8 coefficients of polynomial $a(x) \times x^8$ are known to be zero
- the form of polynomial $b(x)$ is fixed and known.

Division Algorithm - 3

Description of the computation as a recurring process

- there are 16 iteration steps
- initialization

$$r_{16,k} = a_{15+k-7}, \text{ with } k = 0,1,\cdots,7$$

- iteration step $(15 \geq i \geq 0)$

$$r_{i,8} = r_{i+1,7} \oplus q_i = r_{i+1,7} \oplus r_{i+1,7} = 0$$

$$k = 1,2,3,5 \Rightarrow r_{i,k} = r_{i+1,7} \oplus r_{i+1,k-1}$$

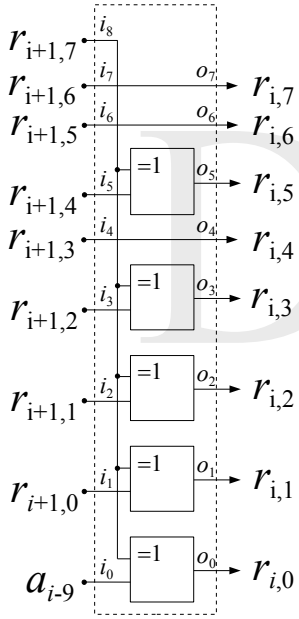
$$k = 4,6,7 \Rightarrow r_{i,k} = r_{i+1,k-1}$$

$$k = 0 \wedge i \geq 8 \Rightarrow r_{i,0} = r_{i+1,7} \oplus a_{i-8}$$

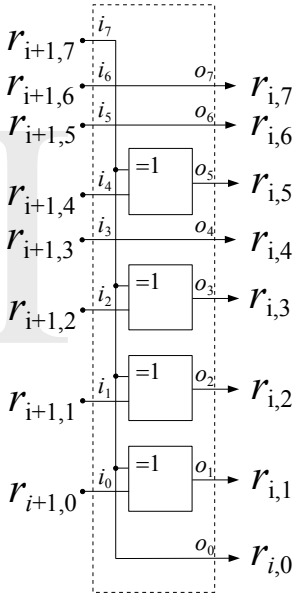
$$k = 0 \wedge i < 8 \Rightarrow r_{i,0} = r_{i+1,7}$$

Division Algorithm - 4

Two basic building blocks are needed.

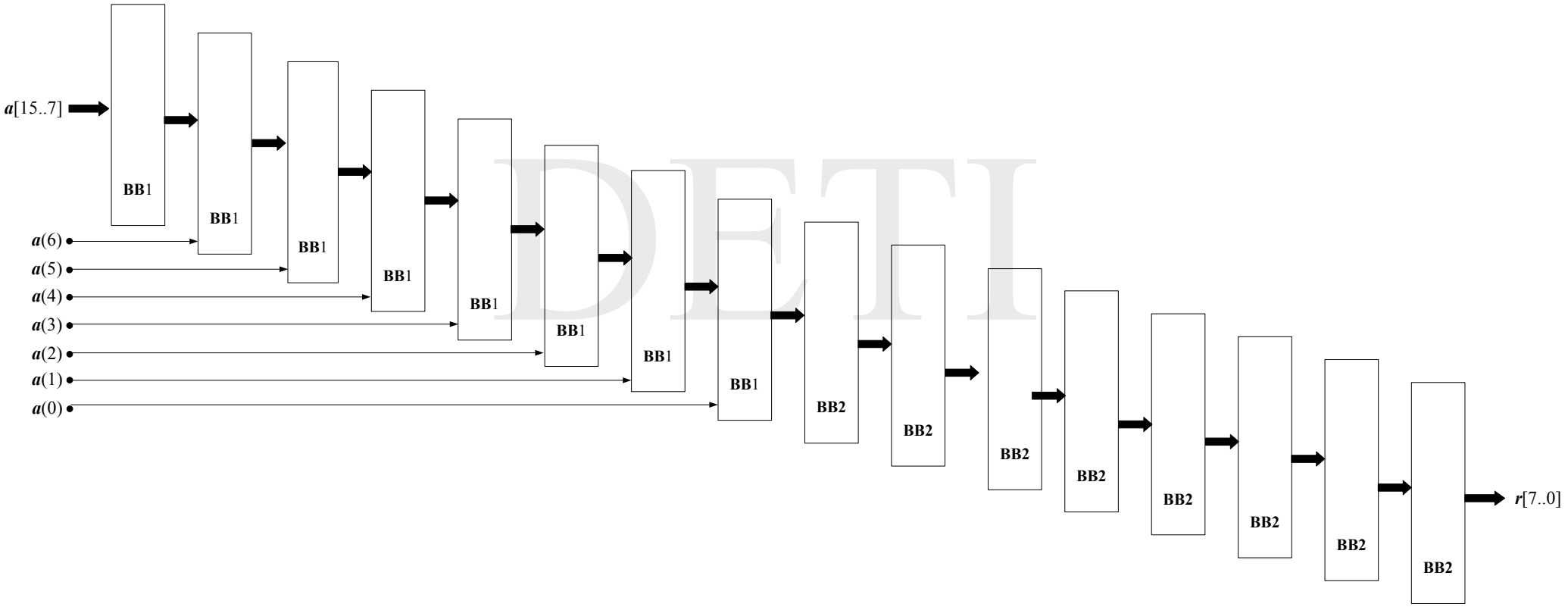


<u>building block of type 1</u>
9 inputs



<u>building block of type 2</u>
8 inputs

Division Algorithm - 5



Division Algorithm - 6

Output to input dependence + cost

iteration number

	r7	r6	r5	r4	r3	r2	r1	r0
16	8000	4000	2000	1000	0800	0400	0200	0100
15	4000	2000	9000	0800	8400	8200	8100	8080
14	2000	9000	4800	8400	C200	C100	C080	4040
13	9000	4800	A400	C200	E100	E080	E040	2020
12	4800	A400	5200	E100	7080	F040	B020	9010
11	A400	5200	A900	7080	B840	F820	D810	4808
10	5200	A900	D480	B840	5C20	7C10	EC08	A404
9	A900	D480	EA40	5C20	2E10	BE08	F604	5202
8	D480	EA40	F520	2E10	1708	5F04	FB02	A901
7	EA40	F520	FA90	1708	8B84	2F82	7D81	D480
6	F520	FA90	FD48	8B84	C5C2	97C1	3EC0	EA40
5	FA90	FD48	7EA4	C5C2	62E1	CBE0	1F60	F520
4	FD48	7EA4	3F52	62E1	3170	E5F0	0FB0	FA90
3	7EA4	3F52	9FA9	3170	18B8	F2F8	07D8	FD48
2	3F52	9FA9	4FD4	18B8	8C5C	797C	83EC	7EA4
1	9FA9	4FD4	27EA	8C5C	462E	BCBE	41F6	3F52
0	**4FD4**	**27EA**	**13F5**	**462E**	**2317**	**DE5F**	**A0FB**	**9FA9**

$a_{15} \cdots a_0$ → 1, if the variable is present in the expression
0, otherwise

- 72 x-or gates are needed.

Division Algorithm - 7

Propagation delay dependence

	pd7	pd6	pd5	pd4	pd3	pd2	pd1	pd0
16	0	0	0	0	0	0	0	0
15	0	0	1	0	1	1	1	1
14	0	1	1	1	2	2	2	1
13	1	1	2	2	3	3	2	1
12	1	2	3	3	4	3	2	2
11	2	3	4	4	4	3	3	2
10	3	4	5	4	4	4	3	3
9	4	5	5	4	5	4	4	4
8	5	5	5	5	5	5	5	5
7	5	5	6	5	6	6	6	5
6	5	6	6	6	7	7	6	5
5	6	6	7	7	8	7	6	5
4	6	7	8	8	8	7	7	6
3	7	8	9	8	8	8	7	6
2	8	9	9	8	9	8	8	7
1	9	9	9	9	9	9	9	8
0	9	9	10	9	10	10	10	9

- 10 x-or propagation time delays in the worst case.

Properties of the remainder - 1

$$[a(x) \times x^8] \; mod \; b(x) = \left[\left(\sum_{n=0}^{15} a_n \times x^n\right) \times x^8\right] \; mod \; b(x) =$$

$$= \left(\sum_{n=0}^{15} a_n \times x^{n+8}\right) \; mod \; b(x) = \sum_{n=0}^{15} \left[a_n \times \left[x^{n+8} \; mod \; b(x)\right]\right]$$

where $b(x) = x^8 + x^5 + x^3 + x^2 + x + 1$ $\left(\text{CRC}-8 \text{ AutoSar}\right)$

Properties of the remainder - 2

$$x^8 \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^5 + x^3 + x^2 + x + 1$$
$$x^9 \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^6 + x^4 + x^3 + x^2 + x$$
$$x^{10} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^7 + x^5 + x^4 + x^3 + x^2$$
$$x^{11} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^6 + x^4 + x^2 + x + 1$$
$$x^{12} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^7 + x^5 + x^3 + x^2 + x$$
$$x^{13} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^6 + x^5 + x^4 + x + 1$$
$$x^{14} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^7 + x^6 + x^5 + x^2 + x$$
$$x^{15} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^7 + x^6 + x^5 + x + 1$$
$$x^{16} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^7 + x^6 + x^5 + x^3 + 1$$
$$x^{17} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$$
$$x^{18} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^7 + x^6 + x^4 + x^2 + 1$$
$$x^{19} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^7 + x^2 + 1$$
$$x^{20} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^5 + x^2 + 1$$
$$x^{21} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^6 + x^3 + x$$
$$x^{22} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^7 + x^4 + x^2$$
$$x^{23} \bmod (x^8 + x^5 + x^3 + x^2 + x + 1) = x^2 + x + 1$$

Properties of the remainder - 4

$$\frac{x^8}{x^8+x^5+x^3+x^2+x+1} = 1 - \frac{x^5+x^3+x^2+x+1}{x^8+x^5+x^3+x^2+x+1} = 1 + \frac{x^5+x^3+x^2+x+1}{x^8+x^5+x^3+x^2+x+1}$$

$$\frac{x^9}{x^8+x^5+x^3+x^2+x+1} = x - \frac{x^6+x^4+x^3+x^2+x}{x^8+x^5+x^3+x^2+x+1} = x + \frac{x^6+x^4+x^3+x^2+x}{x^8+x^5+x^3+x^2+x+1}$$

$$\frac{x^{10}}{x^8+x^5+x^3+x^2+x+1} = x^2 - \frac{x^7+x^5+x^4+x^3+x^2}{x^8+x^5+x^3+x^2+x+1} = x^2 + \frac{x^7+x^5+x^4+x^3+x^2}{x^8+x^5+x^3+x^2+x+1}$$

$$\frac{x^{11}}{x^8+x^5+x^3+x^2+x+1} = x^3 - \frac{x^8+x^6+x^5+x^4+x^3}{x^8+x^5+x^3+x^2+x+1} = x^3 + \frac{x^8+x^6+x^5+x^4+x^3}{x^8+x^5+x^3+x^2+x+1} =$$

$$= x^3+1+\frac{x^5+x^3+x^2+x+1}{x^8+x^5+x^3+x^2+x+1}+\frac{x^6+x^5+x^4+x^3}{x^8+x^5+x^3+x^2+x+1} =$$

$$= x^3+1+\frac{x^6+x^4+x^2+x+1}{x^8+x^5+x^3+x^2+x+1}$$

...

Properties of the remainder - 4

$$\left(\sum_{n=0}^{15} a_n \times x^{n+8}\right) mod\ \left(x^8 + x^5 + x^3 + x^2 + x + 1\right) =$$

$$\begin{aligned}
&= \left(a_2 \oplus a_4 \oplus a_6 \oplus a_7 \oplus a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{14}\right) \times x^7 + \\
&\quad + \left(a_1 \oplus a_3 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_8 \oplus a_9 \oplus a_{10} \oplus a_{13}\right) \times x^6 + \\
&\quad + \left(a_0 \oplus a_2 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_8 \oplus a_9 \oplus a_{12}\right) \times x^5 + \\
&\quad + \left(a_1 \oplus a_2 \oplus a_3 \oplus a_5 \oplus a_9 \oplus a_{10} \oplus a_{14}\right) \times x^4 + \\
&\quad + \left(a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_8 \oplus a_9 \oplus a_{13}\right) \times x^3 + \\
&\quad + \left(a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_6 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{14} \oplus a_{15}\right) \times x^2 + \\
&\quad + \left(a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_{13} \oplus a_{15}\right) \times x + \\
&\quad + \left(a_0 \oplus a_3 \oplus a_5 \oplus a_7 \oplus a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{15}\right)
\end{aligned}$$

- 64 x-or gates are needed
- 11 x-or propagation time delays in the worst case.

Parallel implementation

Following one of the approaches that were described, or some other one that you may devise

- elicit common operations to reduce gate count
- perform them in parallel to reduce time propagation delays.

Bit serial implementation

Following one of the approaches that were described, or some other one that you may devise

- elicit common operations in order to specify the data path
- design the control section so that the bit sequence may proceed smoothly through the data path.