Cyclic Redundancy Check

Cyclic Redundancy Check (CRC) is an error detection method for digital data based on binary division.

CRC algorithm generates a fixed checksum code length.

How is CRC value calculated, how to determine CRC algorithm in embedded applications?

CRC algorithm embedded within the STM32 peripherals computes shift and XOR operations of a subsequent input data in functions of a Generator polynomial (**POLY**) and a programmable Initial CRC value.
Algorithm Input parameters:

- **Input data** also called "**Dividend**". This is the data being transmitted or content of Flash for example.
- **Generator polynomial** or "**Divisor**":

Algebraic polynomial represented as a bit pattern: the power of each term gives the position on the bit and the coefficient gives the value of the bit.
The order of the generator polynomial must not exceed the CRC length.
For a 32-bits CRC calculation, polynomial highest exponent must be 32.
By default, the standard generator polynomial used by the STM32 CRC peripheral is the Ethernet CRC-32 polynomial *0x04C11DB7.* The mathematical representation according to this polynomial is $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$. This presentation is obtained from the binary format of coefficients, where the 32-bit term is always present while the other terms are present only if the coefficient is equal to 1.

- **Initial CRC value**

Initial CRC value gives more security to CRC. It is fixed to 0xFFFFFFFF or programmable by user.
At start up, algorithm sets CRC to the initial CRC value XOR with the dividend.
Once CRC MSB is equal to one, algorithm shifts CRC one bit to the left and XORs it with the generator polynomial.
Otherwise, it only shifts CRC one bit to the left.
Figure below describes the algorithm used in STM32 MCUs.