all one polynomial

Canonical name	AllOnePolynomial
Date of creation	2013-03-22 15:00:26
Last modified on	2013-03-22 15:00:26
Owner	Derk (34)
Last modified by	Derk (34)
Numerical id	7
Author	Derk (34)
Entry type	Definition
Classification	msc 12E10
Synonym	all-one polynomial
Synonym	AOP
Related topic	CyclotomicPolynomial
Related topic	ProofThatTheCyclotomicPolynomialIsIrreducible
Related topic	FactoringAllOnePolynomialsUsingTheGroupingMethod

An *all one polynomial* (*AOP*) is a polynomial used in finite fields, specifically GF(2). The AOP is a 1-equally spaced polynomial.

An AOP of degree m can be written as follows:

$$\mathrm{AOP}(x) = \sum_{i=0}^{m} x^i = x^m + x^{m-1} + \ldots + x + 1$$

Over GF(2) the AOP has many interesting properties, including:

- The Hamming weight of the AOP is $m + 1$.
- The AOP is irreducible polynomial iff $m+1$ is prime and 2 is a primitive root modulo $m + 1$.
- The only AOP that is a primitive polynomial is $x^2 + x + 1$.

Despite the fact that the Hamming weight is large, because of the ease of representation and other improvements there are efficient hardware and software implementations for use in areas such as coding theory and cryptography.