Symmetric Polynomials

A *symmetric polynomial* is a polynomial $P(X_1, X_2, \ldots, X_n)$ in n variables such that if any of the variables of the polynomial are interchanged the same original polynomial results.

Examples:

$$X_1^2 + X_2^2 - 1$$

$$(X_1 + X_2)^5$$

$$X_1 X_2 X_3 + 2 X_1 X_2 + 2 X_1 X_3 + 2 X_2 X_3 - 1$$

Elementary Symmetric Polynomials

The *elementary symmetric polynomial* $e_k(X_1, X_2, \ldots, X_n)$ in n variables is defined as the sum of all products of k-subsets of the n variables. Symbolically,

$$e_k(X_1, X_2, \ldots, X_n) = \sum_{1 \le j_1 < j_2 < \ldots < j_k \le n} X_{j_1} X_{j_2} \ldots X_{j_k}$$

Also,

$$e_0(X_1, X_2, \ldots, X_n) = 1$$

$$e_k(X_1, X_2, \ldots, X_n) = 0 \quad \text{for } k > n$$

Example:

For $n = 4$:

$$e_0(X_1, X_2, X_3, X_4) = 1$$

$$e_1(X_1, X_2, X_3, X_4) = X_1 + X_2 + X_3 + X_4$$

$$e_2(X_1, X_2, X_3, X_4) = X_1 X_2 + X_1 X_3 + X_1 X_4 + X_2 X_3 + X_2 X_4 + X_3 X_4$$

$$e_3(X_1, X_2, X_3, X_4) = X_1 X_2 X_3 + X_1 X_2 X_4 + X_1 X_3 X_4 + X_2 X_3 X_4$$

$$e_4(X_1, X_2, X_3, X_4) = X_1 X_2 X_3 X_4$$

$$e_k(X_1, X_2, X_3, X_4) = 0 \quad \text{for } k > 4$$

Power Sum Symmetric Polynomials

The *power sum symmetric polynomial* $p_k(X_1, X_2, \ldots, X_n)$ in n variables is defined as the sum of the kth powers of the n variables. Symbolically,

$$p_k(X_1, X_2, \ldots, X_n) = \sum_{j=1}^{n} X_j^k$$

Example:

For $n=4$:

$$p_0(X_1, X_2, X_3, X_4) = 4$$

$$p_1(X_1, X_2, X_3, X_4) = X_1 + X_2 + X_3 + X_4$$

$$p_2(X_1, X_2, X_3, X_4) = X_1^2 + X_2^2 + X_3^2 + X_4^2$$

$$p_3(X_1, X_2, X_3, X_4) = X_1^3 + X_2^3 + X_3^3 + X_4^3$$

$$p_4(X_1, X_2, X_3, X_4) = X_1^4 + X_2^4 + X_3^4 + X_4^4$$

$$p_5(X_1, X_2, X_3, X_4) = X_1^5 + X_2^5 + X_3^5 + X_4^5$$

$$\vdots$$

Newton's Identities

The *Newton identities* or *Newton-Girard formulas* give relations between the elementary and power sum symmetric polynomials. In coding theory these identities are used in the Peterson-Gorenstein-Zierler (PGZ) algorithm for decoding binary primitive BCH codes.

The elementary symmetric polynomials may be recursively expressed in terms of the power sum symmetric polynomials as follows:

$$k\, e_k(X_1, X_2, \ldots, X_n) = \sum_{j=1}^{k} (-1)^{j-1} e_{k-j}(X_1, X_2, \ldots, X_n)\, p_j(X_1, X_2, \ldots, X_n)$$

For any $n \geq 1$ and $k \geq 1$.

Evaluating this expression explicitly gives:

$$e_1 = p_1$$

$$2e_2 = e_1 p_1 - p_2$$

$$3e_3 = e_2 p_1 - e_1 p_2 + p_3$$

$$4e_4 = e_3 p_1 - e_2 p_2 + e_1 p_3 - p_4$$

$$\vdots$$

The power sum symmetric polynomials may be recursively expressed in terms of the elementary symmetric polynomials as follows:

$$p_k(X_1, X_2, \ldots, X_n) = (-1)^{k-1} k\, e_k(X_1, X_2, \ldots, X_n)$$

$$+ \sum_{j=1}^{k-1} (-1)^{k-1+j} e_{k-j}(X_1, X_2, \ldots, X_n)\, p_j(X_1, X_2, \ldots, X_n)$$

For any $n \geq 1$ and $k \geq 1$.

Explicitly,

$$p_1 = e_1$$

$$p_2 = e_1 p_1 - 2e_2$$

$$p_3 = e_1 p_2 - e_2 p_1 + 3e_3$$

$$p_4 = e_1 p_3 - e_2 p_2 + e_3 p_1 - 4e_4$$

$$\vdots$$

If the polynomials are over the binary extension field $GF(2^m)$ then:

$$k\, e_k = \begin{cases} 0, & k \text{ even} \\ \text{¿} e_k, & k \text{ odd} \end{cases}$$

$$p_{2k} = p_k^2$$