Primitive polynomial

In field theory, a branch of mathematics, a **primitivem polynomial** is the minimal polynomial of a primitive element of the finite extension field $\text{GF}(p^m)$. In other words, a polynomial $F(X)$ with coefficients in $\text{GF}(p) = \mathbb{Z}/p\mathbb{Z}$ is a primitive polynomial if it has a root $\alpha$ in $\text{GF}(p^m)$ such that
\[
\{0, 1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p^m-2}\}
\]
is the entire field $\text{GF}(p^m)$, and moreover, $F(X)$ is the smallest degree polynomial having $\alpha$ as root.

In ring theory, the term **primitive polynomial** is used for a different purpose, to mean a polynomial over an integral domain $R$ (such as the integers) such that no non-invertible element of $R$ divides all its coefficients at once. This article will not be concerned with the ring theory usage. See Gauss's lemma.

Properties

Because all minimal polynomials are irreducible, all primitive polynomials are also irreducible.

A primitive polynomial must have a non-zero constant term, for otherwise it will be divisible by $x$. Over the field of two elements, $x+1$ is a primitive polynomial and all other primitive polynomials have an odd number of terms, since any polynomial mod 2 with an even number of terms is divisible by $x+1$.

An irreducible polynomial of degree $m$, $F(x)$ over $\text{GF}(p)$ for prime $p$, is a primitive polynomial if the smallest positive integer $n$ such that $F(x)$ divides $x^n - 1$ is $n = p^m - 1$.

Over $\text{GF}(p^m)$ there are exactly $\phi(p^m - 1)/m$ primitive polynomials of degree $m$, where $\phi$ is Euler's totient function.

The roots of a primitive polynomial all have order $p^m - 1$.

Usage

Field element representation

Primitive polynomials are used in the representation of elements of a finite field. If $\alpha$ in $\text{GF}(p^m)$ is a root of a primitive polynomial $F(x)$ then since the order of $\alpha$ is $p^m - 1$ that means that all elements of $\text{GF}(p^m)$ can be represented as successive powers of $\alpha$:
\[
\text{GF}(p^m) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m-2}\}.
\]

When these elements are reduced modulo $F(x)$ they provide the polynomial basis representation of all the elements of the field.

Since the multiplicative group of a finite field is always a cyclic group, a primitive polynomials $f$ is a polynomial such that $x$ is a generator of the multiplicative group in $\text{GF}(p)[x]/f(x)$.
Pseudo-Random bit generation

Primitive polynomials define a recurrence relation that can be used to generate pseudorandom bits. In fact every linear feedback shift register with maximum cycle (that is \(2^{\text{length}} - 1\)) is related with primitive polynomial.

For example, given the primitive polynomial \(x^{10} + x^3 + 1\), we start with a user-specified bit seed (it need not randomly be chosen, but it can be). We then take the 10th, 3rd, and 0th bits of it, starting from the least significant bit, and xor them together, obtaining a new bit. The seed is then shifted left and the new bit is made the least significant bit of the seed. This process can be repeated to generate \(2^{10} - 1 = 1023\) pseudo-random bits.

In general, for a primitive polynomial of degree \(m\), this process will generate \(2^m - 1\) pseudo-random bits before repeating the same sequence.

CRC codes

The cyclic redundancy check (CRC) is an error-detection code that operates by interpreting the message bitstring as the coefficients of a polynomial over \(GF(2)\) and dividing it by a fixed generator polynomial also over \(GF(2)\); see Mathematics of CRC. Primitive polynomials, or multiples of them, are a good choice for generator polynomials because they can reliably detect two bit errors that occur far apart in the message bitstring, up to a distance of \(2^n - 1\) for a degree \(n\) primitive polynomial.

Primitive trinomials

A useful class of primitive polynomials is the primitive trinomials, those having only three nonzero terms, because they are the simplest and result in the most efficient pseudorandom number generators. A number of results give techniques for locating and testing primitiveness of trinomials.

For trinomials over \(GF(2)\), there is a simple test: for every \(r\) such that \(2^r - 1\) is a Mersenne prime, a trinomial of degree \(r\) is primitive if and only if it is irreducible. Recent algorithms invented by Richard Brent have enabled the discovery of primitive trinomials over \(GF(2)\) of very large degree, such as \(x^{6972593} + x^{3037958} + 1\). This can be used to create a pseudo-random number generator of the huge period \(2^{6972593} - 1\), or roughly \(10^{2098959}\).

Irreducible polynomial

In mathematics, the adjective **irreducible** means that an object cannot be expressed as the product of two or more non-trivial factors in a given set. See also factorization.

For any field \(F\), the ring of polynomials with coefficients in \(F\) is denoted by \(F[x]\). A polynomial \(p(x)\) in \(F[x]\) is called **irreducible over** \(F\) if it is non-constant and cannot be represented as the product of two or more non-constant polynomials from \(F[x]\). The property of irreducibility
depends on the field $F$; a polynomial may be irreducible over some fields but reducible over others. Some simple examples are discussed below.

Galois theory studies the relationship between a field, its Galois group, and its irreducible polynomials in depth. Interesting and non-trivial applications can be found in the study of finite fields.

It is helpful to compare irreducible polynomials to prime numbers: prime numbers (together with the corresponding negative numbers of equal magnitude) are the irreducible integers. They exhibit many of the general properties of the concept of 'irreducibility' that equally apply to irreducible polynomials, such as the essentially unique factorization into prime or irreducible factors:

Every polynomial $p(x)$ in $F[x]$ can be factorized into polynomials that are irreducible over $F$. This factorization is unique up to permutation of the factors and the multiplication of the factors by nonzero constants from $F$ (because the ring of polynomials over a field is a unique factorization domain whose units are the nonzero constant polynomials).

The set of roots (in an extension field) of any polynomial over $F$ must either contain no roots of a given irreducible polynomial $p$, or contain all such roots; this is Abel's irreducibility theorem.

**Simple examples**

The following five polynomials demonstrate some elementary properties of reducible and irreducible polynomials:

- $p_1(x) = x^2 + 4x + 4 = (x + 2)(x + 2)$
- $p_2(x) = x^2 - 4 = (x - 2)(x + 2)$
- $p_3(x) = x^2 - 4/9 = (x - 2/3)(x + 2/3)$
- $p_4(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$
- $p_5(x) = x^2 + 1 = (x - i)(x + i)$

Over the ring $\mathbb{Z}$ of integers, the first two polynomials are reducible, the last two are irreducible. (The third, of course, is not a polynomial over the integers.)

Over the field $\mathbb{Q}$ of rational numbers, the first three polynomials are reducible, but the other two polynomials are irreducible.

Over the field $\mathbb{R}$ of real numbers, the first four polynomials are reducible, but $p_5(x)$ is still irreducible.

Over the field $\mathbb{C}$ of complex numbers, all five polynomials are reducible. In fact, every nonzero polynomial $p(x)$ over $\mathbb{C}$ can be factored as
\[ p(x) = a(x - z_1) \cdots (x - z_n) \]

where \( n \) is the degree, \( a \) the leading coefficient and \( z_1, \ldots, z_n \) the zeros of \( p(x) \). Thus, the only non-constant irreducible polynomials over \( \mathbb{C} \) are linear polynomials. This is the Fundamental theorem of algebra.

The existence of irreducible polynomials of degree greater than one (without zeros in the original field) historically motivated the extension of that original number field so that even these polynomials can be reduced into linear factors: from rational numbers (\( \mathbb{Q} \)), to the real subset of the algebraic numbers (\( \mathbb{A} \cap \mathbb{R} \)), and finally to the algebraic subset of the complex numbers (\( \mathbb{A} \cap \mathbb{C} \)). After the invention of calculus those latter two subsets were later extended to all real numbers (\( \mathbb{R} \)) and all complex numbers (\( \mathbb{C} \)).

For algebraic purposes, the extension from rational numbers to real numbers is too "radical": it introduces transcendental numbers, which are not the solutions of algebraic equations with rational coefficients. These numbers are not needed for the algebraic purpose of factorizing polynomials (but they are necessary for the use of real numbers in analysis). The set of algebraic numbers (\( \mathbb{A} \)) is the algebraic closure of the rationals, and contains the roots of all polynomials (including \( i \) for instance). This is a countable field and is strictly contained in the complex numbers – the difference being that this field (\( \mathbb{A} \)) is "algebraically complete" (as are the complexes, \( \mathbb{C} \)) but not analytically complete since it lacks the aforementioned transcendals.

The above paragraph generalizes in that there is a purely algebraic process to extend a given field \( F \) with a given polynomial \( p(x) \) to a larger field where this polynomial \( p(x) \) can be reduced into linear factors. The study of such extensions is the starting point of Galois theory.

**Real and complex numbers**

As shown in the examples above, only linear polynomials are irreducible over the field of complex numbers (this is a consequence of the fundamental theorem of algebra). Since the complex roots of a real polynomial are in conjugate pairs, the irreducible polynomials over the field of real numbers are the linear polynomials and the quadratic polynomials with no real roots. For example, \( x^4 + 1 \) factors over the real numbers as \( (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \).

**Generalization**

If \( R \) is an integral domain, an element \( f \) of \( R \) which is neither zero nor a unit is called irreducible if there are no non-units \( g \) and \( h \) with \( f = gh \). One can show that every prime element is irreducible; the converse is not true in general but holds in unique factorization domains. The polynomial ring \( F[x] \) over a field \( F \) (or any unique-factorization domain) is again a unique factorization domain. Inductively, this means that the polynomial ring in \( n \) indeterminants (over a ring \( R \)) is a unique factorization domain if the same is true for \( R \).
Finite fields

Factorization over a finite field behaves similarly to factorization over the rational or the complex field. However, polynomials with integer coefficients that are irreducible over the field $\mathbb{Q}$ can be reducible over a finite field. For example, the polynomial $x^2 + 1$ is irreducible over $\mathbb{Q}$ but reducible over the field $\mathbb{F}_2$ of two elements. Indeed, over $\mathbb{F}_2$, we have

$$(x^2 + 1) = (x + 1)^2$$

The irreducibility of a polynomial over the integers $\mathbb{Z}$ is related to that over the field $\mathbb{F}_p$ of $p$ elements (for a prime $p$). Namely, if a polynomial over $\mathbb{Z}$ with leading coefficient 1 is reducible over $\mathbb{Z}$ then it is reducible over $\mathbb{F}_p$ for any prime $p$. The converse, however, is not true.