Berlekamp's Algorithm

Some Prerequisites:

- checking polynomial has no repeated factors

$$\boxed{gcd(f(x), f'(x)) = 1}$$

- How to calculate gcd?

$$\boxed{gcd(f, g) = gcd(g, f \% g)}$$

Ex: $f(x) = x^4 + x^3 + x^2 + 1$

$g(x) = x^3 + 1$

$$gcd(f, g) = gcd(x^4 + x^3 + x^2 + 1, x^3 + 1)$$

$$= gcd(x^3 + 1, x^2 + x)$$

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

$x+1$ divides $x^2 + x$

Hence $gcd(x^2 + x, x + 1) = x + 1$

$$gcd(F, g) = x + 1$$

Rank of matrix A:

- **Row echleon form of matrix A:**

→ The first non-zero element in each row called the leading entry = 1

→ Each leading entry is in a column to right of the leading entry in the previous row.

→ Rows with all zero elements, if any are below non-zero rows.

Example 1:

$$\begin{bmatrix} \textcircled{1} & 2 & 3 & 4 \\ 0 & 0 & \textcircled{1} & 3 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

= row echleon form

pivots.

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$$

= row echleon form

Example 2:

$$A = \begin{bmatrix} 2 & 4 & 6 & 8 \\ 1 & 3 & 0 & 5 \\ 1 & 1 & 6 & 3 \end{bmatrix}$$

Find the reduced row echleon form?

Soln:

$$A = \begin{bmatrix} 2 & 4 & 6 & 8 \\ 1 & 3 & 0 & 5 \\ 1 & 1 & 6 & 3 \end{bmatrix}$$

$$\tfrac{1}{2} R_1 \Rightarrow \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 0 & 5 \\ 1 & 1 & 6 & 3 \end{bmatrix}$$

$$\begin{pmatrix} R_2 - R_1 \\ R_3 - R_1 \end{pmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & -3 & 1 \\ 0 & -1 & 3 & -1 \end{bmatrix}$$

$$\begin{pmatrix} R_1 - 2R_2 \\ R_3 + R_2 \end{pmatrix} \quad \begin{bmatrix} 1 & 0 & 9 & 2 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

- **Rank of matrix**

* no. of non-zero rows in the reduced row echlon form.

* **Example:**

$$\begin{bmatrix} 1 & 0 & 9 & 2 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{\text{Rank}} \boxed{\text{Rank} = 2}$$

- **Basis of null space of matrix**

To find basis of null space of matrix A, compute vector form solution of

$$\boxed{Ax = 0}$$

$$\begin{bmatrix} \textcircled{1} & 0 & 9 & 2 \\ 0 & \textcircled{1} & -3 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

↙ ↙ ⤷ free variables.

pivot variables

Find the basis for the null space of the above ~~algorithm~~ matrix ?

Solution:

Let $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$

$Ax = 0$

$$\begin{pmatrix} 1 & 0 & 9 & 2 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 + 9x_3 + 2x_4 \\ x_2 - 3x_3 + x_4 \\ 0 \end{pmatrix} = 0$$

$$x_1 = -9x_3 - 2x_4$$
$$x_2 = 3x_3 - x_4$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} -9x_3 - 2x_4 \\ 3x_3 - x_4 \\ x_3 \\ x_4 \end{pmatrix}$$

$$= x_3 \begin{pmatrix} -9 \\ 3 \\ 1 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} -2 \\ -1 \\ 0 \\ 1 \end{pmatrix}$$

∴ "basis"

• **Theorem**: let F_q be a field. if $f \in F_q[x]$ is a monic polynomial and $h \in F_q[x]$ is such that $h^q \equiv h \bmod f$ then:

$$f(x) = \prod_{c \in F_q} \gcd(f(x), h(x) - c)$$

$$c = 0, 1, 2 \ldots q-1$$

Steps of Berlekamp's algorithm:

1) Check polynomial has no repeated factors

2) Compute $x^{iq} \bmod f(x)$

for q = field & $0 <= i <= n-1$

n = degree of polynomial

3) Get coefficient matrix B from computation of x^{iq}

4) Find $B - I$, I = identity matrix of size $n \times n$

(r)

5) Find rank of matrix B - I

6) Calculate $k = n - r$, k = number of distinct monic irreducible factors.

7) Compute the basis of null space of matrix B - I and our h(x) f reducing polynomial.

8) Using theorem, calculate the gcd (f(x), h(x) - c) where c ∈ Fq

9) we get the required answer.

Ex 1: Factorize $f(x) = x^4 + x^2 + x + 1$ over F_2 by Berlekamp's algorithm ?

Soln: $f(x) = x^4 + x^2 + x + 1$ $\boxed{n = 4}$

(1) $f'(x) = 4x^3 + 2x + 1$

$\gcd(f(x), f'(x)) = 1$

(2) $q = 2,\ i = 0, 1, 2, 3$

Compute $x^{2i} \bmod f(x)$

$x^0 \equiv 1 \bmod f(x)$ — 1st row

$x^2 \equiv x^2 \bmod f(x)$ — 2nd row

$x^4 \equiv 1 + x + x^2 \bmod f(x)$ — 3rd row

$x^6 \equiv 1 + x + x^3 \bmod f(x)$ — 4th row

(3) Coefficient matrix B

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

$$I_{4\times 4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(4) $B - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$

(5) rank of $B - I = 2$

(6) $k = 4 - 2 = 2$ distinct monic irreducible factors.

(7) Basis of $B - I$ = null space of $= (1\ 0\ 0\ 0) \& (0\ 0\ 1\ 1)$

(8) Polynomials corresponding to basis vectors are:

$h_1(x) = 1$

$h_2(x) = x^2 + x^3$

(9) Using theorem,

$q = 2$

$C = 0, 2-1$

$C = 0, 1$

Using polynomial $h_2(x)$

Compute $\boxed{gcd(f(x), h_2(x) - C)}$

$gcd(f(x), h_2(x) - 0) = x + 1$

$gcd(f(x), h_2(x) - 1) = x^3 + x^2 + 1$

Hence the answer is:

$f(x) = (x+1)(x^3 + x^2 + 1)$

Ex2: Factorize $f(x) = x^8 + x^7 + x^4 + x^3 + x + 1$ over F_3 by Berlekamp's Algorithm?

Soln:

$f(x) = x^8 + x^7 + x^4 + x^3 + x + 1$

(1) $f'(x) = 8x^7 + 7x^6 + 4x^3 + 3x^2 + 1 + 0$

Since $gcd(F(x), f'(x)) = 1$, $f(x)$ has no repeated factors.

(2) Now we compute $x^{iq} = x^{3i}$

$q = 3, \; i = 0, 1, 2 - - 7$

$x^0 \equiv 1 \mod f(x)$

$x^3 \equiv x^3 \mod f(x)$

$x^6 \equiv x^6 \mod f(x)$

$x^9 \equiv 1 + 2x^2 + x^3 + 2x^5 + x^7 \mod f(x)$

$x^{12} \equiv x + x^4 + 2x^5 \mod f(x)$

$x^{15} \equiv 1 + x + x^3 + 2x^4 + 2x^7 \mod f(x)$

$x^{18} \equiv 1 + x^4 + 2x^6 \mod f(x)$

$x^{21} \equiv 2 + x^2 + x^5 \mod f(x)$

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 2 & 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 & 2 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$B - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 & 0 & 2 \end{pmatrix}$$

rank of $B - I = 5$

$r = 5$

$n = 8$

$k = n - r = 8 - 5 = 3$ distinct monic irreducible ~~Polyn~~ factors

The null space of B-I contains

$(1\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$ $(0\ 0\ 0\ 1\ 0\ 0\ 0\ 1)$

$(0\ 2\ 2\ 1\ 1\ 1\ 1\ 0)$

The polynomials corresponding to null space are:

$h_1(x) = 1$

$h_2(x) = x^3 + x^7$

$h_3(x) = 2x + 2x^2 + x^3 + x^4 + x^5 + x^6$

First we take $h_2(x)$ & apply theorem 3:

$gcd(f(x), h_2(x) - 0) = 1$

$gcd(f(x), h_2(x) - 1) = 1 + x$

$gcd(f(x), h_2(x) - 2) = 1 + x^3 + x^7$

Since $f(x)$ has three distinct monic irreducible factors, but we have only two., so further factorize $1 + x^3 + x^7$. with $k = 2$. using the same procedure

$$(1 + x^3 + x^7) = (2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6)(2 + x)$$

$$f(x) = (1 + x)(2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6)(2 + x)$$

Now For $(2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6)$, $k = 1$ so it is irreducible, hence we stop here.

Now we take $h_3(x)$, applying theorem we get:

$$gcd(f(x), h_3(x) - 0) = 1 + x$$

$$gcd(f(x), h_3(x) - 1) = 2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6$$

$$gcd(f(x), h_3(x) - 2) = 2 + x$$

~~Reference~~

we get the same factors as for $h_2(x)$

Hence the final answer will be:

$$f(x) = (1 + x)(2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6)(2 + x)$$