8. Let α be a primitive nth root of unity in an extension $\mathrm{GF}(p^m)$ of $\mathrm{GF}(p)$ and let
$$f(X) = \prod_{i \in K} (X - \alpha^i)$$
where K is a subset of $\{0, 1, 2, \ldots, n-1\}$. The coefficients of $f(X)$ are in $\mathrm{GF}(p)$ iff $k \in K$ implies $pk \in K$ modulo n. Comment!

7.3 BERLEKAMP'S ALGORITHM FOR FACTORIZATION OF POLYNOMIALS

We have earlier considered two simple methods for factorization of a polynomial $(x^n - 1)$ over $\mathrm{GF}(q)$. We here give an algorithm due to Berlekamp (1968) for factorization of an arbitrary polynomial.

Let $F = \mathrm{GF}(q)$ be the field of q elements and
$$f(x) = \sum_{i=0}^{m} a_i x^i$$
be a monic polynomial of degree m over F. Let $\mathbf{Q} = (Q_{ij})$ be the square matrix of order m over F in which the ith row is represented by $x^{q(i-1)}$ reduced modulo $f(x)$. For example, if
$$f(x) = x^5 + x^3 + 1$$
and $q = 3$, then the third row of the $\mathbf{Q}$-matrix is $(x^6 \equiv -x - x^4 (\mathrm{mod}\, f(x)))$
$$0 \quad -1 \quad 0 \quad 0 \quad -1$$

Lemma 7.2
Given any polynomial
$$g(x) = \sum_{i=0}^{m-1} g_i x^i$$
over F of degree less than m,
$$g(x)^q - g(x) \equiv 0 (\mathrm{mod}\, f(x))$$
iff the row vector $(g_0 \quad g_1 \quad \cdots \quad g_m)$ is in the null space of $\mathbf{Q} - \mathbf{I}$, where $\mathbf{I}$ is the identity matrix of order m.

Proof
As $q\beta = 0$ for every $\beta \in F$,
$$\begin{aligned} g(x)^q &= g(x^q) \\ &= \sum_{i=0}^{m-1} g_i x^{iq} \\ &\equiv \sum_{i=0}^{m-1} g_i \left(\sum_{k=0}^{m-1} Q_{i+1,k+1} x^k \right) \qquad (\mathrm{mod}\, f(x)) \\ &\equiv \sum_{k=0}^{m-1} \left(\sum_{i=0}^{m-1} g_i Q_{i+1,k+1} \right) x^k \end{aligned}$$

Observe that

$$\sum_{i=0}^{m-1} g_i Q_{i+1,k+1}$$

is the $(k+1)$th entry of the product

$$(g_0 \quad g_1 \quad \cdots \quad g_{m-1})\mathbf{Q}$$

Also g_k is the $(k+1)$th entry of the product

$$(g_0 \quad g_1 \quad \cdots \quad g_{m-1})\mathbf{I}$$

Therefore,

$$\begin{aligned} g(x)^q - g(x) &\equiv \sum_{k=0}^{m-1} \left(\left(\sum_{i=0}^{m-1} g_i Q_{i+1,k+1} \right) - g_k \right) x^k \\ &= 0 \end{aligned}$$

iff

$$\left(\sum_{i=0}^{m-1} g_i Q_{i+1,k+1} \right) - g_k = 0 \quad \forall k, 0 \le k \le m-1$$

or equivalently

$$(g_0 \quad g_1 \quad \cdots \quad g_{m-1})(\mathbf{Q} - \mathbf{I}) = 0$$

Theorem 7.4

$$f(x) = \prod_{s \in F} [\text{g.c.d.}(f(x), g(x) - s)]$$

where

$$g(x) = \sum_{i=0}^{m-1} g_i x^i$$

is such that

$$(g_0 \quad g_1 \quad \cdots \quad g_{m-1})(\mathbf{Q} - \mathbf{I}) = 0$$

Proof
By the above lemma

$$f(x) \mid g(x)^q - g(x)$$

But

$$g(x)^q - g(x) = \prod_{s \in F} (g(x) - s)$$

since for any y

$$y^q - y = \prod_{s \in F} (y - s)$$

Therefore

$$f(x) \mid \prod_{s \in F} (g(x) - s)$$

and hence

$$f(x) = \text{g.c.d.}(f(x), \prod_{s \in F} (g(x) - s))$$

Also

$$\text{g.c.d.}\left(f(x), \prod_{s \in S} (g(x) - s)\right) \Bigg| \prod_{s \in F} (f(x), g(x) - s)$$

or

$$f(x) \Bigg| \prod_{s \in F} \text{g.c.d.}(f(x), g(x) - s) \tag{7.2}$$

On the other hand

$$\text{g.c.d.}(f(x), g(x) - s) \mid f(x)$$

and for $s \neq t$ in F, $g(x) - s$ and $g(x) - t$ are relatively coprime. Therefore, g.c.d.$(f(x), g(x) - s)$ and g.c.d.$(f(x), g(x) - t))$ are coprime, and so

$$\prod_{s \in F} \text{g.c.d.}(f(x), g(x) - s) \mid f(x) \tag{7.3}$$

The polynomial $f(x)$ being monic, it follows from (7.2) and (7.3) that

$$f(x) = \prod_{s \in F} \text{g.c.d.}(f(x), g(x) - s)$$

Examples 7.3

Case (i)
Consider first the polynomial

$$f(x) = x^5 + x^3 + 1$$

over GF(3). The successive powers of x needed are:

$$x^0 = 1$$

$$x^3$$

$$x^6 = -x - x^4$$

$$x^9 = x^2 - x^4 + x^5 = -1 + x^2 - x^3 - x^4$$

$$x^{12} = 1 + x + x^2 + x^4$$

Therefore

$$\mathbf{Q}-\mathbf{I}=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & -1 \\ -1 & 0 & 1 & 1 & -1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Let $(g_0 \quad g_1 \quad \cdots \quad g_4)$ be in the null space of $\mathbf{Q}-\mathbf{I}$. Then

$$-g_3+g_4=0$$

$$-g_1-g_2+g_4=0$$

$$-g_2+g_3+g_4=0$$

$$g_1+g_3=0$$

and

$$-g_2-g_3=0$$

Thus

$$g_1=g_2=-g_3=-g_4$$

and

$$g(x)=g_0+g_1(x+x^2-x^3-x^4) \tag{7.4}$$

Let $g_1=g_0=-1$ and take $s=0$. We then need to find the HCF of $x^4+x^3-x^2-x-1$ and x^5+x^3+1.

$$\begin{array}{lr} x^4+x^3-x^2-x-1 & x^5 \qquad +x^3 \qquad\qquad +1 \\ & \underline{x^5+x^4-x^3-x^2-x \qquad} \\ & -x^4-x^3+x^2+x+1 \end{array}$$

Therefore, the HCF is $x^4+x^3-x^2-x-1$ and we have

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

By multiplying $g(x)$ as in (7.4) by $-g_1^{-1}$, we could have taken

$$g(x)=x^4+x^3-x^2-x+g_0'$$

The above HCF obtained corresponds to taking $s=-g_0'-1$. It is clear that by taking a different value of g_0', we find that $g(x)$ is coprime to x^5+x^3+1.

Since none of the elements of GF(3) is a root of

$$h(x)=x^4+x^3-x^2-x-1$$

this polynomial does not have a linear factor. The only monic irreducible polynomials of degree 2 over GF(3) are

$$x^2+x-1 \qquad x^2+1 \qquad x^2-x-1$$

and none of these is a factor of $h(x)$. Hence $h(x)$ is an irreducible polynomial over GF(3). Hence

$$x^5 + x^3 + 1 = (x - 1)h(x)$$

is a factorization of $f(x)$ as a product of irreducible polynomials.

Case (ii)

Next, consider the binary polynomial

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

For writing the **Q**-matrix, the powers of x needed are

$$\begin{aligned} &x^0 = 1 \qquad x^2 \qquad x^4 \qquad x^6 \\ &x^8 = 1 + x + x^3 + x^7 \\ &x^{10} = 1 + x^4 + x^5 \\ &x^{12} = x^2 + x^6 + x^7 \\ &x^{14} = x + x^2 \end{aligned}$$

Therefore,

$$\mathbf{Q} - \mathbf{I} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Let $\mathbf{g} = (g_0 \quad g_1 \quad \cdots \quad g_7)$ be in the null space of $\mathbf{Q} - \mathbf{I}$. Then

$$\begin{aligned} &g_4 + g_5 = 0 \qquad g_1 + g_4 + g_7 = 0 \qquad g_1 + g_2 + g_6 + g_7 = 0 \\ &g_3 + g_4 = 0 \qquad g_2 + g_4 + g_5 = 0 \qquad g_3 = 0 \qquad g_4 + g_6 + g_7 = 0 \end{aligned}$$

These equations yield

$$g_1 = g_2 = g_3 = g_4 = g_5 = g_6 = g_7 = 0$$

Therefore, $g(x) = g_0$ is a constant and the algorithm does not yield any factors of $f(x)$. Neither 0 nor 1 being a root of $f(x)$, $f(x)$ has no linear factors. As is easily seen, the only irreducible polynomial $x^2 + x + 1$ of degree 2 is not a divisor of $f(x)$. Also $x^3 + x + 1$ and $x^3 + x^2 + 1$ are the only irreducible polynomials of degree 3 and neither of these divides $f(x)$. None of the three irreducible polynomials

$$x^4 + x^3 + 1 \qquad x^4 + x + 1 \qquad x^4 + x^3 + x^2 + x + 1$$

of degree 4 is a divisor of $f(x)$ and it follows that $f(x)$ is an irreducible polynomial.

The above conclusion could easily have been drawn from the following general theorem (the proof of which we omit for the time being).

Theorem 7.5
The number of distinct irreducible factors of $f(x)$ is equal to the dimension of the null space of $\mathbf{Q}-\mathbf{I}$.

Let us now consider one more example:

Examples 7.3 *contd*

Case (iii)
Consider the binary polynomial

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

The relevant powers of x are

$$\begin{aligned}
x^0 &= 1\\
&\quad x^2, x^4, x^6\\
x^8 &= x+x^2+x^3+x^5+x^6\\
x^{10} &= x^3+x^4+x^5+x^7+x^8\\
&= x^3+x^4+x^5+1+x+x^2+x^4+x^5+x+x^2+x^3+x^5+x^6\\
&= 1+x^5+x^6\\
x^{12} &= x^2+x^7+x^8\\
&= x^2+1+x+x^2+x^4+x^5+x+x^2+x^3+x^5+x^6\\
&= 1+x^2+x^3+x^4+x^6
\end{aligned}$$

Therefore,

$$\mathbf{Q}-\mathbf{I}=\begin{pmatrix}0&0&0&0&0&0&0\\0&1&1&0&0&0&0\\0&0&1&0&1&0&0\\0&0&0&1&0&0&1\\0&1&1&1&1&1&1\\1&0&0&0&0&0&1\\1&0&1&1&1&0&0\end{pmatrix}$$

If $(g_0 \quad g_1 \quad \cdots \quad g_6)$ is in the null space of $\mathbf{Q}-\mathbf{I}$, then

$$\begin{array}{llll}
g_5+g_6=0 & g_1+g_4=0 & g_1+g_2+g_4+g_6=0 & \\
g_3+g_4+g_6=0 & g_2+g_4+g_6=0 & g_4=0 & g_3+g_4+g_5=0
\end{array}$$