

### Abstract

Sketch of how to find all primitive polynomials after finding any one of them.

Now that we have found one primitive polynomial  $f(x)$  by searching, we can find all the others.

*Theorem.* If  $f(x)$  is any primitive polynomial with root  $a = x$ , all

$$\phi(p^n - 1)/n$$

primitive polynomials are given by the set

$$\{f_s(x) = (x - a)(x - a^p)(x - a^{p^2}) \dots (x - a^{p^{n-1}}) \mid \gcd(s, p^n - 1) = 1\}$$

*Proof.* We know that all the primitive elements of the field are given by

$$\{a^s \mid \gcd(s, p^n - 1) = 1\}$$

and the minimal polynomial of primitive element  $a^s$  is the primitive polynomial

$$f_s(x) = (x - a)(x - a^p)(x - a^{p^2}) \dots (x - a^{p^{n-1}})$$

We'd need to use finite field arithmetic and raise each element  $a$  to high powers. An idea from Berlekamp is to note that

$$f_s(a^s) = 0$$

for all  $s$  so if we write out

$$f_s(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$$

and

$$M = \begin{pmatrix} | & | & | & \dots & | \\ 1 & a^s & a^{2s} & \dots & a^{(n-1)s} \\ | & | & | & \dots & | \end{pmatrix}$$

where the columns are coefficients of polynomials,

$$a^s = x^s \text{ mod } (f(x), p)$$

we get

$$Mc + c_n a^{sn} = 0$$

Now since  $a^s$  is a primitive element, the set

$$\{1, a^s, a^{2s}, \dots, a^{(n-1)s}\}$$

is a basis. So as a matrix, the columns are all linearly independent, and  $\text{rank}(M) = n$ . Thus we have a unique solution.

$$c = -M^{-1}c_n$$

We can use Gaussian elimination on the matrix  $M$  and back substitute to find the coefficients  $c$  of the primitive polynomial with  $O(n^2)$  operations. However, as the matrix is Toeplitz, there is an  $O(n)$  solution.