Explicit Construction of Irreducible Polynomials over Finite Field F_2 in Cluster Computational Environment*

Ofelya Manukyan

Institute for Informatics and Automation Problems,
1, P. Sevak str., Yerevan, 0014,
Armenia,
e-mail: manofa81@yahoo.com

ABSTRACT

This paper presents some results concerning explicit construction of irreducible polynomials of higher degree over finite field F_2 from the given sequence of primitive polynomials. The explicit construction of irreducible polynomials is based on Theorem 4 by Kyuregyan [1] and on Varshamov's operator. A software package (IPG) has been designed which allows us to constract polynomials described above.

Keywords

Finite fields, irreducible polynomials, Varshamov's operator.

1. INTRODUCTION

Let $L^\theta f(x)$ be the operator of Varshamov:

$$L^\theta f(x) = \frac{1}{\theta(x)} \sum_{u=0}^{\theta} \sum_{v=0}^{n} \theta_u a_v x^{uq^v}$$

where $f(x) = \sum_{u=0}^{n} a_u x^u$ and $\theta(x) = \sum_{v=0}^{m} a_v x^v$, $a_u, \theta_v \in F_2$.

Let $\Sigma_\sigma = \{f_1(x), f_2(x), ..., f_\sigma(x)\}$ be a set of σ primitive polynomials with pairwise relatively prime degrees $n_1, n_2, ..., n_\sigma (n_i > 1)$, respectively, over F_2; $T = \prod_{i=1}^{\sigma} (2^{n_i} - 1)$; $\varphi(x)$ be an irreducible polynomial of degree n over F_2; $\gcd(n, T) = 1$; G_σ be the selection of all possible sequences $\varepsilon = (\varepsilon_1, \varepsilon_2, ..., \varepsilon_\sigma)$ of length σ, where $\varepsilon_i = 0$ or 1. Furthermore, let for any sequences $\varepsilon \in G_\sigma$

$$f(x, \varepsilon, \Sigma_\sigma) = L^x \prod_{i=1}^{\sigma} f_i(x)^{\varepsilon_i},$$

$$xf(x, \varepsilon, \Sigma_\sigma) \equiv R^{(\varepsilon)}(x) (\mathrm{mod}\, \varphi(x)),$$

and $\psi^{(\varepsilon)}(x) = \sum_{u=0}^{n} \psi_u^{(\varepsilon)} x^u$, where $\psi_u^{(\varepsilon)}$ is a nontrivial solution of the congruence

$$\sum_{u=0}^{n} \psi_u^{(\varepsilon)} (R^{(\varepsilon)}(x))^u \equiv 0 (\mathrm{mod}\, \varphi(x)).$$

* The research was supported by ISTC A-1451 project.

Then we have the following theorem.

Theorem 4. The polynomials

$$F(x) = (\varphi(x))^{(-1)^\sigma} \frac{\prod_{\substack{\varepsilon \in G_\sigma \\ 2|(\sigma - |\varepsilon|)}} \psi^{(\varepsilon)}(xf(x, \varepsilon, \Sigma_\sigma))}{\prod_{\substack{\varepsilon \in G_\sigma \\ 2\dagger(\sigma - |\varepsilon|)}} \psi^{(\varepsilon)}(xf(x, \varepsilon, \Sigma_\sigma))}$$

and $\psi^{(v)}(x)$ of degree nT and n, respectively (where $|\varepsilon| = \sum_{i=1}^{\sigma} \varepsilon_i$ and $v \in G_\sigma$), are irreducible over F_2.

In this paper we present an overview of the method to construct explicitly irreducible polynomials of higher degrees over finite field F_2 from the given sequence of primitive polynomials. Further, in section 2 we give the description of a software package IPG (Irreducible Polynomial Generator) provided to construct such polynomials, and gives the details of its implementation under Armenian Grid infrastructure.

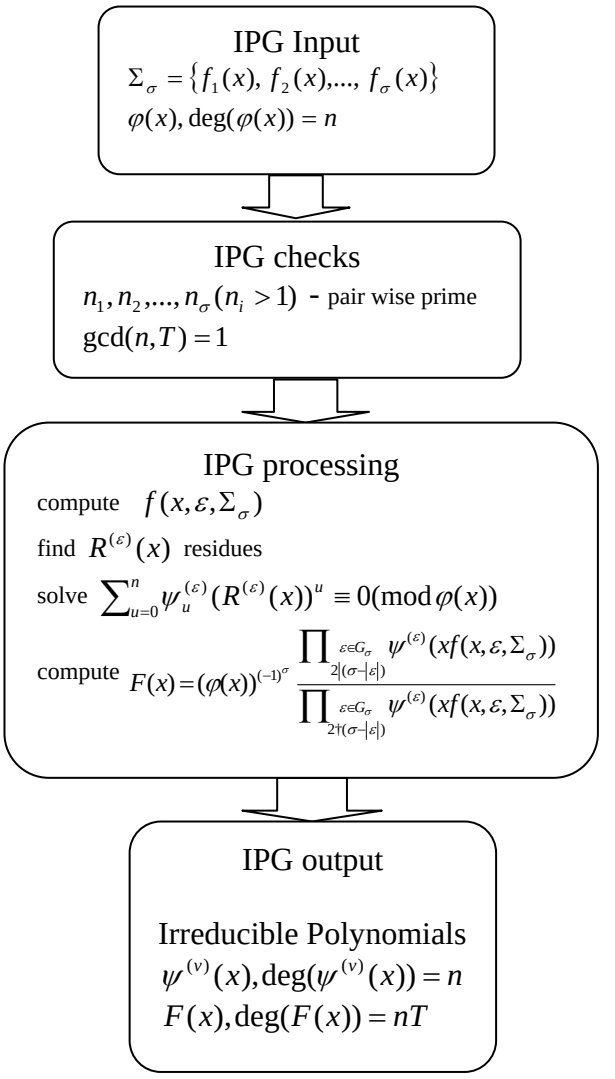
2. IMPLEMENTATION

IPG is a software package which runs on a network cluster using MPI as a scheduler. The Scheme 1.1 overviews the main operational blocks of IPG.

The field operations are performed in the most optimal way as possible. For the optimal computation of residue polynomials $\mathrm{mod}\, \varphi(x)$ we compute and keep the set $F[x]/(\varphi(x))$ (equivalence class) of polynomials in $F[x]$ with degrees less than $\deg(\varphi(x))$. That is as $\varphi(x)$ is an irreducible polynomial of degree n over F_2, or, equivalently, the field element $x = (0...010)$ is the generator of F_{2^n}, $F[x]/(\varphi(x))$ is the set of powers of x modulo $\varphi(x)$. For example, for F_{2^4} with $\varphi(x) = x^4 + x + 1$ irreducible polynomial the computations are summarized in Table 1.1.

To compute $p(x) \bmod \varphi(x)$, where $p(x) = \sum_{u=0}^{m} p_u x^u$ we replace the polynomial members $x^u (0 \le u \le m)$ with the appropriate elements $x^i (0 \le i \le 2^n - 1)$ from the equivalence class $F[x]/(\varphi(x))$:

$$x^u \to x^i, \text{ where } i = u \bmod (2^n - 1)$$



Scheme 1.1 Operational blocks of the software package IPG

i	$x^i \bmod x^4 + x + 1$	vector notation
0	1	(0001)
1	x	(0010)
2	x^2	(0100)
3	x^3	(1000)
4	$x + 1$	(0011)
5	$x^2 + x$	(0110)
6	$x^3 + x^2$	(1100)
7	$x^3 + x + 1$	(1011)
8	$x^2 + 1$	(0101)
9	$x^3 + x$	(1010)
10	$x^2 + x + 1$	(0111)
11	$x^3 + x^2 + x$	(1110)
12	$x^3 + x^2 + x + 1$	(1111)
13	$x^3 + x^2 + 1$	(1101)
14	$x^3 + 1$	(1001)

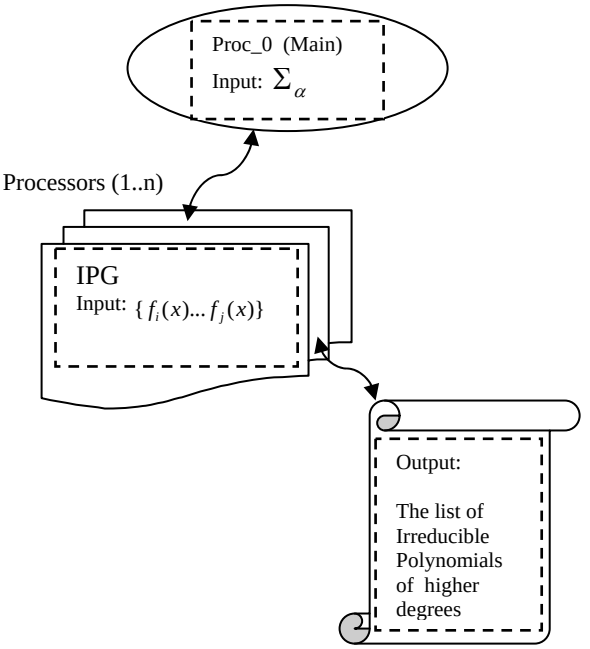
Table1.1 The powers of $x = (0010)$ modulo $\varphi(x) = x^4 + x + 1$

2.1 TASK PARALLELIZATION

The object is to construct irreducible polynomials with even and higher degrees from initially given $\Sigma_\sigma = \{f_1(x), f_2(x), ..., f_\sigma(x)\}$ set of σ primitive polynomials over F_2 with pairwise relatively prime degrees $n_1, n_2, ..., n_\sigma (n_i > 1)$. Let Σ_α be the set of all possible pairs, triples,…, $(\sigma - 1)$-tuples of the set Σ_σ and Σ_σ itself:

$$\Sigma_\alpha = \begin{Bmatrix} \{f_1(x), f_2(x)\}, \{f_1(x), f_3(x)\}, ..., \{f_{\sigma-1}(x), f_\sigma(x)\}, \\ \{f_1(x), f_2(x), f_3(x)\}, \{f_1(x), f_3(x), f_4(x)\}, ..., \{f_{\sigma-2}(x), f_{\sigma-1}(x), f_\sigma(x)\}, \\ ..... \\ \Sigma_\sigma = \{f_1(x), f_2(x), ... f_\sigma(x)\} \end{Bmatrix}$$

Task paralleling in the program is realized as follows: one of the processes is considered as the main (Scheme 2.1 overviews the parallelization in IPG). It distributes the elements of Σ_α among the other processors and registers the outcome. Upon receiving these elements of Σ_α as IPG input, the other processors run IPG and inform the main process on the obtained results, namely send the found irreducible polynomial to the main process. In the end we obtain the full list of irreducible polynomials of higher degrees in explicit forms.



Scheme 2.1 Parallelization in IPG

REFERENCES

[1] Mels K. Kyuregyan, "Recurrent Methods for Constructing Irreducible Polynomials over $GF(2^s)$", *Finite Fields and Their Applications 8*, pp. 52-68, 2002.