The research of the Binary Codes
Program Complication
and Application in Cyber
Physical Systems
Andrii Kostyk¹, Valerii Hlukhov²,
Ivan Zholubak³
¹Computer Engineering Department, Lviv Polytechnic National
University, UKRAINE, Lviv, S. Bandery street 28a,
E-mail: andy989gov@gmail.com
²Computer Engineering Department, Lviv Polytechnic National
University, UKRAINE, Lviv, S. Bandery street 28a,
E-mail: valeriygl@ukr.net
³Computer Engineering Department, Lviv Polytechnic National
University, UKRAINE, Lviv, S. Bandery street 28a,
E-mail: IvanZholubak7@ukr.net

Abstract – The research of the binary codes program
complication and application in Cyber Physical Systems.
Calculation and finding irreducible polynomials for Galois
field GF(pᵐ).

Key words – Mathematical package Maple, Galois field
GF(3ᵐ), Galois field GF(2ᵐ).

I. Introduction
The use of electronic documents offers new opportunities
to exchange information, through a global network and
peripherals. But there is a problem regarding the protection
of electronic documents from a possible modification,
copying, forgery and manipulation. To solve it requires a
variety of means and methods of information security. One
of these methods of information protection is a digital
signature (CPU), which with the help of special software
guarantees the authenticity of the document, its details and
the signing specific person.

II. Irreducible polynomials
To perform multiplication elements Galois fields
important finding irreducible polynomials that form field.
This operation requires considerable time-consuming,
especially for fields with a large order. Using
mathematical package Maple can find such polynomials
for the selected field and assess the time of their location,
allowing you to indirectly evaluate the complexity of
processing elements chosen field. It uses command and
Nextprime time.

Table 1 shows a comparison time of polynomials that
form field for Galois fields with bases 2, 3, 5, 7, 11, 13
and various orders. The value of the order m in each
column of the elected terms of approximate equality in
number elemetiv field GF (pm).

Table 1 shows that there are fields of high and low
time complexity calculation irreducible polynomials,
which indirectly points to the possible complications of
processing elements separate fields. This field of higher
order may have less time complexity (Fig. 1).

TABLE 1

<table>
<thead>
<tr>
<th>p</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>m</td>
<td>998</td>
<td>1578</td>
<td>629</td>
<td>3343</td>
<td>429</td>
<td>289</td>
</tr>
<tr>
<td>time</td>
<td>211</td>
<td>203</td>
<td>133</td>
<td>0.269</td>
<td>0.015</td>
<td>0.031</td>
</tr>
</tbody>
</table>

Fig. 1. Calculating irreducible polynomials
for Galois fields GF(pᵐ)

Table 2

IRREDUCIBLE POLYNOMIAL

<table>
<thead>
<tr>
<th>GF</th>
<th>m=100</th>
<th>m=200</th>
<th>m=400</th>
<th>m=600</th>
<th>m=998</th>
<th>m=2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>GF(2ᵐ)</td>
<td>0.0015</td>
<td>0.0078</td>
<td>0.281</td>
<td>0.031</td>
<td>1.89</td>
<td>36,312</td>
</tr>
<tr>
<td>GF(3ᵐ)</td>
<td>0.062</td>
<td>0.078</td>
<td>0.562</td>
<td>3.843</td>
<td>27.218</td>
<td>64</td>
</tr>
<tr>
<td>GF(5ᵐ)</td>
<td>0.015</td>
<td>1.218</td>
<td>1.093</td>
<td>2.763</td>
<td>45.515</td>
<td>223,156</td>
</tr>
<tr>
<td>GF(7ᵐ)</td>
<td>0.136</td>
<td>0.236</td>
<td>23.328</td>
<td>45.015</td>
<td>6.75</td>
<td>155</td>
</tr>
<tr>
<td>GF(11ᵐ)</td>
<td>1.031</td>
<td>7.546</td>
<td>24.723</td>
<td>15.14</td>
<td>185.937</td>
<td>504.359</td>
</tr>
<tr>
<td>GF(13ᵐ)</td>
<td>0.109</td>
<td>2.343</td>
<td>26.203</td>
<td>79.078</td>
<td>122.67</td>
<td>171.562</td>
</tr>
</tbody>
</table>

Figure 2 shows the time of the irreducible polynomial
for the Galois field GF (2ᵐ) and GF (3ᵐ) with equal
powers m (Table 2).
Fig. 2. Comparison times return irreducible polynomials with the same degrees of Galois fields

Conclusion

The possibility of verification of binary operations on elements of Galois fields using mathematical package Maple.

References