The research of multiplication in the ternary Galois fields

Andrii Kostyk[1], Valerii Hlukhov[2], Leonid Berezko[3]

1. Computer Engineering Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 28a, E-mail: andy989gow@gmail.com

2. Computer Engineering Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 28a, E-mail: valeriygl@ukr.net

3. Computer Engineering Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 28a, E-mail: leonid.berezko@gmail.com

***Abstract* – The research of multiplication in the ternary Galois fields Calculation and finding irreducible polynomials for Galois field GF(p^m). Consider the proposed method of construction serial ternary multiplier element Galois field GF (3^m).**

Keywords – Galois field GF(2^m), Mathematical package Maple, Galois field GF(3^m).

I. Introduction

To protect electronic documents from a possible modification, forgery, copying, use digital signature, to guarantee authenticity

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. Modified Guild cell

To construct the ternary field GF (3^m), used modified Guild cells that are different from the binary field increased number of input and output data. Guild cell has a 6-bit input and 2-bit output. The modification is that the construction does not use cell transfer.

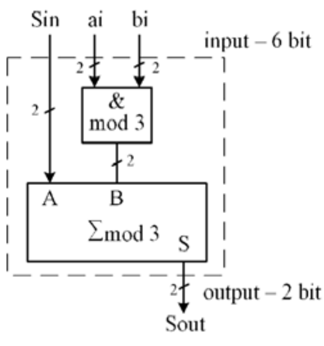


Fig. 1. Modified Guild cell for GF (3^m).

Matrix multiplier for direct and reverse field GF (2^3), shown in Fig. 2.

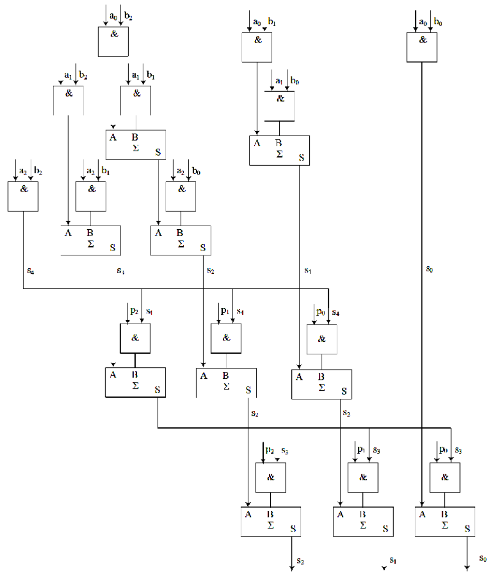


Fig.2. Matrix Multiplier for direct and reverse fields GF(2^3).

III. 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.

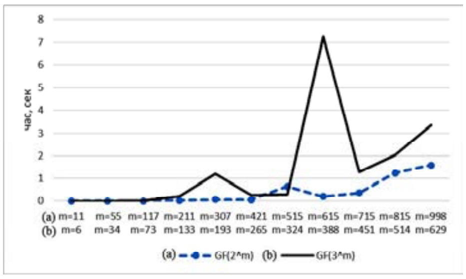
Table 1 shows a comparison time of polynomials that form field for Galois fields with bases 2, 3, 5, 7, 11, 13 and various orders. The value of the order m in each column of the elected terms of approximate equality in number elemetiv field GF (pm).

TABLE 1

CALCULATING IRREDUCIBLE POLYNOMIALS FOR GALOIS FIELDS GF(p^M)

p	m / time						
2	998	815	715	615	421	307	211
	1,578	*1,234*	*0,359*	*0,203*	*0,046*	*0,062*	*0,031*
3	629	514	451	388	265	193	133
	3,343	*2,046*	*1,281*	*7,234*	*0,25*	*1,203*	*0,203*
5	429	351	307	264	181	132	90
	3,656	*2,109*	*1,765*	*2,515*	*0,203*	*0,078*	*0,062*
7	355	290	254	219	149	109	75
	2,203	*1,656*	*0,234*	*0,234*	*1,734*	*0,984*	*0,312*
11	289	235	206	177	121	88	60
	7,062	*4,234*	*4,14*	*0,296*	*0,656*	*0,171*	*0,031*
13	269	220	193	166	113	82	57
	3,39	*0,39*	*8,171*	*0,093*	*1,671*	*0,031*	*0,046*

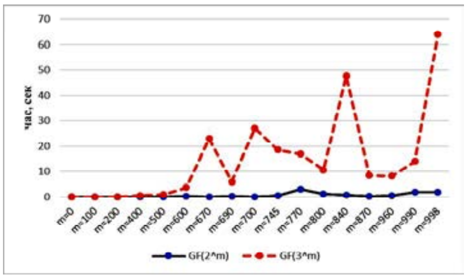
Table 1 shows that there are fields of high and low time complexity calculation irreducible polynomials, which indirectly points to the possible complications of processing elements separate fields.



a) GF(2^m^) and GF(3^m^)

Fig. 3. Calculating irreducible polynomials for Galois fields *GF(p^m).*

Figure 3 shows the time of the irreducible polynomial for the Galois field GF (2m) and GF (3m) with equal powers m (Table 2).



a) GF(2^m) ma GF(3^m)

Fig. 4. Comparison times return irreducible polynomials with the same degrees of Galois fields.

Table 2

Irreducible polynomial

GF	m=100	m=200	m=400	m=600	m=700	m=998	m=2000
GF(2^m)	0	0,015	0,078	0,281	0,031	1,89	36,312
GF(3^m)	0,062	0,078	0,562	3,843	27,218	64	452,328
GF(5^m)	0,015	1,218	1,093	2,703	45,515	223,156	302,796
GF(7^m)	0,156	0,296	23,328	45,015	6,75	155	1133,906
GF(11^m)	1,031	7,546	24	7,234	15,14	185,937	504,359
GF(13^m)	0,109	2,343	26,203	79,078	122,67	171,562	1505,906

Conclusion

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

Considered the construction of a parallel multiplier based on modified cells Hild. Proved its advantages over similar items multiplier binary Galois field GF (2^m).

References

[1] Steininger A., Serra M., Reconfigurable Hardware Implementation of Polynomial Arithmetic over the Finite Field GF(3), Wien, December, 30, pp. 88, 2006.

[2] V. S. Hlukhov, R. M. Elias, A. O. Melnyk, “Osoblyvosti realizatsii na PLIS sektsiinykh pomnozhuvachiv elementiv poliv Halua GF(2m) z nadvelykym stepenem”, Kompiuterno-intehrovani tekhnolohii, Lutsk № 12., 103 – 106 st., 2013.

[3] Merchan J. G. Arithmetic Architectures for Finite Fields GF(p^m) with Cryptographic Applications. Bochum, pp. 221, May, 2004.

[4] T. Berko, V. Hlukhov, “Perevirka prystroiv dlia obrobky tsyfrovykh pidpysiv, shcho gruntuiutsia na eliptychnykh kryvykh”, Naukovo-sotsialnyi zhurnal «Tekhnichni novyny», orhan Ukrainskoho inzhenernoho tovarystva u Lvovi, 1, 53-57 st., 26, 2007.

[5] Deschamps J.P., Imana J.L, Gustavo D., Hardware Implementation of Finite-Field Arithmetic. 2009 The McGraw-Hill Companies, Inc.

[6] Hlukhov V.S., Kostyk A.T., Vykorystannia suchasnykh PLIS dlia opratsiuvannia elementiv poliv Halua (pq). Tezy dlia 9-toi nauk. konf. KhUPS.,178 st., kviten 2013.