An Effective Algorithm for the Synthesis of Irreducible Polynomials over a Galois Fields of Arbitrary Characteristics

ANATOLY BELETSKY
Department of Electronics
National Aviation University
1, Avenue Lyubomir Guzar, Kyiv, 03058
UKRAINE

Abstract: - The known algorithms for synthesizing irreducible polynomials have a significant drawback: their computational complexity, as a rule, exceeds the quadratic one. Moreover, consequently, as a consequence, the construction of large-degree polynomials can be implemented only on computing systems with very high performance. The proposed algorithm is base on the use of so-called fiducial grids (ladders). At each rung of the ladder, simple recurrent modular computations are performers. The purpose of the calculations is to test the irreducibility of polynomials over Galois fields of arbitrary characteristics. The number of testing steps coincides with the degree of the synthesized polynomials. Upon completion of testing, the polynomial is classifieds as either irreducible or composite. If the degree of the synthesized polynomials is small (no more than two dozen), the formation of a set of tested polynomials is carried out using the exhaustive search method. For large values of the degree, the test polynomials are generating by statistical modeling. The developed algorithm allows one to synthesize binary irreducible polynomials up to 2Kbit on personal computers of average performance.

Key-Words: - irreducible and composite polynomials, singular polynomials, fiducial grids, modulo comparability**.**

Received: April 2, 2021. Revised: September 4, 2021. Accepted: September 22, 2021. Published: October 10, 2021.

1 Introduction

Irreducible polynomials (IP) wide used in various fields of mathematics, information technology, a modern theory of information transmission, in the synthesis of noise-like code sequences, in the theory of error-correcting coding, cryptography and other branches of science, and technology [1-10]. Despite the great demand, the synthesis of IP is still a rather complex problem, and, as noted in [11], "finding irreducible polynomials is still obscured. Cryptographic services of highly developed countries have worked on finding polynomials of the highest possible degree, but they hardly cover their results in the open press". The main problem is that known algorithms for the synthesis of IPs are, as a rule, inherent more than quadratic computational complexity. From this, it follows that the costs of computing resources required for their construction increase significantly with an increase in the degree of IP.

Irreducible polynomials can represent in two forms. The first of these is the so-called *polynomial form*, which we will call the *algebraic form*:

$$f(x)=\sum_{k=0}^{n}\alpha_k x^k=\alpha_n x^n+\alpha_{n-1}x^{n-1}+\ldots \\ +\alpha_k x^k+\ldots+\alpha_1 x+\alpha_0 \quad (1)$$

and the second is the *vector form*, which is a set of polynomial coefficients, including zero coefficients α_k of the absent monomials of series (1):

$$f=\alpha_n\alpha_{n-1}\ldots\alpha_k\ldots\alpha_1\alpha_0. \quad (2)$$

The polynomial $\tilde{f}$ is dual to the original polynomial f, formed by the polynomial inversion in algebraic form (1) or coefficients in vector form (2). For example, the vector form of the dual polynomial is:

$$\tilde{f}=\alpha_0\alpha_1\ldots\alpha_k\ldots\alpha_{n-1}\alpha_n.$$

Expressions (1) and (2) are natural forms of writing IP, widely used, for example, in positional number systems, in which the most significant digits locate on the left side of the number.

Recall some basic parameters that characterize polynomials. One is the *polynomial degree* an equal maximum degree of monomial with a nonzero coefficient included in the polynomial. A polynomial degree is denoted $\deg(f(x))$ — for an algebraic and $\deg(f)$ — for a vector form. The second most important parameter of the IP is its *order*, also called the *period* or *exponent* — this is the smallest natural number m at which it turns out to be the divisor of the binomial $x^m - 1$, which is displayed as follows:

$$f(x) \mid x^m - 1 . \tag{3}$$

The order of the polynomial denotes as $\mathrm{ord}(f(x))$ or $\mathrm{ord}(f)$ for algebraic and vector forms, respectively. Thus, for example, since a first-degree polynomial x equal to 10 in vector notation, divisibility (3) for a vector image of polynomials can represent by the formula:

$$f \mid (10)^m - 1 = f \mid 1(0)^{[m]} - 1,$$

where $(0)^{[m]} = \underbrace{00\ldots00}_{m \text{ times}}$.

Finally, we distinguish between primitive polynomials (PrP) and irreducible polynomials that are not primitive. For convenience, the latter will be called simple irreducible polynomials (SIP). The primitive IP are those with the maximum order $L_{n,\max}$, defined by the relation

$$L_{n,\max} = p^n - 1, \tag{4}$$

where is p – a prime number characteristic of the Galois field $GF(p)$ generated by an IP f.

The concept of a primitive polynomial can define differently. For example, an IP is a PrP if and only if the sequence of degrees of the generating element $\theta = 10$ forms modulo f is a m – sequence.

The formula by which the number $M_p(n)$ of irreducible polynomials over the field $GF(p)$ is as follows

$$M_p(n) = \frac{1}{n}\sum_{k|n} \mu(k)\, p^{n/k},$$

where $\mu(k)$ — the Möbius function is defined as follows:

$$\mu(k) = \begin{cases} 1, & \text{if } k = 1; \\ (-1)^l, & \text{if } k \text{ — product of } l \text{ distinct primes,} \\ 0, & \text{in other cases.} \end{cases}$$

TABLE I. MÖBIUS FUNCTION

k	μ	k	μ	k	μ	k	μ
1	1	9	0	17	-1	25	0
2	-1	10	1	18	0	26	1
3	-1	11	-1	19	-1	27	0
4	0	12	0	20	0	28	0
5	-1	13	-1	21	1	29	-1
6	1	14	1	22	1	30	-1
7	-1	15	1	23	-1	31	-1
8	0	16	0	24	0	32	0

Calculating the number of irreducible polynomials over the field $GF(p)$ for several $M_p(n)$ of values n is summarized in Table II.

TABLE II. THE NUMBER OF IP SMALL DEGREE

n	M	n	M
1	2	17	7’710
2	1	18	14’532
3	2	19	27’594
4	3	20	52’377
5	6	21	99’858
6	9	22	190’557
7	18	23	364’722
8	30	24	698’870
9	56	25	1’342’176
10	99	26	2’580’795
11	186	27	4’971’008
12	335	28	9’586’395
13	630	29	18’512’790
14	1’161	30	35’790’267
15	2’182	31	69’273’666
16	4’080	32	134’215’680

From a cursory overview of Table II, it follows that starting at $n = 2$ practically $M(n+1) \approx 2M(n)$. That is means that an increase in the degree of IP by one leads to a doubling of irreducible polynomials. As the degree of polynomials grows, so do the

resources (machine time, memory size, etc.) spent on checking them for irreducibility. Therefore, a formal estimate of the resources required to implement a computational algorithm, called computational complexity, is usually used. The computational complexity $O(\cdot)$ of the known IP synthesis methods [12-14], as a rule, is not less than quadratic; that is, it takes place $O(n^2)$.

The main goal of this study is to develop a new algorithm for the synthesis of irreducible polynomials over Galois fields of arbitrary characteristics, the efficiency of which exceeds the efficiency of the known algorithms for the synthesis of IP.

2 Conceptual Framework for Synthesis of Binary Irreducible Polynomials

Below are some simple, often prominent, or well-known statements, formulated as the axioms (for brevity, we will denote them $\boldsymbol{A}$k, where k — are natural numbers), obtained mainly from empirical facts and greatly facilitating calculating the IP.

$\boldsymbol{A}1$. Vector forms of IP are framed on the left and right by units, i.e.,

$$f_n = 1\alpha_{n-1}\alpha_{n-2}\ldots\alpha_k\ldots\alpha_1 1,$$
$$\alpha_k \in GF(2) = \{0,1\}.$$

$\boldsymbol{A}2$. The weight of the set of internal coefficients α_k of a polynomial f_n must be an odd number, since otherwise f_n is divisible without a remainder by a polynomial of the first degree $f_1 = 11$ and, thus, the polynomial under test turns out to be reducible.

$\boldsymbol{A}3$. The order L_n of the irreducible polynomial f_n coincides with the order of the $GF(2^n)$ field's element $\theta = 10$ generated by the IP.

$\boldsymbol{A}4$. The order L_n of the IP f_n is a divisor of the maximum order $L_{n,\max}$, i.e.

$$L_n \mid L_{n,\max}. \qquad (5)$$

$\boldsymbol{A}5$. A necessary condition for the irreducibility of a binary polynomial f_n is the comparison

$$1(0)^{[2^n-1]} \equiv 1 \pmod{f_n}, \quad n \geq 2. \qquad (6)$$

However, not for all n is mandatory conditions for the irreducibility of the *tested polynomials* (TP).

Let us illustrate the application of the above axioms to solve the problem of synthesizing IP in the range of degrees from 2 to 4. Polynomials $f_0 = 1$ and $f_1 = \{10, 11\}$ belong to the subclass of *degenerate* PrPs. First, we will write the general form of the polynomial of the second degree as $f_2 = 1\alpha_1 1$, $\alpha_1 \in \{0,1\}$. The only variant of the value of the coefficient α_1 in f_2, preserving the condition of the axiom $\boldsymbol{A}2$, is $\alpha_1 = 1$. In this case, the polynomial $f_2 = 111$ turns out to be PrP. Next, let us turn to the general form of 3-degree polynomials $f_3 = 1\alpha_2\alpha_1 1$. There are four variants of binary internal coefficients $\alpha_2\alpha_1 = \{00, 01, 10, 11\}$. Still, only for two of them, namely $\alpha_2\alpha_1 = \{01, 10\}$, the axiom $\boldsymbol{A}2$ conditions are satisfied. Therefore, the permissible values of the coefficients generate the polynomials $f_3^{(1)} = 1011$ and $f_3^{(2)} = 1101$, which are PrP.

Furthermore, finally, consider the procedure for the synthesis of 4-degree IPs, the general form of which is $f_4 = 1\alpha_3\alpha_2\alpha_1 1$. Only such combinations of internal coefficients $\alpha_3\alpha_2\alpha_1 = \{001, 010, 100, 111\}$ have an odd weight. Let us check the divisibility of all four polynomials by IP of degree two $f_2 = 111$. The first polynomial $f_4^{(1)} = 10011$ from the collection is not divisible without a remainder by f_2 and therefore turns out to be irreducible. The polynomial $f_4^{(3)} = 11001$ dual to the polynomial $f_4^{(1)}$ is also irreducible. Both polynomials $f_4^{(1)}$ and $f_4^{(3)}$ are primitive, as seen using the axioms $\boldsymbol{A}3$ and $\boldsymbol{A}4$. The polynomial $f_4^{(2)} = 10101$ is reducible since it is divisible by the polynomial f_2 without remainder. The remaining polynomial $f_4^{(4)} = 11111$ is irreducible as it belongs to a subset of SIPs $(\mathrm{ord}\left(f_4^{(4)}\right) = 5)$. Thus, the considered methods for synthesizing binary IP can be easily generalized to the synthesis of polynomials of small degrees irreducible over a field of odd characteristics $p \geq 3$.

The described technology for the synthesis of binary IPs has limitations on the $n-$degree of polynomials. So, if, $n \geq 28$, the volume of computations increases so much that the PC's resources may be insufficient to determine the entire set of irreducible polynomials f_n. In particular, if $n = 32$, it will be necessary to test for the irreducibility of all odd (by weight) polynomials. The upper estimate of the number is about a billion. Moreover, considering that testing polynomials of 32-degrees for reduced to checking the divisibility of these polynomials by all IPs in the range of degrees from 2 to 16, it becomes evident that determining the complete set of IPs f_{32} requires computational tools of very high performance.

3 Linear-logarithm Algorithm for Testing Polynoms on Irreducibility

Let us introduce (Table III) for the TP auxiliary numerical parameters.

TABLE III. AUXILIARY NUMERIC PARAMETERS

r	1	2	3	4	5	6	7	8	…
t_r	1	3	7	15	31	63	127	255	…

Let's "link" them with the so-called *fiducial grid* (Fig. 1), consisting of a set of parallel straight lines (*grid steps*). Thus, the total number of steps on the ladder coincides with the degree of the polynomial tested for irreducibility f_n.

r 1 2 3 4 5 6 7 8 …
| | | | | | | | …

Fig. 1. Fiducial grid of the IP synthesis algorithm

Table III, the following designations are adopted: r — number of the step of the fiducial grid; t_r — the degree of the binary polynomial CV_r, let's call it the *Coordinate Vector*, the left bit of which is 1, and the rest filled with zeros, that is

$$CV_r = \underset{t_r}{100...0}.$$

Thus, t_r is the size (length) of the zero vector of the polynomial CV_r. The number of zero bits of the polynomial CV_r determined by the formula (4), i.e., $t_r = 2^r - 1$.

Let us rewrite expression (6), presenting it in the following form

$$(10)^{L_{n,\max}} \equiv 1 \pmod{f_n}. \quad (7)$$

The left component of comparison (7) is the coordinate vector

$$CV_n = \underset{2^n-1 \text{ bit}}{1\underbrace{00\ldots0}}. \quad (8)$$

In turn, the corresponding binary vector $L_{n,\max}$ consists exclusively of $2^n - 1$ ones. We call this vector a *Unit Vector*, as the antipode of the zero vector (that is, a vector initialized with ones), and denote

$$UV_n = \underset{2^n-1 \text{ bit}}{11\ldots1}. \quad (9)$$

Let us illustrate relations (6) and (7) with a numerical example, choosing the tested one of the IP of the fourth degree. Let $f_4^{(1)} = 10011$ a priori is PrP. However, first, let us write out the coordinate vector

$$CV_4 = \underset{15 \text{ bit}}{1\underbrace{00\ldots0}}. \quad (10)$$

Dividing the right-hand side of (10) by $f_4^{(1)}$, we get $Res(CV_4)_{f_4^{(1)}} = 1$, where it denoted $Res(a)_b = a \pmod{b}$ — the residue of the number a modulo b. Therefore, according to $\boldsymbol{A}5$, $f_4^{(1)}$— is an irreducible polynomial. Moreover, we arrive at the same result of the SIP variant $f_4^{(3)} = 11111$ since $Res(CV_4)_{f_4^{(3)}}$ is the same as $Res(CV_4)_{f_4^{(1)}}$ equals 1.

Let us turn to an alternative option, choosing TP $f_4 = 10101$. Then, the analyzed polynomial $Res(CV_4)_{f_4} = 1000 \neq 1$, it follows that f_4 — reducible (i.e., composite) polynomial.

The order (length) of the coordinate vectors CV_n, according to (8), increases exponentially with the degree of the polynomials f_n. Moreover, as a consequence, already at $n \geq 30$, it becomes practically impossible to use axiom A5 on standard PCs since the comparison (6) is associated with an insurmountably large expenditure of computer time. However, this problem, which we will call *the nightmare of large numbers*, can be circumvented

by applying the testing polynomials proposed below, called the *linear-logarithmic algorithm*.

Let us display the fiducial grid (Fig. 1) corresponding to the polynomial f_n by a vector $1^{[n]}$ containing n units, i.e., $1^{[n]} = \underbrace{11\ldots11}_{n \text{ bit}}$. Each $r-$th unit in $1^{[n]}$ symbolizes the $r-$th step of the fiducial grid. Can establish the law of changing the orders of the zero digits of the vectors by analyzing the data in Table 3, namely:

$$t_r = 2 \cdot t_{r-1} + 1, \quad t_0 = 0, \quad r = \overline{1,n}. \qquad (11)$$

Let us introduce some notations. First, let $\boldsymbol{S}_r = Res(CV_r)_f$ — the residue of the coordinate vector CV_r by modulo a polynomial f. Relations (11) form the *fundamental basis* of the proposed algorithm for testing binary polynomials on irreducibility, which reduce to a sequence of simple recurrent computations

$$\boldsymbol{S}_r = Res(\boldsymbol{S}_{r-1} \cdot s_k)_f, \ s_r = \boldsymbol{S}_{r-1}0, \ \boldsymbol{S}_0 = 1, \ r = \overline{1,n},$$

or else

$$\boldsymbol{S}_r = Res(\boldsymbol{S}_{r-1}^2 0)_f, \ \boldsymbol{S}_0 = 1, \ r = \overline{1,n}. \qquad (12)$$

When the index r have reached the last rung of the fiducial ladder n and if at the same time $\boldsymbol{S}_n = 1$, then this will mean, in following $\boldsymbol{A}5$, the fulfillment of the necessary conditions for the irreducibility of TP.

Let us compare the methods of testing polynomials for irreducibility using formulas (6) and (12). Suppose that the $n-$degree of TP is 30. According to (6), a number should forms consisting of 1, to the right of which more than a billion zeros should place. Then we should calculate the remainder of this enormous number modulo f_{30}. A billion zeros with the left unit yet admit the possibility of perception. However, if n equal to several thousand, we are already dealing with nightmarishly large numbers. At the same time, by recurrent calculations using formula (12), the solution of the problem of classifying TP of interest to us is achieved in just n steps. The number of stages of recurrent computation is *linearly* related to the degree of the tested polynomial. In turn, n it is a number close to the *logarithm* of the number of zeros in (6) modulo 2. The combination of the last two words, separated by recursion, led to the name of the developed algorithm for the synthesis of irreducible polynomials.

Let us give the sequence of residues (12) a simple interpretation. According to the expression (11) associated with the values listed in the second row of Table 3, the coordinate vector CV_r corresponding to the $r-$step of the fiducial grid can be written in the form

$$CV_r = CV_{r-1} \cdot CV_{r-1}0 = CV_{r-1}^2 0, \qquad (13)$$

which, based on formula (10), can be represented by a binary vector

$$CV_r = 1\underbrace{00\ldots00}_{2^r-1 \text{ bit}} = 1\overbrace{\underbrace{00\ldots00}_{2^{r-1}-1 \text{ bit}}}^{CV_{r-1}}1\overbrace{\underbrace{00\ldots00}_{2^{r-1}-1 \text{ bit}}}^{CV_{r-1}}0. \qquad (14)$$

Calculating the remainders modulo f from the components of equality (14), we arrive at the estimate

$$\begin{aligned} \boldsymbol{S}_r = Res(CV_r)_f &= Res(CV_{r-1}CV_{r-1}0)_f = \\ &= Res(\boldsymbol{S}_{r-1}\boldsymbol{S}_{r-1}0)_f, \end{aligned} \qquad (15)$$

coinciding with the estimate (12).

We will illustrate the algorithm (15) with a numerical example, choosing for testing an a priori irreducible polynomial of the 12-degree $f_{12}^{(1)} = 1000000001111$. The values $\boldsymbol{S}_r$ of the vector CV_r residues modulo $f_{12}^{(1)}$ summarize in Table IV.

TABLE IV. THE SEQUENCE OF RESIDUES GENERATED BY THE POLYNOMIAL $f_{12}^{(1)}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_7 = 110101111110;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_8 = 110101110100$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_9 = 110111111100;$
$\boldsymbol{S}_4 = 1111000;$	$\boldsymbol{S}_{10} = 110100000100;$
$\boldsymbol{S}_5 = 101010011110;$	$\boldsymbol{S}_{11} = 11111100010;$
$\boldsymbol{S}_6 = 110101111101;$	$\boldsymbol{S}_{12} = \boldsymbol{1}.$

The fact that residue $\boldsymbol{S}_{12}$ equal to 1 is evidence of the fulfillment of at least the necessary conditions for the irreducibility of the polynomial $f_{12}^{(1)}$.

The following helps construct an algorithm for the synthesis of IPs.

Statement 1. The residue of the coordinate vector CV_r modulo IP f_n of the degree n reaches unity only at $r = n$; otherwise, when $r < n$

$$CV_r \ (\text{mod}\ f_n) \neq 1 .$$

In other words, if vector CV_r on the modulus f_n at the inner rung of the staircase reaches a value equal to one, then this will mean that f_n is a composite polynomial.

Let us validate statement 1 on numerical examples. In particular, if the degree of IP is a binary-rational number, i.e., $n = 2^m$, where is m a natural number, then the maximum order $L_{n,\max}$ of the polynomial f_n possessed by PrP can be represented by the product of binomials

$$L_{n,\max} = 2^n - 1 = (2^1 + 1)(2^2 + 1)(2^4 + 1)\ldots \\ \ldots(2^k + 1)\ldots(2^{n/2} + 1). \qquad (16)$$

The order L_n of an IP f_n that is not primitive determines by the product of a particular set of binomials in decomposition (16) that make up the set of prime divisors (factors) of a number $L_{n,\max}$. Let us refer to Table III. The bottom row of Table III contains numbers $t_r = 2^r - 1$ that coincide with the maximum order of the $r-$degree polynomials f. There is no such subset of binomials in (16), the product of which could be equal to the binomial t_r. Furthermore, if the unit residue of the coordinate vector CV_r modulo f_n appears on step r of the fiducial grid. In that case, f_n is a composite polynomial, and the degree of one polynomial of the factors coincides with r.

To confirm the formulated conclusion, consider a numerical example. Let a polynomial $f_{10} = 11101000001$ be givens. Then, the sequence of residues generated by the polynomial f_{10} is presente in Table V.

TABLE V. THE SEQUENCE OF RESIDUES GENERATED BY THE POLYNOMIAL f_{10}

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_5 = 1110010;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_6 = 1110000110;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_7 = 1001001011;$
$\boldsymbol{S}_4 = 100110100;$	$\boldsymbol{S}_8 = 1.$

Based on the data in Table V, we arrive at the following result: the polynomial f_{10} is composite, and the degree of one of them is 8, and the second, of course, is 2 (i. e. $f_2 = 111$). Thus, the polynomial f_8 can also turn out to be composite, which, if necessary, can be refined by independent testing. ▲

4 Synthesis of Irreducible Polynomials of Small Degrees

We will classify as small the $n-$degrees of polynomials f_n not exceeding 64. Let us divide the polynomials of small degrees into two groups, including in the first of them polynomials whose degrees belong to the interval [2-32], and in the second – [33-64]. Analytical estimates of the number $M(n)$ of IP of small degrees of the first group are given above in Table II.

We call singular (exceptional) IPs whose degrees are: (a) prime numbers, (b) powers of primes, or (c) the product of two different primes. Singular IRs of minor degrees of the first group highlight by shading in Table VI and for the second group — in Table VII.

TABLE VI. DEGREES OF POLYNOMIALS OF THE FIRST GROUP

	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

TABLE VII. DEGREES OF POLYNOMIALS OF THE SECOND GROUP

33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Based on computer calculations for singular polynomials, empirically established the following position

Theorem 1. A singular polynomial f_n of degree n is irreducible if and only if the residue $\boldsymbol{S}_n$ of the coordinate vector CV_n corresponding to the $n-$th

step of the fiducial grid is equal to 1. I.e., the identity provides $S_n \equiv 1$ (*necessary condition*), and for any values of $r < n$, the residue S_r cannot be equal to 1 (*sufficient condition*).

Let us support Theorem 1 with numerical examples. But first, consider testing a polynomial 15-degrees $f_{15}^{(1)} = 1010011011000111$, a priori irreducible (Table VIII).

TABLE VIII. THE SEQUENCE OF RESIDUES GENERATED BY THE POLYNOMIAL $f_{15}^{(1)}$

$S_1 = 10;$	$S_9 = 1101010110100;$
$S_2 = 1000;$	$S_{10} = 100010100100011;$
$S_3 = 10000000;$	$S_{11} = 11110100001101;$
$S_4 = 10011011000111;$	$S_{12} = 101110110101000;$
$S_5 = 111111111000;$	$S_{13} = 10001100101111;$
$S_6 = 100011110011101;$	$S_{14} = 11011101000110;$
$S_7 = 100000011001001;$	$S_{15} = \mathbf{1}.$
$S_8 = 10110111011;$	

Since the necessary and sufficient conditions of Theorem 1 are satisfied, this means that the polynomial $f_{15}^{(1)}$ is irreducible. Consider further a polynomial $f_{15}^{(2)} = 1010100101000011$. Calculating the residue of the coordinate vectors CV_{15} modulo $f_{15}^{(2)}$, and we obtain Table IX.

TABLE IX. THE SEQUENCE OF RESIDUES GENERATED BY THE POLYNOMIAL $f_{15}^{(2)}$

$S_1 = 10;$
$S_2 = 1000;$
$S_3 = 10000000;$
$S_4 = 10100101000011;$
$S_5 = 1.$

The five-element second and third columns of deductions in Table IX repeat the elements of the first column and omit them. Therefore, the sufficient conditions of Theorem 1 for the polynomial $f_{15}^{(2)}$ are not satisfied since the sequence of residues S_r, $r = \overline{1,15}$, contains three units. Therefore, these are deductions are S_5, S_{10} and S_{15}. So, it means that the polynomial $f_{15}^{(2)}$ is reducible.

Moreover, in the finale, if the TP $f_{15}^{(3)}$ a priori reducible, for example, is formed by the product of two IPs, we obtain the remaining $S_{15} \neq 1$. So that confirmed that $f_{15}^{(3)}$ is a reducible polynomial, as it was initially predetermined.

Polynomials that are not singular, such as polynomials, the degrees of which indicate in the light cells of Tables VI and VII, have several specific features. First, both conditions (both necessary and sufficient) of Theorem 1 are necessary conditions for the irreducibility of *non-singular polynomials* (NSP). And, secondly, a satisfactory condition for the irreducibility of the NSP, as established by computer simulation, is the absence of so-called *excluding divisors* (ED) for such polynomials. The excluding divisors will include those IPs that divide the test non-singular polynomial without a remainder. The set of excluding divisors of the tested degree polynomials denoted. The EDs of the NSP, contained in Tables VI and VII, give in Tables X and XI, respectively. Under the sign " = ", the second column left of Tables is products of prime factors of a number presented together with their multiplicities.

TABLE X. EXCLUSIVE DIVISORS OF NSP OF THE FIRST GROUP

The degree of IP		The degree of ED			
n	=	2	3	4	5
12	$2^2 \cdot 3$	+			
18	$3^2 \cdot 2$		+		
20	$2^2 \cdot 5$	+			
24	$2^3 \cdot 3$	+		+	
28	$2^2 \cdot 7$	+			
30	$2 \cdot 3 \cdot 5$	+	+		+

TABLE XI. EXCLUSIVE DIVISORS OF NSP OF THE SECOND GROUP

The degree of IP		The degree of ED							
n	=	2	3	4	5	6	7	8	9
36	$2^2 \cdot 3^2$	+	+			+			
40	$2^3 \cdot 5$	+		+					
42	$2 \cdot 3 \cdot 7$	+	+				+		
44	$2^2 \cdot 11$	+							
45	$3^2 \cdot 5$		+						
48	$2^4 \cdot 3$	+		+				+	
50	$5^2 \cdot 2$				+				

Continuation of Table XI									
The degree of IP		The degree of ED							
n	=	n	=	n	=	n	=	n	=
52	$2^2 \cdot 13$	+							
54	$3^3 \cdot 2$		+						+
56	$2^3 \cdot 7$	+		+					
60	$2^2 \cdot 3 \cdot 5$	+	+	+	+				
63	$3^2 \cdot 7$		+						

Based on the data in Tables X and XI, we come to generalizations, confirmed by the results of computer modeling:

Statement 2. The sets of excluding divisors $\tilde{d}_n$ of non-singular polynomials f_n are defined by the expressions:

$$\tilde{d}_n \in \begin{cases} \bigcup_{i=1}^{k-1} \overline{p}_1^i, \text{ if } n = p_1^k \cdot p_2, k \geq 2; \\ \bigcup_{i=1}^{k} \overline{p}_i, \text{ if } n = \bigcap_{i=1}^{k} p_i, k > 2; \\ \overline{p}_1 \cup \overline{p}_2 \cup \overline{p}_1 \cdot \overline{p}_2, \text{ if } n = p_1^k \cdot p_2^k, k \geq 2, \end{cases} \quad (17)$$

where p_i is prime numbers, and $\overline{p}_1^i$ — is a collection of irreducible polynomials of degree p_1^i.

Of course, the system (17) does not exhaust a small fraction of the various variants of the expansion of the $n-$ degrees of the TP f_n. Each of them has its own set of excluding divisors $\tilde{d}_n$. However, for applications, for example, in cryptography, as a rule, it turns out that they are pretty enough.

The following empirical established.

Theorem 2. A non-singular polynomial f_n of $n-$ degree is irreducible if and only if the only residue of the coordinate vector CV_r modulo f_n one is the residue corresponding to the $n-$ step of the fiducial grid. That is when the identity $\boldsymbol{S}_n \equiv 1$ (*necessary condition*) ensures no excluding divisors for the tested polynomial (*sufficient condition*).

Let us look at numerical examples.

Example 1. Consider a non-singular polynomial $f_{18}^{(1)} = 1010011010110101011$. The sequence of residues $\boldsymbol{S}_r$ of coordinate vectors CV_r modulo $f_{18}^{(1)}$ presents in Table XII. However, the lower half sequence residues repeat the upper half and, on this basis, are thrown out of Table.

TABLE XII. THE SEQUENCE OF RESIDUES GENERATED BY THE POLYNOMIAL $f_{18}^{(1)}$

$\boldsymbol{S}_1 = 10;$
$\boldsymbol{S}_2 = 1000;$
$\boldsymbol{S}_3 = 10000000;$
$\boldsymbol{S}_4 = 1000000000000000;$
$\boldsymbol{S}_5 = 10100100100011100;$
$\boldsymbol{S}_6 = 100000011111111001;$
$\boldsymbol{S}_7 = 1101000000010110110;$
$\boldsymbol{S}_8 = 1000111011011000;$
$\boldsymbol{S}_9 = \mathbf{1}.$

As follows from Table XII, the necessary condition for the irreducibility of TP so not met. And this means that $f_{18}^{(1)}$ — a reducible polynomial.

Example 2. Let $f_{18}^{(2)} = 10100110110100011011$. The set of residues corresponding to the polynomial $f_{18}^{(2)}$ summarizes in Table XIII.

TABLE XIII. The Sequence of Residues Generated by the Polynomial $f_{18}^{(2)}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_{10} = 100111101101101011;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_{11} = 111011101101100;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_{12} = 1111001110010001;$
$\boldsymbol{S}_4 = 1000000000000000;$	$\boldsymbol{S}_{13} = 101111101101101001;$
$\boldsymbol{S}_5 = 10111101110110100;$	$\boldsymbol{S}_{14} = 10000110011010000;$
$\boldsymbol{S}_6 = 1101101100101000001;$	$\boldsymbol{S}_{15} = 1110011111110110000;$
$\boldsymbol{S}_7 = 1101001011001000011;$	$\boldsymbol{S}_{16} = 10011000001001010;$
$\boldsymbol{S}_8 = 1110111110101000011;$	$\boldsymbol{S}_{17} = 1111001001111000111;$
$\boldsymbol{S}_9 = 1111001100010000;$	$\boldsymbol{S}_{18} = \mathbf{1}.$

Even though the necessary irreducibility conditions are satisfied, the polynomial is not free from the exclusive divisor $\tilde{d}_n$. Following Table 10, it turns out to be PrP of the 3-degree $f = 1011$. Therefore, $f_{18}^{(2)}$ — a reducible polynomial.

And finally, let it be

$$f_{18}^{(3)} = 1101010111001011001.$$

The set of residues formed on the fiducial grid by a polynomial $f_{18}^{(3)}$ presents in Table XIV. The polynomial $f_{18}^{(3)}$ has no excluding divisors. Therefore, $f_{18}^{(3)}$ — an irreducible polynomial.

TABLE XIV. THE SEQUENCE OF RESIDUES GENERATED BY THE POLYNOMIAL $f_{18}^{(3)}$

$S_1 = 10;$	$S_{10} = 100111101101101111;$
$S_2 = 1000;$	$S_{11} = 111110111000101001;$
$S_3 = 10000000;$	$S_{12} = 110001011011000101;$
$S_4 = 1000000000000000;$	$S_{13} = 1011111011111110;$
$S_5 = 10111101110110100;$	$S_{14} = 111000111010010110;$
$S_6 = 1101101100101000 01;$	$S_{15} = 101000110101101011;$
$S_7 = 1010101001010100 01;$	$S_{16} = 10010111110100;$
$S_8 = 1011101000001101 10;$	$S_{17} = 110110101101010;$
$S_9 = 1100000010100 1100;$	$S_{18} = \mathbf{1}.$

And in the conclusion of this section, we formulate criteria for the irreducibility of polynomials f_n of even degrees n, all of whose digits contain ones. Such polynomials refer to above as "vectors of units". The following observations are apparent.

Theorem 3. A unit vector $1^{[n+1]}$ of $(n+1)-$order is an irreducible polynomial f_n of even degree n if and only if $(n+1) \mid L_{n,\max}$ (*necessary conditions*), while $(n+1) \nmid L_{n/2,\max}$ (*sufficient conditions*).

The results of the application of Theorem 3 illustrate in Tables XV and XVI.

TABLE XV. IRREDUCIBILITY TESTS FOR POLYNOMIALS $1^{[n+1]}$ OF EVEN DEGREES

The first group of IPs of small degrees					
Deg	NC	SC	Deg	NC	SC
4	+	+	20	–	
6	–		22	+	–
8	–		24	–	
10	+	+	26	–	
12	+	+	28	+	+
14	–		30	+	–
16	+	–	32	–	
18	+	+			

Shading in Tables XV and XVI, the degrees of polynomials $1^{[n+1]}$ are distinguished for which both *necessary* (NC) and *sufficient* (SC) *conditions* of irreducibility are satisfied.

TABLE XVI. IRREDUCIBILITY TESTS FOR POLYNOMIALS $1^{[n+1]}$ OF EVEN DEGREES

The second group of IPs of small degrees					
Deg	NC	SC	Deg	NC	SC
34	–		50	–	
36	+	+	52	–	
38	–		54	–	
40	+	–	56	–	
42	+	+	58	–	
44	–		60	–	
46	+	–	62	–	
48	–		64	–	

Continuation of Table XVI

5 Classification of IP of Binary-Rational Degrees

A to *binary-rational* (the term borrows from [15]), we mean polynomials whose degrees n equals 2^k. Such IPs wide used in cryptography and other areas of discrete mathematics. The polynomials f_n under consideration belong to the group of singular IPs. Their synthesis bases on Theorem 1. The tested polynomial is irreducible if the residue of the coordinate vectors CV_k on modules f_n reach a unit value only at the last $n-$th step of the fiducial grid. Singular polynomials of binary-rational degrees are free of only divisors. The listed properties of polynomials greatly simplify the procedure for their synthesis. However, the problem remains due to the significant expenditures of computer time in estimating the order of polynomials and, accordingly, classifying them into primitive (IP of maximum order) and simple irreducible (not primitive) polynomials.

Let us supplement the axiomatic foundations of IP synthesis presented in Section 2 with several helpful information concerning polynomials of binary-rational degrees. Let us denote:

1) $D_{1,n} = \{d_1, d_2, \ldots d_k, \ldots, d_m\}$ — is a subset of prime divisors of maximal order $L_{n,\max}$ PrP f_n ordered in ascending order, excluding trivial divisors;

2) $D_{l,n} = \{\bullet\}$ — ordered subsets of composite divisors $L_{n,\max}$ formed by combinations m elements of the subset $D_{1,n}$ by l, $l = \overline{2, m-1}$, excluding the divisor $L_{n,\max}$. The parameter m is equal to the number of prime divisors $L_{n,\max}$;

3) $D_n = D_{1,n} \cup D_{l,n}$ — complete ordered set of divisors $L_{n,\max}$ composed of elements of subsets $D_{1,n}$ and $D_{l,n}$.

Polynomials of binary-rational degrees have a remarkable property, the essence of which is as follows. Since n — is an even number, the order of $L_{n,\max}$ represented by the decomposition

$$L_{n,\max} = 2^n - 1 = \left(2^{n/2} - 1\right) \cdot \left(2^{n/2} + 1\right), \quad (18)$$

where $n/2$ is also an even number, since by definition $n = 2^k$.

Based on the above property, it is easy to write down the expansion of a number $L_{n,\max}$ for polynomials of binary-rational degrees. The decomposition chain of binomial (18) shows below using an example $n = 32$:

$$\begin{aligned} L_{32,\max} &= 2^{32} - 1 = \\ &= (2^{16} - 1) \cdot (2^{16} + 1) = \\ &= (2^8 - 1) \cdot (2^8 + 1) \cdot (2^{16} + 1) = \\ &= (2^4 - 1) \cdot (2^4 + 1) \cdot (2^8 + 1) \cdot (2^{16} + 1) = \\ &= (2^2 - 1) \cdot (2^2 + 1) \cdot (2^4 + 1) \cdot (2^8 + 1) \cdot (2^{16} + 1) = \\ &= (2^1 + 1) \cdot (2^2 + 1) \cdot (2^4 + 1) \cdot (2^8 + 1) \cdot (2^{16} + 1), \end{aligned}$$

according to which the *prime divisors*, composed of the factors of the bottom row of expansion (19),

$$D_{1,32} = 3, 5, 17, 257, 65'537, \quad (20)$$

The complete ordered set of maximal order $L_{32,\max}$ divisors of 32-degree polynomials is as follows:

$$F_k = 2^{2^k} + 1, \quad k = \overline{0,4}. \quad (21)$$

The complete ordered set of maximal order divisors of 32-degree polynomials is as follows:

$D_{32} = \{3, 5, 15, 17, 51, 85, 255, 257, 771, 1'285, 3'855,$
$1'285, 3'855, 4'369, 13'107, 21'845, 65'535, 65'537,$
$196'611, 327'685, 983'055, 1'114'129, 3'342'387,$
$5'570'645, 16'711'935, 16'843'009, 50'529'027,$
$84'215'045, 252'645'135, 286'331'153, 858'993'459,$
$1'431'655'765\}.$ (22)

If f_n is the IP degree n and set D_n contains the element d, which provides $f_n \mid (x^d - 1)$, then f_n is the SIP of order d, otherwise — PrP. Thus, the generalized form of prime divisors, as follows from relations (20) and (21), can be represented as:

$$D_{1,2^{k+1}} = \bigcup_{i=0}^{k} F_i, \quad (23)$$

moreover, starting from $k = 5$ the Fermat number F_k, they turn out to be composite [16, 17].

The sequence of prime divisors (23) of binomial (18) provides the possibility of determining the complete set D_n of divisors of the maximum order $L_{n,\max}$ of IP f_n. The number of components N_n of the set D_n, for binary-rational values n, is determined by the formula

$$N_n = \sum_{k=1}^{\log_2 n - 1} \binom{\log_2 n}{k} = n - 2. \quad (19)$$

With growth n, the costs of computer time increase, associated with the classification of the tested polynomials (calculating their orders and assigning them either to SIP classes or PrP). However, these costs can reduce by taking into account the following empirically established.

Statement 3. The minimum order of IP of a binary-rational degree $n = 2^k$ exceeds the order of PrP degree $\bar{n} = 2^{k-1}$, i.e.,

$$\mathrm{ord}_{\min}(f_n) > 2^{\bar{n}} - 1. \quad (24)$$

In particular, based on inequality (24), the subset of divisors highlighted by the shading in sequence (22) can be excluded from the procedure for calculating the order of the tested polynomials f_{32}.

Suppose the degree of binary-rational polynomials does not exceed 16. Then, the synthesis of IP well relies on enumerating all possible variants of polynomials with their subsequent check for irreducibility. When $n \geq 32$ a complete search, at least on a PC, becomes almost impossible to implement. The only way to form such polynomials is their stochastic modelling. As shown by the results of experimental verification, for the formation of one IP of the degree of 2 Kbit, the computer time spent on computers of average

productivity is about 2.5 hours, which is an entirely satisfactory result.

6 Synthesis Over a Field of Odd Characteristics

In this section, we solve the problem of IP synthesis over a Galois field of characteristic $p \geq 3$. For the numerical parameters associated with polynomials over $GF(p)$, $p \geq 3$, we add one more index p.

Let us refer to Table III. In its bottom line, the parameter t_r determines the number of zeros contained in the binary coordinate vector CV_r, which corresponds to the $r-$steps of the fiducial grid. Thus, for the $p-$number system has $t_{r,p} = p^r - 1$ and, for example, if $p = 3$, Table III is transformed into the following Table XVII.

TABLE XVII. NUMERICAL PARAMETERS OF THE FIDUCIAL GRID FOR CHARACTERISTICS $p = 3$

r	1	2	3	4	5	6	7	8	…
$t_{r,3}$	2	8	26	80	242	728	2186	65600	…

The approximation of the numerical sequence $t_{r,p}$ has the form

$$t_{r,3} = 3 \cdot t_{r-1,3} + 2, \quad t_{0,3} = 0. \qquad (25)$$

Based on a comparison of expressions (11) - (13) and (25), we arrive at the following generalized relations

$$t_{r,p} = p \cdot t_{r-1,p} + (p-1), \quad t_{0,p} = 0;$$

and

$$\boldsymbol{S}_{r,p} = Res(\boldsymbol{S}_{r-1,p}^{\,p}\underbrace{0...0}_{p-1})_f, \quad \boldsymbol{S}_{0,p} = 1. \qquad (26)$$

Let's look at numerical examples. First, let us choose as the testable polynomial $f_5^{(1)} = 102112$, which is irreducible a priori over $GF(3)$. Then, using the recurrent formula (26), we calculate the sequence of residues modulo $f_5^{(1)}$ and summarize it in Table XVIII.

As an alternative, consider a polynomial $f_5^{(2)}$ that is not a priori irreducible. For example, suppose that $f_5^{(2)}$ it forms by a modular product of two IPs over $GF(3)$. Let such $f_3 = 1121$ and $f_2 = 112$ generating a composite polynomial $f_5^{(2)} = 1121 \overset{3}{\otimes} 112 = 122222$. The polynomial $f_5^{(2)}$ corresponds to the residues given in Table XIX.

TABLE XVIII. THE SEQUENCE OF RESIDUES GENERATED BY THE POLYNOMIAL $f_5^{(1)}$

$\boldsymbol{S}_1 = 100;$
$\boldsymbol{S}_2 = 2022;$
$\boldsymbol{S}_3 = 22222;$
$\boldsymbol{S}_4 = 12021;$
$\boldsymbol{S}_5 = 1.$

TABLE XIX. THE SEQUENCE OF RESIDUES GENERATED BY THE POLYNOMIAL $f_5^{(2)}$

$\boldsymbol{S}_1 = 100;$
$\boldsymbol{S}_2 = 22101;$
$\boldsymbol{S}_3 = 22121;$
$\boldsymbol{S}_4 = 11010;$
$\boldsymbol{S}_5 = 11221.$

Tables contents XVIII and XIX confirm the preliminary information regarding the polynomials $f_5^{(1)}$ and $f_5^{(2)}$. Finally, we note that the technology of IP over $GF(p)$, $p \geq 3$, synthesis remains as simple as for binary polynomials.

7 Conclusion

The main result of the article is the development of a new algorithm for synthesizing irreducible polynomials in a wide range of degrees, reaching several Kbits. Unfortunately, the known algorithms for generating IPs have a significant drawback: their computational complexity is, as a rule, no less than quadratic. Moreover, it follows that an IP of large degrees is necessary to involve very high-performance computational resources.

The proposed synthesis algorithm bases on the so-called fiducial grids (ladders), the number of steps coincides with the degree of the synthesized polynomials. At each rung of the ladder, most straightforward recurrent modular computations of the same type perform, after which the polynomial under test is uniquely classified either as irreducible or as composite.

References:

[1] Prasolov V.V., Polynomials. - M .: MTsNMO, (2001). — 336 p. — ISBN 5-900916-73-1.
[2] Lidl R., Niederreiter H. Finite Fields. Cambridge University Press (1996).
[3] Vasilenko O.N. Number-theoretic algorithms in cryptography. - M .: MTsNMO, (2003). — 328 p. — ISBN 5-94057-103-4.
[4] Fomichev, V.M. Discrete mathematics and cryptography. - M .: Dialogue -MIFI, (2013). — 397 p. — ISBN 978-5-86404-185-7.
[5] Beletsky A., Kovalchuk A., Novikov K., Poltoratskyi D. Algorithm for synthesizing irreducible polynomials of linear complexity. // Ukrain Information Security Research Journal (2020), VOL. 22, № 2, pp. 74-87.
[6] Titov S.S., Torgashov A.V. Generation of irreducible polynomials connected by the power dependence of the roots. // Management, computer technology and informatics. - Tomsk: Proceedings of the Tomsk State. Univer., (2010). — № 2 (22). — pp. 310-317.
[7] Schneier B. Applied Cryptography. Protocols, algorithms and source texts in the C+ language. — M.: Triumph, (2002). — 816 p. — ISBN: 5-89392-055-4.
[8] Blahut R.E. Theory and Practice of Error Control Codes. — Addison-Wesley Publishing Company Reading, (1984). — 500 p.
[9] Peterson, W.W., Weldon, E.J. Error-Correcting Codes, MIT Press, Cambridge, MA (1972).
[10] Mc-Williams F.J., Sloane N.A. Theory of error-correcting codes. - M: Communication, (1979). — 744 p.
[11] Zhelnikov V. Cryptography from papyrus to computer. — M: ABF, (1996). — 355 p.
[12] Mazurkov M.I. An efficient algorithm for finding primitive irreducible polynomials. / M. I. Mazurkov, V.S. Dmitrenko, E.A. Konopaka. // Proceedings of UNDIRT. - Odessa, (2005). — № 1. — pp. 32-35.
[13] Berlekamp E.R. Algebraic Coding Theory. — McGraw-Hill Education, (1968). — ISBN 0-89412-063-8.
[14] Leukhin A.N., Bakhtin S.A. A new algorithm for the synthesis of all irreducible polynomials over a given finite field. Wikipedia [online], Available at: http://bio.marstu.net/data/ materials/conf/mmro13/mmro13pdf/ LEUKHIN_SI_2.pdf.
[15] Trakhtman A.M., Trakhtman V.A. Fundamentals of the theory of discrete signals at finite intervals. - M: Sov. radio, (1975). — 208 p.
[16] Wilfrid Keller. Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$, Math. of Comp., 41 (1983). — P. 661-673.
[17] Fermat number. Wikipedia [online], Available at:https://ru.wikipedia.org/wiki/