On a quick multiplication in normal bases of finite fields

A. A. BOLOTOV and S. B. GASHKOV

Abstract — We estimate the complexity of transition from normal bases to standard ones and discuss the related problems of effective realization of arithmetic operations in finite fields of high dimensionality.

The work was supported by the Russian Foundation for Basic Research, grant 99–01–01175, the Program of support of leading scientific schools, grant 00–15–96103, the Program ‘Universities of Russia,’ and by the Federal program ‘Integration,’ joint project A0110.

1. INTRODUCTION

In the sixties, Berlekamp in [1] remarked that the large finite fields are of academic interest only. At the present time, this is not the case. For example, it is impossible to imagine the public-key cryptology without these fields. Therefore, in the last twenty years, we observe the growing interest to circuit and program realizations of the arithmetic of high dimensional (up to 1000 and higher) finite fields.

The efficiency of realization of the arithmetic operations in finite fields essentially depends on the choice of representation of elements of the field, in particular, for this purpose, different bases of finite fields can be used.

It seems likely that from this point of view the normal bases are the most appropriate, since raising to the power $q$ in $GF(q^n)$ is reduced in these bases to a cyclic shift of the coordinates. The normal bases have long been known in algebra (they were discovered more than a century ago) and many investigations carried out from that time were concentrated on the question how to construct such bases (see, for example, the comments to the list of references in [18]), however only 12 years ago specialists in algebraic cryptology from Canada ([19]) discovered the optimal normal bases, which permitted to approach to another important question concerning the normal bases, how to use them. This discovery led to a new rise of investigations and publications on this subject (see [6, 13, 14, 15, 18]).

The optimal normal bases exist not in all fields, therefore the normal bases of low complexity close to optimal are of interest (see [6, 13, 21, 22]).

Note that for the first time such bases were found in 1985 (before the discovery of the optimal bases) by V. M. Sidelnikov [23], who proved that for any $t$ which divides $p$,
\[ q - 1, \text{ or } q + 1, \text{ where } q = p^r, \text{ in the field } GF(q^t) \text{ there exists a normal basis } \{ \omega_i \} \text{ with the multiplication table} \]

\[ \omega_i \omega_j = \alpha_{i-j} \omega_i + \alpha_{i+j} \omega_j + \gamma, \quad i \neq j, \]

where the indices of \( \alpha \) are taken modulo \( t \), \( \alpha_k \) and \( \gamma \) belong to \( GF(q) \), and the cases where \( \gamma = 0 \) are determined.

The interest to the optimal normal bases is connected partly with possible applications in cryptology on elliptic curves (see, for example, [2]).

The known constructions of circuits for multiplication in finite fields in normal and other bases (see, for example, [6]) are usually of the form of finite automaton circuits consisting of logic elements and shift registers with feedback. The complexity of such circuits (by it we mean the number of elements of the circuit) is linear, and the running time (measured, as the rule, in the so-called clock-cycles) also linearly depends on the number of inputs (the dimension of the field). If these constructions are represented as logic (Boolean) circuits, then the complexity is naturally quadratic and the running time (the lag) is defined by their depth and depends logarithmically on the number of inputs of the circuit.

In the case of program implementation of the algorithms mentioned above, the running time is estimated by the Boolean (bit) complexity of the algorithms. Sometimes, instead of the Boolean complexity, the arithmetic complexity is considered, which is measured in the number of arithmetic operations of the algorithm in the basic field.

However, for the measures of complexity mentioned above there exist quicker than quadratic algorithms of multiplication in the standard bases, for example, the Karatsuba algorithm or the asymptotically quicker Schönhage algorithm [20].

The basic idea of the present paper consists in the use of two bases (the standard and normal bases) for execution of the arithmetic operations in order to realize the advantages of the bases. Namely, it is more convenient to carry out the multiplication in the standard basis (see, for example, [8, 9, 10]), and the normal bases are more effective for raising to the power \( q \). It is natural that the transitions from one basis to the other should be realized quickly as well.

For this purpose, we investigate the complexity of transitions from the normal bases to standard ones and back. Further this complexity is referred to as the transitive complexity of normal bases.

It appears that the normal bases (but not only them) possess a low transitive complexity. Further the normal bases with low transitive complexity are referred to as the normal bases with quick multiplication. For quick execution of multiplication in these bases, we first go to the appropriate standard basis, execute the multiplication, and go back.

The use of these bases accelerates the standard computer algorithms of exponentiation (raising to a power) and inversion (calculation of the inverse element). Note that the algorithms of exponentiation play the main role in many cryptographic protocols.

2. BASES OF FINITE FIELDS

In this section, we give a short review of notions and results on the standard and normal (including optimal) bases. A more complete information can be found in [6].
2.1. **Standard and normal bases**

Recall the notion of the standard basis in finite fields. We use the standard notation of the theory of finite fields (see, for example, [1, 5, 6, 7]). We denote by $GF(q^n)$ the finite field of order $q^n$ considered as the extension of degree $n$ of the field $GF(q)$ of order $q$. As a representation of elements of $GF(q^n)$ we use polynomials of degree at most $n - 1$ with coefficients from $GF(q)$. If the polynomials are written in the standard basis $B = \{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\}$ (in this case, the element $\alpha$ is called the generator of the basis), then the addition of elements of $GF(q^n)$ is reduced to the component-wise addition in $GF(q)$ of the vectors of the coefficients of the corresponding polynomials, and the multiplication of elements of the field is the multiplication of the corresponding polynomials over $GF(q)$, which is carried out modulo the irreducible over $GF(q)$ polynomial $g(x)$ determining the representation of the field.

Sometimes, instead of the standard basis, it is convenient to use the so-called normal basis, that is, the basis of the form $B = \{\alpha^q^0, \alpha^q^1, \ldots, \alpha^q^{n-1}\}$ generated by the generator $\alpha$ of the standard basis, which is the root of the irreducible over $GF(q)$ polynomial $g(x)$ in the splitting field $GF(q^n)$. The normal basis exists for any $n$ (see, for example, [1, 6], where the number of normal bases is calculated), but it is generated not by any irreducible polynomial $g(x)$, since the powers of $\alpha$ in the basis should be linearly independent over $GF(q)$.

If the system of powers $\{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\}$ forms the normal basis, then any element $\zeta$ of $GF(q^n)$ is uniquely represented in the form

$$\zeta = x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2} + \cdots + x_{n-1}\alpha^{q^{n-1}}$$

with the coefficients $x_0, \ldots, x_{n-1}$ from $GF(q)$.

As in the normal basis, the operation of addition in the normal basis is the component-wise addition of the vectors of the coefficients in $GF(q^n)$.

The operation of raising to the power $q$ (and consequently, to any power $q^m$) in the normal basis is the cyclic shift of the coefficients, since

$$\zeta^q = x_{n-1}\alpha + x_0\alpha^q + x_1\alpha^{q^2} + \cdots + x_{n-2}\alpha^{q^{n-1}}.$$

Consider the multiplication in the normal basis.

According to [19] the complexity $C_B$ of an arbitrary normal basis

$$B = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$$

is the number of non-zero elements in the matrix $T$, whose $i$th row is the vector of coefficients of the element $\alpha \alpha^{q^i}$ of the field $GF(q^n)$ with respect to the basis $B$, that is,

$$\alpha \alpha^{q^i} = \sum_{j=0}^{n-1} t_{i,j} \alpha^{q^j}.$$
This definition is motivated by the following algorithm for multiplication in the normal basis $B$ (the Massey–Omura algorithm, see, for example, [6]).

Let

$$
\xi = \sum_{i=0}^{n-1} x_i \alpha^q^i, \quad \zeta = \sum_{j=0}^{n-1} y_j \alpha^q^j
$$

be arbitrary elements of $GF(q^n)$ expanded in terms of the normal basis $B$. Then their product can be calculated by the formula

$$
\pi = \xi \zeta = \sum_{i,j=0}^{n-1} x_i y_j \alpha^q^{i+j} = \sum_{i,j=0}^{n-1} x_i y_j \alpha^{(i-j+1)q^j},
$$

where the difference $i - j$ is calculated modulo $n$, and since

$$
\alpha^{(i-j+1)q^j} = (\alpha^q^{i-j+1}) q^j = \left(\sum_{k=0}^{n-1} t_{i-j,k} q^k\right) q^j
$$

$$
= \sum_{k=0}^{n-1} t_{i-j,k} q^{k+j} = \sum_{m=0}^{n-1} t_{i-j,m-j} q^{m},
$$

where the difference $m - j$ and the sum $k + j$ are also calculated modulo $n$, we have

$$
\pi = \sum_{m=0}^{n-1} p_m \alpha^q^m,
$$

where

$$
p_m = \sum_{i,j=0}^{n-1} t_{i-j,m-j} x_i y_j.
$$

Defining the matrix $A$ by the equalities $a_{i,j} = t_{i-j,-j}$, where $i - j$ and $m - j$ are calculated modulo $n$, we see that the previous formula can be rewritten in the form

$$
p_m = \sum_{i,j=0}^{n-1} t_{i-j,m-j} x_i y_j = \sum_{k,l=0}^{n-1} l_{k-l,-l} x_k m y_{l+m}
$$

$$
= \sum_{i,j=0}^{n-1} a_{i,j} x_i m y_{j+m} = \sum_{i,j=0}^{n-1} a_{i,j} S^m(x_i) S^m(y_j),
$$

where $S^m$ is the operation of the cyclic shift of the coordinates of the vector by $m$ coordinates, and

$$
A(x, y) = \sum_{i,j=0}^{n-1} a_{i,j} x_i y_j
$$

is the bilinear form related to the matrix $A$. 
The matrix $A$ is symmetric and the number of the non-zero elements of the matrix and the sum of the elements are the same as for the matrix $T$. In order to calculate the bilinear form $A(x, y)$, it suffices to execute $2C_B + n - 1$ additions and multiplications in the field $GF(q)$. If we neglect the time needed for realization of the cyclic shifts, then the complexity of multiplication over the normal basis of the field $GF(q^n)$ is estimated as $n(2C_B + n - 1)$ operations in the field $GF(q)$, as can be seen from the following main formula:

$$\xi \xi = A(\xi, \xi)\alpha + A(\xi^{q^{-1}}, \xi^{q^{-2}})\alpha^{q^{-2}} + A(\xi^{q^{-3}}, \xi^{q^{-4}})\alpha^{q^{-4}} + \cdots + A(\xi^q, \xi^q)\alpha^{q^{n-1}}.$$ 

Thus, the arithmetic complexity of multiplication depends only on the number $C_B$ of non-zero elements of the matrix $A$. The upper bound of the complexity of multiplication over an arbitrary normal basis is cubic.

The matrix (the multiplication table in the basis $B$) uniquely determines the operation of multiplication in the field under consideration.

The following result on the complexity of normal basis is proved in [19].

**Theorem 1.** For any normal basis $B$ of the field $GF(q^n)$, the complexity $C_B$ is at least $2n - 1$. Moreover, if $q = 2$, then the complexity is odd.

The normal bases for which this bound is attained are called optimal.

### 2.2. Optimal normal bases and normal bases of low complexity

The optimal normal bases are described in [19]. They can be successfully used in the Massey–Omura multiplier. Later in [14], it was shown that there are no other normal bases except the optimal bases found in [19].

Optimal bases exist not in all fields, therefore of interest are the bases which are not optimal but have a low complexity, that is, the bases with $C_B(n) = O(n)$. The use of such bases in the Massey–Omura multiplier also leads to the estimate $O(n^2)$ for the arithmetic complexity.

In [13], such bases were constructed with the use of Gaussian periods, whose applications in cryptology are considered in [15, 16]. Another method of constructing bases of low complexity is given in [21] (see also [22]).

The bases suggested by Sidelnikov (see [23]), strictly speaking, are unsuitable for Massey–Omura multiplier, but a modification of this multiplier with the use of these bases also has the complexity $O(n^2)$.

Three types of normal bases in the field $GF(q^n)$ are distinguished by the type of constructing.

The optimal normal bases of the first type can be constructed if $n + 1 = p$ is a prime number and $q$ is a primitive root modulo $p$. In this case, the generator of the normal basis is one of the primitive roots of the $p$th degree of the unity element of the field $GF(q^n)$.

The optimal normal bases of the second type appear if $2n + 1 = p$ is a prime number and $q$, as in the first case, is a primitive root modulo $p$. The generator of such a basis is the element $\alpha = \zeta + \zeta^{-1}$, where $\xi$ is a primitive root of the $p$th degree of the unity element of the field $GF(q^{2n})$.

The optimal normal bases of the third type is generated in the case where $2n + 1 = p$ is a prime number, $p \equiv 3 \pmod{4}$, and $q$ is a quadratic residue modulo $p$ and any quadratic
residue is represented as a power of $q$ modulo $p$ (or, in other words, the order of the element $q$ modulo $p$ equals $n$). As in the case of the second type, the generator of a basis of the third type is $\alpha = \zeta + \zeta^{-1}$, where $\zeta$ is a primitive root of the $p$th degree of the unity element of the field $GF(q^{2n})$.

3. ON THE OPTIMAL TRANSITIVE COMPLEXITY
OF THE OPTIMAL NORMAL BASES

3.1. Estimating the complexity of transition from optimal normal bases of the first type
to standard bases and back

The implemented standard algorithms for multiplication in the optimal normal bases prove
to be slower (see [10]) than the algorithms for multiplication in the standard bases even in
fields of small dimensionality (150–350) and become still worse with rise of dimensionality.
A comparison of the standard and normal types of bases suggests to accelerate the arithmetic
in finite fields by using the advantages of both of them. Indeed, it is better to execute
multiplication in the standard representation of the field $GF(q^n)$, but raising to a power is
quicker in the normal representation.

To realize this idea, the matrices of transition from a normal basis to a standard one
and back are needed, and they can be not sparse but dense, therefore the complexity of
transition from one basis to another in the worst case will be $O(n^2/ \log n)$ (even if the
Lupanov–Konovaltsev method [12] will be used for multiplication of a matrix by a vector).

In the case of a sparse matrix, the transitive complexity can be even not higher than
linear, for example, in the case where the number of non-zero elements of the transition
matrices is $O(n)$. Thus, the problem of searching for normal bases with easily calculated
matrices of transition to standard bases and back appears worthy of investigation.

This problem is easily solved in the case of optimal normal bases of the first type. Recall
that the first type normal bases appear only if $n + 1 = p$ is a prime number and $q$ is a
primitive root modulo $p$.

Further the complexity means the arithmetic complexity in the class of circuits with
operations of addition and multiplication in the field $GF(q)$.

**Theorem 2.** The transition from a standard basis of $GF(q^n)$ to the corresponding (with
the same generator) optimal normal basis of the first type (of course, if it exists for this $n$)
and back can be realized with a linear complexity.

**Proof.** It is easy to see that in this case the basis $\{\zeta, \ldots, \zeta^n\}$ (not quite standard) coincides up to permutation with the optimal normal basis

$$\{\zeta, \zeta q, \zeta q^2, \ldots, \zeta q^{n-1}\},$$

since the sequence of numbers $1, q, q^2, \ldots, q^{n-1}$, taken modulo $p$, coincides with some
permutation of the sequence $\{1, 2, \ldots, n\}$ because $\zeta$ is a primitive root of the $p$th degree of
the unity element of the field $GF(q^n)$ and $q$ is a primitive root modulo $p$.

Therefore it is obvious that the transition from the basis $\{\zeta, \ldots, \zeta^n\}$ to the normal basis

$$\{\zeta, \zeta q, \zeta q^2, \ldots, \zeta q^{n-1}\}$$
and back is performed with complexity at most $n$.

Note that $\zeta$ is a root of the irreducible over $GF(q)$ polynomial

$$1 + x + \ldots + x^n = \frac{x^p - 1}{x - 1}.$$  

The standard basis for the transition is the basis $\{1, \zeta, \ldots, \zeta^{n-1}\}$. It is clear that this basis can be expressed with linear complexity in terms of the basis $\{\zeta, \ldots, \zeta^n\}$, since

$$\zeta^n = 1 + \zeta + \ldots + \zeta^{n-1},$$

and the basis $\{\zeta, \ldots, \zeta^n\}$ in view of the formula

$$1 = \zeta + \ldots + \zeta^{n-1} + \zeta^n,$$

can be expressed with linear complexity in terms of the basis $\{1, \zeta, \ldots, \zeta^{n-1}\}$. As a result, the transition from the optimal normal basis

$$\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{n-1}}\}$$

to the standard basis $\{1, \zeta, \ldots, \zeta^{n-1}\}$ and back is performed with linear complexity.

The multiplication in the standard basis $\{1, \zeta, \ldots, \zeta^{n-1}\}$ is, as usual, reduced to multiplication of polynomials over the field $GF(q)$ with consequent reduction modulo the irreducible polynomial

$$f(x) = 1 + x + \ldots + x^n,$$

corresponding to the basis. Note that the division with residual by this polynomial can be performed with linear complexity.

Indeed, suppose that we have to divide a polynomial $g(x)$ of degree $2n - 2$ by $f(x)$ and find the residual (only it is really needed), that is, we have to express $g(x)$ in the form

$$g(x) = f(x)h(x) + r(x),$$

where the degree of $r(x)$ is less than $n$. Multiplying both the sides of this equality by $x - 1$, we obtain

$$g(x)(x - 1) = (x^p - 1)h(x) + r(x)(x - 1),$$

and since the degree of $r(x)(x - 1)$ is less than $n + 1 = p$, we find that $r(x)(x - 1)$ is the residual of division $g(x)(x - 1)$ by $x^p - 1$.

For the multiplication of $g(x)$ by $x - 1$, it suffices to execute $2n - 2$ additions (in $GF(q)$), the division of the result by $x^p - 1$ requires $n - 3$ additions, and finally the division of the residual $r(x)(x - 1)$ by $x - 1$ with the use of the Horner scheme requires $n$ additions.

3.2. Estimating the complexity of transition from optimal normal bases of the second and third types to standard bases and back (binary case)

We begin with several auxiliary assertions (the first lemma is valid in the general case).

Let $\alpha = \alpha_1$ be the generator of the optimal normal basis

$$\{\alpha_1, \ldots, \alpha_n\}$$
of the second type of the field $GF(q^n)$, it is also the generator of the corresponding standard basis
$$\{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\}$$
that is, $\alpha_1 = \alpha = \zeta + \zeta^{-1}$, and for any $k \leq n$,
$$a_k = \alpha^{q^k - 1} = \zeta^{q^k - 1} + \zeta^{-q^k - 1},$$
where $\zeta$ is a primitive root of 1 of degree $p = 2n + 1$ in $GF(q^{2n})$.

Let $q = p^r$, where $p$ is a prime number and $\alpha = \zeta + \zeta^{-1}$. We consider an auxiliary sequence $a_0, a_1, \ldots$, generated by the element $\alpha$. We set $a_0 = 2$ (of course, $a_0 = 0$ if $p = 2$) and
$$a_k = \zeta^k + \zeta^{-k}, \quad k = 1, 2, \ldots, \quad a_1 = \alpha_1.$$

**Lemma 1.** For any $k \geq 1$, the recurrences
$$a_{k+1} = a_k a_1 - a_{k-1},$$
$$a_{p^k} = a^{p^k},$$
$$a_{p^k+i} = a_i a^{p^k} - a_{p^k-i}$$
hold.

**Proof.** To prove the first formula, note that
$$(\zeta^k + \zeta^{-k})(\zeta + \zeta^{-1}) = \zeta^{k-1} + \zeta^{-k+1} + \zeta^{k+1} + \zeta^{-k-1},$$
that is, $a_{k+1} a_1 - a_{k-1} = a_{k+1}$.

The second formula is obvious.

The third formula is checked directly:
$$a_{p^k+i} = \zeta^{p^k+i} + \zeta^{-p^k-i} = (\zeta^{p^k} + \zeta^{-p^k})(\zeta^i + \zeta^{-i}) - (\zeta^{p^k-i} + \zeta^{-p^k+i})$$
$$= a_{p^k} a_i - a_{p^k - i} = a_{p^k} a_i - a_{p^k - i}.$$

The recurrences proved in the lemma make it possible to write out the formulas of transition from the normal basis to the almost standard basis
$$\{\alpha^1, \ldots, \alpha^n\}.$$ Indeed, from the lemma it follows that for any $i \geq 1$ the element $\alpha_i$ of the normal basis is expressed as a value of some polynomial of degree $i$ over $GF(q)$, that is,
$$\alpha_i = f_i(\alpha) = \sum_{j=1}^i f_{i,j} \alpha^j.$$

If we represent all $\alpha_i$ of the normal basis in such a form, then we obtain the transition matrix $F_n = (f_{i,j})$ from the almost standard basis to the normal basis.

The following two auxiliary theorems concern the binary case (that is, the case where $p = 2$) and contain estimates of the density $S(F_n)$ (the number of non-zero elements) of the matrix $F_n$. 

Theorem 3. The density of the transition matrix from a standard basis of the field \(GF(2^n)\) to the corresponding normal basis of the second or the third type is \(O(n^{\log_2 3})\).

Proof. For \(n = 2^k - 1\), the matrix \(F_n\) constructed by the formulas of Lemma 1 is of the form

\[
\begin{pmatrix}
F_n & o_n & O_n \\
0 & 1 & 0 \\
G_n & o_n & F_n
\end{pmatrix}
\]

where \(o_n\) is the zero column-vector of height \(n\), \(O_n\) is the \(n \times n\) zero matrix, and the matrix \(G_n\) is the mirror image of the matrix \(F_n\) as reflected from the middle row, that is, \(G_n = I_n F_n\), where \(I_n = \delta_{i,n-i+1}\) is the matrix with ones on the secondary diagonal and zeros at the remaining entries.

For example, the matrix \(F_7\) is of the form

\[
F_7 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1
\end{pmatrix}
\]

If we divide the matrix into 4 square submatrices, removing the middle row and the middle column, then we see that the upper-left \(3 \times 3\) square is symmetric to the lower-left square about the horizontal and is equal to the lower-right square. The middle row and the middle column contain exactly a single one placed on their intersection. The matrix is lower triangular with ones on the main diagonal.

Indeed, in the general case, according to Lemma 1, for \(0 \leq i \leq 2^k\)

\[
\sum_{j=1}^{2^k+i} f_{2^k+i,j} \alpha^j = a_{2^k+i} = a_i \alpha^{2^k} + a_{2^k-i}
\]

\[
= \sum_{j=1}^{i} f_{i,j} \alpha^{2^k+j} + \sum_{j=1}^{2^k-i} f_{2^k-i,j} \alpha^j,
\]

hence, \(f_{2^k+i,j} = f_{2^k-i,j}\) for \(0 \leq j \leq 2^k\) and \(f_{2^k+i,2^k+i} = f_{i,j}\) for \(1 \leq j \leq 2^k\).

With the use of this representation, for the density of the sequence of matrices \(F_n\) we obtain the recurrence

\[
S(F_{2n+1}) = 3S(F_n) + 1, \quad n \geq 3, \quad S(F_3) = 4,
\]

which leads to the recurrence

\[
S(F_{2^k-1}) = 3S(F_{2^k-1-1}) + 1, \quad k \geq 2, \quad S(F_3) = 4.
\]

Setting \(l(k) = S(F_{2^k-1})\), we arrive at the linear recurrence

\[
l(k) = 3l(k-1) + 1, \quad l(2) = 4.
\]
with the solution

\[ l(k) = (3^k - 1)/2. \]

Setting \( n = 2^k - 1 \) and using the representation \( 3^k = (2^k)^{\log_2 3} = (n + 1)^{\log_2 3} \), we obtain

\[ S(F_n) = l(k) = ((n + 1)^{\log_2 3} - 1)/2 = O(n^{\log_2 3}). \]

In the general case, the estimate

\[ S(F_n) = O(n^{\log_2 3}) \]

remains true, since choosing \( k \) so that

\[ 2^k - 1 < n \leq 2^{k+1} - 1, \]

we see that the matrix \( F_n \) is the main submatrix of the matrix \( F_m, m = 2^k - 1 \), and therefore

\[ S(F_n) \leq S(F_m) = O(m^{\log_2 3}) = O(n^{\log_2 3}). \]

Let us estimate the density of the transition matrix \( F'_n \) from a standard basis of \( GF(2^n) \) to the corresponding normal basis. We denote by \( B_n \) the transition matrix from the standard basis to the almost standard basis, then \( F'_n = F_n B_n \), and it can be directly checked that all elements of the matrix \( B_n \) are zeros, except the elements \( b_{i,i+1} = 1 \) and some elements of the bottom row \( b_{n,j} \), and for the elements of the matrix \( F'_n \)

\[ f'_{i,1} = f_{i,n} b_{n,1} = \delta_{i,n} b_{n,1}, \]
\[ f'_{i,j} = f_{i,j-1} + f_{i,n} b_{n,j} = f_{i,j-1} + \delta_{i,n} b_{n,j}, \]

since the matrix \( F_n \) is lower triangular and for their elements the equalities \( f_{i,n} = \delta_{i,n} \), where \( \delta_{i,n} \) is the Kronecker symbol, are true. Adding these equalities, we obtain

\[
S(F'_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} f_{i,j} + \sum_{j=1}^{n} b_{n,j} = S(F_n) - 1 + \sum_{j=1}^{n} b_{n,j} \\
\leq S(F_n) - 1 + n = O(n^{\log_2 3}).
\]

We denote by \( L(F_n) \) the complexity of the linear transformation determined by the matrix \( F_n \) (the least number of operations of addition modulo 2 needed for calculating this transformation).

**Theorem 4.** The estimate

\[ L(F_n) \leq \frac{n}{2} \log_2 n + 2n = O(n \log_2 n) \]

holds.

**Proof.** It is more convenient to estimate the complexity of the transformation determined by the transposed matrix \( F_n^T \). According to the well-known theorem on relationship of complexities of transposed matrices (see, for example, [17]) this complexity equals \( L(F_n) \).
Besides, we have to estimate the complexity of transition from the coordinates in the normal basis \(\sum_{i=1}^{n} x_i a_i\) to the coordinates in the almost standard basis \(\sum_{i=1}^{n} y_i a^i\), which is determined just by the matrix \(F_n^T\). Let \(2^k \leq n < 2^{k+1} - 1\), then using the formulas from Lemma 1

\[
\sum_{i=1}^{n} y_i a^i = \sum_{i=1}^{n} x_i a_i = \sum_{i=1}^{2^k} x_i a_i + \sum_{i=2^k+1}^{n} x_i a_i \\
= \sum_{i=1}^{2^k} x_i a_i + \sum_{i=1}^{n-2^k} x_i + 2^k a_{i+2^k} \\
= \sum_{i=1}^{2^k} x_i a_i + \sum_{i=1}^{n-2^k} x_i + 2^k a_{i+2^k} (a^{2^k} a_i + a_{2^{k-1}}) \\
= x_2^k a_{2^k} + \sum_{i=1}^{2^k} x_i a_i + \sum_{i=2^{k+1}-n}^{2^k-1} (x_i + x_2^k + 1 - x_{i+n}) a_i + a^{2^k} \sum_{i=1}^{n-2^k} x_i a_{i+2^k},
\]

introducing the column vectors

\[
X = \{x_1, \ldots, x_n\}^T, \\
X_1 = \{x_1, \ldots, x_2^{k+1} - n-1, x_2^{k+1} - n + x_n, \ldots, x_2^{k-1} + x_2^{k+1}, x_2^n\}^T, \\
X_2 = \{x_1 + 2^k, \ldots, x_n\}^T,
\]

and row vectors

\[
Y_2 = \{y_1 + 2^k, \ldots, y_n\}, \\
Y_1 = \{y_1, \ldots, y_{2^k}\},
\]

we obtain

\[
\sum_{i=1}^{n} y_i a^i = \sum_{i=1}^{n} x_i a_i = \sum_{i=1}^{2^k} X_1,i a_i + a^{2^k} \sum_{i=1}^{n-2^k} X_2,i a_i \\
= \sum_{i=1}^{2^k} Y_1,i a^i + \sum_{i=1}^{n-2^k} Y_2,i + 2^k a_{i+2^k},
\]

and consequently,

\[
F_n^T \otimes X = (y_1^\prime \ldots y_n^\prime) = (Y_1, Y_2) = (F_{2^k}^T \otimes X_1, F_{n-2^k}^T \otimes X_2),
\]

where \(\otimes\) is the operation of multiplication of a matrix by a vector in \(GF(2)\). Note that the last equality can be obtained directly being based only on the structure of the matrix \(F_n\).

It remains to estimate the complexity of the transformation determined by the matrix \(F_n^T\). According to (1)

\[
L(2^{m+1}) \leq 2^m - 1 + 2L(2^m), \quad m \leq k - 1, \quad L(2) = 2.
\]
By induction it can be directly checked that
\[ L(2^m) = 2^{m-1}m + 1. \]
For an arbitrary \( n \) such that \( 2^k < n < 2^{k+1} \), we obtain
\[ L(n) \leq L(2^k) + L(n - 2^k) + n - 2^k. \]
Representing \( n \) in binary system as
\[ n = 2^{k_s} + \ldots + 2^{k_1}, \]
where \( k_s > \ldots > k_1 \), we obtain
\[
L(n) \leq 2^{k_s-1}k_s + \ldots + 2^{k_1-1}k_1 + s - 1 + (n - 2^{k_s}) + \ldots + (n - 2^{k_s} - \ldots - 2^{k_2}) \\
\leq \frac{n}{2} \log_2 n + c \frac{n}{2},
\]
where
\[ c = \frac{2}{2} + \frac{3}{4} + \frac{4}{8} + \frac{5}{16} + \ldots < 4. \]

**Theorem 5.** The complexity \( B(n) \) of transition in \( GF(2^n) \) from an optimal normal basis of the second or third type to the corresponding standard basis and back satisfies the inequality
\[ B(n) \leq \frac{n}{2} \log_2 n + 3n. \]

**Proof.** We denote by \( \alpha = \zeta + \zeta^{-1} \) the generator of the standard basis
\[ A = \{1, \alpha^1, \ldots, \alpha^{n-1}\} \]
and the basis of the first or third type
\[ B = \{\alpha^{2^0}, \alpha^{2^1}, \ldots, \alpha^{2^{n-1}}\}. \]

The transition from the normal basis to the standard basis will be realized through the chain of four bases
\[ B \rightarrow B' \rightarrow A' \rightarrow A \]
and the transformation of the coordinates of an element \( f \) of the field \( GF(2^n) \) in these bases
\[ f = \sum_{i=1}^{n} x_i \alpha^{2^{i-1}} = \sum_{i=1}^{n} x'_i a_i = \sum_{i=1}^{n} y'_i \alpha^i = \sum_{i=1}^{n} y_i \alpha^{2^{i-1}}, \]
where
\[ a_i = \zeta^i + \zeta^{-i}, \quad B' = \{a_1, \ldots, a_n\}, \quad A' = \{\alpha^1, \ldots, \alpha^n\}. \]

The transition from the basis \( B \) to the basis \( B' \) and the transformation of the coordinates \( \vec{x} \) to the coordinates \( \vec{x}' \) is realized by permutation of the basis elements, since there exists a permutation \( \pi(i) \) of the numbers \( \{1, \ldots, n\} \) such that for any \( i = 1, \ldots, 2n \)
\[
2^i \pmod{p} = \pm \pi(i) \in \{1, \ldots, n\}. \]
Indeed, for the basis of the second type, the sequence of powers

\[ 1, 2, 2^2, \ldots, 2^{2n-1}, \]

taken modulo \( p \), coincides with some permutation

\[ \pi(1), \ldots, \pi(2n) \]

of the set \( \{1, \ldots, 2n\} \), since 2 is a primitive root modulo \( p \). Using the equality

\[ 2^{k+n} = -2^k \pmod{p} \]

(by the Fermat theorem \( 2^{2n} = 1 \pmod{p} \), and consequently, \( 2^n = -1 \pmod{p} \)) we obtain (2).

For the basis of the third type, the number 2 is a quadratic residue modulo \( p \), therefore all powers

\[ 2^k \pmod{p}, \quad k = 1, \ldots, n-1, \]

form a permutation of the set of all quadratic residues modulo \( p \), since there are exactly \( n \) residues. If we take into account the fact that \( p \) equals 3 modulo 4 and therefore \(-1\) is a quadratic non-residue modulo \( p \), since otherwise there exists a number \( r \) such that \( -1 = r^2 \pmod{p} \) that contradicts the Fermat theorem:

\[ r^{p-1} = (r^2)^{(p-1)/2} = (-1)^{(p-1)/2} = -1 \pmod{p}, \]

and the fact that the product of a residue and non-residue is a non-residue, we conclude that the sequence \(-2^k \pmod{p}, k = 0, \ldots, n-1\), is a permutation of the set of all quadratic residues modulo \( p \). As a result we obtain that in this case formula (2) is also true.

Thus, the basis \( \{a_1, \ldots, a_n\} \) is a permutation of the basis \( \{a, \ldots, a^{2^{n-1}}\} \). The negative indices can be replaced by the corresponding positive indices according to the equality

\[ a_i = \zeta^i + \zeta^{-i} = a_{-i} \]

by the formula \( a^{2^i} = a|_{\pi(i)} \), (or for coordinates \( x_i = x_{\pi(i)} \)). Therefore in what follows we assume that the indices are positive and omit the sign of module of a number.

It is obvious that \( B' \) is also a basis, since it is simply a permutation of the basis \( B \). Thus, the complexity \( L_{BB'}(n) \) of the transition \( B \rightarrow B' \) is \( O(n) \), and if instead of the program implementation we consider the circuit implementation, then \( L_{BB'}(n) = 0 \).

The transition from the basis \( B' \) to the basis \( A' \) and the transformation of the coordinates \( \tilde{x}' \) to the coordinates \( \tilde{y}' \) is, in view of Theorem 4, of the complexity which satisfies the inequality

\[ L(n) \leq \frac{n}{2} \log_2 n + 2n. \]

The transition from the basis \( A' \) to the basis \( A \) and the transformation of the coordinates \( \tilde{y}' \) to the coordinates \( \tilde{y} \). Using recurrence (1), it is possible to construct the minimal annihilator polynomial \( m_\alpha \) (it has to be constructed only once, before the application of the transition algorithm, and therefore the complexity of this construction is not taken into account), that is,

\[ m_\alpha = f_n(\alpha) = b_1 \alpha^0 + \ldots + b_n \alpha^n = 0, \quad (3) \]
where $\alpha$ is the generator of the bases and not all coefficients $b_i$ are zeros. We will write out an explicit transition from the coordinates $\vec{y}'$ in the almost standard basis $A'$ to the coordinates $\vec{y}$ in the standard basis $A$. Taking into account (3), we find that

$$\sum_{i=1}^{n} y'_i \alpha^i = \sum_{i=1}^{n-1} y'_i \alpha^i + y'_n \left( \sum_{i=0}^{n-1} b_i \alpha^i \right).$$

and, rearranging the coefficients, we obtain

$$\sum_{i=1}^{n} y'_i \alpha^i = \sum_{i=1}^{n-1} \alpha^i (y'_i + b_i y'_n) + y'_n \alpha^0 = \sum_{i=1}^{n-1} y_i \alpha^i + y_0 \alpha^0.$$

Hence it is seen that the complexity of the transition from the almost standard basis $A'$ to the standard basis $A$ satisfies the inequality

$$L_{A'A}(n) \leq (n - 1).$$

Thus, we estimated the complexities of all transformations, it remains to sum these complexities:

$$L_{BA}(n) = L_{BB'}(n) + L_{B'A'}(n) + L_{A'A}(n) \leq \frac{n}{2} \log_2 n + 3n.$$
Hence it is seen that the complexity of the transition from the standard basis $A$ to the almost standard basis $A'$ satisfies the inequality $L_{AA'}(n) \leq n - 1$.

The transition from the basis $A'$ to the basis $B'$ and the transformation of the coordinates $\bar{y}'$ to the coordinates $\bar{x}'$. We consider the transformation

$$(x'_1 \ldots x'_n) = (F^{-1}_{n-2k})^T \otimes \begin{pmatrix} y''_1 \\ \vdots \\ y''_n \end{pmatrix},$$

of multiplication of the vector $Y^T$ by the matrix $(F^{-1}_{2k+1})^T$ (the inverse to the matrix from Theorem 4) with the use of (1). In this formula, the vectors $X_1$, $X_2$, are recurrently transformed to the vectors

$$Y_1 = (y''_1, \ldots, y''_{2k}), \quad Y_2 = (y'_{2k+1}, \ldots, y'_n),$$

which form the vector $Y = (y'_1, \ldots, y'_n)$. It is clear that the inverse transformation $(F^{-1}_{n-2k})^T \otimes Y_2^T$ transfers the vector $Y_2$ to $X_2$, and in order to obtain the vector $X_1$, we have to perform the transformation $(F^{-1}_{2k})^T \otimes Y_1^T$. Since

$$X_1 = \{x_1, \ldots, x_{2k+1-n-1}, x_{2k+1-n} + x_n, \ldots, x_{2k-1} + x_{2k+1}, x_{2k}\}^T,$$
$$X_2 = \{x_{1+2k}, \ldots, x_n\}^T,$$

to reconstruct the vector $X = \{x_1, \ldots, x_n\}$ with the use of these vectors, it is sufficient to add (modulo 2) the components of $X_2$ to the corresponding $n - 2k$ components of the vector $X_1$.

Continuing inductively the described transformation, we transfer the coordinates $\bar{y}'$ in the almost normal basis $B'$ with complexity

$$L^{-1}(n) \leq n - 2^k + L^{-1}(2^k) + L^{-1}(n - 2^k),$$

and, as before, obtain the estimate

$$L_{B'A'}(n) \leq \frac{n}{2} \log_2 n + 2n.$$

The transition from the basis $B'$ to the basis $B$ and from the coordinates $\bar{x}'$ to $\bar{x}$ is realized by means of the permutation inverse to $\pi(i)$ (see (3)), and its complexity is estimated as before, that is,

$$L_{B'B}(n) = 0.$$

As a result, we find that

$$L_{AB}(n) = L_{AA'}(n) + L_{A'B'}(n) + L_{B'B}(n) \leq \frac{n}{2} \log_2 n + 3n.$$
Note that while we calculated the inverse transformation \((F_n^{-1})^T\) for \(n = 2^{k+1} - 1\), we in fact obtained the matrix identity

\[
(F_n^T)^{-1} = \begin{pmatrix}
(F_m^T)^{-1} & o_m & G_m \\
0 \ldots 0 & 1 & 0 \ldots 0 \\
o_m & o_m & (F_m^T)^{-1}
\end{pmatrix},
\]

where \(m = (n - 1)/2\) and the matrix \(G_m = I_m(F_m^T)^{-1}\) is the symmetric reflection of the matrix \((F_m^T)^{-1}\) with respect to the middle row.

Note also that this identity, in the same way as the similar identity

\[
F_n^{-1} = \begin{pmatrix}
F_m^{-1} & o_m & O_m \\
0 \ldots 0 & 1 & 0 \ldots 0 \\
G_m & o_m & F_m^{-1}
\end{pmatrix},
\]

where \(m = (n - 1)/2\) and the matrix \(G_m = F_m^{-1}I_m\) is the mirror image of the matrix \(F_m^{-1}\) as reflected from the middle column, can be checked directly. By using these identities, as in Theorem 3, it is possible to prove that the density of the inverse matrix

\[
S(F_n^{-1}) = O(n^{\log_2 3})
\]

and the same density has the transition matrix from the normal basis of the second or third type to the standard basis of the field \(GF(2^n)\).

### 3.3. On the explicit formulas of transition and the minimal polynomials for optimal normal bases

In this section, we consider the general case \(q = p^r\). We define the sequence of polynomials \(f_i(x)\) over \(GF(q)\) by the recurrence

\[
f_{i+1}(x) = xf_i(x) - f_{i-1}(x), \quad f_1(x) = x, \quad f_0 = 2.
\]

By induction it is easy to check that

\[
f_i(\xi + \xi^{-1}) = \xi^i + \xi^{-i}
\]

for any element \(\xi\).

As was noted above, these polynomials determine the formulas of transition from standard bases to normal bases of the second and third types.

The sequence \(f_i(x)\) can be formally extended to negative indices, then, obviously, \(f_{-i}(x) = f_i(x)\).

This sequence is similar in a sense to a sequence of the Chebyshev polynomials. In the same way as for the Chebyshev polynomials, it is easy to check that the polynomials with even numbers are even, that is, contain only monomials of even degrees, and the polynomials with odd numbers are odd. Therefore, it is convenient to represent them in the form

\[
f_i(x) = \sum_{j=0}^{[i/2]} a_{i,j}(-1)^j x^{i - 2j},
\]
where the coefficients are given in Lemma 2.

For the sequence under consideration, the Chebyshev identity
\[ f_{ij}(x) = f_i(f_j(x)) = f_j(f_i(x)) \]
is true. To prove this identity, it suffices to set \( x = \zeta + \zeta^{-1} \):
\[ f_i(f_j(\zeta + \zeta^{-1})) = f_i(\zeta^i + \zeta^{-i}) = \zeta^{ij} + \zeta^{-ij} = f_{ij}(\zeta + \zeta^{-1}). \]

It is easy to check that one more Chebyshev identity
\[ f_{i+j}(x) + f_{i-j}(x) = f_i(x)f_j(x) \]
holds. Indeed,
\[ \zeta^{i+j} + \zeta^{-i-j} + \zeta^{i-j} + \zeta^{-i+j} = (\zeta^i + \zeta^{-i})(\zeta^j + \zeta^{-j}). \]

**Lemma 2.** The equalities (with coefficients taken modulo \( p \))
\[ f_i(x) = \sum_{j=0}^{[i/2]} a_{i,j}(-1)^j x^{i-2j}, \]
\[ a_{i,j} = \binom{i-j}{j} + \binom{i-j-1}{j-1}, \quad x^i = \sum_{j=0}^{[i/2]} \binom{i}{j} f_{i-2j}, \]
where \( f_0 = 1 \), are true.

**Proof.** The base of induction is checked directly. In view of the identity
\[ f_{i+1}(x) = xf_j(x) - f_{i-1}(x), \]
to justify the induction step, it suffices to check that
\[ a_{i+1,j} = a_{i,j} + a_{i-1,j-1}. \]
The last equality follows from the Pascal identity
\[ a_{i,j} + a_{i-1,j-1} = \binom{i-j}{j} + \binom{i-j-1}{j-1} + \binom{i-j-1}{j-1} + \binom{i-j}{j-2} = \binom{1+i-j}{j} + \binom{i-j}{j-1} = a_{i+1,j}. \]

In order to prove the second identity, it is sufficient to multiply both sides of the required identity by \( x \) and again to apply the Pascal identity:
\[ x^{i+1} = x^{i+1} = \sum_{j=0}^{[i/2]} \binom{i}{j} x f_{i-2j} = \sum_{j=0}^{[i/2]} \binom{i}{j} (f_{1+i-2j} + f_{i-2j-1}) \]
\[ = f_{i+1} + \sum_{j=1}^{[i/2]} \left( \binom{i}{j} + \binom{i}{j-1} \right) f_{i-2j-1} = \sum_{j=0}^{[i/2]} \binom{i+1}{j} f_{1+i-2j}. \]
For the sake of completeness, we formulate the known theorem (see [6]) on the minimal annihilator polynomial of the optimal normal bases of the second and third types.

**Theorem 6.** Let \(2n + 1\) be a prime number and \(q = p^r\) be a primitive root modulo \(2n + 1\) or \(2n + 1 \equiv 3 \mod 4\) and \(q\) generate all quadratic residues modulo \(2n + 1\), then the polynomial \(g_n(x)\) over \(GF(q)\) determined by the recurrence

\[
g_0 = 1, \quad g_1(x) = x + 1, \quad g_k(x) = xg_{k-1}(x) - g_{k-2}(x), \quad k \geq 2,
\]

coincides with the minimal annihilator polynomial \(m_\alpha\) of the element \(\alpha\) and the roots of this polynomial form an optimal normal basis of the second, respectively, the third type of the field \(GF(q^n)\).

In addition to this theorem we point out how to calculate in the explicit form the coefficients of the minimal polynomial. Indeed, using the mentioned recurrence, we can check by induction that \(g_k(x) - g_{k-1}(x) = f_k(x)\) for \(k > 0\), that is,

\[
g_k(x) = f_k(x) + \ldots + f_1(x) + 1,
\]

and therefore, if

\[
g_n(x) = \sum_{j=0}^{n} g_{n,j}x^j,
\]

then by Theorem 6

\[
g_{n,j} = \sum_{i=0}^{\lfloor (n-j)/2 \rfloor} a_{2i+j,i}(-1)^i = (-1)^{\lfloor (n-j)/2 \rfloor} \binom{(n+j)/2}{j}
\]

(the calculations are modulo \(p\)). Of course, if \(p = 2\), then the factor \((-1)^{\lfloor (n-j)/2 \rfloor}\) can be omitted.

By virtue of the well-known Lucas theorem (see, for example, [3]) the binomial coefficient \(\binom{a}{b}\) modulo \(p\) can be calculated by \(O(v_p(b))\) operations in \(GF(p)\) with the use of the formula

\[
\prod_{i=1}^{m} \binom{a_i}{b_i},
\]

where \(0 \leq a_i, b_i < p, 1 \leq i \leq m\), are elements of the \(p\)-ary representation of \(a\) and \(b\), respectively, and

\[
v_p(b) = \sum_{i=1}^{m} b_i.
\]

Therefore, calculating sequentially, by adding one, the \(p\)-ary expansions of \(\lfloor (n+j)/2 \rfloor\) and \(j\), and using the above remark, we can calculate the coefficients of the polynomial \(g_n(x)\) with complexity \(O(pn \log_p n)\).

The same assertion is naturally true for the complexity of calculating the polynomial \(f_n(x)\). For calculating the whole sequence of polynomials \(f_1(x), \ldots, f_n(x)\) or \(g_1(x), \ldots, g_n(x)\), it is natural to use the determining recurrence that leads to a quadratic estimate of the complexity.
**3.4. Estimating the complexity of transition from optimal normal bases of the second and third types to the standard bases in the general case**

Let now \( 2n + 1 \) be a prime number and \( q = p^r \) be either a primitive root modulo \( 2n + 1 \) or \( 2n + 1 \equiv 3 \pmod{4} \) and \( q \) generate all quadratic residues modulo \( 2n + 1 \). Let \( \zeta \) be a primitive root of the unity of degree \( 2n + 1 \) in \( GF(q^{2n}) \), \( \alpha_i = \zeta^i + \zeta^{-i} / \alpha = \alpha_1 \). Then, as noted above, \( \{\alpha_1, \ldots, \alpha_n\} \) is the optimal normal basis (more precisely, a permutation of the basis) in the field \( GF(q^n) \), which can be considered as the vector space over \( GF(q) \).

Consider the \( m \)-dimensional, \( m \leq n \), subspace of \( GF(q^n) \) generated by the basis \( \{\alpha_0, \ldots, \alpha_{m-1}\} \) or by the equivalent basis \( \{1, \alpha, \ldots, \alpha^{m-1}\} \). Denote by \( L(m) \) the complexity of the transformation of coordinates from the basis \( \{\alpha_0, \ldots, \alpha_{m-1}\} \) to the basis \( \{1, \alpha, \ldots, \alpha^{m-1}\} \) and back (the complexity means the number of arithmetic operations in the field \( GF(q) \)).

**Theorem 7.** For \( m \leq n \),

\[
L(m) = O(pm \log p m).
\]

**Proof.** First we prove that for \( s = p^k s', m \leq s \)

\[
L(s + m) \leq L(s) + L(m) + m(3s'/2 + 2).
\]  

(5)

Note that \( \alpha_i = f_i(\alpha) \) and set \( \alpha_0 = 1 \). Consider the representation of an arbitrary element in the basis \( \{\alpha_0, \ldots, \alpha_{s+m-1}\} \)

\[
\sum_{i=0}^{s-1} x_i \alpha_i + \sum_{i=0}^{m-1} x_{i+s} \alpha_{i+s}.
\]  

(6)

Since \( \alpha_{i+s} = \alpha_s \alpha_i - \alpha_{s-i} \), representation (6) can be written in the form

\[
\sum_{i=0}^{s-1} y_i \alpha_i + \alpha_s \sum_{i=0}^{m-1} z_i \alpha_i,
\]  

(7)

where \( y_i = x_i - x_{2s-i} \) for \( i \geq s - m + 1 \) and \( y_i = x_i \) in the remaining cases, \( z_i = x_{i+s} \) for \( i > 0 \) and \( z_0 = x_s/2 \). The transition from (6) to (7) can be performed with complexity \( m \) and the reverse transition is of the same complexity.

With complexity \( L(s) + L(m) \), we can calculate vectors of the coefficients \( (y_i'), (z_j') \) such that the element under consideration can be written in the form

\[
\sum_{i=0}^{s-1} y_i' \alpha_i + \alpha_s \sum_{i=0}^{m-1} z_i' \alpha_i.
\]  

(8)

According to Lemma 2

\[
\alpha_s = \alpha_{p^k s'} = f_{s'}(\alpha_{p^k}) = f_{s'}(\alpha_{p^k}) = \sum_{j=0}^{[s'/2]} a_{s',j} (-1)^j \alpha (s'-2j)p^k,
\]  

(9)
and the number of coefficients in this formula not equal to one is at most \([s'/2]\). Using (9), we can reduce (8) for \(m < s\) to the form

\[
\sum_{i=0}^{s+m-1} x_i \alpha^i
\]

with complexity \((s' + 1)m\). As a result we obtain the upper estimate of the complexity of the direct transformation equal to

\[
L(s) + L(m) + m(s' + 2).
\]

While estimating the reverse transition, we calculate with complexity \(L(s) + L(m)\) the vectors of the coefficients \((v_i), (w_j)\) such that (10) is reduced to the form

\[
\sum_{i=0}^{s-1} v_i \alpha_i + \alpha^x \sum_{i=0}^{m-1} w_i \alpha_i.
\]

According to Lemma 2

\[
\alpha^x = (\alpha_{p^k})^{s'} = \sum_{j=0}^{[s'/2]} \binom{s'}{j} f_{s'-2j}(\alpha_{p^k}) = \sum_{j=0}^{[s'/2]} \binom{s'}{j} \alpha_{(s'-2j)p^k}.
\]

Using (12) (and replacing, if required, \(\alpha_0\) by 2), we can reduce (11) to the form

\[
\sum_{i=0}^{s-1} v_i \alpha_i + \sum_{i=0}^{m-1} b_j \sum_{j=0}^{[s'/2]} w_i \alpha_i \alpha_{(s'-2j)p^k}
\]

with complexity \(([s'/2])m\) and then, replacing \(\alpha_i \alpha_{(s'-2j)p^k}\) by \(\alpha_i \alpha_{(s'-2j)p^k} + \alpha_{i-(s'-2j)p^k}\), we reduce (13) to the form

\[
\sum_{i=0}^{s+m-1} x_i \alpha_i
\]

with complexity \(2([s'/2] + 1)m\). As a result, the upper estimate of the complexity of the inverse transformation is equal to

\[
L(s) + L(m) + m(3s'/2 + 2),
\]

and inequality (5) is thus proved.

Now we prove the recurrence inequality

\[
L(p^{k+1}) \leq pL(p^k) + \frac{3}{4}p^{k+2} + p^{k+1} \lceil \log_2 p \rceil.
\]
We represent $p$ as $s + m$, where $s = \lceil p/2 \rceil$, $m = \lfloor p/2 \rfloor$, and applying (5) obtain

$$L(p^{k+1}) \leq L(p^k s) + L(p^k m) + p^k (3sm/2) + p^k (s + m).$$

Using (5) and applying the same method of bisection to the estimates $L(p^k s)$, $L(p^k m)$ and so on, we obtain by induction that for any $s \leq p$

$$L(p^k s) \leq sL(p^k) + p^k \lambda(s),$$

where the function $\lambda$ satisfies the inequality

$$\lambda(s + m) \leq \lambda(s) + \lambda(m) + 3sm/2 + s + m, \quad \lambda(1) = 0.$$

Further, it is checked by induction that

$$\lambda(s) \leq \frac{3}{4} s^2 + s[\log_2 s].$$

Estimate (14) follows from this inequality.

By induction we deduce from (14) that

$$L(p^k) \leq \frac{3}{4} p^{k+1} k + p^k k[\log_2 p]$$

in turn, this inequality implies that

$$L(p^k s) \leq sL(p^k) + p^k \lambda(s)$$

$$\leq \frac{3s}{4} p^{k+1} k + p^k s k[\log_2 p] + \frac{3}{4} s^2 p^k + p^k s[\log_2 s]$$

$$\leq \frac{3s}{4} p^{k+1} k + p^k s k[\log_2 p] + O(p^{k+1}).$$

(15)

Representing $n$ in the $p$-ary number system in the form

$$n = n_0 p^k + \ldots + n_k = N_0 + N_1, \quad N_0 = n_0 p^k,$$

and applying (5) and (15), we find that

$$L(n) \leq L(N_0) + L(N_1) + N_1 (3n_0/2 + 2)$$

$$\leq L(N_1) + n_0 p^k (3pk/4 + k[\log_2 p]) + O(p^{k+1}).$$

Repeating the same approach, we obtain the inequalities

$$L(n) \leq (n_0 p^k + \ldots + n_k)k(34/4p + [\log_2 p]) + O(p^{k+1})$$

$$\leq nk(3p/4 + [\log_2 p]) + O(pn) = O(pnk).$$

We denote by $B(n)$ the complexity of transition from an optimal normal basis of the second or third type to the corresponding standard basis or the complexity of the reverse transition in the field $GF(q^n)$.

The following generalisation of Theorem 5 is true.
Theorem 8. The estimate

\[ B(n) = O(pn \log p n) \]

is true.

Proof. The proof is similar in main to the proof of Theorem 5. The transition from the normal basis

\[ B_\alpha = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\} \]

to the basis \( \{\alpha_1, \ldots, \alpha_n\} \) is realized by a permutation of the elements as in the proof of Theorem 5. Since the sums of elements of both bases are equal to each other and are equal to the trace of the element \( \alpha \), this sum belongs to \( GF(q) \) and is not equal to zero (otherwise the elements of the basis would be linearly dependent). Therefore the basis \( \{\alpha_1, \ldots, \alpha_n\} \) is equivalent to the basis \( \{\alpha_0, \ldots, \alpha_{n-1}\} \) and the transition from one basis to another is realized with linear complexity similar to the transition from the standard basis to the almost standard basis in the proof of Theorem 5.

To estimate the complexity of transition from the basis \( \{\alpha_0, \ldots, \alpha_{n-1}\} \) to the standard basis \( \{1, \ldots, \alpha^{n-1}\} \) and back, we use Theorem 7 instead of Theorem 4.

3.5. On the measure of closeness of the normal and standard bases

We denote by \( C_{q,\beta}^\alpha(n) \) the complexity of transition in the field \( GF(q^n) \) form the normal basis \( B_\alpha \) to the standard basis \( B_\beta \), more precisely, the maximum of the complexities of the direct and inverse transformations of the coordinates in one basis to the coordinates in the other. Then

\[ C_q^\alpha(n) = \min C_{q,\beta}^\alpha(n) \]

is a measure of closeness of the normal basis \( B_\alpha \) to standard bases.

It is obvious that

\[ C_q^\alpha(n) \leq C_{q,\alpha}^\alpha(n). \]

We introduce the functions

\[ c_q(n) = \min C_q^\alpha(n) \]

and

\[ C_q(n) = \max C_q^\alpha(n). \]

Then the results of the previous subsections can be formulated in the following way.

If in the field \( GF(q^n) \) there exists an optimal normal basis of the first type, then

\[ c_q(n) \leq n - 1, \]

and if there is no such a basis but a basis of the second or third type exists, then

\[ c_q(n) \leq O(n \log_2 n). \]

Using the Lupanov–Konovaltsev method (see [12]) for estimating the complexity of an arbitrary \( n \)-dimensional operator over \( GF(q) \), it is possible to show that

\[ C_q(n) = O(n^2 / \log_q n). \]
Theorem 9. The estimate

\[ C_q(n) - c_q(n) \leq 2M_q(n) + n = O(n \log n \log \log n) \]

is true.

Proof. Let

\[ c_q(n) = C_{q,\beta}^\alpha(n), \quad C_q(n) = C_{q,\beta}^A(n). \]

Then

\[ C_q(n) - c_q(n) \leq C_{q,\beta}^A(n) - C_{q,\beta}^\alpha(n). \]

It is clear that the complexity of a product of linear operators does not exceed the sum of their complexities, therefore

\[ C_q(n) - c_q(n) \leq C_{q,\beta}^{A,\alpha}(n), \]

where \( C_{q,\beta}^{A,\alpha}(n) \) is the complexity of transition from the basis \( B^\alpha \) to the normal basis \( B^A \). If the bases coincide, then the complexity is obviously equal to zero. Otherwise, as we know (see [5, 6]), the transition matrix from a normal basis to another normal basis is cyclic as well as the transpose matrix.

The complexity of an operator with a cyclic matrix is equal to that of the operator of the so-called cyclic convolution, which, as we know (see, for example, [3]), is reduced to two transformations of usual convolution and \( n \) operations of additions, and the usual convolution is simply an operation of multiplication of two polynomials of degree \( n - 1 \). The theorem is thus true.

The behaviour of the function \( c_q(n) \) in the general case is not known to the authors.

4. ON THE COMPLEXITY OF IMPLEMENTATION OF ARITHMETIC OPERATIONS IN FINITE FIELDS

4.1. On the estimates of complexity of arithmetic operations in finite fields

Let the finite field \( GF(q^n) \) be represented by the standard basis \( B_\alpha \) generated by a root \( \alpha \) of an irreducible over \( GF(q) \) polynomial \( g(x) \) of degree \( n \). We denote the complexity of the operation of multiplication of polynomials of degree \( n - 1 \) over \( GF(q) \) by \( M_q(n) \). According to [20]

\[ M_q(n) = O(n \log n \log \log n). \]

We denote by \( M_{q,g}^s(n) \) the complexity of the operation of multiplication in the field \( GF(q^n) \) with representation given above. Multiplication in this case is reduced to multiplication of polynomials over \( GF(q) \) and subsequent division with residual of the result by the polynomial \( g(x) \), therefore if we neglect the complexity of the preliminary calculation of some polynomial \( f(x) \) depending only on \( g(x) \), then it is known that

\[ M_{q,g}^s(n) = 3M_q(n) + O(n) \]

independently of the choice of \( g(x) \). Further we sometimes omit the indices of \( M_{q,g}^s(n) \).
In some cases this estimate can be improved. Indeed, if \( g(x) \) contains \( k \) monomials, then the complexity of reduction modulo \( g(x) \) is has an upper estimate \( kn \) and therefore

\[
M_{q,g}^s(n) \leq M_q(n) + (2k + 1)n,
\]

and in the case \( q = 2 \)

\[
M_{q,g}^s(n) \leq M_q(n) + kn.
\]

With high probability we can find the irreducible polynomial with \( k = 3 \), otherwise, if there is no irreducible trinomial of degree \( n \), then we always can take \( k = 5 \), since an irreducible polynomial with five terms exists (this is checked experimentally but not proved). On the complexity of generating irreducible polynomial see, for example, [11].

In the estimates given above, it is assumed that the complexity of the operations of addition and multiplication in \( GF(q) \) equals one. It is natural in the case \( q = 2 \), but if \( q = p^k \), where \( p \) is a prime number, then it is natural to estimate the bit complexity of multiplication in \( GF(q) \) as

\[
M(GF(q)) \leq M(GF(p))M_q^s(k),
\]

\[
M(GF(p)) \leq 3M(\log_2 p) + O(\log_2 p),
\]

where \( M(m) = O(m \log m \log \log m) \) is the bit complexity of multiplication of \( m \)-digit binary numbers. Note also that for \( p \) which are Mersenne and Fermat prime numbers the estimate

\[
M(GF(p)) \leq (\log_2 p) + O(\log_2 p)
\]

is true.

For the bit complexity in the field \( GF(q^n) \) (provided the elements of the field are represent by the coordinates in a given basis \( B \) over \( GF(q) \)) the estimate

\[
M(GF(q^n)) \leq M(GF(q))M_{q,g}^s(n)
\]

is true.

Raising element of the field \( GF(q^n) \) to the power \( q \) is realized by insertion of zeros into the sequence of the coefficients of the polynomial representing the element with consequent reduction modulo \( g \). As a result (with regard to the above remark) we obtain the estimate \( K_q(n) = O(n) \) (not proved rigorously) for raising to the power \( q \).

Let us estimate the complexity of multiplication in \( GF(q^n) \) in the case where the optimal normal basis is of the first type and the operations in the field \( GF(q) \) are used. In order to execute multiplication, we go to the standard basis according to Theorem 2 with (circuit) complexity \( 2n - 2 \) and then perform multiplication in the standard basis and return to the normal basis with complexity \( n - 1 \).

According to the remark after Theorem 2 we obtain the estimate

\[
M^{O1}(GF(q^n)) \leq M^s_q(n) + 7n - 8.
\]

For the bases of the second and third types, we similarly obtain the estimate

\[
M^{O2}(GF(q^n)) \leq 3M^s_q(n) + \frac{3n}{2} \log_2 n + O(n).
\]
which is asymptotically three times greater, since the generating irreducible polynomial \( g \) in the corresponding standard bases (calculated in Theorem 6) appears to be non-trivial and for the reduction modulo \( g \) the general estimate for \( M_g(n) \) given above should be used.

Below we denote by \( M^O(GF(q^n)) \) the minimal complexity of multiplication in the field \( GF(q^n) \) provided that the elements of the field are represented in some normal basis.

4.2. Estimating the complexity of raising to a power and inversion in finite fields

Note that the complexity of raising an arbitrary element of \( GF(q^n) \) to a power \( d < q^n \) (in the field \( GF(q) \)) can be estimated with the use of some results on additive chains [4] as

\[
O\left(n \log_q d + \frac{M(GF(q^n)) \log_q d}{\log_q \log_q d}\right),
\]

since for raising to a power \( d \) it suffices to execute \( \log_q d + O(1) \) operations of raising to the power \( q \) and asymptotically \( \log_q d / \log_q \log_q d \) non-trivial multiplications.

It is known that for almost all \( d \) it is impossible to decrease the order of the second summand, but, for example, for \( d = q^n - 2 \) it can be done with the use of the equalities

\[
\begin{align*}
q^n - 2 &= q(q^{n-1} - 1) + q - 2, \\
q^{2m} - 1 &= (q^m - 1)(q^m + 1), \\
q^{2m+1} - 1 &= q(q^{2m} - 1) + q - 1.
\end{align*}
\]

Since according to the Fermat identity \( f^{-1} = f^{q^n-2} \), the inverse operation in the field requires at most

\[
\lambda_2(n - 1) + v_2(n - 1) + \log_2 q + o(\log_2 q)
\]

multiplications and \( n - 1 \) raisings to the power \( q \), where \( \lambda_2(n) = \lfloor \log_2(n - 1) \rfloor \) and \( v_2(n) \) is the number of ones in the binary representation of \( n \). Therefore the complexity of inversion in the standard basis satisfies the inequality

\[
I(GF(q^n)) \leq (n - 1)K_q(n) + (\lambda_2(n - 1) + v_2(n - 1) + \log_2 q + o(\log_2 q))M(GF(q^n)),
\]

and the same estimate is valid for the complexity \( D(GF(q^n)) \) of division.

Let us estimate the inversion operation in optimal normal bases (the case of standard bases was investigated in [9]).

Raising to the power \( q \) is easily executed, therefore we have the estimate

\[
I^O(GF(q^n)) \leq (\lambda_2(n - 1) + v_2(n - 1) + \log_2 q + o(\log_2 q))M^O(GF(q^n)).
\]

Of course, this estimate is valid only for \( n \) for which optimal normal bases exist. Similarly, the complexity of raising to an arbitrary power \( d < q^n \) in optimal normal bases is estimated as

\[
O\left(\frac{M^O(GF(q^n)) \log d}{\log \log d}\right).
\]
4.3. More on estimating the complexity of multiplication in normal bases

It was shown above that the complexity of multiplication in finite fields with optimal normal bases asymptotically is the same as in standard bases. But such bases exist not for all \( n \). Further we give examples of other normal bases where the complexity of multiplication remains less than the trivial quadratic estimate.

Research \([13]\) contains examples of normal bases \( B \) with linear complexity \( C_B \). The complexity of the standard algorithm for multiplication in such bases admits a quadratic estimate. The bases \( B^\alpha \) mentioned above are generated in the fields \( GF(q^n) \) by elements of the form

\[
\alpha = \zeta + \zeta^\gamma + \ldots + \zeta^{\gamma^{k-1}},
\]

where \( p = kn+1 \) is a prime number, \( \zeta \) is a primitive root of degree \( p \) of the unity element of the field \( GF(q^kn) \), which is an extension of the field \( GF(q^n) \), \( \gamma \) is a primitive root of degree \( k \) of the unity element of the residue ring of order \( p \), which together with \( q \) generates the whole multiplicative group of non-zero residues modulo \( p \), that is, each number from 1 to \( kn \) can be uniquely represented in the form

\[
q^i\gamma^j, \quad 0 \leq j < k, \quad 0 \leq i < n.
\]

It is known that in this case the minimal polynomial \( m_\zeta \) over \( GF(q) \) annihilating the element \( \zeta \) is the polynomial

\[
F_{p-1} = x^{p-1} + \ldots + 1,
\]

and the field \( GF(q^n) \) is generated by the standard basis

\[
B_\zeta = \{1, \zeta, \ldots, \zeta^{kn-1}\}.
\]

Since the elements of the basis \( B^\alpha \) are of the form

\[
\alpha q^i = \zeta q^i + \zeta^\gamma q^i + \ldots + \zeta^{\gamma^{k-1}} q^i,
\]

that is, are the sums of distinct elements of the almost standard basis

\[
B'_\zeta = \{\zeta, \ldots, \zeta^{kn}\},
\]

the transition matrix from the coordinates in the basis \( B^\alpha \) to the coordinates in the basis \( B'_\zeta \) has a single one in each row and therefore the corresponding transformation is of zero complexity (and linear in the case of program implementation). The inverse transformation (defined only on the corresponding subspace) is of zero circuit complexity by the same reasons. The complexity of direct and reverse transition from the standard basis \( B_\zeta \) to the almost standard basis \( B'_\zeta \) over \( GF(q) \) was estimated in the proof of Theorem 2, and in the case under consideration equals \( kn - 1 \).

Taking into account the remark made after Theorem 2, we obtain the estimate of the complexity of multiplication in the basis \( B_\zeta \)

\[
M^s_{q,F_{kn}}(kn) \leq (M^s_q(kn) + 4kn - 5),
\]

which implies the estimate of the complexity of multiplication in the normal basis \( B^\alpha \)

\[
M^O(GF(q^n)) \leq (M^s_q(kn) + 7kn - 8)M(GF(q)). \tag{16}
\]
In the case \( k = 1, 2 \), the bases under consideration are bases of the first and second types and for \( k = 1 \) the estimate obtained above coincides with the estimate given in the preceding subsection. For \( k = 2 \) this estimate is slightly better asymptotically than the estimate

\[
M^{O^2}(GF(q^n)) \leq (3M_q^s(n) + \frac{3n}{2} \log_2 n + O(n)M(GF(q)),
\]

obtained above for the bases both the second and third types, since \( M_q^s(2n) \) is asymptotically less than \( 3M_q^s(n) \), but in practice the comparison of these estimates is not so clear. For large \( k \) the efficiency of the estimate (16) decreases, but for \( k = O(n^{1-\epsilon}) \) it remains infinitesimal with respect to the quadratic estimate.

4.4. On products of bases
We consider the following well-known construction of (Kronecker) product of bases (see, for example, [5, 6]). Let \( m \) and \( n \) be mutually prime positive integers, and

\[
B_1 = \{\alpha_1, \ldots, \alpha_n\}, \quad B_2 = \{\beta_1, \ldots, \beta_m\}
\]

be arbitrary bases in the fields \( GF(q^n) \) and \( GF(q^m) \) respectively. Then the intersection of these fields coincides with the field \( GF(q) \), and both the fields are contained in \( GF(q^{nm}) \) with the basis (over \( GF(q) \)) equal to the product of the bases

\[
B_1 \otimes B_2 = \{\alpha_1 \beta_1, \ldots, \alpha_n \beta_m\}.
\]

The product of standard bases is not a standard basis, and the authors know no non-trivial estimates of the closeness of this basis to the standard bases. However, the complexity of multiplication in the field \( GF(q^{nm}) \) with this product as the basis is easily estimated as

\[
M_{B_1 \otimes B_2}(GF(q^{nm})) \leq M_{B_1}(GF(q^n))M_{q^n.g}(m) \leq M_{q,f}(n)M_{q^m.g}(m),
\]

where \( g \) is the irreducible polynomial of degree \( m \) over \( GF(q) \) generating the basis \( B_2 \) and \( f \) is the irreducible polynomial of degree \( n \) over \( GF(q) \) generating the basis \( B_1 \).

However, as it is known [5, 6], the product \( B^\alpha \otimes B^\beta \) of normal bases \( B^\alpha \subset GF(q^n) \) and \( B^\beta \subset GF(q^m) \) coincides, up to a permutation of elements, with the normal basis

\[
B^\gamma \subset GF(q^{nm}), \quad \gamma = \alpha \beta.
\]

Let us consider also the product of standard bases \( B^\alpha \otimes B^\beta \). It is clear that the complexity of the transition from the basis \( B^\alpha \otimes B^\beta \) to the basis \( B^\alpha \otimes B^\beta \) admits the upper estimate

\[
nC_q^\beta(m) + mC_q^\alpha(n).
\]

Indeed, if an arbitrary element of \( GF(q^{nm}) \) is written in both bases as

\[
\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x_{i,j} q^i \beta^j = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x'_{i,j} \alpha^i \beta^j.
\]
then for the transformation of the matrix \((x_{i,j})\) over \(GF(q)\) to the matrix \((x_{i,j}')\) over the same field it is sufficient to apply \(n\) times (in the corresponding direction) the transformation \(C_{q,\beta}^{\beta}(m)\) to the rows of the matrix \((x_{i,j})\) in order to obtain the equality

\[
\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \alpha^{q^i} \beta^j = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \beta^j \alpha^{q^i}.
\]

and then to apply \(m\) times the transformation \(C_{q,\alpha}^{\alpha}(n)\) to the columns of the obtained matrix \((x_{i,j}')\) over the same field \(GF(q)\) in order to obtain the equality

\[
\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x_{i,j}' \beta^j = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \beta^j x_{i,j}' \alpha^{q^i}.
\]

It follows from (17) and (18) that for an appropriate choice of the elements \(\alpha\) and \(\beta\) (or, what is the same, the polynomials \(f\) and \(g\)) and for \(\gamma = \alpha \beta\) the complexity of multiplication in the normal basis in \(GF(q^{nm})\) satisfies the inequality

\[
M^O(GF(q^{nm})) \leq M_{B^\gamma}(GF(q^{nm}))
\]

\[
\leq M_{q,f}^s(n)M_{q,g}^{\alpha\beta}(m) + nC_{q,\beta}^{\beta}(m) + mC_{q,\alpha}^\alpha(n)
\]

\[
\leq M_{q,f}^s(n)M_{q,g}^{\alpha\beta}(m) + nc_q(m) + mc_q(n).
\]

Taking into account the Schönhage estimate [20] and the trivial estimate given above for \(c_q(m)\), we obtain

\[
M^O(GF(q^{nm})) = O(nm \log n \log m \log \log n \log \log m) + O(nm(m+n)/\log q(n+m)).
\]

In order to obtain the estimate of the bit complexity, the estimates given above should be multiplied by \(M(GF(q))\).

In the case where for \(c_q(m)\) or \(c_q(n)\) there are non-trivial estimates, for example, where optimal normal bases exist for \(n\) and \(m\), the last term can be replaced by a smaller estimate, for example, in the just mentioned case it can be replaced by \(O(nm)\log q(n+m)\). The last assertion in the obvious way is extended to the Kronecker products of several bases. In the cases mentioned above the last term is less in order and can be omitted.

The Kronecker product of bases can be also defined in the case where \(m\) and \(n\) are not necessarily mutually prime numbers, but then the basis \(B_2 = \{\beta_1, \ldots, \beta_m\}\) should be chosen in \(GF(q^{nm})\) and over the field \(GF(q^m)\).

For the product of standard bases, the complexity of multiplication in the field \(GF(q^{nm})\) can be again estimated as

\[
M_{B_1 \otimes B_2}(GF(q^{nm})) \leq M_{q,f}^s(n)M_{q,g}^{\alpha\beta}(m),
\]

but here \(g\) is the irreducible polynomial of degree \(m\) over the field \(GF(q^n)\) generating the basis \(B_2\).

Consider the product \(B^\alpha \otimes B^\beta\) of normal bases \(B^\alpha \subset GF(q^n)\) and \(B^\beta \subset GF(q^{mn})\), where \(B^\beta\) is the basis over \(GF(q^n)\). This product is a normal basis, but it is clear that raising
to the power \( q^n \) in this basis is reduced to a permutation of coordinates, no longer cyclic. Therefore the complexity of raising to the power \( q^n \) in this basis, as in a normal basis, is zero, and such bases can be used for decreasing the complexity of raising to a power and the inverse operation in the field \( GF(q^{nm}) \) if we find for it an algorithm of low complexity for multiplication.

For this purpose, we consider, as above, the product of the corresponding standard bases \( B_\alpha \otimes B_\beta \). In the case under consideration the complexity of transition from the basis \( B_\alpha \otimes B_\beta \) to the basis \( B_\alpha \otimes B_\beta \) admits the upper bound

\[
C_{q^n,\beta}^\beta (m) + mC_{q,\alpha}^\alpha (n). \tag{20}
\]

Indeed, if an arbitrary element of \( GF(q^{nm}) \) is written in both bases as

\[
\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x_{i,j} \alpha^i \beta^j = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x'_{i,j} \alpha^i \beta^j,
\]

then in order to transform the matrix \( (x_{i,j}) \) over \( GF(q) \) to the matrix \( (x'_{i,j}) \) over the same field, it is sufficient to apply \( m \) times the transformation \( C_{q,\alpha}^\alpha (n) \) to the rows of the matrix \( (x_{i,j}) \) and obtain the equality

\[
\sum_{i=0}^{n-1} \alpha^{q^i} \sum_{j=0}^{m-1} x'_{i,j} \beta^j = \sum_{j=0}^{m-1} \beta^{q^j} \sum_{i=0}^{n-1} x_{i,j} \alpha^i,
\]

and then to apply once the transformation \( C_{q^n,\beta}^\beta (m) \) to the columns of the obtained matrix \( (x'_{i,j}) \) over the field \( GF(q^n) \) and arrive at the equality

\[
\sum_{j=0}^{m-1} \beta^{q^j} \sum_{i=0}^{n-1} x''_{i,j} \alpha^i = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x'_{i,j} \alpha^i \beta^j.
\]

It follows from (19) and (20) that for an appropriate choice of the elements \( \alpha \) and \( \beta \) (or, what is the same, the polynomials \( f \) and \( g \)) the complexity of multiplication in \( GF(q^{nm}) \) in some basis with zero complexity of raising to the power \( q \) admits the upper bound

\[
M_{q,f}^i (n) M_{q^n,g}^z (m) + c_{q^n} (m) + mc_q (n). \tag{21}
\]

Taking into account an estimate from [20] and the trivial estimate for \( c_{q^n} (m) \) given above, we obtain from (21) that

\[
M^O (GF(q^{nm})) = O(nm \log n \log m \log \log n \log \log m) + O(nm)(m + n)/\log_q(n + m).
\]

In order to obtain estimates for the bit complexity, the estimates given above should be multiplied by \( M(GF(q)) \).
REFERENCES