Finite Field Towers: Iterated Presentation and Complexity of Arithmetic

Valentine B. Afanassiev and Alexander A. Davydov

Institute for Information Transmission Problems, Russian Academy of Sciences, Bol’shoj Karetnyj per. 19, GSP-4, Moscow 101447, Russia
E-mail: afanv@iitp.ru, adav@iitp.ru

Communicated by Stephen D. Cohen

Received January 5, 2000; revised October 30, 2000; published online January 30, 2002

Finite field towers \(GF(q^P)\) are considered, where \(P = p_1^{n_1} p_2^{n_2} \ldots p_n^{n_n}\) and all primes \(p_i\) are distinct factors of \((q - 1)\). Under this condition irreducible binomials of the form \(x^d - c\) can be used for recursive extension of finite fields. We give description of an infinite sequence of irreducible binomials, new effective algorithms for fast multiplication and inversion in the tower, and finite and asymptotic estimates of arithmetic complexity. It is important that the achievable asymptotic estimate of the complexity has the form \(O(\log Q \log \log Q)\), where \(\log_2 r \geq \xi \geq 1\) and \(\gamma\) is the minimal factor of \(q - 1\).

1. INTRODUCTION

Iterated presentations for infinite towers of extended fields, complexity of their arithmetic, and close problems were considered, e.g., in [1–17], and the references therein. The most fundamental results on iterated presentation are given in [10]. Useful ideas and details for construction of irreducible polynomials are considered in [11]. The necessary basic theorems are given in [13, 14]. The review of known results on finite field presentation and complexity of arithmetics can be found in [17].

Complexity of arithmetic (multiplication and inversion) over some towers was considered briefly in [1, 2, 12]. It was shown there that the complexity of

\(^1\)This work was supported in part by Swedish Royal Academy of Sciences.
multiplication and inversion could be less than a quadratic function of the finite field dimension. Our goal is decreasing of arithmetic complexity for finite fields due to their structure. We intend to investigate a tower structure of a finite field and a special choice of the tower parameters which brings the lower upper estimate for the complexity. A part of this work was briefly presented in [3–5].

The problem of fast arithmetic over $GF(p^m)$, $p$ prime, can be treated as fast polynomial multiplication and inversion by modulo irreducible polynomial of the degree $m$. A known method uses embedding of the polynomial coefficients into the proper surrogate field $F(\lambda)$, $\lambda > 2mp^2$, with effective Fast Fourier Transform (FFT) over $F(\lambda)$ [9, 15]. Then the complexity of fast polynomial multiplication could be $O(m \log m)$ operations in $F(\lambda)$ and $O(m \log^2 m)$ for fast polynomial inversion based on the Fast Euclidean Procedure [7]. This way is highly universal but its main weak point is related to the choice of a surrogate field with effective FFT. Moreover, if $p$ is fixed and $m$ is growing it is natural to use the complexity measure based on the arithmetic complexity for the ground field $GF(p)$. Then the surrogate field gives an additional factor of order $\log m$, at least. So, we could expect an estimate not better than $O(m \log^2 m)$ operations in $GF(p)$ for multiplication and not better than $O(m \log^3 m)$ for inversion. Another scheme of calculation of the same complexity can be made in a tower $K_0 = GF(q) \rightarrow K_1 = GF(q^k) \rightarrow K_2 = GF((q^k)^{m/k})$ where $k|m$ and $q^k \geq 2^m$. The subfield $K_1$ can be used now for fast multiplication in $K_2$ based on FFT.

To improve the complexity estimate we use the last scheme recursively as proposed in the current paper. This idea leads to the estimate $O(m \log^2 m)$ with $\xi < 2$ for multiplication. Our approach gives an improvement by order $O(\log m)$ for infinite subset of finite field set. The main points of our approach are the following:

- a ground field $GF(q)$ is fixed and the extension degree $m$ of $GF(q^m)$ is growing,
- all arithmetic operations are reduced to the fixed ground field,
- only subfield structure of the finite field is used for fast multiplication and inversion over the given field.

So, we do not need any surrogate field for fast calculation but we need an iterated field structure like a tower. As a penalty for this approach, the tower structure defines strongly the recursive structure of fast calculation procedures and, as a consequence of this, we lose universality. The efficiency of our method is growing with the number of factors of $m$. It may be that the main motivation for this research, except for a complexity investigation, is to find a very simple implementation of towers arithmetic.

Let $GF(q)$ be a Galois field of $q$ elements. An extensions of $GF(q)$ to a field $GF(q^p)$ is called a $p$-extension. Let $P = \{p_1, p_2, \ldots, p_t\}$ be a set of distinct primes $p_1, p_2, \ldots, p_t$ with $t \geq 1$, where $p_1 \cdot p_2 \cdot \ldots \cdot p_t | (q - 1)$. Given a set of
nonnegative integers \( \{n_{j,k}, j = 1, 2, \ldots, h, k = 1, 2, \ldots, t\} \) where \( n_{j,k} \geq 1 \) at least for one \( k \) for every \( j = 1, 2, \ldots, h \), we introduce integers \( P_j \) of the form

\[
P_j = \prod_{k=1}^{t} p_{j,k}^{n_{j,k}}, \quad n_{j,k} \geq 0.
\]

The iterated design of a \( P \)-tower is defined level by level. The \( j \)th level of a \( P \)-tower \( K_h, j \leq h \), is a \( P \)-extension of a subfield \( K_{j-1} \) starting from a ground field \( K_0 = GF(q) \). After \( h \) consecutive extensions we get a \( P \)-tower

\[
K_h = GF(q^{P_1^{n_1} P_2^{n_2} \cdots P_t^{n_t}}) = GF(q^{p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}})
\]
where

\[
S(h, k) = \sum_{j=1}^{h} n_{j,k}, \quad S(0, k) = 0, k = 1, 2, \ldots, t.
\]

Everywhere in the paper we use the polynomial basis of an extended finite field. By definition, a \( P \)-extension \( K_{j-1} \rightarrow K_j \) is obtained with a monic polynomial \( f_j(x) \) of degree \( P_j \), irreducible over \( K_{j-1} \). As it is known \( x \in K_j \) is one of the roots of \( f_j(x) \) [10]. Having a sequence of polynomials \( f_j(x) \) of degrees \( P_j, j = 1, 2, \ldots, h \), we obtain an iterated presentation of a tower \( GF(q^{p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}}) \) over the ground field \( GF(q) \) [10, Definition 3.1]. Infinite sequences \( f_j(x) \) and \( n_{j,k}, j = 1, 2, 3, \ldots, k = 1, 2, \ldots, t \), give an iterated presentation of infinite towers \( GF(q^{p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}}) \). As usual \( GF^*(q) = GF(q) \setminus \{0\} \) and \( K_h^* = GF^*(q^{P_1^{n_1} P_2^{n_2} \cdots P_t^{n_t}}) \).

The main results of the paper are the \( P \)-tower structures with new algorithms for multiplication and inversion that give an almost linear complexity estimate with the tower dimension (similar to the Schönhage–Strassen estimate [16] for integers).

The paper is organized as follows. In Section 2 we give a modification and development of the known iterated presentations for infinite towers and develop a new iterated presentation for infinite \( P \)-towers. In Section 3 we give new algorithms for fast multiplication and multiplicative inversion adopted to the \( P \)-towers. In Section 4 we derive recursive equations for complexity of the multiplication and inversion algorithms and obtain exact solutions of these equations. In Section 5 asymptotic estimates of the arithmetic complexity for \( P \)-towers are considered.

2. ITERATED PRESENTATION FOR TOWERS OF FIELDS

Let \( (a, b) \) be g.c.d. of integers \( a \) and \( b \). The following iterated presentations for towers have been described in [10, Chap. 3, 11, Theorem 6].
Theorem 1 [10]. Let a ground field GF(q) be given and let p be an integer such that
\[ p \neq 2 \text{ is prime, } \quad (p, q) = 1, \quad q \text{ is primitive modulo } p, \]
\[ q^{p-1} \not\equiv 1 \pmod{p^2}. \]  
(3)

Then an infinite tower GF(q^{(p-1)/p^j}) consisting of fields GF(q^{h_j}), j = 0, 1, 2, ..., where \( h_0 = 1, h_j = (p-1)p^{j-1} \) for \( j \geq 1 \), can be constructed with polynomials \( f_j(x) \), irreducible over GF(q^{h_{j-1}}), such that \( f_1(x) = x^{p-1} + \cdots + x^2 + x + 1 \) and \( f_j(x) = x^p - \beta_{j-1} \) where \( \beta_{j-1} \) is a root of \( f_{j-1}(x) \), \( j = 2, 3, 4, ... \).

Theorem 2 [11]. Let a ground field GF(q) be given with \( q \equiv 1 \pmod{4} \) and let \( c \) be a non-square in GF(q). Then an infinite tower GF(q^{2^j}) consisting of fields GF(q^{2^{j-1}}), \( j = 0, 1, 2, ... \), can be constructed with binomials \( f_j(x) \), irreducible over GF(q^{2^{j-1}}), such that \( f_1(x) = x^2 - c \) and \( f_j(x) = x^2 - \beta_{j-1} \) where \( \beta_{j-1} \) is a root of \( f_{j-1}(x) \), \( j = 2, 3, 4, ... \).

Similar results were obtained in [11] for \( q \equiv 3 \pmod{4} \).

The next result [8, Chap. V, Theorem 19] is very important for the present paper, see also [13, Theorem 2.3.4, Corollary 2.3.6, 14, Theorem 3.7.5].

Theorem 3 [8]. Let \( \kappa \) be a primitive element of a field GF(q) and let \( P \) be an integer such that all its prime divisors are divisors of \( q - 1 \). We assume that \( v \) is an integer with \( (v, P) = 1 \). Let \( q \equiv 1 \pmod{4} \) if \( P \equiv 0 \pmod{4} \). Then monic polynomials of degree \( P \) and order \( P(q - 1)/(v, q - 1) \), irreducible over GF(q), have the form \( x^P - \kappa^v \).

We consider now a modification of the iterative representations from [10, 11] to obtain an infinite sequence of irreducible binomials for the case when
\[ p_k | (q - 1), \quad k = 1, 2, \ldots, t, \quad \text{all } p_k \text{ are distinct primes}, \]
\[ q \equiv 1 \pmod{4} \text{ if } 2 \in \{ p_1, p_2, \ldots, p_t \}, \quad t \geq 1. \]  
(4)

Under conditions (4) all prime divisors of an integer \( P_j \) of the form (1) are divisors of \( q - 1 \).

Theorem 4. Let the conditions (4) hold for a field \( K = GF(q) \). Assume that \( P_1 = \prod_{k=1}^{l} p_k^{n_k} \) is an integer of the form (1), \( \kappa \) is a primitive element of the field \( K \), and a field \( E = GF(q^{P_1}) \) is a \( P_1 \)-extension of \( K \) with an irreducible binomial \( x^{P_1} - \kappa^v \) where \( v \in \{ 0, 1, \ldots, q - 2 \} \), \( (v, P_1) = 1 \). Let \( \beta \in E \) be a root of \( x^{P_1} - \kappa^v \) and let \( P_2 = \prod_{k=1}^{l} p_k^{n_k^2} \) be an integer of the form (1) with \( (v, P_2) = 1 \). Then \( x^{P_2} - \beta \) is a polynomial irreducible over the extended field \( E \).
Proof. Since $\beta$ is a root of $x^{P_i} - \kappa^v$ we have $\beta^{P_v} = \kappa^v$. For the integer $P = P_1 P_2 = \prod_{k=1}^t p_k^{n_{j,k}}$ of the form (1) it holds that $(v, P) = 1$ because $(v, P_1) = (v, P_2) = 1$. Hence, by Theorem 3, the binomial $x^{P_i} - \kappa^v$ is irreducible over $K$. Let $\gamma$ be a root of $x^{P_i} - \kappa^v$. Then $\gamma$ generates a field $GF(q^{P_i})$ and so the minimal polynomial of $\gamma$ over $E$ has degree $P_2$. We have $\gamma^{P_i P_2} = \kappa^v = \beta^{P_i}$ and may choose $\gamma$ such that $\gamma^{P_2} = \beta$. Then $x^{P_2} - \beta$ is the minimal polynomial of $\gamma$ over $E$ and hence $x^{P_2} - \beta$ is irreducible over $E$.}

Under conditions (4) we introduce the integer $\Gamma = \prod_{k=1}^t p_k$.

**Corollary 1.** Under conditions of Theorem 4 let $(v, \Gamma) = 1$. Then the binomial $x^{P_2} - \beta$ is irreducible over the extended field $E$ for any integer $P_2$ of the form (1).

**Proof.** If $(v, \Gamma) = 1$ then $(v, P_2) = 1$ for any integer $P_2$ of the form (1).

**Corollary 2.** Given a ground field $K_0 = GF(q)$, a set $P = \{p_1, p_2,\ldots, p_t\}$ of prime factors of $(q - 1)$, nonnegative integers $n_{j,k}, j = 1, 2, 3,\ldots, k = 1, 2,\ldots, t$, where $n_{j,k} \geq 1$ at least for $k$ one for every $j$, and the conditions (4), assume that a field $K_1 = GF(q^{P_i})$ is a $P_1$-extension of $K_0$ with an irreducible binomial $f_1(x) = x^{P_1} - \kappa_0^v$ where $P_1 = \prod_{k=1}^t p_k^{n_{j,k}}$ is an integer of the form (1), $\kappa_0$ is a primitive element of the field $K_0$, $v \in \{0, 1,\ldots, q - 2\}$, $(v, \Gamma) = 1$. Then an infinite $P$-tower $GF(q^{P_1 p_2^t\ldots p_2^{P_1}})$ can be obtained by consecutive $P$-extensions over $K_1$ with binomials $f_j(x) = x^{P_j} - \beta_{j-1}$, irreducible over $K_{j-1}$, where $j = 2, 3, 4,\ldots, \beta_{j-1}$ is a root of a binomial $f_{j-1}$, $P_j = \prod_{k=1}^t p_k^{n_{j,k}}$ are integers of the form (1), and $K_j = GF(q^{P_1 p_2^t\ldots p_2^{P_1}})$ is a subfield of $GF(q^{P_1 p_2^t\ldots p_2^{P_1}})$ for all $j = 0, 1, 2,\ldots$.

**Proof.** If $p_j|(q - 1)$ then $p_j|(q^c - 1)$ for any integer $c$. So, one can use Corollary 1 iteratively.

**Remark 1.** The conditions (3) are not equivalent to the conditions (4) with $t = 1$. As a consequence of that, towers based on Theorems 1 and 2 might be different from $P$-towers in Corollary 2. By Fermat’s little theorem, $p|(q^{p-1} - 1)$ if $p$ is prime and $q \neq 0 (mod p)$. Hence, if $p \geq 3$ and we consider $GF(q^{P_1})$ as a ground field then a $P$-tower of Corollary 2 can be constructed. On the other hand, if $p|(q - 1)$ then $q \equiv 1 (mod p)$ and $q$ is not primitive modulo $p$. In this case if $q \neq (q')^{p-1}$ for any $q'$ or $q = (q')^{p-1}$ where $q'$ is not primitive modulo $p$ then a tower of Theorem 1 cannot be designed. For example, the towers of Theorem 1 cannot be obtained if $p|(q - 1)$ and $q$ is prime. Note also that a tower of Corollary 2 for $t = 1, p_1 = 2, n_{j,1} = 1$ for all $j$ coincides with the tower of Theorem 2.
3. MULTIPLICATION AND INVERSION ALGORITHMS

We give effective algorithms of multiplication and multiplicative inversion for $\mathbb{P}$-towers from Corollary 2. The scheme of fast multiplication of arbitrary elements $A$ and $B$ of a $\mathbb{P}$-tower reduces one multiplication in the field $K_j$ on the $j$th level to some number of multiplications in the field $K_{j-1}$ on the $(j-1)$st level of the tower. So this scheme is adopted to a $\mathbb{P}$-tower structure.

For an element $A$ of a field $GF(q^p)$ we use a polynomial notation $A(x)$ or just a vector $(a_0, a_1, \ldots, a_{p-1})$ of its coefficients from $GF(q)$. Given $A, B \in K_j$ we want to compute $C = AB$ or $C(x) = A(x)B(x) \pmod{f_j(x)}$ in the polynomial form where $f_j(x) = x^{p^j} - \psi_j$, $j = 2, 3, 4, \ldots$, and

$$A(x) = \sum_{i=0}^{p_j-1} a_i x^i, \quad B(x) = \sum_{i=0}^{p_j-1} b_i x^i, \quad C(x) = \sum_{i=0}^{p_j-1} c_i x^i,$$

where $a_i, b_i, c_i \in K_{j-1}, i = 0, 1, \ldots, p_j-1$.

Let $\psi_j = \beta_{j-1} \in K_{j-1}$ and $\beta_{j-1}$ be a root of the monic irreducible polynomial $f_{j-1}(x)$. Let the polynomial $T(x) = \sum_{i=0}^{2p_{j-2}} t_i x^i, t_i \in K_{j-1}, i = 0, 1, \ldots, 2P_j - 2$, of the degree $2P_j - 2$ over $K_{j-1}$ be the product of $A(x)$ and $B(x)$ and let $\delta$ be a positive integer.

**Procedure of Fast Multiplication.**

- Step 1. Given $A(x)$ and $B(x)$ calculate values $T(\lambda_u) = A(\lambda_u)B(\lambda_u)$ in at least $2P_j - 1$ distinct points $\lambda_u$ such that $u = 1, 2, \ldots, \mu_j, 2P_j - 1 \leq \mu_j$, and

$$\lambda_u \in \begin{cases} K_{j-\delta}, & \mu_j \leq |K_{j-\delta}|, \text{ if } j \geq \delta \\ K_0, & \mu_j \leq |K_0|, \text{ if } j < \delta, \end{cases} \quad (5)$$

where $|K_{j-\delta}| = q^{p_1p_2\cdots p_{j-2}}$.

- Step 2. Restore the polynomial $T(x)$ of a degree less than $2P_j - 1$ from the values $T(\lambda_u), u = 1, 2, \ldots, \mu_j$, by the Lagrange interpolation formula.

- Step 3. Calculate $C(x) = T(x) \pmod{f_j(x)}$ as a remainder of the usual division procedure.

**Remark 2.** To obtain values $A(\lambda_u)$ and $B(\lambda_u)$ in $\mu_j$ distinct points $\lambda_u$ on Step 1 and restore the polynomial $T(x)$ on Step 2 we can multiply the coefficient vector of the corresponding polynomial by the proper constant matrix depending on $\lambda_u$. FFT over the subfield $K_{j-\delta}$ is the evident choice to speed up these calculations. One can use FFT on Step 1 and the corresponding inverse FFT on Step 2. The weight of $f_j(x)$ is important for Step 3. The best case is achieved when $f_j(x)$ is a binomial. The used scheme of calculations is a well known scheme with FFT, which is adopted to a $\mathbb{P}$-tower structure.
Now we give in detail the general method for *fast multiplicative inversion* \([3]\) based on the fact that the norm \(N_{K_j/K_{j-1}}(A)\) of an element \(A\) from a field \(K_j\) over a subfield \(K_{j-1}\) belongs to this subfield \([13, 14]\); see also (1). Thus, we have

\[
A \in K_j = GF(Q^p), \quad N_{K_j/K_{j-1}}(A) = \prod_{i=0}^{p_j-1} A^{Q^i} \in K_{j-1} = GF(Q),
\]

where \(Q = q^{p_1, p_2, \ldots, p_{j-1}}\). Using the notation \(N_j(A) = N_{K_j/K_{j-1}}(A)\) we define the *adjoint norm* \(N_j^r(A)\) of \(A\) as

\[
N_j^r(A) = A^{-1}N_j(A) = \prod_{i=1}^{p_j-1} A^{Q^i}. \quad (6)
\]

So, by relation (6) the inversion of \(A\) over the given field has reduced to inversion of its norm over a subfield

\[
A^{-1} = N_j^r(A)(N_j(A))^{-1}. \quad (7)
\]

For calculation of \(N_j^r(A)\) we use the following products of exponents

\[
\Phi_m(A) = \prod_{i=1}^{2^m} A^{Q^i}, \quad (\Phi_m(A))Q^i = \prod_{i=i+1}^{i+2^m} A^{Q^i}, \quad (\Phi_m(A))Q^{2^m} = \prod_{i=2^m+1}^{2^{m+1}} A^{Q^i}.
\]

Let \(L_j = \lfloor \log_2(P_j - 1) \rfloor\) and let \(B_j \leq L_j + 1\) be the weight of binary form of an integer \(P_j - 1 = \sum_{i=1}^{B_j} 2^{\omega_i}, \omega_i < \omega_{i+1}, \omega_i \in \{0, 1, \ldots, L_j\}, i = 1, 2, \ldots, B_j\).

*The Procedure of Fast Inversion of \(A \in K_j\) Based on (7).*  
- **Step 1.** Iterative calculation of values \(\Phi_0(A), \Phi_1(A), \ldots, \Phi_{L_j}(A)\), by the relations

  \[
  \Phi_0(A) = A^Q, \quad \Phi_{m+1}(A) = \Phi_m(A) \cdot (\Phi_m(A))Q^{2^m}, \quad m = 0, 1, \ldots, L_j - 1.
  \]

- **Step 2.** Calculation of the \(N_j^r(A)\) value on the base of the binary representation of the integer \(P_j - 1\).

  \[
  N_j^r(A) = \Phi_{\omega_1}(A) \prod_{i=2}^{B_j} (\Phi_{\omega_i}(A))Q^{\omega_i}, \quad R_i = \sum_{u=1}^{i-1} 2^{\omega_u}, i = 2, 3, \ldots, B_j.
  \]

- **Step 3.** Calculation of the norm

  \[
  N_j(A) = A \cdot N_j^r(A), \quad \text{where } A, N_j^r(A) \in K_j, \quad N_j(A) \in K_{j-1}.
  \]
• Step 4. Inversion of the norm $N_j(A)$ over the subfield $K_{j-1}$

$$a = (N_j(A))^{-1}, \quad \text{where } a, N_j(A) \in K_{j-1}.$$  

• Step 5. Calculation of $A^{-1}$ in the field $K_j$

$$A^{-1} = a \cdot N_j(A), \quad a \in K_{j-1}, \quad A^{-1}, N_j(A) \in K_j.$$  

4. COMPLEXITY OF ARITHMETIC

The complexity of a calculation procedure we define as the weighted sum of the number of arithmetic operations of the prescribed classes. To simplify analysis we consider only the class of additive operations, multiplication of two arbitrary elements (nonscalar multiplication), and inversion of an arbitrary element. An operation from the additive class we denote as a $P$-operation. In the field $K_j$, i.e., on the $j$th level of a $P$-tower, a $P$-operation has the property

$$C_j \leq P_j C_{j-1}, \quad j \geq 1,$$

where $C_j$ is the complexity of an operation over a field $K_j$ and $P_j$ is given by (1). We qualify as $P$-operations over $K_j$, the following: addition of two arbitrary elements from the field $K_j$, multiplication of an arbitrary element from $K_j$ by an element from its subfield $K_u, u < j$, and multiplication of an arbitrary element from $K_j$ by the constant term $\psi_{j+1} \in K_j$ of the binomial $f_{j+1}(x) = x^{P_j + 1} - \psi_{j+1} = x^{P_j} - \beta_j$, see Corollary 2. Note that in the polynomial representation $\psi_{j+1} = \beta_j = (0, 1, 0, \ldots, 0) = x$. Hence,

$$A\psi_{j+1} \pmod{f_j(x)} = \sum_{i=0}^{P_j-1} a_i x^{i+1} \pmod{x^{P_j} - \psi_j} = (a_{P_j-1} \psi_j, a_0, a_1, \ldots, a_{P_j-2}).$$

It is natural to assume that the complexity of rearrangement of coordinates is not greater than the complexity of multiplication by $\psi_j$. So multiplication by $\psi_{j+1}$ is equivalent to a $P$-operation, indeed.

4.1. Complexity of Multiplication

On the $j$th level of the $P$-tower Step 1 takes $\mu_j \geq 2P_j - 1$ multiplications of arbitrary elements over the subfield $K_{j-1}$ for calculation of $T(\lambda_u) = A(\lambda_u) B(\lambda_u)$. Let $\varepsilon_j$ be the total number of $P$-operations on this level. The main content of $\varepsilon_j$ is additions and multiplications by the Fourier
constants in FFT procedure on Steps 1 and 2. Another part is calculation of \( C(x) \) on Step 3. Calculation of \( C(x) \) as the residue \( T(x) \) (mod \( x^{P_j} - \psi_j \)) can be realized by the following rule:

\[
c_i = t_i + \psi_j t_{i + P_j}, \quad i = 0, 1, \ldots, P_j - 2, \quad c_{P_j - 1} = t_{P_j - 1}.
\]  

(8)

By (8), Step 3 contains \( 2P_j - 2 \) additions and multiplications of elements from \( K_{j-1} \) by \( \psi_j \in K_{j-1} \).

The recursive equations for the complexity of fast multiplication over \( K_h \) in a \( \mathbf{P} \)-tower can be written as

\[
\mathcal{M}_h = \mu_h \mathcal{M}_{h-1} + \ell_h \mathcal{C}_{h-1}, \quad \mathcal{C}_h = P_h \mathcal{C}_{h-1},
\]  

(9)

where \( \mathcal{M}_h \) is the complexity of multiplication in a \( \mathbf{P} \)-tower \( K_h \), \( \mathcal{C}_h \) is the complexity of a \( P \)-operation over \( K_h \), and \( P_h \) is given by (1). For a ground field \( GF(q) \) the complexity of multiplication is \( \mathcal{M}_0 \) and \( \mathcal{C}_0 \) is complexity of additive operation (addition and multiplication by a constant from \( GF(q) \)).

**Theorem 5.** The exact solution of the recursive system (9) for a \( \mathbf{P} \)-tower has the form

\[
\mathcal{M}_h = \mathcal{M}_0 \prod_{j=1}^{h} \mu_j + \mathcal{C}_0 \sum_{u=1}^{h} \ell_u \prod_{j=1}^{u-1} P_j \prod_{j=u+1}^{h} \mu_j.
\]  

(10)

**Proof.** We prove the theorem by induction on \( h \) taking into account the fact \( \mathcal{C}_h = \mathcal{C}_0 \prod_{j=1}^{h} P_j \), that can be easily verified. \( \blacksquare \)

4.2. Complexity of Inversion

The crucial part of the inversion routine is the calculation of all \( \Phi_m(A) \) on Step 1. The kernel of that is raising to a power \( Q' \) over the field \( K_j \). Let

\[
D = \sum_{i=0}^{P_j - 1} d_i x^i \in K_j, \quad d_i \in K_{j-1}, \quad i = 0, 1, \ldots, P_j - 1.
\]

Let \( c_{i,l} \) and \( g_{i,l} \) be non-negative integers such that \( iQ' = c_{i,l} P_j + g_{i,l} \), \( g_{i,l} \in \{0, 1, \ldots, P_j - 1\} \), \( i \in \{1, 2, \ldots, P_j - 1\} \). Since \( d_i^{Q'} = d_i \) and \( x^{P_j} \equiv \psi_j^c \) (mod \( x^{P_j} - \psi_j \)), we have

\[
D^{Q'} \pmod {x^{P_j} - \psi_j} = \sum_{i=0}^{P_j - 1} d_i^{Q'} x^{iQ'} \pmod {x^{P_j} - \psi_j} = \sum_{i=0}^{P_j - 1} d_i \psi_j^{c_{i,l}} x^{g_{i,l}}.
\]  

(11)

Steps 1 and 2 need raising to the power \( Q' \) over \( K_j \). From (11) we see that raising to the power \( Q' \) over \( K_j \) takes \( P_j - 1 \) multiplications of an element \( d_i \in K_{j-1} \) by a constant \( \psi_j^{c_{i,l}} \in K_{j-1} \). The complexity of such multiplication is approximated as complexity of nonscalar multiplication over \( K_{j-1} \). Additions in (11) are \( P \)-operations over \( K_{j-1} \). So, raising to the power \( Q' \) over \( K_j \)
takes \( P_j - 1 \) nonscalar multiplications over \( K_{j-1} \) and the same number \( P \)-operations over \( K_{j-1} \). Unlike the multiplication over a field \( K_j \) the algorithm for multiplicative inversion has to use both nonscalar multiplications over \( K_{j-1} \) and \( K_j \).

Let \( \mu_j \) (respectively \( \mu_j' \)) be the number of nonscalar multiplications over a field \( K_{j-1} \) (respectively \( K_j \)) in the inversion algorithm over \( K_j \). Let \( \nu_j \) be the number of \( P \)-operations over \( K_{j-1} \) in this algorithm. Steps 1 and 2 of the inversion algorithm contain respectively \( \nu_j \) and \( \nu_j' \) nonscalar multiplications over \( K_j \). Steps 1 and 2 need \( \nu_j \) \# \( 1 \) and \( \nu_j' \) \# \( 1 \) raising to the power \( Q \) over \( K_j \). Step 3 has one nonscalar multiplication over \( K_j \). Step 5 needs \( P_j \) nonscalar multiplications over \( K_j \). Hence for a \( P \)-tower with a \( P \)-extension on the \( j \)th level we have

\[
\mu_j = L_j + B_j \leq 2L_j + 1 = 2\lceil \log_2 (P_j - 1) \rceil + 1.
\]

Similarly, since raising to the power \( Q \) over \( K_j \) takes \( P_j - 1 \) nonscalar multiplications and the same number \( P \)-operations over \( K_{j-1} \) (see comment to (11)), we obtain

\[
\mu_j' = (L_j + B_j)(P_j - 1) + P_j, \quad \nu_j' = (L_j + B_j)(P_j - 1).
\]

Recursive equations for complexity \( \mathcal{D}_h \) of multiplicative inversion in a \( P \)-tower \( K_h \) are

\[
\mathcal{D}_h = \mathcal{D}_{h-1} + \mu_h \mathcal{M}_{h-1} + \mu_h' \mathcal{M}_h + \nu_h \mathcal{C}_{h-1},
\]
\[
\mathcal{M}_h = \mu_h \mathcal{M}_{h-1} + \nu_h \mathcal{C}_{h-1}, \quad \mathcal{C}_h = P_h \mathcal{C}_{h-1},
\]

where the last two relations coincide with (9) and \( \mathcal{D}_0 \) is the complexity of inversion for the ground field \( GF(q) \).

**Theorem 6.** The exact solution of the recursive system (14) for a \( P \)-tower has the form

\[
\mathcal{D}_h = \mathcal{D}_0 + \sum_{k=0}^{B-1} \left( \mu_{k+1} + \mu_k' \right) \mathcal{M}_k + \mathcal{C}_0 \sum_{k=1}^{B} \nu_k \prod_{i=1}^{k-1} P_i, \quad \mu_{j+1} = \mu_0' = 0,
\]

where \( \mathcal{M}_k \) is defined in Theorem 5.

**Proof.** The proof can be obtained by induction on \( h \).  

**Remarks.** The estimation of the complexity of calculation in (11) ignores the complexity of storage and calculation of the constants \( \psi_{i,j}^{\mu,l} \) for all \( i, j, l \).
It can be simply shown that this additional term does not change the order of the complexity estimates.

5. ASYMPTOTIC ESTIMATES OF COMPLEXITY FOR \( \mathbf{P} \)-TOWERS

5.1. FFT Complexity

Using FFT essentially improves the complexity of arithmetic for \( \mathbf{P} \)-towers. FFT of order \( \mu_j \) should be used on the \( j \)th level of a \( \mathbf{P} \)-tower where \( \mu_j \) must be a factor of \( |K_{j-\delta}| - 1 \) and \( K_{j-\delta} \) is the field of FFT constants. So, to use FFT we have to choose \( \mu_j \) such that 
\[ 2P_j - 1 \leq \mu_j (q^{P_1 P_2 \cdots P_{j-\delta}} - 1) \]
where \( P_j = \gamma P_j (q^{P_1 P_2 \cdots P_{j-\delta}} - 1) \), 
\[ P_j | P_2 \cdots P_{j-\delta}, \quad j \geq \delta \geq 1, \quad (16) \]
where \( \gamma \geq 2 \) is the smallest prime factor of \( (q - 1) \). If \( K_0 \neq GF(2^n) \) then \( \gamma = 2 \), otherwise \( \gamma \geq 3 \). By definitions (1), (2), and (16), we can choose \( n_{j,i} \leq S(j - \delta, i) \). We need this restriction on \( n_{j,i} \) to embed FFT constants into some subfield on each level of the tower. So, using the FFT brings a constraint on the tower structure. Let \( U(n) \) be the total number of additions and multiplications by constants in Fourier transform of order \( n \) for the case \( \delta > 1 \) when both operations belong to additive class. For FFT Cooley–Tukey, see, e.g., [9], it holds, with the assumption \( U(p_i) \leq 2p_i^2 \), that 
\[ U(\gamma P_j) = U(\gamma p_1^{n_{j,1}} p_2^{n_{j,2}} \cdots p_t^{n_{j,t}}) \leq g \gamma P_j \left( \gamma + \sum_{i=1}^{t} p_i n_{j,i} \right), \]
where \( g \) is a positive constant. It is important that the ground field \( GF(q) \) and, hence, the set of prime factors \( p_1, \ldots, p_t \) are fixed, and the product of them is a factor of \( q - 1 \). Thus taking into account (16) we can majorize the complexity of FFT procedure on the \( j \)th level of the tower by the inequalities 
\[ U(\gamma P_j) \leq g \gamma P_j \left( \gamma + p_t \sum_{i=1}^{t} n_{j,i} \right) \leq g \gamma P_j \left( \gamma + (q - 1) \sum_{i=1}^{t} n_{j,i} \right), \quad (17) \]
where \( p_1 < p_2 < \cdots < p_t \) and \( p_1 p_2 \cdots p_t | (q - 1) \).
5.2. Complexity of Multiplication and Inversion

Returning to fast multiplication we see that on Steps 1 and 2 FFT carry out operations with elements $a_i$, $b_i$, $t_i$ of a field $K_{j-1}$. It means, any $\delta \geq 1$ is available and $K_{j-\delta} \subseteq K_{j-1}$. When $\delta \geq 2$ is used we have $K_{j-\delta} \subset K_{j-1}$. Thus, a field of FFT constants is a proper subfield of $K_{j-1}$ and multiplication of elements $a_i$, $b_i$, $t_i$ by FFT constants are $P$-operations.

In the case $\delta = 1$, FFT constants belong to $K_{j-\delta} = K_{j-1}$. So, we have multiplication of arbitrary elements by constants in the same field which is not a $P$-operation. Thus the estimate for $\mu_j$ has to be changed as $2P_j + \frac{1}{2}U(\gamma P_j)$. But this changes for the worse the resulting complexity. Therefore we consider the case $\delta > 1$ further.

Note also that the product of two polynomials of a degree $P$ modulo a polynomial $f(x)$ of the degree $P + 1$ could not be computed with less than $2(P + 1) - t$ nonscalar multiplications where $t$ is the number of prime factors of $f(x)$ [9, Sect. 3.8]. Since $f_j(x)$ of degree $P_j$ is irreducible we have $t = 1$. Therefore, the bound $2P_j - 1 \leq \mu_j$ should hold; cf. (5) and (16). See also [17, Sect. 4.3] and references therein where the lower bound is given on the number of necessary nonscalar multiplications for the product of two polynomials. The value $\mu_j = 2P_j - 1$ is minimal and usually has to be used if we apply FFT of some other than exponential order.

Substituting $\mu_j = \gamma P_j$ and $U(\gamma P_j)$ instead of $\varepsilon_j$ in (10) we obtain after simple modification

$$M_h < \left( M_0 + g\gamma^h C_0 \left( \frac{\gamma}{\gamma - 1} + \sum_{u=1}^{h} \gamma^{-u} \sum_{i=1}^{t} n_{u,i} \right) \right) \gamma^h \prod_{j=1}^{h} P_j,$$

For our purpose it is enough to use only the right estimate from (17), which leads to the result

$$M_h < \left( M_0 + g\gamma^h C_0 \left( \frac{\gamma}{\gamma - 1} + (q - 1) \sum_{u=1}^{h} \gamma^{-u} \sum_{i=1}^{t} n_{u,i} \right) \right) \gamma^h \prod_{j=1}^{h} P_j. \quad (18)$$

For the fast inversion procedure the weights $\mu'_h$, $\mu''_h$, and $\varepsilon'_h$ in (12), (13), and (15) can be estimated as

$$\mu'_j \leq 2\lfloor \log_2(P_j - 1) \rfloor + 1 < 2 \sum_{k=1}^{t} n_{j,k} \log(q - 1), \quad (19)$$

$$\mu''_j \leq 2 \sum_{k=1}^{t} n_{j,k} \log(q - 1) + P_j, \quad \varepsilon'_j \leq 2 \sum_{k=1}^{t} n_{j,k} \log(q - 1). \quad (20)$$
Substitution of these weights and (18) into (15) is evident. The only nontrivial thing is related to the estimation of $\sum_{u=1}^{h} \gamma^{-u} \sum_{i=1}^{t} n_{u,i}$ in (18).

5.3. Optimization of the Tower: General Case

The goal of optimization is to diminish $\sum_{u=1}^{h} \gamma^{-u} \sum_{i=1}^{t} n_{u,i}$ in (18) by optimization of the tower structure. We define the optimized $\mathbf{P}$-tower as a tower with exponentially growing $\sum_{i=1}^{t} n_{u,i}$. Taking into account (2), (16), and the conditions $n_{j,i} \leq S(j-\delta, i)$ we can write the following approximation for $N(j) = \sum_{i=1}^{t} n_{j,i}$

$$N(j) = S(j-\delta), \quad S(j) = S(j-1) + N(j), \quad N(j) = N(j-1) + N(j-\delta),$$

(21)

where $S(j) = \sum_{i=1}^{t} S(j, i)$ and $j > \delta \geq 1$. The well known solution for $N(j)$ of the recursion (21) is a linear combination of exponents of all roots of the characteristic equation $z^\delta - z^{\delta-1} - 1 = 0$. This equation has exactly one real positive root $\kappa$. For our purpose it is sufficient to use the exponential approximation $N(j) = c\kappa^j$ for $j > \delta$, where $c$ is a positive constant. By direct substitution one can check that $\kappa = 2$ for $\delta = 1$ and $1 < \kappa < 2$ for $\delta \geq 2$. Since $2 \leq \gamma \leq p_i \leq (q - 1)$ we can take $\gamma = 2$ to get an upper estimate of $\sum N(u)\gamma^{-u}$. Thus we obtain

$$N(j) = c\kappa^j, \quad \sum_{u=1}^{h} N(u)\gamma^{-u} \leq \frac{c\kappa}{\gamma - \kappa} \leq \frac{c\kappa}{2 - \kappa} \text{ for } \delta > 1.$$  

(22)

Now we are ready to formulate the final result on complexity of arithmetic for a finite field which is designed as a tower.

**Theorem 7.** Given a ground field $GF(q)$ and a subset $\mathbf{P} = \{p_1, p_2, \ldots, p_t\}$ of prime factors of $(q - 1)$ let $N(j) = \sum_{i=1}^{t} n_{j,i}$ be majorized by exponent $c\kappa^j$, where $1 < \kappa \leq 2$. Then for the corresponding (optimized) $\mathbf{P}$-tower $K_h$ designed by iterative extensions of the degree $P_i = p_1^{n_1} p_2^{n_2} \ldots p_t^{n_t}$ the asymptotic upper estimates of complexity of multiplication $\mathcal{M}_h$ and inversion $\mathcal{D}_h$, which are reduced to arithmetic operations over the ground field, are

$$\mathcal{M}_h < g_1 \gamma^h \prod_{i=1}^{t} P_i \quad \text{for } \delta > 1,$$

(23)

$$\mathcal{D}_h < g_2 \mathcal{M}_h \kappa^h \log_2 (q - 1) < g_3 (2\gamma)^h \prod_{i=1}^{t} P_i \quad \text{for } \delta > 1,$$

(24)
where all constants $g_i$ are positive and independent of $h$ and $\gamma$ is the minimal prime factor of $q - 1$, $2 \leq \gamma | (q - 1)$.

**Proof.** The relation $N(j) = \sum_{i=1}^{t} n_{j,i} = S(j - \delta), j > \delta$, means that we use the maximal values of $n_{j,i}$ satisfying (16) on every $j$th level of a $P$-tower with $j > \delta$. The estimate (23) follows from (18), (21), and (22).

By (23), for large $h$ we have $\mathcal{M}_h \gg \mathcal{M}_{h-1}$. By using this fact the inequalities (24) follow from (15) with substitutions (19) instead of (20) instead of $\mu_j$ and $\varepsilon_j$, where $N(h) \leq c \xi^h \leq 2^h$ from (22). Then using (23) we obtain both inequalities of (24).

To show our result for the $P$-tower in the form comparable with the Schönhage–Strassen estimate [16] we can rewrite (23) and (24) as functions of the field cardinality $Q$. Let $Q_j = q^{p_j \cdots p_1}$. Then log $Q_j = P_1 P_2 \cdots P_t \log q$ and log log $Q_j < \sum_{i=1}^{t} \sum_{k=1}^{t} n_{i,k} \log q < 2h+1 \log q$ according to the conditions (22) and the proof of Theorem 7. Then we get $M_h$ of (23) and $D_h$ of (24) for $\delta > 1$ as functions of $Q_h$ of the following type:

$$\mathcal{M}_h \simeq O(\log Q_h \log^\delta \log Q_h), \quad 1 \leq \xi \simeq \log_2 \gamma, \quad (25)$$

$$D_h \simeq O(\log Q_h \log^{1+\xi} \log Q_h). \quad (26)$$

So, the asymptotic estimate (25) for complexity of multiplication in a $P$-tower of a finite field is very similar to the asymptotic estimate by Schönhage–Strassen for integer multiplication.

5.4. **The Worst Case**

To demonstrate how the complexity estimate depends on the tower structure we consider one particular case when $t = 1$ and all $n_{j,i} = 1$. This case is called a $P$-tower. So we have $p|(q - 1)$ and $P_j = p$. Then $S(h) = h$ and $K_h = GF(q^h)$. Other changes in (9) and (14) are $\mu_j = \mu'$, $\mu'' = \mu''$, $\varepsilon_j = \varepsilon'$, $\mu_j = \mu$, $\varepsilon_j = \varepsilon$, for all $j$.

**Theorem 8.** Let $K_h$ be a $P$-tower. Then the exact solutions of the recursive systems (9) and (14) for the $P$-tower are

$$\mathcal{M}_h = \left( \mathcal{M}_0 + \frac{\mathcal{C}_0 \varepsilon}{\mu - p} \right) \mu^h + \frac{\mathcal{C}_0 \varepsilon}{\mu - p} p^h, \quad (27)$$

$$D_h = \mathcal{D}_0 + (\mathcal{M}_0 + \Omega) \frac{\mu'' \mu + \mu'}{\mu - 1} \mu^h - \frac{(\mu'' p + \mu') \Omega - \varepsilon'}{p - 1} p^h + m, \quad (28)$$
where

\[ \Omega = \frac{\sigma_0 \xi}{\mu - p}, \quad m = \mathcal{M}_0 - \frac{\mu(\mathcal{M}_0 + \Omega)(\mu'' + \mu')}{\mu - 1} - \frac{p\Omega(\mu'' + \mu') + \epsilon'}{p - 1}. \]

**Proof.** We use (10) and the relation \( \mu^h - p^h = (\mu - p)\sum_{u=1}^{h} p^{u-1} \mu^{h-u} \) for the estimate (27). Substitution of (27) into (15) and the fact \( \mu^h - 1 = (\mu - 1)\sum_{u=1}^{h} \mu^{u-1} \) give the estimate (28). ■

We consider an asymptotic estimate for the fast multiplication algorithm. We do not use FFT here because \( p \) is constant and it might be that the effective FFT of the order \( \mu \) does not exist for \( \mu \) comparable with \( 2p \). Step 1 contains approximately \( 4(p-1)\mu \) additions and multiplications to obtain values \( A(\lambda) \) and \( B(\lambda) \) in \( \mu \) distinct points \( \lambda_u \). Step 2 can be executed as multiplication of \( T(x) \) by the \( (2p - 2) \times (2p - 2) \) constant matrix. All operations mentioned are \( P \)-operations. Taking into account (5) and (8), we have in (9), \( \varepsilon < gp^2 \). As above, \( g \) and \( g_i \) are positive constants independent of \( h \). Given \( \mu = 2p - 1 < 2p \) in (27) we get the following asymptotic upper estimate of multiplication complexity \( \mathcal{M}_h \) for a \( p \)-tower \( K_h \),

\[ \mathcal{M}_h < \left( \mathcal{M}_0 + \frac{\sigma_0 \xi}{p - 1} \right) 2^{h} p^h < (\mathcal{M}_0 + g_1 p \sigma_0) 2^{h} p^h < g 2^{h} p^h. \] (29)

Now we consider the fast multiplicative inversion algorithm. By (12) and (13) with \( n_{j,i} = 1 \), we have for a \( p \)-tower

\[ \varepsilon < g_1 p^2, \quad \mu' < 2p \log_2 p + p, \quad \mu'' < 2 \log_2 p, \quad \varepsilon' < 2p \log_2 p. \]

In (28), \( m \) is independent of \( h \). From (28) we get the following asymptotic upper estimate of inversion complexity \( \mathcal{D}_h \) for a \( p \)-tower \( K_h \),

\[ \mathcal{D}_h < \left( \mathcal{M}_0 + \frac{\sigma_0 \xi}{p - 1} \right) (3 \log_2 p + 0.5) 2^{h} p^h < g 2^{h} p^h. \] (30)

Comparing (29) and (30) we see that the asymptotic complexities of multiplication and multiplicative inversion for a \( p \)-tower have the same order. Using FFT does not improve much the asymptotic estimates of the complexity for \( p \)-towers. Rewriting (29) and (30) through the field cardinality we have

\[ \mathcal{M}_h \approx \mathcal{D}_h \approx (\log Q)^{1+1/\log p} \text{ where } Q = q^p. \]

So, the optimized \( P \)-tower has much better complexity estimates (25) and (26). The \( p \)-tower gives the worst case which is not so bad for the medium field size and it is very difficult to find a better scheme for small enough finite fields.
6. CONCLUSION

The main result of the current paper is a demonstration of a general $P$-tower with good asymptotic estimates of arithmetic complexity. We would like to note that the tower structure is very rich in spite of it not being universal. In itself a $P$-tower is a rich enough object. Nevertheless it can be generalized in different directions by using the same technology of fast calculations in a tower. For example, two generalizations of tower structures of the current paper can be given.

The tower structures can be supplemented with levels of a $\rho$-extension where $\rho$ is the ground field characteristic. It is known that an irreducible trinomial $x^\rho - x - \beta$ exists for any $\rho$. So, reducing a polynomial by the modulo trinomial of this form is a little bit more complex than for the irreducible binomial. Thus iterative construction of a tower can be defined by a sequence of integers $P_1, P_2, \ldots, P_h$ of the form (1) where additionally some of $P_j = \rho$. The resulting complexity for this case has the same bounds as the worst and the best estimates for the $P$-tower.

The next generalization is also almost evident. Each level of a tower can be treated as a new (intermediate) ground field. Thus an expanded set of prime factors can be used on succeeding levels of the tower.

ACKNOWLEDGMENT

We appreciate so much the anonymous referees for their attention and very useful comments and help.

REFERENCES

5. V. B. Afanassiev and A. A. Davydov, Iterated presentation and complexity of arithmetic for tower of extended fields $GF(q^k)$, $p|(q - 1)$, in “Proceedings of the Sixth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT-VI, Pskov, Russia, 1998,” pp. 1–4.


