Journal of Mathematical Sciences, Vol. 76, No. 6, 1995

LINEAR RECURRING SEQUENCES OVER RINGS AND MODULES

V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, and A. A. Nechaev UDC 512.628.4 519.1

To the 80th anniversary of the birth of Alexander Illarionovich Uzkow (1913–1990)

Introduction

Linear recurring sequences (LRS) over fields are well-known subjects of research in applied algebra and discrete mathematics (see, e.g., [5, 18, 37, 52, 133]), dating back to Fibonacci. The foundations of the theory of linear recurring sequences were laid by Moivre, D. Bernoulli, L. Euler, and Lagrange [100, 106, 124]. Later on it was developed by Lucas [127], P. L. Chebyshev [72], and A. A. Markov [40]. The period of the 20s and 30s was connected with R. D. Charmichael [86], M. Ward [166, 167], M. Hall [113], L. E. Dickson [100], and H. T. Engstrom [104, 105]. They began to study properties of linear recurrences which were used later in radar-location, coding theory, generation of pseudo-random numbers, etc. (see [4, 5, 37, 39]).

The peculiarity of the modern stage of the theory of linear recurring sequences is connected with the consideration of multidimensional recurrences over rings and modules based on effective usage of commutative algebra. On the one hand, this offers new possibilities for advancement in the solution of applied problems. On the other hand, this theory now becomes useful in ring theory, in particular, in the theory of QF-modules (Section 4) and in the theory of Hopf algebras (Section 14).

Here we present some fundamental concept and results of the theory of linear recurring sequences over rings and modules and their applications. Of course, the authors give in more detail those results that are close to their mathematical interests. In particular, an attempt has been made to construct a general algebraic theory of k-LRS over modules, paying explicit attention to periodic k-sequences, to properties of linear recurrences over finite rings and especially over Galois rings, and also to methods of constructing codes based on such recurrences.

The list of references is rather far from being complete in the whole theory of LRS. We have deliberately not included many important papers on recurrences over fields and on Fibonacci sequences and their generalizations. However, our bibliography is rather complete as far as articles on recurrences over rings and k-linear recurring sequences are concerned. This text is not merely a review but mostly an exposition of the authors' points of view on the subject and on recent development of the theory "sur le motifs" of the given titles.

The authors recall with great respect and warmth Professor Alexander Illarionovich Uzkow and devote this work to the 80th anniversary of his birth (8 August, 1913). His lectures, reports (in particular, on meetings of the Moscow Mathematical Society, on the seminar of O. Yu. Schmidt, and later on the seminars of the chair of higher algebra of Moscow University), and articles [64–68] were very inspiring and influenced the mathematical tastes of the authors for many years, and, to a considerable extent, stimulated the appearance of this text.

Translated from Itogi Nauki i Tekhniki, Seriya Sovremennaya Matematika i Ee Prilozheniya. Tematicheskie Obzory. Vol. 10, Algebra–2, 1994.

1072-3374/95/7606-2793$12.50

Chapter 1.

GENERAL PROPERTIES OF LINEAR RECURRING SEQUENCES OVER MODULES

1. Main Definitions and Examples [37, 46, 49, 52, 81, 86, 91, 105, 136, 137, 139, 143, 145, 146, 150, 151, 166, 167]

In what follows, R is a commutative ring with identity e, $M =_R M$ is an R-module. If we define $a\alpha = \alpha a$ for $\alpha \in M$, $a \in R$, then we may consider M as an R-bimodule.

Let us define the usual linear recurring sequences over M (or 1-LRS, see, for example, [46]). Let $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$. Any function $\mu : \mathbb{N}_0 \to R$ is called a *sequence over the module* M. The set of all such sequences is denoted by $M^{(1)}$. The product of a polynomial $G(x) = \sum_{s \geq 0} g_s x^s \in R[x]$ and a sequence $\mu \in M^{(1)}$ is defined by

$$G(x)\mu = \nu, \qquad \nu \in M^{(1)}, \qquad \nu(i) = \sum_{s \geq 0} g_s \mu(i+s) \text{ for } i \in \mathbb{N}_0. \tag{1.1}$$

Thus, on $M^{(1)}$ a module structure over the ring of polynomials $\mathcal{P} = R[x]$ is given.

1.1. Definition. We say that a sequence $\mu \in M^{(1)}$ is a *linear recurring sequence* (LRS) of order m over M if there exists a monic polynomial $F(x) \in R[x]$ (i.e., a polynomial with leading coefficient e) of degree m such that $F(x)\mu = 0$. In this case, $F(x)$ is called a *characteristic polynomial* of the sequence μ, and the row $\mu(\overline{0, m-1}) = (\mu(0), \ldots, \mu(m-1))$ is called the *initial vector of the sequence* μ (with respect to $F(x)$). A characteristic polynomial of μ of the least degree is called a *minimal polynomial*, and its degree is called the *rank* (or the *linear complexity*) of the LRS μ. Notation: rank μ. Note that, generally speaking, a minimal polynomial of a sequence is not uniquely defined.

For a subset $\mathcal{M} \subset M^{(1)}$ the annihilator of $\mathcal{M}$ in $\mathcal{P}$ is defined as the ideal

$$\mathrm{An}_{\mathcal{P}}(\mathcal{M}) = \{F(x) \in \mathcal{P} |\ F(x)\mathcal{M} = 0\}.$$

A sequence $\mu \in M^{(1)}$ is an LRS if and only if $\mathrm{An}_{\mathcal{P}}(\mu)$ is a *monic ideal*, i.e., $\mathrm{An}_{\mathcal{P}}(\mu)$ contains a monic polynomial.

1.2. Example: geometric progression. For any $\alpha \in M$, $q \in R$, the sequence $\mu = (\alpha, q\alpha, \ldots, q^i\alpha, \ldots)$ is an LRS of order 1 over M with characteristic polynomial $F(x) = x - q$ and initial vector $\mu(0) = (\alpha)$. Moreover, $\mathrm{An}_{\mathcal{P}}(\mu) = \mathcal{P}(x-q) + \mathcal{P} \cdot \mathrm{An}_R(\alpha)$.

1.3. Example: arithmetic progression. For any $\alpha, \delta \in M$, the sequence $\nu \in M^{(1)}$ of the elements of $\nu(i) = \alpha + \delta i$ is an LRS of second order with characteristic polynomial $F(x) = (x-e)^2$ and initial vector $(\alpha, \alpha+\delta)$. If $\mathrm{An}_R(\delta) = 0$, then $F(x)$ is a unique minimal polynomial of ν. If $a \in \mathrm{An}_R(\delta)$, then $F(x) + a(x-e)$ is another minimal polynomial of ν.

1.4. Example: congruente sequence. The sequence $\xi \in M^{(1)}$, defined for given $\alpha, \delta \in M$, $q \in R$ by

$$\xi(0) = \alpha, \qquad \xi(i+1) = q\xi(i) + \delta, \qquad i \in \mathbb{N}_0,$$

is an LRS of second order with characteristic polynomial $F(x) = (x-e)(x-q)$ and initial vector $\xi(\overline{0,1}) = (\alpha, q\alpha + \delta)$. Geometric and arithmetic progressions are special cases of the sequence ξ, respectively, for $\delta = 0$

and $q = e$. The polynomial $F(x)$ is the minimal polynomial of ξ if and only if either $\delta \notin R\alpha$ or $\delta = c\alpha$ for some $c \in R$ and $F(c+q)\alpha \neq 0$. Such sequences over the residue rings $\mathbf{Z}_{2^n}$, $\mathbf{Z}_{10^n}$ are rather useful in modeling pseudorandom numbers in computers [18].

1.5. Example: a Fibonacci sequence is the LRS $u \in \mathbf{Z}^{(1)}$ with characteristic polynomial $F(x) = x^2 - x - 1$ and initial vector $u(\overline{0,1}) = (0,1)$. Thus, $u(i+2) = u(i+1) + u(i)$, $i \in \mathbb{N}_0$. This sequence was introduced by Leonardo of Pisa (Fibonacci) in *Book of the Abacus* (1202) in connection with the "problem of the reproduction of rabbits."

1.6. Example: linear sequence. Let ${}_RM = {}_R(\alpha_1, \ldots, \alpha_m)$ be a finitely generated R-module (f.g.-R-module), and let $\alpha \in M$, $\varphi \in \operatorname{End}_R(M)$. Then the sequence $\alpha^\varphi = (\alpha, \varphi(\alpha), \ldots, \varphi^i(\alpha), \ldots)$ is an LRS of order m with characteristic polynomial $F(x) = \chi_\varphi(x) = \chi_A(x) = |xE - A|$, where A is a matrix over R, such that $(\varphi(\alpha_1), \ldots, \varphi(\alpha_m)) = (\alpha_1, \ldots, \alpha_m)A$, i.e., A is one of the matrices of the endomorphism φ in the generating system $(\alpha_1, \ldots, \alpha_m)$. Moreover, the rank $\alpha^\varphi \leq \partial({}_RM)$, where $\partial({}_RM)$ is the minimal cardinality of the generating set of the module ${}_RM$.

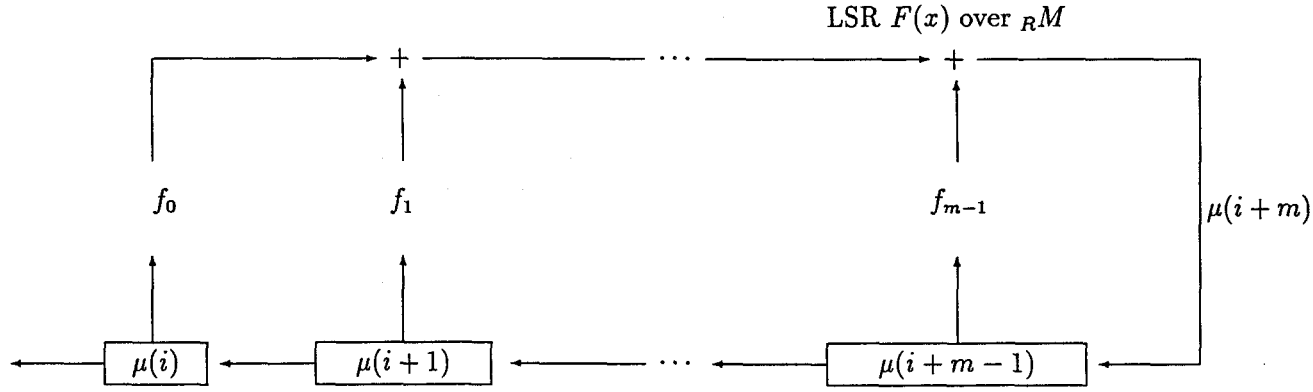
1.7. Example. The sequence $(2, 3, 5, 7, \ldots)$ of all prime numbers is not an LRS over $\mathbf{Z}$.

1.8. Example. Any sequence $\mu \in M^{(1)}$ of the form

$$\mu = (\mu_0, 0, \mu_1, 0, 0, \mu_2, 0, 0, 0, \mu_3, \ldots),$$

containing an infinite series of nonzero terms, is not an LRS over M.

1.9. Linear shift register. Any LRS μ with characteristic polynomial $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0$ can be obtained as an output of the following linear sequential circuit, called the *linear shift register* (LSR) *with the characteristic polynomial* $F(x)$ *over* M:

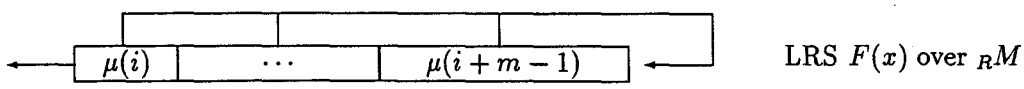


Here $\boxed{\mu(s)}$ is the storage location containing the element $\mu(s) \in M$;

f_s is the block of multiplication on f_s;

$+$ is the block of addition in M.

This register can be depicted in the following abbreviated form:



Note that the content $\mu(\overline{i, i+m-1})$ of the register on the i-th step is connected with the initial content $\mu(\overline{0, m-1})$ by the following formula:

$$\mu(\overline{i, i+m-1}) = \mu(\overline{0, m-1})S(F)^i, \tag{1.2}$$

where

$$S(F) = \begin{pmatrix} 0 & 0 & \dots & 0 & f_0 \\ e & 0 & \dots & 0 & f_1 \\ 0 & e & \dots & 0 & f_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e & f_{m-1} \end{pmatrix}$$

is the *accompanying matrix of the polynomial* $F(x)$.

The simple technical and program realization of such a register was the main reason for the wide usage of linear recurrences in different applications (e.g., see [4, 5, 7]).

1.10. Proposition. *The set* $\mathcal{L}M^{(1)}$ *of all linear recurrences over a module* M *is a submodule of the module* ${}_{\mathcal{P}}M^{(1)}$. *For any subset* $I \subset \mathcal{P}$ *the set*

$$L_M(I) = \{\mu \in M^{(1)} \mid I\mu = 0\}$$

is a $\mathcal{P}$*-submodule in* ${}_{\mathcal{P}}M^{(1)}$. *Moreover,* $L_M(I) \subset \mathcal{L}M^{(1)}$ *if and only if* (I) *is a monic ideal.*□

1.11. Definition. For any unitary ideal I of the ring $\mathcal{P}$, we call the set of recurrences $L_M(I)$ an LRS-*family over the module* M.

1.12. Remark. In Definition 1.1, the condition "$F(x)$ is a monic polynomial" may be changed to the condition "the leading coefficient of $F(x)$ is invertible," but, in the general case, this condition is not equivalent to the condition "the leading coefficient of $F(x)$ is a regular element." For example, let $R = S/J$, where $S = \mathbf{Z}[y_0, y_1, \dots]$ is the polynomial ring over $\mathbf{Z}$ in the infinite set of variables, $J = (y_0 - 2y_1, y_1 - 2y_2, \dots)$. Then the sequence $\mu \in R^{(1)}$ of elements of the form $\mu(i) = y_i + J$ is annihilated by the polynomial $F(x) = 2x - 1$, but it is not a linear recurrence.

However, for example, for sequences over $\mathbf{Z}$ the situation is different.

1.13. Proposition. *Let* $I = (F_1(x), \dots, F_t(x))$ *be an ideal of the ring* $\mathbb{Z}[x]$. *Then the condition* $L_{\mathbf{Z}}(I) \neq 0$ *is equivalent to the following condition: the polynomials* $F_1(x), \dots, F_t(x)$ *have a common integer algebraic root in the algebraic closure* $\tilde{\mathbb{Q}}$ *of the field* $\mathbb{Q}$. *Let* $\alpha_1, \dots, \alpha_r$ *be all integer algebraic roots of the polynomials* $F_1(x), \dots, F_t(x)$ *in* $\tilde{\mathbb{Q}}$, *and* $k_1, \dots, k_r$ *be the minimum of multiplicities of these roots for the above polynomials. Then*

$$L_{\mathbf{Z}}(I) = L_{\mathbf{Z}}(F(x)), \text{ where } F(x) = (x - \alpha_1)^{k_1} \dots (x - \alpha_r)^{k_r}.$$

□ The polynomial $F(x)$ is a monic polynomial of the maximal degree from $\mathbf{Z}[x]$, which divides polynomials $F_1(x), \dots, F_t(x)$. Hence $L_{\mathbf{Z}}(F(x)) \subset L_{\mathbf{Z}}(I)$. If $L_{\mathbf{Z}}(I) \neq 0$, then $L_{\mathbf{Z}}(I)$ is a free abelian group and its rank k is less than or equal to the maximum of degrees of polynomials $F_1(x), \dots, F_t(x)$. Let $u_1, \dots, u_k$ be a free generating system of the group $L_{\mathbf{Z}}(I)$. Then $(xu_1, \dots, xu_k) = (u_1, \dots, u_k)A$ for some integer matrix A, and each of the sequences $u_1, \dots, u_k$ is annihilated by the characteristic polynomial $\chi_A(x)$ of the matrix A. Therefore, $L_{\mathbf{Z}}(I) \subset L_{\mathbf{Z}}(\chi_A(x))$ and $F(x) | \chi_A(x)$. On the other hand, the family $L_{\mathbf{Z}}(I)$ is not annihilated by any nonzero polynomial of degree less than k, hence $\chi_A(x) | F_s(x)$, $s \in \overline{1,t}$. Since all roots of $\chi_A(x)$ in $\tilde{\mathbb{Q}}$ are integer algebraic numbers, we have $\chi_A(x) | F(x)$. Therefore, $L_{\mathbf{Z}}(F) = L_{\mathbf{Z}}(I) = L_{\mathbf{Z}}(\chi_A)$. □

An important generalization of the above definitions is the concept of a k-LRS. For sequences over a field, this was studied, e.g., in [91], and for sequences over a module — in [49, 137]. We call a any function $\mu : \mathbf{N}_0^k \to M$ *k-sequence* over a module ${}_RM$. We write $\mu = \mu(\mathbf{z})$, where $\mathbf{z} = (z_1, \dots, z_k)$ is the row of free variables over $\mathbf{N}_0$. The set $M^{(k)}$ of all k-sequences over M is an R-module relative to the usual operations over functions.

Let $\mathcal{P}_k = R[x_1, \dots, x_k] = R[\mathbf{x}]$ be polynomial ring of k variables. For any $\mathbf{s} = (s_1, \dots, s_k) \in \mathbf{N}_0^k$ denote the monomial $x_1^{s_1} \dots x_k^{s_k}$ by $\mathbf{x}^{\mathbf{s}}$. Then any polynomial $F(\mathbf{x}) \in \mathcal{P}_k$ can be represented in the form $F(\mathbf{x}) = \sum_{\mathbf{s}} f_{\mathbf{s}} \mathbf{x}^{\mathbf{s}}$. We determine the structure of a $\mathcal{P}_k$-module on $M^{(k)}$ defining the multiplication of polynomial $F(\mathbf{x}) \in \mathcal{P}_k$ on

the k-sequence $\mu \in M^{(k)}$ by

$$F(\mathbf{x})\mu = \nu, \qquad \nu \in M^{(k)}, \qquad \nu(\mathbf{z}) = \sum_{\mathbf{s}} f_{\mathbf{s}}\mu(\mathbf{z}+\mathbf{s}). \tag{1.3}$$

Let us consider the annihilator of a subset $\mathcal{M} \subset M^{(k)}$ in the ring $\mathcal{P}_k$:

$$\operatorname{An}(\mathcal{M}) = \operatorname{An}_{\mathcal{P}_k}(\mathcal{M}) = \{F(\mathbf{x}) \in \mathcal{P}_k |\ F(\mathbf{x})\mathcal{M} = 0\}.$$

Evidently, $\operatorname{An}(\mathcal{M})$ is an ideal of $\mathcal{P}_k$.

1.14. Definition. An ideal I of the ring $\mathcal{P}_k = R[x_1, \ldots, x_k]$ is called *monic* if there exist monic polynomials $F_1(x), \ldots, F_k(x) \in R[x]$ (of one variable) such that

$$F_1(x_1), \ldots, F_k(x_k) \in I. \tag{1.4}$$

Such a system of polynomials is called a *system of elementary polynomials* of the monic ideal I, and the ideal $(F_1(x_1), \ldots, F_k(x_k))$ is called an *elementary ideal.*

It is easy to see that if I is a monic ideal, then the factor-ring $\mathcal{P}_k/I$ is a finitely generated R-module. If R is a Noetherian ring, then the converse is also true (for the case where R is a field, see [91]).

1.15. Definition. We say that a sequence $\mu \in M^{(k)}$ is a *k-linear recurring sequence* (k-LRS) over a module M if $I = \operatorname{An}(\mu)$ is a monic ideal. In this case, polynomials (1.4) are called *elementary characteristic polynomials* of the k-LRS μ.

1.16. Proposition. *The set $\mathcal{L}M^{(k)}$ of all k-LRS $\mu \in M^{(k)}$ is a submodule of $\mathcal{P}_k$-module $M^{(k)}$. For any subset $I \subset \mathcal{P}_k$ the set*

$$L_M(I) = \{\mu \in M^{(k)} |\ I\mu = 0\}$$

is also a submodule of this module. Moreover, $L_M(I) \subset \mathcal{L}M^{(k)}$ if and only if (I) is a monic ideal of $\mathcal{P}_k$. □

1.17. Definition. If I is a monic ideal of $\mathcal{P}_k$, then the set $L_M(I)$ is called a k-LRS-*family* over the module ${}_RM$.

Note that the k-LRS-family $L_M(I)$ is annihilated by the ideal I, and hence the $\mathcal{P}_k$-module $L_M(I)$ may be considered as a module over the ring $S = \mathcal{P}_k/I$.

1.18. Definition. The ring $S = \mathcal{P}_k/I = R[\theta_1, \ldots, \theta_k]$, where $\theta_s = x_s + I$, will be called *an operator's ring* of the ideal I (of the family $L_M(I)$). If $I = \operatorname{An}(\mu)$ for some $\mu \in M^{(k)}$, then S is said to be an operator's ring of the k-sequence μ.

Consider a few examples.

1.19. k-geometric progression. Let $\alpha \in M$, $\mathbf{q} = (q_1, \ldots, q_k) \in R^{(k)}$. Then the k-sequence $\mu \in M^{(k)}$ of the form $\mu(\mathbf{z}) = \mathbf{q}^{\mathbf{z}}\alpha$ is a k-LRS, $\mu \in L_M(x_1 - q_1, \ldots, x_k - q_k)$.

1.20. k-arithmetic progression. Let $\alpha_0, \alpha_1, \ldots, \alpha_k \in M$ and $\mu(\mathbf{z}) = \alpha_0 + \alpha_1 z_1 + \ldots + \alpha_k z_k$. Then $\mu \in L_M((x_1 - e)^2, \ldots, (x_k - e)^2)$.

1.21. k-congruent sequence. Let $\alpha_0, \alpha_1, \ldots, \alpha_k \in M$, $q_1, \ldots, q_k \in R$,

$$(q_s - e)\alpha_t = (q_t - e)\alpha_s \text{ for } s, t \in \overline{1,k}. \tag{1.5}$$

Let $\vec{E}_s$ be the s-th row of the identity $k \times k$-matrix E over $\mathbf{Z}$. Define the sequence $\mu \in M^{(k)}$ by

$$\mu(\mathbf{0}) = \alpha_0, \qquad \mu(\mathbf{z} + \vec{E}_s) = q_s\mu(\mathbf{z}) + \alpha_s, \qquad s \in \overline{1,k}.$$

In view of (1.5), the sequence μ is defined correctly and $\mu \in L_M((x_1 - e)(x_1 - q_1), \ldots, (x_k - e)(x_k - q_k))$.

1.22. k-linear sequence. Let ${}_RM$ be a finitely generated R-module, $\alpha \in M$, $\varphi_1, \ldots, \varphi_k \in \operatorname{End}_R(M)$, $\varphi_s\varphi_t = \varphi_t\varphi_s$ for $s, t \in \overline{1,k}$. Then the sequence $\mu \in M^{(k)}$ such that $\mu(\mathbf{z}) = \varphi_1^{z_1} \ldots \varphi_k^{z_k}(\alpha)$ is a k-LRS over M, and the characteristic polynomials $\chi_{\varphi_1}(x_1), \ldots, \chi_{\varphi_k}(x_k)$ of the endomorphisms $\varphi_1, \ldots, \varphi_k$ respectively (see Example 1.6) are elementary characteristic polynomials of μ.

1.23. The sum of independent 1-LRS. Let $F_1(x),\dots,F_k(x)$ be monic polynomials over R and $\mu_s \in L_M(F_s)$, $s \in \overline{1,k}$. Define the k-sequence $\mu = \mu_1 \dot{+} \dots \dot{+} \mu_k \in M^{(k)}$ by $\mu(\mathbf{z}) = \mu_1(z_1) + \dots + \mu_k(z_k)$. Then $\mu \in L_M(G_1(x_1),\dots,G_k(x_k))$, where $G_s(x) = F_s(x)$, if $F_s(e) = 0$, and $G_s(x) = F_s(x)(x-e)$ in the opposite case.

1.24. The direct sum of 1-LRS. Let $F_1(x),\dots,F_k(x)$ be the same as in 1.23, $M_1,\dots,M_k$ be R-modules and $\mu_s \in L_M(F_s(x))$, $s \in \overline{1,k}$. Let μ be a k-sequence over the module $M = M_1 \oplus \dots \oplus M_k$ given by $\mu(\mathbf{z}) = (\mu_1(z_1),\dots,\mu_k(z_k))$. Then $\mu \in L_M(G_1(x_1),\dots,G_k(x_k))$, where $G_1,\dots,G_k$ are the same as in 1.23.

1.25. The tensor product of 1-LRS over the ring R. Let $F_1(x),\dots,F_k(x)$ be the same as in 1.23, and $u_s \in L_R(F_s)$, $s \in \overline{1,k}$. Define the k-sequence $u \in R^{(k)}$ by $u(\mathbf{z}) = u_1(z_1)\dots u_k(z_k)$. Then $u \in L_R(F_1(x_1),\dots,F_k(x_k))$. Moreover, the R-module $L_R(F_1,\dots,F_k)$ is generated by the set of all such sequences u (where u_s runs through $L_R(F_s)$ for $s \in \overline{1,k}$). For any R-module N, any R-multilinear map $\varphi : L_R(F_1) \times \dots \times L_R(F_k) \to N$ can be included in commutative diagram

$$\begin{array}{ccc} L_R(F_1) \times \dots \times L_R(F_k) & \xrightarrow{\varphi_0} & L_R(F_1(x_1),\dots,F_k(x_k)), \\ & \searrow^{\varphi} & \downarrow \psi \\ & & N \end{array}$$

where $\varphi_0((u_1,\dots,u_k)) = u$. Therefore,

$$L_R(F_1(x_1),\dots,F_k(x_k)) = L_R(F_1) \underset{R}{\otimes} \dots \underset{R}{\otimes} L_R(F_k)$$

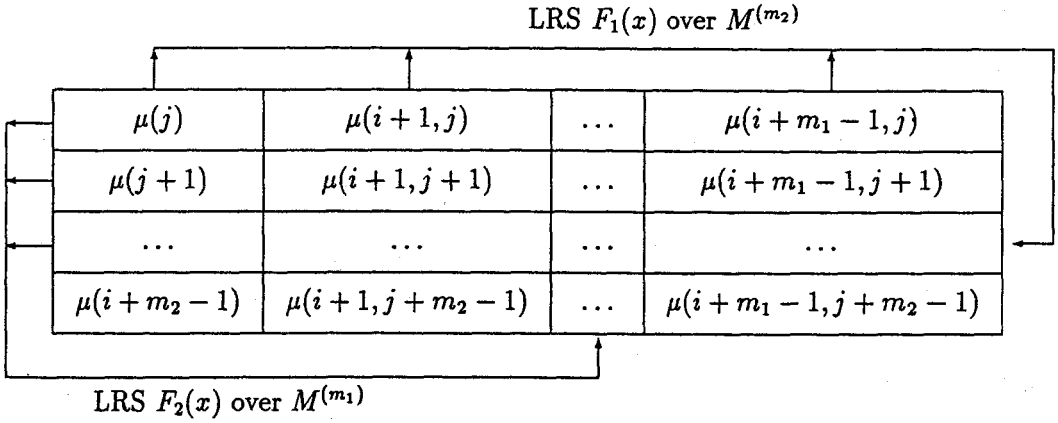
is the tensor product of R-modules, and $u = u_1 \otimes \dots \otimes u_k$.

1.26. The tensor product of 1-LRS over modules. Let $F_s(x)$, M_s, and μ_s be as in Example 1.23, and let $M = M_1 \underset{R}{\otimes} \dots \underset{R}{\otimes} M_k$. Define the k-sequence μ over M by $\mu(\mathbf{z}) = \mu_1(z_1) \otimes \dots \otimes \mu_k(z_k))$. Then $\mu \in L_M(F_1(x_1),\dots,F_k(x_k))$, the set of all such k-LRS μ (when $F_s(x)$, M_s are fixed) generates the R-module $L_M(F_1,\dots,F_k)$ and

$$L_M(F_1,\dots,F_k) = L_{M_1\otimes\dots\otimes M_k}(F_1,\dots,F_k) = L_{M_1}(F_1) \underset{R}{\otimes} \dots \underset{R}{\otimes} L_{M_k}(F_k).$$

Consequently, $\mu = \mu_1 \otimes \dots \otimes \mu_k$.

1.27. 2-linear shift register. Let $F_1(x)$, $F_2(x) \in R[x]$ be monic polynomials of degrees m_1 and m_2 respectively. Then any 2-LRS $\mu \in L_M(F_1(x), F_2(x))$ can be realized by means of the following circuit.



Denote by $\hat{\mu}(i,j)$ the $m_1 \times m_2$-matrix described by the storage locations of the circuit on the (i,j)-th step. Then

$$\hat{\mu}(i,j) = (S(F_2)^T)^j \cdot \hat{\mu}(0,0) \cdot S(F_1)^i,$$

where $S(F)$ is the accompanying matrix for $F(x)$ (see 1.9). Such sequences over finite fields were studied in [115, 116, 128, 143–146, 153–159].

2. Generating Systems of LRS-Families

A. 1-LRS-families [37, 46, 52, 105]. We fix a monic polynomial $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0 \in R[x]$ and consider the family $L_M(F)$. From (1.2), follows

2.1. Proposition. *Each recurrence $\mu \in L_M(F)$ is uniquely determined by its initial vector $\mu(\overline{0, m-1})$. A system $\{\mu_1, \ldots, \mu_n\} \subset L_M(F)$ of recurrences generates the R-module $L_M(F)$ if and only if the system of their initial vectors generates the R-module M^m of m-rows over M.* □

Let $e_0^F, \ldots, e_{m-1}^F$ be recurrences from $L_R(F)$ such that

$$\begin{pmatrix} e_0^F(\overline{0, m-1}) \\ \ldots \\ e_{m-1}^F(\overline{0, m-1}) \end{pmatrix} = E \tag{2.1}$$

(the identity matrix over R). As in [37, 127], we call $e^F = e_{m-1}^F$ the *impulse sequence*. It follows from (2.1) and (1.2) that

$$S(F)^i = \begin{pmatrix} e_0^F(\overline{i, i+m-1}) \\ \ldots \\ e_{m-1}^F(\overline{i, i+m-1}) \end{pmatrix}. \tag{2.2}$$

Let $M[x]$ be the $\mathcal{P}$-module of polynomials over M with natural multiplication of $H(x) \in \mathcal{P}$ on $\Phi(x) \in M[x]$. If $M = R\alpha_1 + \ldots + R\alpha_r$, then $M[x] = \mathcal{P}\alpha_1 + \ldots + \mathcal{P}\alpha_r$. Considering M as an R-bimodule, define the product of a polynomial $\Phi(x) = \sum \varphi_i x^i \in M[x]$ on a sequence $u \in R^{\langle 1 \rangle}$ by

$$\Phi(x)u = \mu, \qquad \mu \in M^{\langle 1 \rangle}, \qquad \mu(z) = \sum \varphi_i u(z+i).$$

It is evident that $M[x]L_R(F) \subset L_M(F)$.

2.2. Proposition. *Let $M = R\alpha_1 + \ldots + R\alpha_r$. Then*

$$L_M(F) = \sum_{t=0}^{m-1} \sum_{s=1}^{r} Re_t^F \alpha_s = \sum_{s=1}^{r} L_R(F)\alpha_s = e_0^F M \dot{+} \ldots \dot{+} e_{m-1}^F M, \tag{2.3}$$

$$L_M(F) = \mathcal{P}e^F\alpha_1 + \ldots + \mathcal{P}e^F\alpha_r = M[x]e^F = M[x]L_R(F). \tag{2.4}$$

If M is a free R-module of rank r, then $L_M(F)$ is a free R-module of rank mr. If R is an Artinian ring, then $\partial_{\mathcal{P}}(L_M(F)) = \partial_R(M)$, $\partial_R(L_M(F)) = m\partial_R(M)$ (see. 1.6).

□ (2.3) follows from (2.1) and 2.1. It also follows from 2.1 that $e^F, xe^F, \ldots, x^{m-1}e^F$ is a basis of a free R-module $L_R(F)$, and $L_R(F) = \mathcal{P}e^F$. This implies (2.4). The proof of the latter equalities is reduced to a local Artinian ring and to its residue field (see Section 15). □

Any polynomial $\Phi(x) \in M[x]$ can be uniquely divided by a monic polynomial $F(x) \in \mathcal{P}$; denote the remainder by $\operatorname{Res}(\Phi(x)/F(x))$.

2.3. Proposition. (a) *Any recurrence $\mu \in L_M(F)$ is uniquely represented in the form*

$$\mu = \Phi(x)e^F, \qquad \Phi(x) \in M[x], \qquad \deg \Phi(x) < m. \tag{2.5}$$

The polynomial $\Phi(x) = \Phi_\mu(x)$ in this representation is called the generator of the LRS μ (relatively to the characteristic polynomial $F(x)$) [113], *and has the following form:*

$$\Phi_\mu(x) = \mu(0)x^{m-1} + \sum_{s=1}^{m-1} (\mu(s) - f_{m-1}\mu(s-1) - \ldots - f_{m-s}\mu(0))x^{m-1-s}. \tag{2.6}$$

(b) *The generator of a sequence* $\nu \in L_M(F)$ *such that* $\nu = H(x)\mu$, $H(x) \in \mathcal{P}$ *is given by*

$$\Phi_\nu(x) = \operatorname{Res}(H(x)\Phi_\mu(x)/F(x)). \tag{2.7}$$

In particular, $\mu(i)$ *is the coefficient of* x^{m-1} *in the polynomial* $\operatorname{Res}(x^i\Phi_\mu(x)/F(x))$.

(c) *A sequence* $u \in L_R(F)$ *satisfies the condition* $L_M(F) = M[x]u$ *if and only if* $F(x)M[x]+\Phi_u(x)M[x] = M[x]$, *i.e., polynomials* $F(x)$ *and* $\Phi_u(x)$ *are* $M[x]$*-comaximal.*

□ (a) Representation (2.5) stems from (2.4) and from the main property of the impulse sequence: $\operatorname{An}_{\mathcal{P}}(e^F) = \mathcal{P}F(x)$. To prove (2.6) it is sufficient to note that $\mu = \mu(0)e_0^F + \ldots + \mu(m-1)e_{m-1}^F$. Hence, $\Phi_\mu(x) = \mu(0)\Phi_0(x) + \ldots + \mu(m-1)\Phi_{m-1}(x)$, where

$$\Phi_s(x) = \Phi_{e_s^F}(x) = x^{m-s-1} - f_{m-1}x^{m-s-2} - \ldots - f_{s+2}x - f_{s+1}.$$

For other proofs of this equality and those of (b), (c), see [46, 113]. □

2.4. Example. Let $\operatorname{tr}(A) = a_{11} + \ldots + a_{mm}$ be the trace of a matrix $A = (a_{ij})_{m\times m}$ over a ring R. Then for the sequence $\sigma^F \in R^{\langle 1\rangle}$ of elements $\sigma^F(i) = \operatorname{tr}(S(F)^i)$, $i \in \mathbf{N}_0$, we have $\sigma^F \in L_R(F)$, $\Phi_{\sigma^F}(x) = F'(x)$ (the formal derivative with respect to x).

We now describe a system of generators of the family $L_M(I)$, where I is a finitely generated monic ideal of the form $I = (F(x), G_1(x), \ldots, G_n(x))$. Since $L_M(I) \subset L_M(F)$, then, by Proposition 2.1, in order to describe $L_M(I)$, it is sufficient to find conditions on the initial vector $\mu(\overline{0, m-1})$ of $\mu \in L_M(F)$, which are equivalent to $\mu \in L_M(I)$. Let

$$\operatorname{Res}(G_j(x)/F(x)) = g_0^{(j)} + \ldots + g_{m-1}^{(j)}x^{m-1}, \qquad j \in \overline{1, n},$$

$$\operatorname{Res}(x^t/F(x)) = c_0^{(t)} + \ldots + c_{m-1}^{(t)}x^{m-1}, \qquad t \in \overline{0, 2m-2}.$$

Consider the following linear forms on M^m:

$$l_t(y_0, \ldots, y_{m-1}) = c_0^{(t)}y_0 + \ldots + c_{m-1}^{(t)}y_{m-1}, \qquad t \in \overline{0, 2m-2}.$$

2.5. Proposition. *A sequence* $\mu \in L_M(F)$ *belongs to* $L_M(I)$ *if and only if the row* $\mu(\overline{0, m-1})$ *is a solution of the system of linear equations*

$$\begin{cases} \sum\limits_{s=1}^{m-1} g_s^{(j)} l_{i+s}(y_0, \ldots, y_{m-1}) = 0, \\ j \in \overline{1, n}, \quad i \in \overline{0, m-1}. \end{cases} \tag{2.8}$$

This system can also be written in the form

$$(y_0, \ldots, y_{m-1})(G_1(S(F)), \ldots, G_n(S(F))) = (0, \ldots, 0). \tag{2.9}$$

□ $\mu \in L_M(I) \Leftrightarrow \nu_s = 0$, $s \in \overline{1, n}$, where $\nu_s = G_s(x)\mu \Leftrightarrow \nu_s(\overline{0, m-1}) = (0, \ldots, 0)$, $s \in \overline{1, n} \Leftrightarrow$ (2.8). □

Thus, the construction of a system of generators of the R-module $L_M(I)$ is reduced to the construction of a system of generators of the R-module of solutions of the system of linear equations (2.8). Methods of solving such systems are described in [11, 12].

B. Systems of generators of k-LRS-families [12, 49, 67, 91, 128, 137, 143, 145, 146, 154–158]. Fix elementary polynomials $F_s(x_s) \in \mathcal{P}_k$, $s \in \overline{1, k}$. Let $m_s = \deg F_s(x_s)$. Consider the family $L_M(F_1, \ldots, F_k)$. Denote by $\leq$ the natural order on $\mathbf{N}_0$ and the induced partial order on $\mathbf{N}_0^k$. For $\mathbf{m} = (m_1, \ldots, m_k)$, $\mathbf{1} = (1, \ldots, 1)$, define a polyhedron

$$\Pi = \Pi(\mathbf{m}) = \{\mathbf{i} \in \mathbf{N}_0^k \mid \mathbf{i} \leq \mathbf{m} - \mathbf{1}\}.$$

For a sequence $\mu \in M^{\langle k\rangle}$ we define the *polyhedron of values* by

$$\mu(\Pi) = \{\mu(\mathbf{i}) \mid \mathbf{i} \in \Pi\}.$$

Let M^Π be the set of all such polyhedrons. Then M^Π is an R-module, isomorphic to the module ${}_RM^m$ of rows of length $m = m_1 \dots m_k$.

Introduce a lexicographical linear ordering $\preceq$ on $\mathbf{N}_0^k$. We write $\mathbf{i} \preceq \mathbf{j}$ for $\mathbf{i}, \mathbf{j} \in \mathbf{N}_0^k$, if in the sequence of integers

$$(j_1 + \dots + j_k) - (i_1 + \dots + i_k), \qquad j_1 - i_1, \dots, j_k - i_k$$

the first nonzero number is positive. Then all points of the polyhedron Π form a chain

$$\mathbf{0} = \mathbf{i}_0 \preceq \mathbf{i}_1 \preceq \dots \preceq \mathbf{i}_{m-1}. \tag{2.10}$$

The elements of the polyhedron of values $\mu(\Pi)$ are ordered in the same way. Thus, $\mu(\Pi)$ can be written as a vector $(\mu(\mathbf{0}), \mu(\mathbf{i}_1), \dots, \mu(\mathbf{i}_{m-1})) \in M^m$ of length m.

For $\mathbf{j} \in \mathbf{N}_0^k$ we set

$$H^{\mathbf{j}}(\mathbf{x}) = \prod_{s=1}^{m} \operatorname{Res}(x_s^{j_s}/F_s(x_s)) = \sum_{\mathbf{i} \in \Pi} h_{\mathbf{i}}^{\mathbf{j}} \mathbf{x}^{\mathbf{i}}. \tag{2.11}$$

2.6. Lemma. *For any $\mu \in L_M(F_1, \dots, F_k)$, $\mathbf{j} \in \mathbf{N}_0^k$, the value $\mu(\mathbf{j})$ is uniquely determined by the polyhedron $\mu(\Pi)$ of initial values by the following formula:*

$$\mu(\mathbf{j}) = \sum_{\mathbf{i} \in \Pi} h_{\mathbf{i}}^{\mathbf{j}} \mu(\mathbf{i}). \tag{2.12}$$

□ $\mu(\mathbf{j}) = \nu(\mathbf{0})$, where $\nu = \mathbf{x}^{\mathbf{j}}\mu = H^{\mathbf{j}}(\mathbf{x})\mu$. □

For $\mathbf{j} \in \Pi$, let $e_{\mathbf{j}}^{F_1, \dots, F_k} = e_{\mathbf{j}}^{\mathbf{F}}$ be the recurrence $u \in L_R(F_1, \dots, F_k)$, which has exactly one nonzero value $u(\mathbf{j}) = e$ in $u(\Pi)$. Obviously, $e_{\mathbf{j}}^{\mathbf{F}}(\mathbf{z}) = e_{j_1}^{F_1}(z_1) \dots e_{j_k}^{F_k}(z_k)$, i.e., in the notation of 1.24,

$$e_{\mathbf{j}}^{\mathbf{F}} = e_{j_1}^{F_1} \otimes \dots \otimes e_{j_k}^{F_k}. \tag{2.13}$$

As for a 1-LRS, we call $e^{\mathbf{F}} = e_{\mathbf{m}-\mathbf{1}}^{\mathbf{F}}$ the *impulse recurrence* from $L_R(F_1, \dots, F_k)$.

Let $M[\mathbf{x}] = M[x_1, \dots, x_k]$ be the $\mathcal{P}_k$-module of all polynomials over the module M of k variables with natural multiplication of polynomials from $\mathcal{P}_k$ on the polynomials from $M[\mathbf{x}]$.

2.7. Proposition. *If $M = R\alpha_1 + \dots + R\alpha_r$, then*

$$L_M(F_1, \dots, F_k) = \sum_{\mathbf{j} \in \Pi} \sum_{s=1}^{r} Re_{\mathbf{j}}^{\mathbf{F}} \alpha_s = \sum_{s=1}^{r} L_R(F_1, \dots, F_k)\alpha_s = \sum_{\mathbf{j} \in \Pi} \oplus e_{\mathbf{j}}^{\mathbf{F}} M, \tag{2.14}$$

$$L_M(F_1, \dots, F_k) = \mathcal{P}_k e^{\mathbf{F}} \alpha_1 + \dots + \mathcal{P}_k e^{\mathbf{F}} \alpha_r = M[\mathbf{x}] e^{\mathbf{F}} = M[\mathbf{x}] L_R(F_1, \dots, F_k). \tag{2.15}$$

If M is a free R-module of rank r, then $L_M(F_1, \dots, F_k)$ is a free R-module of rank mr. If R is an Artinian ring, then $\partial_{\mathcal{P}}(L_M(F_1, \dots, F_k)) = \partial_R(M)$, $\partial_R(L_M(F_1, \dots, F_k)) = m\partial_R(M)$.

□ The proof is analogous to the proof of 2.2. We take into account that the system of sequences

$$\{\mathbf{x}^{\mathbf{j}} e^{\mathbf{F}} \mid \mathbf{j} \in \Pi\} = \{e^{\mathbf{F}}, \mathbf{x}^{j_1} e^{\mathbf{F}}, \dots, \mathbf{x}^{j_{m-1}} e^{\mathbf{F}}\}$$

is a basis of the free R-module $L_R(F_1, \dots, F_k)$ (see [49, 137]). □

Let $\operatorname{Res}(H(\mathbf{x})/\mathbf{F})$ be the residue of the polynomial $H(\mathbf{x}) \in M[\mathbf{x}]$ modulo ideal $(F_1(x_1), \dots, F_k(x_k))$ (i.e., the result of k divisions with a remainder of $H(\mathbf{x})$ on $F_1(x_1), \dots, F_k(x_k)$).

2.8. Proposition. (a) *Any recurrence $\mu \in L_M(F_1, \dots, F_k)$ is uniquely represented in the form*

$$\mu = \Phi(\mathbf{x}) e^{\mathbf{F}}, \text{ where } \Phi(\mathbf{x}) \in M[\mathbf{x}], \qquad \deg_{x_s} \Phi(\mathbf{x}) < m_s, \qquad s \in \overline{1, k}. \tag{2.16}$$

The polynomial $\Phi(\mathbf{x}) = \Phi_\mu(\mathbf{x})$ in this representation, called the generator of μ, has the form

$$\Phi_\mu(\mathbf{x}) = \sum_{\mathbf{i} \in \Pi} \Big(\sum_{\mathbf{t} \le \mathbf{m}-\mathbf{i}-\mathbf{1}} \mu(\mathbf{t}) a_{t_1+i_1+1}^{(1)} \dots a_{t_k+i_k+1}^{(k)} \Big) \mathbf{x}^{\mathbf{i}}, \tag{2.17}$$

where $F_s(x_s) = \sum_{t\geq 0} a_t^{(s)} x_s^t$ *for* $s \in \overline{1,k}$.

(b) *If* $\nu = H(\mathbf{x})\mu$, *where* $H(\mathbf{x}) \in \mathcal{P}_k$, *then* $\Phi_\nu(\mathbf{x}) = \mathrm{Res}\,(H(\mathbf{x})\Phi_\mu(\mathbf{x})/\mathbf{F})$.

(c) *If* $u \in L_R(F_1,\ldots,F_k)$, *then* $L_M(F_1,\ldots,F_k) = M[\mathbf{x}]u$ *iff*

$$F_1(x_1)M[\mathbf{x}] + \ldots + F_k(x_k)M[\mathbf{x}] + \Phi_u(\mathbf{x})M[\mathbf{x}] = M[\mathbf{x}],$$

i.e., the polynomials $F_1,\ldots,F_k$, Φ_u *are* $M[x]$*-comaximal.*

□ (2.16) follows from (2.15) and from the condition $\mathrm{An}\,(e^{\mathbf{F}}) = (F_1(x_1),\ldots,F_k(x_k))$. Since $\mu = \sum_{\mathbf{i}\in\Pi} \mu(\mathbf{i}) e_{\mathbf{i}}^{\mathbf{F}}$, we have $\Phi_\mu(\mathbf{x}) = \sum_{\mathbf{i}\in\Pi} \mu(\mathbf{i})\Phi_{\mathbf{i}}(\mathbf{x})$, where $\Phi_{\mathbf{i}}(\mathbf{x}) = \Phi_{e_{\mathbf{i}}^{\mathbf{F}}}(\mathbf{x})$. Now (2.17) follows from (2.6) and from the equality $\Phi_{\mathbf{i}}(\mathbf{x}) = \Phi_{i_1}(x_1)\ldots\Phi_{i_k}(x_k)$, where $\Phi_{i_s}(x_s)$ is a generator of $e_{i_s}^{F_s}$, $s \in \overline{1,k}$. The last proposition is a consequence of Example 1.24 and of the relations

$$e_{\mathbf{i}}^{\mathbf{F}} = e_{i_1}^{F_1} \otimes \ldots \otimes e_{i_k}^{F_k} = \Phi_{i_1}(x_1)\ldots\Phi_{i_k}(x_k)\cdot(e^{F_1}\otimes\ldots\otimes e^{F_k})$$

$$= \Phi_{i_1}(x_1)\cdot\ldots\cdot\Phi_{i_k}(x_k)\cdot e^{\mathbf{F}}.\square$$

Now we describe the system of generators of the R-module $L_M(I)$ for an arbitrary monic finitely generated ideal $I \lhd \mathcal{P}_k$, satisfying (1.4). We may suppose that I has a system of generators of the form

$$F_1(x_1),\ldots,F_k(x_k), \qquad G_1(\mathbf{x}),\ldots,G_n(\mathbf{x}), \tag{2.18}$$

where

$$G_r(\mathbf{x}) = \sum_{\mathbf{i}\in\Pi} g_{r,\mathbf{i}}\mathbf{x}^{\mathbf{i}}, \qquad r \in \overline{1,n}. \tag{2.19}$$

Consider the set $\mathrm{Res}\,(I/\mathbf{F}) = \{\mathrm{Res}\,(H(\mathbf{x})/\mathbf{F}(\mathbf{x})|\ H(\mathbf{x}) \in I\}$.

2.9. Lemma. *The set* $\mathrm{Res}\,(I/\mathbf{F})$ *is the* R*-module generated by*

$$G_r^{\mathbf{u}}(\mathbf{x}) = \mathrm{Res}\,(\mathbf{x}^{\mathbf{u}}G_r(\mathbf{x})/\mathbf{F}), \qquad \mathbf{u}\in\Pi, \qquad r\in\overline{1,n}. \tag{2.20}$$

In the notations of (2.11), (2.19),

$$G_r^{\mathbf{u}}(\mathbf{x}) = \sum_{\mathbf{i}\in\Pi} g_{r,\mathbf{i}}^{\mathbf{u}}\mathbf{x}^{\mathbf{i}}, \text{ where } g_{r,\mathbf{i}}^{\mathbf{u}} = \sum_{\mathbf{j}\in\Pi} g_{r,\mathbf{j}}h_{\mathbf{i}}^{\mathbf{u}+\mathbf{j}}.\square$$

2.10. Proposition. *Let*

$$H_1(\mathbf{x}),\ldots,H_w(\mathbf{x}) \tag{2.21}$$

be a system of generators of the R*-module* $\mathrm{Res}\,(I/\mathbf{F})$, *and*

$$H_v(\mathbf{x}) = \sum_{\mathbf{i}\in\Pi} h_{v,\mathbf{i}}\mathbf{x}^{\mathbf{i}}, \qquad v\in\overline{1,w}.$$

Then a k*-LRS* $\mu \in L_M(F_1(x_1),\ldots,F_k(x_k))$ *belongs to* $L_M(I)$ *iff its polyhedron of initial values* $\mu(\Pi)$ *is a solution of the system of linear equations*

$$\Big\{\sum_{\mathbf{i}\in\Pi} h_{v,\mathbf{i}}x(\mathbf{i}) = 0, \qquad v\in\overline{1,w}, \tag{2.22}$$

where $\{x(\mathbf{i})|\ \mathbf{i}\in\Pi\}$ *is a system of independent indeterminates in* M.

□ (2.22) is equivalent to

$$\Big\{\sum_{\mathbf{i}\in\Pi} g_{r,\mathbf{i}}^{\mathbf{u}}x(\mathbf{i}) = 0, \qquad \mathbf{u}\in\Pi, \qquad r\in\overline{1,n}. \tag{2.23}$$

Let $\delta_r = G_r(\mathbf{x})\mu$. Then $\mu \in L_M(I)$ iff $\delta_1 = \ldots = \delta_n = 0$, i.e., $\delta_r(\Pi) = 0$, $r \in \overline{1,n}$. This means that $\mu(\Pi)$ is a solution of (2.23), since $\delta_r(\mathbf{u}) = \sum_{\mathbf{i}\in\Pi} g_{r,\mathbf{i}}^{\mathbf{u}}\mu(\mathbf{i})$. □

2.11. Corollary. *Let $\mu'_1, \ldots, \mu'_l \in M^{\Pi}$ be a system of generators of the R-module of solutions of the system of linear equations* (2.22). *Then the set $\{\mu_1, \ldots, \mu_l\} \subset L_M(F_1, \ldots, F_k)$ of recurrences with initial values $\mu_t(\Pi) = \mu'_t$, $t \in \overline{1,l}$, generates the R-module $L_M(I)$.* □

2.12. Proposition. *Let M be a finitely generated module over a Noetherian ring R. Then for any monic ideal $I \lhd \mathcal{P}_k$ the family $L_M(I)$ is a finitely generated over R $\mathcal{P}_k$-submodule of module $\mathcal{L}M^{(k)}$. For any submodule $\mathcal{M}$ of the $\mathcal{P}_k$-module $M^{(k)}$, the following conditions are equivalent:*

(a) *$\mathcal{M}$ is a finitely generated R-module;*

(b) *$\mathcal{M}$ is a finitely generated submodule of the $\mathcal{P}_k$-module $\mathcal{L}M^{(k)}$;*

(c) $\mathrm{An}(\mathcal{M})$ *is a monic ideal.*

□ (a) $\Rightarrow$ (b) Any k-sequence $\mu \in \mathcal{M}$ is an LRS. Actually, for any $s \in \overline{1,k}$ the R-submodule $(\mu, x_s\mu, x_s^2\mu, \ldots)_R$ of $\mathcal{M}$ is finitely generated. Therefore, $x_s^{m_s}\mu \in (\mu, x_s\mu, \ldots, x_s^{m_s-1}\mu)$ for some $m_s \in \mathbb{N}$, i.e., μ is annihilated by the elementary polynomial $F_s(x_s) \in \mathcal{P}_k$ of degree m_s.

(b) $\Rightarrow$ (c) By the condition, $\mathcal{M} = \mathcal{P}_k\mu_1 + \ldots + \mathcal{P}_k\mu_l$ and $\mathrm{An}(\mu_t)$ is a monic ideal for $t \in \overline{1,l}$. Then $\mathrm{An}(\mathcal{M})$ contains the monic ideal $\mathrm{An}(\mu_1) \ldots \mathrm{An}(\mu_l)$.

(c) $\Rightarrow$ (a) Suppose that $\mathrm{An}(\mathcal{M})$ contains an elementary ideal $(F_1(x_1), \ldots, F_k(x_k))$. Then $\mathcal{M} \subset L_M(\mathrm{An}(\mathcal{M})) \subset L_M(F_1, \ldots, F_k)$. The last R-module is finitely generated by 2.7. □

C. Generating function of a k-LRS.

2.13. Definition. The *generating function* of a k-sequence $\mu \in M^{(k)}$ is formal power series

$$\mathfrak{S}_\mu(\mathbf{x}) = \sum_{\mathbf{i} \in \mathbb{N}_0^k} \mu(\mathbf{i})\mathbf{x}^{\mathbf{i}}$$

from the $\mathcal{P}_k$-module $M[[\mathbf{x}]]$ of all formal power series over M.

A description of the generating function of an LRS is closely connected with its generator and characteristic polynomial. For LRS over a field, such a description was obtained in [91]. In the general case we have

2.14. Proposition. *The generating function of a k-LRS $\mu \in \mathcal{L}M^{(k)}$ with elementary characteristic polynomials $F_1(x_1), \ldots, F_k(x_k)$ is the rational function*

$$\mathfrak{S}_\mu(\mathbf{x}) = \frac{\Phi^*_\mu(\mathbf{x})}{F_1^*(x_1) \ldots F_k^*(x_k)},$$

where $F_s^*(x_s) = x_s^{m_s} F_s(1/x_s)$, $s \in \overline{1,k}$, and $\Phi^*_\mu(\mathbf{x}) = \mathbf{x}^{\mathbf{m}-\mathbf{1}}\Phi_\mu(1/x_1, \ldots, 1/x_k)$. Conversely, if the generating function of a k-sequence $\mu \in M^{(k)}$ has the form

$$\mathfrak{S}_\mu(\mathbf{x}) = \frac{\sum_{\mathbf{i} \in \Pi(\mathbf{m})} \alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}}{\prod_{s=1}^k (e + b_1^{(s)}x_s + \ldots + b_{m_s}^{(s)}x_s^{m_s})}.$$

then μ is a k-LRS with elementary characteristic ideal

$$(x_1^{m_1} + b_1^{(1)}x_1^{m_1-1} + \ldots + b_{m_1}^{(1)}, \ldots, x_k^{m_k} + b_1^{(k)}x_k^{m_k-1} + \ldots + b_{m_k}^{(k)})$$

and with generator

$$\Phi_\mu(\mathbf{x}) = \sum_{\mathbf{i} \in \Pi(\mathbf{m})} \alpha_{\mathbf{m}-\mathbf{i}-\mathbf{1}}\mathbf{x}^{\mathbf{i}}.$$

□ In both cases, the proof consists in multiplying the series $\mathfrak{S}_\mu(\mathbf{x})$ by the denominator of the fraction from the right part. □

D. Binomial basis and analytical representation of recurrences [29, 37, 47, 70, 91]. Here we consider the situation where an LRS $\mu \in L_M(F_1(x_1), \ldots, F_k(x_k))$ can be represented as an explicit function of

i. A long list of papers on this problem starts with the Fibonacci sequence and is essentially a generalization of the properties of arithmetical and geometrical progressions (Examples 1.2, 1.3, 1.18, 1.19).

2.15. Definition. For $a \in R$, $l \in \mathbf{N}_0$, the sequence $a^{[l]} \in R^{(1)}$, defined by

$$a^{[l]}(\overline{0,l}) = (0,\dots,0,e), \qquad a^{[l]}(i) = \binom{i}{l} \cdot a^{i-l} \text{ for } i > l,$$

is called the *binomial sequence* of order $l+1$ with root a. In particular,

$$0^{[l]} = (0,\dots,0,e,0,0,\dots),$$

$$e^{[l]} = \Big(0,\dots,0,e,\binom{l+1}{l}e,\binom{l+2}{l}e,\dots\Big).$$

The binomial identity $\binom{i+1}{l} - \binom{i}{l} = \binom{i}{l-1}$ implies that $(x-a)a^{[l]} = a^{[l-1]}$, $l \geq 1$, and, further, we have the following

2.16. Lemma. *The sequence $a^{[l]}$ is an impulse LRS with minimal polynomial $G(x) = (x-a)^{l+1}$, i.e., $a^{[l]} = e^G$, and $\operatorname{An}(a^{[l]}) = \mathcal{P}G(x)$, $L_R((x-a)^{l+1}) = \mathcal{P}a^{[l]} = Ra^{[0]} \dotplus \dots \dotplus Ra^{[l]}$.* □

2.17. Definition. We say that a polynomial $F(x) \in \mathcal{P}$ has a *canonical linear decomposition* over R if

$$F(x) = (x-a_1)^{l_1+1}\dots(x-a_t)^{l_t+1}, \tag{2.24}$$

where $x-a_1,\dots,x-a_t \in \mathcal{P}$ are pairwise comaximal (i.e., $a_i - a_j \in R^*$ for $i \neq j$).

2.18. Theorem. *If a monic polynomial $F(x) \in \mathcal{P}$ has a canonical linear decomposition* (2.24), *then the set of binomial sequences*

$$a_1^{[0]},\dots,a_1^{[l_1]},a_2^{[0]},\dots,a_t^{[l_t]}$$

is a basis of the free R-module $L_R(F)$, and every recurrence $u \in L_R(F)$ can be uniquely represented in the form

$$u(i) = \sum_{s=1}^{t}\sum_{l=0}^{l_s} c_{sl}\binom{i}{l}a_s^{i-l}, \qquad i \geq 0. \tag{2.25}$$

Here the coefficients $c_{sl} \in R$ are the unique solution of the system of linear equations

$$\sum_{s=1}^{t}\sum_{l=0}^{l_s} c_{sl}a_s^{[l]}(\overline{0,m-1}) = u(\overline{0,m-1}),$$

where $m = l_1 + \dots + l_t + t = \deg F(x)$.

□ Since $x-a_i$, $x-a_j$ are relatively prime, $L_R(F) = L_R((x-a_1)^{l_1+1}) \dotplus \dots \dotplus L_R((x-a_t)^{l_t+1})$ (see Section 4 below). By Lemma 2.16, u can be uniquely represented in the form

$$u = \sum_{s=1}^{t} u_s = \sum_{s=1}^{t}\sum_{l=0}^{l_s} c_{sl}a_s^{[l]}, \qquad c_{sl} \in R. \quad \square \tag{2.26}$$

As an example of decomposition (2.25), consider the Fibonacci sequence over $\mathbf{Z}$ (see 1.5):

$$u(i) = \frac{1}{\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^i - \frac{1}{\sqrt{5}}\Big(\frac{1-\sqrt{5}}{2}\Big)^i.$$

Under conditions of Theorem 2.18, we call the decomposition (2.25) (or (2.26)) an *analytical representation of the* LRS u.

2.19. Proposition. *Let u have an analytical representation* (2.26), *and let $c_s \in R^{(1)}$ be sequences of the form $c_s = (c_{s0}, c_{s1}, \dots, c_{s,l_s}, 0, 0, \dots)$, $s \in \overline{1,t}$. Then*

$$\operatorname{An}(u_s) = \{H(x) \in \mathcal{P} |\ H(x + a_s) \in \operatorname{An}(c_s)\}, \tag{2.27}$$

$$\operatorname{An}(u) = \operatorname{An}(u_1) \cdot \ldots \cdot \operatorname{An}(u_t).$$

In particular, if x^{m_s} is a minimal polynomial of the LRS c_s, then rank $u = m_1 \dots m_t$, and $(x - a_1)^{m_1} \cdot \ldots \cdot (x - a_t)^{m_t}$ is a minimal polynomial of the LRS u.

□ For $G(x) \in \mathcal{P}$, by (2.26), $G(x - a_s)u_s = \sum_{l=0}^{l_s} v_s(l) a_s^{[l]}$, where $v_s = G(x)c_s$. Hence, $G(x - a_s)u_s = 0$ iff $v_s(0) = \ldots = v_s(l_s - 1) = 0$, i.e., if $v_s = G(x)c_s = 0$. This implies (2.27). □

In the general case we have

2.20. Theorem. *Let $F_1(x_1), \dots, F_k(x_k)$ be monic polynomials over R with canonical linear decompositions*

$$F_r(x) = (x - a_{r1})^{l_{r1}+1} \cdot \ldots \cdot (x - a_{r,t_r})^{l_{r,t_r}+1}, \qquad r \in \overline{1,k}.$$

Let $M = R\alpha_1 + \ldots + R\alpha_n$. Then the R-module $L_M(F_1(x_1), \dots, F_k(x_k))$ is generated by the system of sequences

$$a_{1s_1}^{[l_1]} \otimes \ldots \otimes a_{ks_k}^{[l_k]} \alpha_j, \qquad 1 \le s \le t, \qquad 0 \le l \le l_s = (l_{1s_1}, \dots, l_{ks_k}), \qquad j \in \overline{1,n}.$$

□ It follows from (2.14) and 1.24 that

$$L_M(F_1, \dots, F_k) = \sum_{j=1}^{n} L_R(F_1) \otimes \ldots \otimes L_R(F_k)\alpha_j.$$

Now our theorem follows from 2.18. □

Thus, for any recurrence $\mu \in L_M(F_1, \dots, F_k)$ there exist coefficients $\{c_{s,j}^{l}\} \subset R$ (with limitations to indexes as in 2.20) such that

$$\mu(i) = \sum_{j,s,l} c_{s,j}^{l} \binom{i_1}{l_1} \cdots \binom{i_k}{l_k} a_{1s_1}^{i_1 - l_1} \cdots a_{ks_k}^{i_k - l_k} \alpha_j. \tag{2.28}$$

2.21. Definition. Decomposition (2.28) is called an *analytical representation of the k-LRS μ* over the module M.

2.22. Remark. It is quite possible (see Section 15) that $F_1, \dots, F_k$ have no canonical linear decompositions over R, but there exists an extension S of R and monic polynomials $G_1(x), \dots, G_k(x) \in S[x]$ such that $G_r(x)$ has a canonical linear decomposition over S and $F_r(x) | G_r(x)$ for $r \in \overline{1,k}$. In this case, any sequence $u \in L_R(F_1, \dots, F_k)$ lies in $L_S(G_1, \dots, G_k)$ and has an analytical representation over S.

Now let $\mu \in L_M(F_1, \dots, F_k)$ be a sequence over an R-module M. Sometimes we can get an analytical representation of μ. For example, suppose that the R-module homomorphism $\varphi : M \to S \underset{R}{\otimes} M$, where $\varphi(\alpha) = e \otimes \alpha$, is a monomorphism (for example, if M is a flat (projective, free) R-module [14, 16, 169], or if ${}_RR$ is a direct summand of ${}_RS$). Then any sequence $\mu \in M^{(k)}$ can be considered as a k-sequence over the S-module $S \underset{R}{\otimes} M$ if we identify M and $\varphi(M)$. In this situation, μ has an analytical representation over the S-module $S \underset{R}{\otimes} M$.

3. Generating Systems of LRS-Annihilators

In the general case, it is quite a difficult problem to obtain a description of the annihilator $\operatorname{An}(\mu)$ of a k-sequence $\mu \in M^{(k)}$ (even for $k = 1$, $M = R$). For example, there exists no algorithm of verification of the equality $\operatorname{An}(\mu) = 0$ if we do not have some additional information about μ. But if we know that μ is an

LRS with elementary characteristic polynomials of degrees $m_1, \ldots, m_k$, then we can reduce the description of $\mathrm{An}(\mu)$ to the solution of a system of linear equations over M.

A. Description of the annihilator of a 1-LRS [12, 37, 46, 52, 91, 136].

3.1. Definition. The matrix

$$\mathcal{G}_m(\mu) = \begin{pmatrix} \mu(0) & \ldots & \mu(m-1) \\ \mu(1) & \ldots & \mu(m) \\ \ldots & \ldots & \ldots \\ \mu(m-1) & \ldots & \mu(2m-2) \end{pmatrix} = \begin{pmatrix} \mu(\overline{0, m-1}) \\ \mu(\overline{1, m}) \\ \ldots \\ \mu(\overline{m-1, 2m-2}) \end{pmatrix}$$

is called the *Hankel matrix* of order m of the sequence $\mu \in M^{(1)}$.

3.2. Proposition. *A polynomial $A(x) = \sum_{j=0}^{m-1} a_j x^j \in \mathcal{P}$ annihilates a sequence $\mu \in M^{(1)}$ if and only if*

$$(a_0, \ldots, a_{m-1})\mathcal{G}_m(x^t\mu) = (0, \ldots, 0) \text{ for any } t \in \mathbb{N}_0.$$

If μ is an LRS of order m, then this condition holds if and only if $(a_0, \ldots, a_{m-1})$ is a solution in $R^{(m)}$ of the system of linear equations

$$(y_0, \ldots, y_{m-1})\mathcal{G}_m(\mu) = (0, \ldots, 0). \tag{3.1}$$

Moreover, $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0 \in \mathcal{P}$ is a characteristic polynomial of μ if and only if $(f_0, \ldots, f_{m-1})$ is a solution of the system

$$(f_0, \ldots, f_{m-1})\mathcal{G}_m(\mu) = \mu(\overline{m, 2m-1}). \tag{3.2}$$

If the R-module $\mathcal{K}(\mathcal{G}_m(\mu))$ of all solutions of (3.1) in $R^{(m)}$ is generated by the system of rows $A_s = (a_{s0}, \ldots, a_{s,m-1})$, $s \in \Omega$, then $\mathrm{An}(\mu) =_{\mathcal{P}} (F(x), A_s(x), s \in \Omega)$, where $A_s(x) = \sum_{j=0}^{m-1} a_{sj}x^j$. □

If we know a characteristic polynomial $F(x) \in \mathcal{P}$ of $\mu \in \mathcal{L}M^{(1)}$, then we can describe $\mathrm{An}(\mu)$ in terms of the generator $\Phi_\mu(x)$ of μ.

3.3. Lemma. *For any monic polynomial $F(x) \in \mathcal{P}$ the annihilator $\mathrm{An}_{M[x]}(e^F)$ of the impulse recurrence e^F in the module $M[x]$ is given by $\mathrm{An}_{M[x]}(e^F) = F(x)M[x]$.*

□ It is sufficient to note that $\mathrm{An}_{M[x]}(e^F) \supset F(x)M[x]$ and that e^F is not annihilated by polynomials from $M[x]$ of degree less than $\deg F(x)$. □

3.4. Proposition. *The annihilator of the recurrence $\mu \in L_M(F)$ is given by*

$$\mathrm{An}(\mu) = (F(x)M[x] : \Phi_\mu(x)) = \{H(x) \in \mathcal{P} \mid H(x)\Phi_\mu(x) \in F(x)M[x]\}.$$

In particular, if $F(x)$ and $\Phi_\mu(x)$ are $M[x]$-comaximal, i.e.,

$$F(x)M[x] + \mathcal{P}\Phi_\mu(x) = M[x], \tag{3.3}$$

then

$$\mathrm{An}(\mu) = \mathcal{P}F(x). \tag{3.4}$$

For any $\mu \in M^{(1)}$ the condition (3.4) is equivalent to each of the following conditions:

(a) *μ is an LRS with unique minimal polynomial $F(x)$;*

(b) *the system of rows of the matrix $\mathcal{G}_m(\mu)$ is free over R and $(f_0, \ldots, f_{m-1})$ is a solution of (3.2).* □

3.5. Corollary. *If R is a field, then any LRS $u \in L_R(F)$ has a unique minimal polynomial $M_u(x) \in \mathcal{P}$, and*

$$M_u(x) = \frac{F(x)}{(F(x), \Phi_u(x))}. \tag{3.5}$$

B. Annihilators of k-LRS-families [12, 49, 91, 128, 137, 143, 146, 156, 158]. We are going to describe a system of generators of the annihilator $\mathrm{An}(\mathcal{M})$ of the family

$$\mathcal{M} = \mathcal{P}_k\nu_1 + \ldots + \mathcal{P}_k\nu_l \tag{3.6}$$

for given $\nu_1, \dots, \nu_l \in \mathcal{LM}^{(k)}$. Suppose that we know the degrees $m_1, \dots, m_k$ of some elementary characteristic polynomials $F_1(x_1), \dots, F_k(x_k)$ of the family $\mathcal{M}$. Then we can evaluate these polynomials. For example, the row $(f_0^{(1)}, \dots, f_{m_1-1}^{(1)})$ of coefficients of the polynomial $F_1(x_1) = x_1^{m_1} - f_{m_1-1}^{(1)} x^{m_1-1} - \dots - f_0^{(1)} \in R[x_1]$ is a solution of the following system of $lm_1 \dots m_k$ linear equations over M:

$$\begin{cases} (y_0, \dots, y_{m-1})\mathcal{G}_{m_1}(\mu_t(z_1, i_2, \dots, i_k)) = \mu_t(\overline{m_1, 2m_1 - 1}, i_2, \dots, i_k), \\ t \in \overline{1,l}, \ \ (i_2, \dots, i_k) \in \Pi(m_2, \dots, m_k). \end{cases}$$

where, for a given $t \in \overline{1,l}$ and $(i_2, \dots, i_k) \in \Pi(m_2, \dots, m_k)$, the sequence $\mu_t(z_1, i_2, \dots, i_k)$ is a 1-LRS, obtained from the k-LRS $\mu_t(\mathbf{z})$ by fixing of $z_2, \dots, z_k$.

Suppose that we have already found polynomials

$$F_1(x_1), \dots, F_k(x_k) \in \mathrm{An}\,(\mathcal{M}). \tag{3.7}$$

Let R be Noetherian. Then the system of generators of $\mathrm{An}\,(\mathcal{M})$ is the finite set of polynomials

$$F_1(x_1), \dots, F_k(x_k), \qquad H_1(\mathbf{x}), \dots, H_w(\mathbf{x}) \tag{3.8}$$

where $H_1(\mathbf{x}), \dots, H_w(\mathbf{x})$ is the system of generators of the R-module $\mathrm{Res}\,(\mathrm{An}\,(\mathcal{M})/\mathbf{F})$ (see Section 2B). Note that, by (3.6) and (3.7), $\mathcal{M}$ is an f.g.-R-module generated by

$$\nu_s^{\mathbf{u}} = \mathbf{x}^{\mathbf{u}} \nu_s, \qquad \mathbf{u} \in \Pi = \Pi(m_1, \dots, m_k), \qquad s \in \overline{1,l} \tag{3.9}$$

and, by (3.7), (2.11),

$$\nu_s^{\mathbf{u}}(\mathbf{j}) = \sum_{\mathbf{i} \in \Pi} \nu_s(\mathbf{i}) h_{\mathbf{i}}^{\mathbf{u}+\mathbf{j}}, \qquad \mathbf{j} \in \mathbb{N}_0^k, \qquad \mathbf{u} \in \Pi, \qquad s \in \overline{1,l} \tag{3.10}$$

3.6. Proposition. *Let $\nu_1, \dots, \nu_l$ be a set of generators of $\mathcal{P}_k$-module $\mathcal{M}$. Then the polynomial $H(\mathbf{x}) = \sum_{\mathbf{i} \in \Pi} h_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \in \mathcal{P}_k$ belongs to $\mathrm{An}\,(\mathcal{M})$ if and only if the polyhedron $H_\Pi = \{h_{\mathbf{i}} | \ \mathbf{i} \in \Pi\}$ of its coefficients is a solution of the following system of linear equations over M:*

$$\Big\{ \sum_{\mathbf{i} \in \Pi} y_{\mathbf{i}} \mu_s(\mathbf{i}) = 0, \qquad s \in \overline{1,l}. \tag{3.11}$$

where $\{y_{\mathbf{i}} | \ \mathbf{i} \in \Pi\}$ is a system of independent variables in R. If $H_{1\Pi}, \dots, H_{w\Pi}$ is a system of generators of the module of solutions in R^Π of system (3.11)*, then the system of polynomials* (3.8) *generates* $\mathrm{An}\,(\mathcal{M})$.

□ Let $\delta_s = H(\mathbf{x})\nu_s$, $s \in \overline{1,l}$. Then $H(\mathbf{x}) \in \mathrm{An}\,(\mathcal{M})$ iff $\delta_s(\mathbf{u}) = 0$ for $\mathbf{u} \in \Pi$, $s \in \overline{1,l}$. Since $\delta_s(\mathbf{u}) = \sum_{\mathbf{i} \in \Pi} h_{\mathbf{i}} \nu_s^{\mathbf{u}}(\mathbf{i})$, the last condition is true iff H_Π is a solution of the system

$$\Big\{ \sum_{\mathbf{i} \in \Pi} y_{\mathbf{i}} \nu_s^{\mathbf{u}}(\mathbf{i}) = 0, \qquad \mathbf{u} \in \Pi, \qquad s \in \overline{1,l}.$$

which is equivalent to the system (3.11). □

Analogously to 3.4, the annihilator of any k-LRS μ can be described in terms of the generator $\Phi_\mu(\mathbf{x})$.

3.7. Lemma. *For any set of elementary polynomials $F_1(x_1), \dots, F_k(x_k) \in \mathcal{P}_k$ the annihilator of the impulse recurrence $e^{\mathbf{F}}$ in $M[\mathbf{x}]$ is given by*

$$\mathrm{An}_{M[\mathbf{x}]}(e^{\mathbf{F}}) = F_1(x_1)M[\mathbf{x}] + \dots + F_k(x_k)M[\mathbf{x}].$$

□ The definition of $e^{\mathbf{F}}$ implies that $e^{\mathbf{F}}$ is not annihilated by the polynomial $\Phi(\mathbf{x}) \in M[\mathbf{x}]$ of the form $\Phi(\mathbf{x}) = \sum_{\mathbf{i} \in \Pi} \alpha_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$. □

3.8. Proposition. *The annihilator of LRS $\mu \in L_M(F_1(x_1), \dots, F_k(x_k))$ in $\mathcal{P}_k$ is given by*

$$\mathrm{An}\,(\mu) = (F_1(x_1)M[\mathbf{x}] + \dots + F_k(x_k)M[\mathbf{x}] : \ \Phi(\mathbf{x})).$$

If polynomials $F_1(x_1), \dots, F_k(x_k)$, $\Phi_\mu(\mathbf{x})$ *are* $M[\mathbf{x}]$*-comaximal, then* $\operatorname{An}(\mu) = (F_1(x_1), \dots, F_k(x_k))$. □

C. k-LRS with a given annihilator. Note that if R is a field, then any monic ideal $I \lhd \mathcal{P}$ is the annihilator of some LRS over R: if $I = \mathcal{P}F(x)$, then $I = \operatorname{An}(e^F)$. But if R is not a field, this is not true. For example, there is no sequence $u \in \mathbf{Z}^{(1)}$ such that $\operatorname{An}(u) = (x, 2)$. Thus, we have the following problem: a system of generators of a monic ideal $I \lhd \mathcal{P}_k$, is given, and it is necessary to find a k-sequence $u \in \mathcal{L}R^{(k)}$ with $\operatorname{An}(u) = I$, or to prove that there exists no such u. This problem was solved only for Artinian rings of principal ideals [46] (see Section 16). An analogous problem can be formulated for linear recurrences over a module ${}_RM$. We mention some results in this area in Section 4. Here we formulate

3.9. Proposition. *Let* $I \lhd \mathcal{P}_k$ *be a monic ideal,* $S = \mathcal{P}_k/I$, $\theta_s = x_s + I \in S$ *for* $s \in \overline{1,k}$. *Then the sequence* μ *over the module* ${}_RS$ *of the form* $\mu(\mathbf{z}) = \theta^{\mathbf{z}} = \theta_1^{z_1} \dots \theta_k^{z_k}$ *is a* k*-LRS, and* $\operatorname{An}(\mu) = I$.

□ Let $H(\mathrm{x}) \in \mathcal{P}_k$ and $\nu = H(\mathrm{x})\mu$. Then $\nu(\mathbf{z}) = H(\theta)\theta^{\mathbf{z}}$. Therefore, $\nu = 0 \Leftrightarrow H(\theta) = 0 \Leftrightarrow H(\mathrm{x}) \in I$. □

4. Some Relations between LRS-Families and Their Annihilators

A. The 1-LRS families over a field. The relations which we consider below in this section are generalizations of the following well-known relations for 1-LRS families over a field P (see, for example, [36, 46]).

4.1. Theorem. *For any monic polynomials* $F(x)$, $G(x) \in \mathcal{P} = P[x]$, *the following equalities hold:*

$$L_P(F) + L_P(G) = L_P([F, G]); \tag{4.1}$$

$$L_P(F) \cap L_P(G) = L_P((F, G)). \tag{4.2}$$

Any 1-LRS family $\mathcal{M}$ *over the field* P *has the form* $\mathcal{M} = L_P(F)$ *for some monic polynomial* $F(x) \in \mathcal{P}$ *and is a cyclic* $\mathcal{P}$*-module:* $\mathcal{M} = \mathcal{P}e^F$. *For any* u, $v \in \mathcal{L}P^{(1)}$ *we have*

$$v \in \mathcal{P}u \Leftrightarrow M_v(x) | M_u(x). \tag{4.3}$$

Any monic (i.e., nonzero) ideal I *of the ring* $\mathcal{P}$ *is an annihilator of some LRS over the field* P. □

Some generalization of these results for a k-LRS over a field are given in [91].

B. The k-LRS families over a Noetherian ring [49, 91, 137, 145]. In what follows, R is a Noetherian ring and ${}_RM$ is an f.g.-R-module. Let $\mathfrak{A}_k = \mathfrak{A}_k(R)$ be the set of all monic ideals of the ring $\mathcal{P}_k = R[x_1, \dots, x_k]$ and $\mathfrak{M}_k = \mathfrak{M}_k(M)$ be the set of all $\mathcal{P}_k$-submodules, finitely generated over R, of the module $M^{(k)}$. In this case, by 2.12, any element $\mathcal{M} \in \mathfrak{M}_k$ is a submodule of $\mathcal{L}M^{(k)}$ and maps An and L_M determine the pair of the Galois correspondences

$$\operatorname{An} : \mathfrak{M}_k \to \mathfrak{A}_k, \qquad L_M : \mathfrak{A}_k \to \mathfrak{M}_k. \tag{4.4}$$

This means that for any $\mathcal{M} \in \mathfrak{M}_k$, $I \in \mathfrak{A}_k$

$$\mathcal{M} \subset L_M(\operatorname{An}(\mathcal{M})), \qquad I \subset \operatorname{An}(L_M(I)). \tag{4.5}$$

In some cases these inclusions may be strict. For example, let $R = P[y_1, y_2]/J$, where P is a field, $J = (y_1^2, y_2^2, y_1, y_2)$ (see [68]). Then $R = P[\alpha_1, \alpha_2]$, $\alpha_s = y_s + J$, R is a P-algebra of dimension 3 over P with the basis e, α_1, α_2, and $\mathfrak{N}(R) = P\alpha_1 + P\alpha_2$ is the unique maximal ideal of R, $\mathfrak{N}(R)^2 = 0$. For the ideal $I = (x, \alpha_1)$ of $R[x]$, the family $L_R(I)$ consists of all sequences $u = (u(0), 0, 0, \dots)$, where $u(0) \in \mathfrak{N}(R)$. But then $\operatorname{An}(L_R(I)) = (x, \alpha_1, \alpha_2) \neq I$. Analogously we can construct a family $\mathcal{M} \in \mathfrak{M}_1$ such that $\mathcal{M} \neq L_M(\operatorname{An}(\mathcal{M}))$.

4.2. Proposition. *For any ideals* I_1, $I_2 \in \mathfrak{A}_k$ *and modules* $\mathcal{M}_1$, $\mathcal{M}_2 \in \mathfrak{M}_k$,

$$\operatorname{An}(\mathcal{M}_1 + \mathcal{M}_2) = \operatorname{An}(\mathcal{M}_1) \cap \operatorname{An}(\mathcal{M}_2); \tag{4.6}$$

$$L_M(I_1 + I_2) = L_M(I_1) \cap L_M(I_2); \tag{4.7}$$

$$\operatorname{An}(\mathcal{M}_1 \cap \mathcal{M}_2) \supseteq \operatorname{An}(\mathcal{M}_1) + \operatorname{An}(\mathcal{M}_2); \tag{4.8}$$

$$L_M(I_1 \cap I_2) \supseteq L_M(I_1) + L_M(I_2). \tag{4.9}$$

If the maps An *and* L_M *are bijections, then the inclusions* (4.5), (4.8), (4.9) *are equalities.* □

In the general case, the inclusions (4.8), (4.9) are strict. Examples can be constructed for the ring $R = P[\alpha_1, \alpha_2]$ defined above. But we must note the following special case.

4.3. Proposition. *If* I_1, I_2 *are comaximal ideals of* $\mathcal{P}_k$, *then*

$$L_M(I_1 \cap I_2) \supseteq L_M(I_1) \dot{+} L_M(I_2) \tag{4.10}$$

is a direct sum. Moreover, in this case $L_M(I_1 \cap I_2)$ *is a cyclic* $\mathcal{P}_k$*-module iff the modules* $L_M(I_s)$, $s = 1, 2$, *are cyclic.* □

C. The criteria for the Galois correspondences between LRS-families and monic ideals to be bijective [14, 16, 43, 49, 65, 66, 68, 69, 77, 134, 135, 137, 146, 169]. If $M = R$ is a field and $k = 1$, then the correspondences (4.4) are bijections, and the inclusions (4.5), (4.8), (4.9) are equalities. Naturally the following question arises: which modules ${}_RM$ satisfy the same conditions, i.e., for which modules is the theory of linear recurring sequences analogous to the theory of linear recurring sequences over a field? The problem is reduced to Artinian rings and modules.

4.4. Lemma. *If* ${}_RM$ *is an f.g.-R-module over a Noetherian ring* R *and the correspondence* $L_M : \mathfrak{A} \to \mathfrak{M}_k$ *is injective, then* R *is an Artinian ring.*

□ The R-module $\mathcal{M} = L_M(x_1, \ldots, x_k)$ is isomorphic to ${}_RM$. If R has a strictly descending chain of ideals — $R \supset J_1 \supset J_2 \supset \ldots$ — then $\mathcal{M}$ has a strictly ascending chain of submodules — $0 \subset \mathcal{M}_1 \subset \mathcal{M}_2 \subset \ldots$ — where $\mathcal{M}_s = L_M(x_1, \ldots, x_k, J_s)$. But the last chain cannot be infinite. □

For any subsets $J \subset R$, $N \subset M$ we define the following annihilators:

$$\mathrm{An}_M(J) = \{\alpha \in M |\ J\alpha = 0\}, \qquad \mathrm{An}_R(N) = \{r \in R |\ rN = 0\}.$$

4.5. Definition. We say that ${}_RM$ is a *quasi-Frobenius* module (QF-module) if for any ideal $J \subset R$ and submodule $N \subset {}_RM$

$$\mathrm{An}_R(\mathrm{An}_M(J)) = J, \qquad \mathrm{An}_M(\mathrm{An}_R(N)) = N.$$

A ring R is called *quasi-Frobenius* if ${}_RR$ is a QF-module.

Examples of QF-rings are fields, Galois rings, and Artinian principal ideal rings.

These definitions are compatible with the definitions from [77, 169]. From the results of these papers it follows that for any Artinian ring R there exists a unique (up to isomorphism) QF-module ${}_RQ$. This module Q is the minimal injective cogenerator in the category of R-modules, and defines the Morita-duality in this category. If R is a local ring with maximal ideal $\mathfrak{N}(R)$, then an faithful module ${}_RM$ is quasi-Frobenius iff any of the following conditions hold:

(a) $\mathrm{An}_M(\mathfrak{N}(R))$ is a minimal submodule of ${}_RM$;

(b) $\mathrm{An}_M(\mathfrak{N}(R))$ is a cyclic R-module;

(c) $\mathrm{An}_M(\mathfrak{N}(R))$ is a nonzero intersection of all submodules of ${}_RM$.

4.6. Theorem. *For a finitely generated module* ${}_RM$ *over an Artinian ring* R, *the following conditions are equivalent:*

(a) ${}_RM$ *is a QF-module;*

(b) *the Galois correspondences* (4.4) *are bijective;*

(c) *for any monic ideal* I *of the ring* $\mathcal{P}_k$ *the family* $L_M(I)$ *is a QF-module over the ring of operators* $S = \mathcal{P}_k/I$, *and any module* $\mathcal{M} \in \mathfrak{M}_k$ *is a QF-module over the ring of operators* $S = \mathcal{P}_k/\mathrm{An}(\mathcal{M})$;

(d) *the inclusions* (4.8) *and* (4.9) *are equalities;*

(e) *for any recurrences* μ, $\nu \in \mathcal{L}M^{(k)}$ *the implications*

$$\nu \in \mathcal{P}_k\mu \Leftrightarrow \mathrm{An}(\mu) \subset \mathrm{An}(\nu)$$

are true.

□ (a) ⇒ (b) Suppose that the conditions of Proposition 2.10 and Corollary 2.11 hold. Then the R-module $\mathcal{M} = L_R(I)$ is generated by the set of k-LRS $\mu_1, \ldots, \mu_l$ such that $\mu_1(\Pi), \ldots, \mu_l(\Pi)$ is a generating set of the R-module of the solutions of the system (2.22) in M^Π. Since M is a QF-module, we may state [137] that the R-module of solutions in R^Π of the dual system (3.11) is generated by the set of rows (polyhedrons) $H_{1\Pi}, \ldots, H_{w\Pi}$ of the matrix of the system (2.22). Hence, according to 3.6, the system of polynomials (3.8) generates the ideal $\mathrm{An}(\mathcal{M}) = \mathrm{An}(L_M(I))$, and, therefore, $\mathrm{An}(L_M(I)) = I$. The equality $L_M(\mathrm{An}(\mathcal{M})) = \mathcal{M}$ for $\mathcal{M} \in \mathfrak{M}_k$ is proved analogously.

(b) ⇒ (c) Let $\mathcal{M} = L_M(I)$. Then for any submodule $\mathcal{K} \subset \mathcal{M}$ the equalities $\mathrm{An}_S(\mathcal{K}) = \tilde{J} = J/I$ hold, where $J = \mathrm{An}(\mathcal{K}) \supset I$ and

$$\mathrm{An}_{\mathcal{M}}(\mathrm{An}_S(\mathcal{K})) = \mathrm{An}_{\mathcal{M}}(\tilde{J}) = L_M(J) = L_M(\mathrm{An}(\mathcal{K})) \overset{(b)}{=} \mathcal{K}.$$

The equality $\mathrm{An}_S(\mathrm{An}_{\mathcal{M}}(\tilde{J})) = \tilde{J}$ for any ideal $\tilde{J}$ of the ring S is proved analogously.

(c) ⇒ (d) In order to prove that inclusions (4.9) are equalities, denote $\mathcal{M} = \mathcal{M}_1 + \mathcal{M}_2$, $I = \mathrm{An}(\mathcal{M})$. Then $\mathcal{M}$ is a QF-module over the ring $S = \mathcal{P}_k/I$. Since $\mathrm{An}_S(\mathcal{M}_1 \cap \mathcal{M}_2) = \mathrm{An}(\mathcal{M}_1 \cap \mathcal{M}_2)/I$ and $\mathrm{An}_S(\mathcal{M}_t) = \mathrm{An}(\mathcal{M}_t)/I$ for $t = 1, 2$, it is sufficient to prove that

$$\mathrm{An}_S(\mathcal{M}_1 \cap \mathcal{M}_2) = \mathrm{An}_S(\mathcal{M}_1) + \mathrm{An}_S(\mathcal{M}_2).$$

This follows from the equality

$$\mathrm{An}_{\mathcal{M}}(\mathrm{An}_S(\mathcal{M}_1) + \mathrm{An}_S(\mathcal{M}_2)) = \mathrm{An}_{\mathcal{M}}(\mathrm{An}_S(\mathcal{M}_1)) \cap \mathrm{An}_{\mathcal{M}}(\mathrm{An}_S(\mathcal{M}_2))$$

and from the definition of the QF-module ${}_S\mathcal{M}$. The equality (4.8) is proved analogously.

(d) ⇒ (a) It is sufficient to examine the case where R is a local Artinian ring. Let ${}_RM$ not be a QF-module. Then $\mathrm{An}_{\mathcal{M}}(\mathfrak{N}(R))$ is not a cyclic R-module, and there exist elements $\alpha_1, \alpha_2 \in M \backslash 0$ such that $\mathfrak{N}(R)\alpha_1 = \mathfrak{N}(R)\alpha_2 = 0$, $R\alpha_1 \cap R\alpha_2 = 0$. Let $\mathcal{M}_s$, $s = 1, 2$, be the family of all k-LRS $\mu \in \mathcal{L}M^{\langle k \rangle}$ such that $\mu(0) \in R\alpha_s$ and $\mu(\mathrm{i}) = 0$ for all $\mathrm{i} \neq 0$. Then $\mathcal{M}_1 \cap \mathcal{M}_2 = 0$ and $\mathrm{An}(\mathcal{M}_1 \cap \mathcal{M}_2) = \mathcal{P}_k$, but $\mathrm{An}(\mathcal{M}_1) = \mathrm{An}(\mathcal{M}_2) = (x_1, \ldots, x_k, \mathfrak{N}(R))$. Therefore, (4.8) is a strict inclusion and (d) is not true.

(a) ⇒ (e) The implication $\nu \in \mathcal{P}_k\mu \Rightarrow \mathrm{An}(\mu) \subset \mathrm{An}(\nu)$ is evident. Let $\mathrm{An}(\mu) \subset \mathrm{An}(\nu)$. Then $L_M(\mathrm{An}(\mu)) \subset L_M(\mathrm{An}(\nu))$, and since (b) is true we have $L_M(\mathrm{An}(\mu)) = \mathcal{P}_k\mu$, $L_M(\mathrm{An}(\nu)) = \mathcal{P}_k\nu$. Hence $\nu \in \mathcal{P}_k\mu$.

(e) ⇒ (a) We may assume that R is a local ring. Let ${}_RM$ not be a QF-module and α_1, α_2 be the same as in the proof of the implication (d) ⇒ (a). Let us consider the sequences $\mu_1, \mu_2 \in \mathcal{L}M^{\langle k \rangle}$ such that $\mu_s(0) = \alpha_s$, $\mu(\mathrm{i}) = 0$ for $\mathrm{i} \neq 0$, $s = 1, 2$. Then $\mathrm{An}(\mu_1) = \mathrm{An}(\mu_2)$, but $\mathcal{P}_k\mu_1 \neq \mathcal{P}_k\mu_2$ since $R\mu_1 \neq R\mu_2$. This contradicts (e). □

Thus, the properties of linear recurrences over a module generalize the properties of LRS over a field iff this module is a QF-module. The following result gives an essential supplement of Proposition 1.7 and shows an interesting connection between cyclic LRS-families and QF-rings.

4.7. Theorem. *Let ${}_RQ$ be a quasi-Frobenius module. Then for any monic ideal I of the ring $\mathcal{P}_k$ the following conditions are equivalent:*

(a) $I = \mathrm{An}(\mu)$ *for some recurrence* $\mu \in \mathcal{L}Q^{\langle k \rangle}$;

(b) $\mathcal{M} = L_Q(I)$ *is a cyclic $\mathcal{P}_k$-module;*

(c) $S = \mathcal{P}_k/I$ *is a quasi-Frobenius ring.*

□ (a) ⇒ (b) By Theorem 4.6(b), $L_Q(I) = L_Q(\mathrm{An}(\mu)) = \mathcal{P}_k\mu$.

(b) ⇒ (c) According to Theorem 4.6(c), $\mathcal{M}$ is a QF-module over the ring S, and since ${}_S\mathcal{M}$ is a cyclic module, we have ${}_S\mathcal{M} \cong {}_SS$.

(c) ⇒ (a) The modules ${}_SS$ and ${}_S\mathcal{M}$ are quasi-Frobenius. Therefore, ${}_SS \cong {}_S\mathcal{M}$ and $\mathcal{M}$ is a cyclic $\mathcal{P}_k$-module. If $\mathcal{M} = \mathcal{P}_k\mu$, then by Theorem 4.6(b), $I = \mathrm{An}(\mu)$. □

4.8. Corollary. *Let $F_1(x_1),\dots,F_k(x_k)$ be monic polynomials from $\mathcal{P}_k$ and $S=\mathcal{P}_k/(F_1(x_1),\dots,F_k(x_k))$. Then S is a QF-ring iff R is a QF-ring.*

□ The S-module $\mathcal{M}=L_M(F_1(x_1),\dots,F_k(x_k))$ is cyclic: $\mathcal{M}=\mathcal{P}_k e^{\mathbf{F}}=Se^{\mathbf{F}}$. If R is a QF-ring, then by Theorem 4.6(c) ${}_S\mathcal{M}$ is a QF-module, and, by Theorem 4.7, S is a QF-ring.

Let S be a QF-ring and R not be a QF-ring. We may suppose that R is a local ring. Then there exist a_1, $a_2\in \operatorname{An}_R(\mathfrak{N}(R))$ such that $Ra_1\cap Ra_2=0$ (see, for example, [43]). Let us consider the submodules $\mathcal{M}_t=\mathcal{P}_k a_t e^{\mathbf{F}}=Sa_te^{\mathbf{F}}$ $(t=1,2)$ of the S-module $\mathcal{M}$. Then $\mathcal{M}_1\neq\mathcal{M}_2$, but $\operatorname{An}_S(\mathcal{M}_1)=\operatorname{An}_S(\mathcal{M}_2)=\mathfrak{N}(R)S$. Since ${}_S\mathcal{M}$ is a QF-module (a cyclic module over a QF-ring), we have $\mathcal{M}_1=\operatorname{An}_{\mathcal{M}}(\operatorname{An}_S(\mathcal{M}_1))=\mathcal{M}_2$. We have come to a contradiction. □

Property (c) of Theorem 4.6 makes it possible to construct a QF-module over any Artinian commutative ring S as a k-LRS family over some principal ideal ring. In fact, it is known that the ring S can be represented as $S=R[\pi_1,\dots,\pi_k]$, where R is the subring of principal ideals of S. Then $S=\mathcal{P}_k/I$ for some monic ideal I of $\mathcal{P}_k=R[x_1,\dots,x_k]$. Since R is a QF-ring, Theorem 4.6(c) implies that $L_R(I)$ is the required QF-module over S.

5. Periodic Sequences and Recurring Sequences

A. Period and defect of a 1-sequence [18, 24, 26, 37, 70, 79, 80, 86, 99, 102–104, 113, 123, 127, 129, 136, 150, 151, 165–167]. The results stated below are, in some sense, a generalization of the well-known results about recurrences over fields and rings.

Recall that a sequence $\mu\in M^{(1)}$ is called *periodic* if there exist $d\in\mathbb{N}_0$ and $t\in\mathbb{N}$ such that

$$x^d(x^t-e)\mu=0. \tag{5.1}$$

5.1. Proposition. *For a periodic sequence $\mu\in M^{(1)}$ there exist parameters $D(\mu)\in\mathbb{N}_0$ (defect) and $T(\mu)\in\mathbb{N}$ (period) such that for any $d\in\mathbb{N}_0$, $t\in\mathbb{N}$ the condition* (5.1) *is equivalent to the condition*

$$d\geq D(\mu),\qquad T(\mu)|t.\square \tag{5.2}$$

Evidently, each periodic sequence is an LRS. The converse is not true. But we have the following

5.2. Proposition. *If ${}_RM$ is a finite module, then each LRS $\mu\in M^{(1)}$ is periodic. Moreover, if the* $\operatorname{rank}\mu=m$, *then*

$$D(\mu)+T(\mu)\leq|M|^m. \tag{5.3}$$

□ If $n=|M|^m$, then the sequence $\mu,x\mu,\dots,x^n\mu$ contains a repetition. □

5.3. Proposition. *If μ, $\nu\in M^{(1)}$ are periodic sequences, then $\lambda=\mu+\nu$ is a periodic sequence and*

$$D(\lambda)\leq\max\{D(\mu),D(\nu)\},\qquad T(\lambda)|[T(\mu),T(\nu)].$$

Moreover,

(a) *if $D(\mu)\neq D(\nu)$, then*

$$D(\lambda)=\max\{D(\mu),D(\nu)\}; \tag{5.4}$$

(b) *if $(T(\mu),T(\nu))=1$, then*

$$T(\lambda)=[T(\mu),T(\nu)]; \tag{5.5}$$

(c) *if the annihilators of the sequences μ and ν are comaximal, then the equalities* (5.4), (5.5) *are true.* □

The set $\pi M^{(1)}$ of all periodic sequences over M is a submodule of the $\mathcal{P}$-module $\mathcal{L}M^{(1)}$.

5.4. Definition. We say that a periodic sequence is *reversible* (*purely periodic*), if $D(\mu)=0$, and *degenerating* if $\mu(i)=0$ for all $i\geq D(\mu)$. We denote the sets of all reversible and degenerating periodic sequences over M by $\mathcal{R}M^{(1)}$ and $\mathcal{D}M^{(1)}$ respectively.

5.5. Proposition. *The $\mathcal{P}$-module $\pi M^{(1)}$ is a direct sum of the submodules: $\pi M^{(1)}=\mathcal{D}M^{(1)}\dotplus\mathcal{R}M^{(1)}$.*

□ In order to decompose a sequence $\mu \in \pi M^{(1)}$ into the sum $\mu = \mu^{(d)} + \mu^{(r)}$, where $\mu^{(d)} \in \mathcal{D}M^{(1)}$, $\mu^{(r)} \in \mathcal{R}M^{(1)}$, it is sufficient to find $k \in \mathbf{N}$ such that $kT(\mu) = l > D(\mu)$. Then $\mu^{(r)} = x^l\mu$. □

B. Multipliers and the reduced period. These characteristics of periodic sequences over residue rings and finite principal ideal rings were introduced in [52, 86, 150, 151, 161].

5.6. Definition. Define the *support* of a sequence $\mu \in M^{(1)}$ as the R-submodule $\mathrm{Supp}\,(\mu)$ of the module ${}_RM$, generated by all elements $\mu(i)$, $i \in \mathbf{N}_0$. We call the sequence μ *faithful* if $\mathrm{Supp}\,(\mu)$ is a faithful R-module (i.e., if $\mathrm{An}_R(\mu) = \mathrm{An}_R(\mathrm{Supp}\,(\mu)) = 0$). An endomorphism $\varphi \in \mathrm{End}_R(\mathrm{Supp}\,(\mu))$ is called the *multiplier* of the sequence μ if there exists $t \in \mathbf{N}$ such that the sequence $\varphi(\mu) = (\varphi(\mu(0)), \varphi(\mu(1)), \ldots)$ has the form

$$\varphi(\mu) = x^t\mu. \tag{5.6}$$

We denote the set of all multipliers of the sequence μ by $\mathrm{Mult}\,(\mu)$.

If the set $\mathrm{Mult}\,(\mu)$ is not empty, then it is a commutative subsemigroup of the semigroup of all endomorphisms of the module $\mathrm{Supp}\,(\mu)$. The sequence μ is degenerating iff $0 \in \mathrm{Mult}\,(\mu)$, and it is reversible iff the semigroup $\mathrm{Mult}\,(\mu)$ contains the identity endomorphism ε.

5.7. Proposition. *If* $\mathrm{Supp}\,(\mu)$ *is an f.g.-R-module and* $\mathrm{Mult}\,(\mu) \neq \varnothing$, *then* μ *is an LRS.*

□ Let $\varphi \in \mathrm{Mult}\,(\mu)$ and $\varphi(\mu) = x^t\mu$. Our conditions imply that there exists a monic polynomial $F(x) \in R[x]$ such that $F(\varphi) = 0$. Then $\mu \in L_M(F(x^t))$. □

The example $(0, 1, 2, \ldots) \in L_{\mathbf{Z}}((x-1)^2)$ shows that the converse of Proposition 5.7 is not true.

5.8. Theorem. *Let $\mu \in M^{(1)}$ be a faithful sequence. Then the following conditions are equivalent:*

(a) *μ is a reversible sequence;*

(b) $\mathrm{Mult}\,(\mu) \ni \varepsilon$;

(c) $\mathrm{Mult}\,(\mu)$ *is a subgroup of the group* $\mathrm{Aut}\,(\mathrm{Supp}\,(\mu))$;

(d) $\mathrm{Mult}\,(\mu)$ *is a finite cyclic subgroup of the group* $\mathrm{Aut}\,(\mathrm{Supp}\,(\mu))$.

Under condition (a), *the group* $\mathrm{Mult}\,(\mu)$ *is called the group of multipliers of the recurrence μ. It satisfies the condition*

$$|\mathrm{Mult}\,(\mu)| \text{ divides } T(\mu). \tag{5.7}$$

□ (b) ⇒ (c) In view of the condition (b), we have $x^t\mu = \varepsilon(\mu) = \mu$ for some $t \in \mathbf{N}$. Let $\varphi \in \mathrm{Mult}\,(\mu)$. Then $\varphi^t(\mu) = \mu$. Since μ is a faithful sequence, $\varphi^t = \varepsilon$.

(c) ⇒ (d) Let t_0 be the minimum of numbers $t \in \mathbf{N}$ such that there exists $\varphi \in \mathrm{Mult}\,(\mu)$ with the property (5.6), and let $x^{t_0}\mu = \varphi_0(\mu)$, $\varphi_0 \in \mathrm{Mult}\,(\mu)$. Then for any $\varphi \in \mathrm{Mult}\,(\mu)$ the condition (5.6) implies that $t_0 | t$ and if $t = t_0 s$, then $\varphi = \varphi_0^s$. Hence $\mathrm{Mult}\,(\mu) = \langle\varphi_0\rangle$. Now (5.7) is obvious. □

5.9. Definition. For a reversible sequence $\mu \in M^{(1)}$ the parameter

$$T_r(\mu) = \min\{t \in \mathbf{N} \mid \exists \varphi \in \mathrm{Mult}\,(\mu) : x^t\mu = \varphi(\mu)\}$$

will be called the *reduced period* of the recurrence μ.

It is easy to see that

$$T(\mu) = |\mathrm{Mult}\,(\mu)| \cdot T_r(\mu). \tag{5.8}$$

C. Periodic k-sequences. In special cases (where $k = 2, 3$ and $M = R$ is a finite field) some of the definitions, introduced below, were considered in [128, 144, 153, 154].

There are two approaches to the definition of a periodic k-sequence. The first of them is connected with the concepts of vector-period [154] and regular extract.

5.10. Definition. A nonzero vector $\mathbf{t} \in \mathbf{N}_0^k$ is called a *vector-period* of the sequence $\mu \in M^{\langle k\rangle}$ if $\mathbf{x}^{\mathbf{l}}(\mathbf{x}^{\mathbf{t}} - e)\mu = 0$ for some $\mathbf{l} \in \mathbf{N}_0^k$. A subgroup $\mathfrak{P}(\mu)$ of the group $(\mathbf{Z}^k, +)$, generated by all vector-periods of μ, will be called its *group of periods*. If μ has no vector-periods, then $\mathfrak{P}(\mu) = 0$.

5.11. Lemma. *The set $\mathfrak{P}^+(\mu)$ of all nonzero nonnegative vectors from $\mathfrak{P}(\mu)$ coincides with the set of all vector-periods of the sequence μ.* □

5.12. Proposition. *For any subgroup $\mathcal{G} < \mathbf{Z}^k$ which is generated by the set $\mathcal{G}^+$ of all of its nonnegative vectors, there exists a k-sequence $\mu \in R^{(k)}$ such that $\mathfrak{P}(\mu) = \mathcal{G}$.*

□ $\mu(\mathbf{t}) = e$ if $\mathbf{t} \in \mathcal{G}^+$, and $\mu(\mathbf{t}) = 0$ if $\mathbf{t} \notin \mathcal{G}^+$. □

5.13. Definition. Let $\mathbf{l} \in \mathbf{N}_0^k$, $\mathbf{d} \in \mathbf{N}_0^k \backslash \mathbf{0}$. We call a 1-sequence $\mu^{[\mathbf{l},\mathbf{d}]}(z) = \mu(\mathbf{l}+\mathbf{d}z)$ a *regular* $(\mathbf{l},\mathbf{d})$*-extract* (or an *extract in the direction* $\mathbf{d}$) of the sequence μ. We say that the sequence μ is $(\mathbf{l},\mathbf{d})$*-periodic* (*periodic in the direction* $\mathbf{d}$) if $\mu^{[\mathbf{l},\mathbf{d}]}$ is a periodic sequence for any $\mathbf{l} \in \mathbf{N}_0^k$.

5.14. Proposition. *For a k-sequence $\mu \in M^{(k)}$ the following statements are equivalent:*

(a) *the abelian group $\mathfrak{P}(\mu)$ of periods of the sequence μ has rank k;*

(b) *the ideal* $\mathrm{An}(\mu)$ *contains polynomials* $\mathbf{x}^{\mathbf{l}_1}(\mathbf{x}^{\mathbf{t}_1} - e), \ldots, \mathbf{x}^{\mathbf{l}_k}(\mathbf{x}^{\mathbf{t}_k} - e)$ *such that* $\operatorname{rank}\{\mathbf{t}_1, \ldots, \mathbf{t}_k\} = k$;

(c) *there exists a system $\mathbf{d}_1, \ldots, \mathbf{d}_k \in \mathbf{N}_0^k$ of rank k and a system $\mathbf{l}_1, \ldots, \mathbf{l}_k \in \mathbf{N}_0^k$ such that μ is $(\mathbf{l}_s, \mathbf{d}_s)$-periodic for $s \in \overline{1,k}$;*

(d) *for any direction $\mathbf{d} \in \mathbf{N}_0^k \backslash \mathbf{0}$ there exists $\mathbf{l} \in \mathbf{N}_0^k$ such that the sequence μ is $(\mathbf{l},\mathbf{d})$-periodic.* □

But it is possible that a sequence satisfying the conditions of Proposition 5.14, has nonperiodic regular extract.

5.15. Example. The sequence $\mu \in \mathbf{Z}^{(2)}$ of the form

1	2	3	4	...
1	1	1	1	...
1	1	1	1	...

satisfies the condition $x_2(x_1 - 1)$, $x_2(x_2 - 1) \in \mathrm{An}(\mu)$, but its first row is a nonperiodic 1-sequence.

5.16. Example. The sequence $\mu \in M^{(2)}$ of the form

α	0	α	0	0	α	0	0	0	α	...
0	α	0	α	0	α	...				
α	0	α	0	α	0	...				

where $\alpha \neq 0$, satisfies the condition $x_2(x_1^2 - e)$, $x_2(x_2^2 - e) \in \mathrm{An}(\mu)$, but it is not an LRS.

5.17. Definition. A sequence $\mu \in M^{(k)}$ satisfying the conditions (a)-(d) of Proposition 5.14 will be called a *near-periodic sequence*. We say that μ is a *periodic* (*reversible*) *sequence* if any regular $(\mathbf{l},\mathbf{d})$-extract of this sequence is a periodic (reversible) 1-sequence. A nonreversible near-periodic sequence is called a *defect sequence*.

5.18. Proposition. *For a k-sequence $\mu \in M^{(k)}$ the following statements are equivalent:*

(a) *μ is a periodic (respectively reversible) sequence;*

(b) *the ideal* $\mathrm{An}(\mu)$ *contains a system of elementary polynomials of the form $x_1^{l_1}(x_1^{t_1} - e), \ldots, x_k^{l_k}(x_k^{t_k} - e)$ (respectively of the form $x_1^{t_1} - e, \ldots, x_k^{t_k} - e$) for some $l_s \in \mathbf{N}_0$, $t_s \in \mathbf{N}$, $s \in \overline{1,k}$;*

(c) *the sequence μ is periodic (respectively reversible) in each of the directions $\mathbf{e}_1, \ldots, \mathbf{e}_k$, where $\mathbf{e}_s$ is the s-th row of the identity matrix.* □

Examples 5.15 and 5.16 show that under the condition (c) the system $\mathbf{e}_1, \ldots, \mathbf{e}_k$ cannot be substituted by the arbitrary system $\mathbf{d}_1, \ldots, \mathbf{d}_k$ of rank k. The sequences in these examples are periodic in each direction except for $\mathbf{e}_1$.

5.19. Corollary. *Any periodic k-sequence is an LRS.* □

Example 5.15 shows that the converse of this corollary is not true.

5.20. Proposition. *The reversibility of the sequence $\mu \in M^{(k)}$ is equivalent to the condition*

$$\forall \mathbf{i} \in \mathbf{N}_0^k \ \exists \mathbf{j} \in \mathbf{N}_0^k : \ \mathbf{x}^{\mathbf{j}}(\mathbf{x}^{\mathbf{i}}\mu) = \mu.$$

If the sequence μ is reversible, then for any $\mathbf{i} \in \mathbf{N}_0^k$ the sequence $\nu = \mathbf{x}^{\mathbf{i}}\mu$ is also reversible and $\mathfrak{P}(\nu) = \mathfrak{P}(\mu)$; for any $\mathbf{t} \in \mathfrak{P}(\mu)$, we have $\mathbf{x}^{\mathbf{t}}\mu = \mu$. □

The second approach to the definition of a periodic k-sequence is connected with the following conception.

5.21. Definition. The set $\mathcal{O}(\mu)$ of all k-sequences $\nu \in M^{(k)}$ of the form $\nu = \mathbf{x}^{\mathbf{i}}\mu$, $\mathbf{i} \in \mathbf{N}_0^k$, is called a *trajectory* of μ.

5.22. Proposition. *A sequence $\mu \in M^{(k)}$ is periodic iff its trajectory $\mathcal{O}(\mu)$ is finite, and it is reversible iff $\mathcal{O}(\mu) = \mathcal{O}(\mathbf{x}^{\mathbf{i}}\mu)$ for any $\mathbf{i} \in \mathbf{N}_0^k$.* □

5.23. Definition. For a periodic sequence μ the set $\mathcal{T}(\mu)$ of all reversible elements of its trajectory $\mathcal{O}(\mu)$ is called the *cycle* of the sequence μ, and its cardinality $T(\mu) = |\mathcal{T}(\mu)|$ is called the *period* of the sequence μ. The set of all defect elements of the trajectory $\mathcal{O}(\mu)$ is denoted by $\mathcal{D}(\mu)$, and its cardinality $D(\mu) = |\mathcal{D}(\mu)|$ is called the *defect* of the sequence μ. The sequence μ is said to be *degenerating* if it is periodic and its cycle contains only the zero sequence, i.e., $\mathcal{T}(\mu) = \{0\}$.

Thus, $D(\mu) + T(\mu) = |\mathcal{O}(\mu)|$, and a periodic sequence μ is reversible iff $D(\mu) = 0$, i.e., $\mathcal{T}(\mu) = \mathcal{O}(\mu)$. A periodic sequence is degenerating iff $\mathbf{x}^{\mathbf{i}} \in \mathrm{An}\,(\mu)$ for some $\mathbf{i} \in \mathbf{N}_0^k$.

5.24. Proposition. *If $\mu \in M^{(k)}$ is a periodic sequence, then*

$$\mathcal{T}(\mu) = [\mathbf{Z}^k : \mathfrak{P}(\mu)], \tag{5.9}$$

where the right-hand part is the index of the subgroup $\mathfrak{P}(\mu)$ of the group $(\mathbf{Z}^k, +)$. □

5.25. Proposition. *If ${}_RM$ is a finite module and μ is an LRS from $\mathcal{L}M^{(k)}$, then μ is a periodic sequence and*

$$|\mathcal{O}(\mu)| \leq |\mathcal{P}_k/\mathrm{An}\,(\mu)|. \tag{5.10}$$

□ If elementary characteristic polynomials have the degrees $m_1, \ldots, m_k$, then each recurrence $\mathbf{x}^{\mathbf{i}}\mu$ belongs to $L_M(\mathrm{An}\,(\mu))$ and is uniquely determined by its values on the polyhedron $\Pi = \Pi(\mathbf{m})$. The number of all different recurrences of this form does not exceed $|M^{\Pi}| = |M|^m$, where $m = m_1 \ldots m_k$. Therefore, $|\mathcal{O}(\mu)| < \infty$. The inequality (5.10) follows from the definition of $\mathcal{O}(\mu)$ and from the fact that the right-hand part of (5.10) is equal to the number of all different k-sequences of the form $F(\mathbf{x})\mu$, $F(\mathbf{x}) \in \mathcal{P}_k$. □

The following result gives us an interesting relation between the properties of reversible sequences and the properties of associated rings.

5.26. Theorem. *Let $\mu \in M^{(k)}$, and let $S = \mathcal{P}_k/\mathrm{An}\,(\mu)$ be the operator ring of μ* (see 1.18)), *$\theta_s = x_s + \mathrm{An}\,(\mu)$ for $s \in \overline{1,k}$. Then the sequence μ is reversible iff $\theta_1, \ldots, \theta_k$ are the elements of finite order from the multiplicative group S^* of the ring S. If μ is a reversible sequence, then*

$$T(\mu) = |\langle \theta_1, \ldots, \theta_k \rangle| \leq |S^*| \leq |S| - 1, \tag{5.11}$$

where $\langle \theta_1, \ldots, \theta_k \rangle$ is a subgroup of the group S^* generated by $\theta_1, \ldots, \theta_k$. The equality

$$T(\mu) = |S^*| \tag{5.12}$$

holds iff

$$S^* = \langle \theta_1, \ldots, \theta_k \rangle. \tag{5.13}$$

If μ is a faithful reversible sequence, then

$$T(\mu) = |S| - 1 \tag{5.14}$$

if and only if the following three conditions hold:

(a) *$R = GF(q)$ is a Galois field;*

(b) *$\mathrm{An}\,(\mu)$ is a maximal ideal of the ring $\mathcal{P}_k = GF(q)[x_1, \ldots, x_k]$ (i.e., $S = GF(q^n)$ for some $n \in \mathbf{N}$);*

(c) *the equality* (5.13) *is true.*

□ We may consider the $\mathcal{P}_k$-module $\mathcal{P}_k\mu$ as an S-module if we define $\theta_s\mu = x_s\mu$, $s \in \overline{1,k}$. Then for any polynomial $H(\mathbf{x}) \in \mathcal{P}_k$ the condition $H(\mathbf{x})\mu = 0$ is equivalent to the condition $H(\theta) = 0$. By Proposition 5.24, μ is reversible iff for each $\mathbf{i} \in \mathbf{N}_0^k$ there exists $\mathbf{j} \in \mathbf{N}_0^k$ such that $\theta^{\mathbf{i}+\mathbf{j}} = e$. This means that $\theta_1, \ldots, \theta_k$ are the elements of finite order in S^*.

If μ is a reversible sequence, then the cardinality of its cycle $T(\mu) = O(\mu)$ is equal to the number of different elements of the form $\theta = \theta_1^{i_1} \dots \theta_k^{i_k}$. This implies the relations (5.11) and the equivalency of (5.12) and (5.13). Now it is clear that (5.14) implies $S^* = S \backslash 0$. In this case, S is a field, and (a)–(c) are true. The converse is evident. □

We denote the $\mathcal{P}_k$-modules of all periodic, reversible, and degenerating k-sequences over ${}_RM$ by $\pi M^{(k)}$, $\mathcal{R}M^{(k)}$, and $\mathcal{D}M^{(k)}$ respectively.

5.27. Proposition.

$$\pi M^{(k)} = \mathcal{R}M^{(k)} \dot{+} \mathcal{D}M^{(k)}. \tag{5.15}$$

□ In order to obtain the decomposition of a sequence $\mu \in \pi M^{(k)}$ into the sum of reversible $\mu^{(r)}$ and degenerating $\mu^{(d)}$ sequences, it is sufficient to find a vector-period $\mathbf{t} \in \mathfrak{P}(\mu)$ such that $\mathbf{x}^{\mathbf{t}}\mu$ is a reversible sequence. Then $\mu^{(r)} = \mathbf{x}^{\mathbf{t}}\mu$. □

For a description of the cycles of a reversible LRS, we can use

5.28. Proposition. *Let $\mu \in \mathcal{R}M^{(k)}$. Suppose that one of the following conditions holds:*

(a) *$M = M_1 \dot{+} M_2$ is a direct sum of R-modules and $\mu = \mu_1 + \mu_2$, where $\mu_s \in \mathcal{R}M_s^{(k)}$, $s = 1, 2$;*

(b) *$\mathrm{An}(\mu) = I_1 I_2$, where $I_1 + I_2 = \mathcal{P}_k$, and $\mu = \mu_1 + \mu_2$, $\mu_s \in L_M(I_s)$, $s = 1, 2$.*

Then $\mathfrak{P}(\mu) = \mathfrak{P}(\mu_1) \cap \mathfrak{P}(\mu_2)$. In particular, if $k = 1$, then $T(\mu) = [T(\mu_1), T(\mu_2)]$.

□ In both cases the condition $\mathbf{x}^{\mathbf{t}}\mu = \mu$ is equivalent to the condition $\mathbf{x}^{\mathbf{t}}\mu_s = \mu_s$ for $s = 1, 2$. □

6. Periodic Ideals and Polynomials

The problem of calculating the period and defect of a linear recurrence μ can be solved as the problem of calculating the analogous parameters of the ideal $\mathrm{An}(\mu)$ (the usefulness of such an approach has already been noted in [113]).

A. Periodic ideals of polynomials of one variable [21, 26, 37, 48, 113, 123].

6.1. Definition. An ideal I of the ring $\mathcal{P} = \mathcal{P}_1$ (respectively a polynomial $F(x) \in \mathcal{P}$) is called *periodic* if there exist numbers $d \in \mathbb{N}_0$, $t \in \mathbb{N}$ such that

$$x^d(x^t - e) \in I \text{ (respectively } F(x) \mid x^d(x^t - e)). \tag{6.1}$$

The minimal d and t with the property (6.1) (if they exist) are called the *defect* and *period* of the ideal I (respectively of the polynomial $F(x)$) and are denoted by $D(I)$ and $T(I)$ ($D(F)$ and $T(F)$).

6.2. Lemma. *If I is a periodic ideal, then for any $d \in \mathbb{N}_0$, $t \in \mathbb{N}$ the condition (6.1) is equivalent to the conditions $d \geq D(I)$, $T(I) \mid t$.* □

Evidently, each periodic ideal is monic, but the converse in the general case is not true.

6.3. Proposition. *A sequence $\mu \in M^{(1)}$ is periodic iff $\mathrm{An}(\mu)$ is a periodic ideal. In this case $D(\mu) = D(\mathrm{An}(\mu))$ and $T(\mu) = T(\mathrm{An}(\mu))$.* □

6.4. Proposition. *Let I be an ideal of $\mathcal{P}$, $S = \mathcal{P}/I$, and $\theta = x + I \in S$. Then I is a periodic ideal iff the sequence $u = (e, \theta, \dots, \theta^i, \dots)$ over the ring S is periodic. If u is a periodic sequence, then $D(I) = D(u)$, $T(I) = T(u)$.* □

6.5. Proposition. *A monic polynomial $F(x) \in \mathcal{P}$ is periodic iff the recurrence $e^F \in L_R(F)$ is periodic. In this case $D(F) = D(e^F)$, $T(F) = T(e^F)$.* □

6.6. Theorem. *Let R be a finite ring. Then for an ideal I of the ring $\mathcal{P}$ the following conditions are equivalent:*

(a) *$S = \mathcal{P}/I$ is a finite ring;*

(b) *I is a periodic ideal;*

(c) *I is a monic ideal.*

Under these conditions

$$D(I)+T(I)\le |S|, \tag{6.2}$$

and if $|S|>2$, *then*

$$D(I)+T(I)\le |S|-1. \tag{6.3}$$

If $|S|>2$, *then the equality*

$$D(I)+T(I)=|S|-1 \tag{6.4}$$

holds iff either $S=GF(2)[x]/(x^2)$ *and* $D(I)+T(I)=3$ *or* S *is a finite field and the ideal* I *has the form* $I=(F(x),J)$, *where* J *is the maximal ideal of* R (*i.e.,* $\bar{R}=R/J=GF(q)$) *and* $F(x)$ *is a monic polynomial of degree* m *over* R *such that its image* $\bar{F}(x)$ *under the canonical epimorphism* $R[x]\to\bar{R}[x]$ *satisfies the condition* $T(\bar{F})=q^m-1$. *In the last case* $D(I)=0$, $T(I)=q^m-1$.

□ The proof of the equivalence of the conditions (a)–(c) is standard. Now let $D(I)+T(I)=N$. Then, in the notations of Proposition 6.4, N is the number of different elements in the sequence u, and these elements are $e,\theta,\dots,\theta^{N-1}$. This implies (6.2). If $N\ge|S|-1$, then $N=|S|$ and $S=\{e,\theta,\dots,\theta^{N-1}\}$. This is possible only if $N=2$, $\theta=0$, and $S=GF(2)$. This implies (6.3).

Let (6.4) be true, i.e., $N=|S|-1$. If $\theta\notin S^*$, then $N\le|\theta S|+1\le(|S|/2)+1$, and since $N=|S|-1$, we have $|S|=4$, $N=3$ and $S=GF(2)[x]/(x^2)$. If $\theta\in S^*$, then $S^*=\{e,\theta,\dots,\theta^{N-1}\}$ and S is a field. Let $\varphi:\mathcal{P}\to S=\mathcal{P}/I$ be the canonical epimorphism. Then $\varphi(R)=GF(q)$ is a subfield of S and $\varphi(R)\cong\bar{R}=R/J$, where $J=I\cap R$ is the maximal ideal of R. Let $\psi:R[x]\to\bar{R}[x]$ be the natural homomorphism induced by the canonical epimorphism $R\to\bar{R}$, and let $\bar{I}=\psi(I)$. Then $S\cong\bar{R}[x]/\bar{I}$ and $\bar{I}$ is an ideal generated by an irreducible polynomial from $\bar{R}[x]$. Therefore, I contains a monic polynomial $F(x)$ such that $\bar{I}=(\bar{F}(x))$ and $I=(F(x),J)$. Let $\deg F(x)=m$. Then $|S|=|\bar{R}|^m=q^m$, and the root $\theta\in S$ of the polynomial $\bar{F}(x)$ is a primitive element of the field S, i.e., $T(\bar{F})=q^m-1$. □

6.7. Corollary. *Any monic polynomial* $F(x)$ *over a finite ring* R *is periodic. If* $\deg F(x)=m$, $|R|^m\ge2$, *then* $D(F)+T(F)\le|R|^m-1$. □

6.8. Proposition. *For monic ideals* I_1, I_2 *of the ring* $\mathcal{P}$, *the ideal* $I=I_1\cap I_2$ *is periodic iff each of the ideals* I_1, I_2 *is periodic. In this case,* $D(I)=\max\{D(I_1),D(I_2)\}$, $T(I)=[T(I_1),T(I_2)]$. □

In this statement we cannot substitute the intersection of the ideals for their product. For example, the ideal $I_1=(x-1)\subset\mathbf{Z}[x]$ is periodic, but the ideal $I_1^2=((x-1)^2)$ is not.

6.9. Corollary. *Let* $F_1(x)$, $F_2(x)\in R[x]$ *be coprime monic polynomials. Then* $F(x)=F_1(x)F_2(x)$ *is a periodic polynomial iff* $F_1(x)$, $F_2(x)$ *are periodic polynomials. In this case* $D(F)=\max\{D(F_1),D(F_2)\}$, $T(F)=[T(F_1),T(F_2)]$.

□ $(F)=(F_1)\cdot(F_2)=(F_1)\cap(F_2)$. □

6.10. Definition. We call a periodic ideal I (respectively a monic periodic polynomial $F(x)$) *reversible* if $D(I)=0$ (respectively $D(F)=0$), and we call I a *degenerating ideal* if $x^{D(I)}\in I$ (respectively $F(x)|x^{D(F)}$).

6.11. Proposition. *Any periodic ideal* $I\triangleleft\mathcal{P}$ *can be uniquely represented as the intersection* $I=I^{(r)}\cap I^{(d)}$ *of a reversible ideal* $I^{(r)}$ *and a degenerating ideal* $I^{(d)}$.

□ If $T(I)=t$, $D(I)=l$, then $I^{(r)}=I+(x^t-e)\mathcal{P}$, $I^{(d)}=I+x^l\mathcal{P}$. □

6.12. Remark. In general, a monic periodic polynomial $F(x)$ cannot be represented as the product $F(x)=F^{(r)}(x)F^{(d)}(x)$, where $F^{(r)}(x)$ is a reversible and $F^{(d)}(x)$ a degenerating polynomial. For example, the polynomial $F(x)=x^2-4x-3$ over the ring $\mathbf{Z}_6$ has no such representation. But such a representation exists for polynomials over a local Artinian ring (see Section 16).

6.13. Proposition. *A monic polynomial over a finite ring* R *is reversible iff its constant term is invertible in* R. □

Now we can make Proposition 5.5 more precise.

6.14. Proposition. *If* I *is a periodic ideal, then* $L_M(I)=L_M(I^{(r)})\dotplus L_M(I^{(d)})$, *where* $L_M(I^{(d)})=$

$L_M(I) \cap \mathcal{D}M^{(1)}$ *is the family of all degenerating recurrences of* $L_M(I)$ *and* $L_M(I^{(r)}) = L_M(I) \cap \mathcal{R}M^{(1)}$ *is the family of all reversible recurrences of* $L_M(I)$. □

In general, the problem of calculating the period and defect of a monic ideal $I \lhd \mathcal{P}$ defined by a given generating system of polynomials is rather difficult. If there exists an algorithm of solving systems of linear equations over R (see [12]), then we can propose the following algorithm of calculation of $D(I)$ and $T(I)$. Let $I = (F(x), G_1(x), \ldots, G_n(x))$, where $F(x)$ is a monic polynomial.

6.15. Lemma. *A polynomial* $H(x) \in \mathcal{P}$ *belongs to the ideal* I *iff the system of linear equations*

$$(G_1(S(F)), \ldots, G_n(S(F)))z = H(S(F)) \downarrow_1$$

is solvable. Here $S(F)$ *is the accompanying matrix of the polynomial* $F(x)$ (see 1.9), *and* $H(S(F)) \downarrow_1$ *is the first column of the matrix* $H(S(F))$.

□ If $z = (z_0^{(1)}, \ldots, z_{m-1}^{(1)}, z_0^{(2)}, \ldots, z_{m-1}^{(n)})$ is a solution of our system, then $H(x) = Z_1(x)G_1(x) + \ldots + Z_n(x)G_n(x) + Z(x)F(x)$, where $Z(x) \in \mathcal{P}$, $Z_s(x) = z_0^{(s)} + z_1^{(s)}x + \ldots + z_{m-1}^{(s)}x^{m-1}$. □

Now if $|\mathcal{P}/I| = N$, then $T(I)$ can be calculated as the minimal $t \in \mathbf{N}$ with the property

$$\operatorname{Res}(x^t - e/F) \cdot \operatorname{Res}(x^N/F) \in I,$$

and $D(I)$ can be calculated as the minimal $l \in \mathbf{N}_0$ such that

$$\operatorname{Res}(x^l/F) \cdot \operatorname{Res}(x^{T(I)} - e/F) \in I.$$

B. Periodic ideals of polynomials of k variables.

6.15. Definition. We call an ideal $I \lhd \mathcal{P}_k$ *periodic* (*reversible*) if there exist parameters $l_1, \ldots, l_k \in \mathbf{N}_0$, $t_1, \ldots, t_k \in \mathbf{N}$ such that

$$x_s^{l_s}(x_s^{t_s} - e) \in I \text{ for } s \in \overline{1,k} \tag{6.5}$$

(respectively

$$(x_s^{t_s} - e) \in I \text{ for } s \in \overline{1,k}). \tag{6.6}$$

A periodic ideal is said to be *degenerating* if for some $\mathbf{l} \in \mathbf{N}_0^k \backslash 0$

$$x^{\mathbf{l}} \in I. \tag{6.7}$$

Let $S = \mathcal{P}_k/I = R[\theta_1, \ldots, \theta_k]$, where $\theta_s = x_s + I \in S$, is the operator ring of the ideal I (see 1.18). Denote by $\mathcal{O}(I)$ the subsemigroup $[e, \theta_1, \ldots, \theta_k\rangle$ of the semigroup $(S, \cdot)$ generated by $e, \theta_1, \ldots, \theta_k$, and call it the *orbital semigroup of the ideal* I.

6.17. Proposition. *Let* I *be an ideal of* $\mathcal{P}_k$. *Then*

(a) (I *is a periodic ideal*) $\Leftrightarrow$ ($|\mathcal{O}(I)| < \infty$);

(b) (I *is a reversible ideal*) $\Leftrightarrow$ ($|\mathcal{O}(I)| < \infty$, $\mathcal{O}(I) < S^*$);

(c) (I *is a degenerating ideal*) $\Leftrightarrow$ ($|\mathcal{O}(I)| < \infty$, $0 \in \mathcal{O}(I)$).

□ The conditions (6.5)–(6.7) are equivalent respectively to the conditions

$$[e, \theta_s >= \{e, \theta_s, \ldots, \theta_s^{l_s+t_s-1}\}, \qquad s \in \overline{1,k};$$

$$\theta_s^{t_s} = e, \qquad s \in \overline{1,k};$$

$$\theta^{\mathbf{l}} = \theta_1^{l_1} \ldots \theta_k^{l_k} = 0. \square$$

Recall that, according to the Frobenius theorem [17, 37], some natural power of any element of a finite semigroup is an idempotent. For a periodic ideal I, denote by $\varepsilon_s = \varepsilon_s(I)$, $s \in \overline{1,k}$, the idempotent of the semigroup $[\theta_s\rangle$. We denote the product of all idempotents of the semigroup $\mathcal{O}(I)$ by $\varepsilon = \varepsilon(I)$.

6.18. Lemma. *If* I *is a periodic ideal of* $\mathcal{P}_k$, *then* $\varepsilon = \varepsilon_1 \cdot \ldots \cdot \varepsilon_k$ *and* $\varepsilon\mathcal{O}(I) = T(I)$ *is a subgroup of the semigroup* $\mathcal{O}(I)$ *with the unit* ε.

□ Let $\varepsilon = \theta_1^{a_1} \dots \theta_k^{a_k}$ and $\theta_s^{b_s} = \varepsilon_s$, $s \in \overline{1,k}$. Then $\varepsilon = \varepsilon^{b_1 \cdot b_k} = \varepsilon_1 \cdot \dots \cdot \varepsilon_k$. Obviously ε is the unit of the group $T(I)$, and some natural power of any element of $\mathcal{T}(I)$ is equal to ε. □

6.19. Definition. We call the group $\mathcal{T}(I)$ the *cycle group* of the periodic ideal I, and we call its cardinality $T(I) = |\mathcal{T}(I)|$ the *period* of I. The parameter $D(I) = |\mathcal{O}(I)| - |\mathcal{T}(I)|$ is called the *defect* of the ideal I. If $D(I) > 0$, then the ideal I will be called *defected.*

6.20. Proposition. *A periodic ideal I is reversible iff $\mathcal{T}(I) = \mathcal{O}(I)$ (i.e., $D(I) = 0$) and it is degenerating iff $\mathcal{T}(I) = 0$.* □

6.21. Definition. We call a vector $\mathbf{t} \in \mathbf{N}_0^k \backslash 0$ a *vector-period* of the ideal I if there exists $\mathbf{l} \in \mathbf{N}_0^k \backslash 0$ with $\theta^{\mathbf{l}+\mathbf{t}} = \theta^{\mathbf{l}}$ (i.e., $\mathbf{x}^{\mathbf{l}}(\mathbf{x}^{\mathbf{t}} - e) \in I$). The subgroup $\mathfrak{P}(I)$ of the group $(\mathbf{Z}^k, +)$ generated by all vector-periods of the ideal I is called its *group of periods.*

Note that if I is a periodic ideal, then each element $\varepsilon\theta_s$ of the group $\mathcal{T}(I)$ has a finite order. For any vector $\mathbf{t} \in \mathbf{Z}^k$ define

$$\varepsilon\theta^{\mathbf{t}} = (\varepsilon\theta_1)^{t_1} \dots (\varepsilon\theta_k)^{t_k}.$$

6.22. Proposition. *If $I \lhd \mathcal{P}_k$ is a periodic ideal, then $\mathfrak{P}(I)$ is a subgroup of rank k of the group $(\mathbf{Z}^k, +)$, and*

$$\mathfrak{P}(I) = \{\mathbf{t} \in \mathbf{Z}^k \mid \varepsilon\theta^{\mathbf{t}} = \varepsilon\}; \tag{6.8}$$

$$\mathcal{T}(I) \cong \mathbf{Z}^k/\mathfrak{P}(I); \qquad T(I) = [\mathbf{Z}^k : \mathfrak{P}(I)]. \tag{6.9}$$

□ Determine the group epimorphism $\varphi : \mathbf{Z}^k \to \mathcal{T}(I)$, $\varphi(\mathbf{r}) = \varepsilon\theta^{\mathbf{r}}$. If $\mathbf{t} \in \mathfrak{P}(I)$, then $\varepsilon\theta^{\mathbf{l}} = \varepsilon\theta^{\mathbf{l}+\mathbf{t}}$ for some $\mathbf{l} \in \mathbf{N}_0^k \backslash 0$. Since $\varepsilon = \theta_1^a \dots \theta_k^a$ for a suitable $a \in \mathbf{N}$, we have $\varepsilon = \varepsilon\theta^{a\mathbf{l}} = \varepsilon\theta^{a\mathbf{l}+\mathbf{t}} = \varepsilon\theta^{\mathbf{t}}$, i.e., $\mathbf{t} \in \operatorname{Ker}\varphi$. If $\mathbf{t} \in \operatorname{Ker}\varphi$, then $\varepsilon\theta^{\mathbf{t}} = \varepsilon$, and $\mathbf{t} \in \mathfrak{P}(I)$ since $\varepsilon = \theta_1^a \dots \theta_k^a$. □

Recall that we may consider the family $L_M(I)$ as an S-module if we define $F(\theta)\mu = F(\mathbf{x})\mu$ for any $F(\mathbf{x}) \in \mathcal{P}_k$, $\mu \in L_M(I)$.

6.23. Proposition. *If $\mu \in M^{(k)}$ is a periodic (reversible) sequence, then $I = \operatorname{An}(\mu)$ is a periodic (reversible) ideal. If I is a periodic ideal of $\mathcal{P}_k$, then any sequence $\mu \in L_M(I)$ is periodic. Moreover, μ is reversible iff $\mu = \varepsilon\mu$. If $\mu \in L_M(I)$, then*

$$\mathcal{O}(\mu) = \mathcal{O}(I)\mu; \tag{6.10}$$

$$\mathcal{T}(\mu) = \mathcal{T}(I)\mu; \tag{6.11}$$

$$\mathfrak{P}(I) < \mathfrak{P}(\mu); \tag{6.12}$$

$$D(\mu) \le D(I); \qquad T(\mu) | T(I). \tag{6.13}$$

If, in addition, $I = \operatorname{An}(\mu)$, then

$$\mathfrak{P}(\mu) = \mathfrak{P}(I); \qquad D(\mu) = D(I); \qquad T(\mu) = T(I). \tag{6.14}$$

□ The first statement follows from 5.18 and 6.16. The equality (6.10) follows from Definitions 5.21, 6.16, and from the equality $\mathbf{x}^{\mathbf{i}}\mu = \theta^{\mathbf{i}}m$.

Any sequence $\nu = \delta\mu$, where $\delta \in \mathcal{T}(I)$, is reversible, since for any $\mathbf{i} \in \mathbf{N}_0^k$ we have $\theta^{\mathbf{i}}\delta \in \mathcal{T}(I)$ and hence there exists $\mathbf{j} \in \mathbf{N}_0^k$ such that $\theta^{\mathbf{j}}(\theta^{\mathbf{i}}\delta) = \delta$. This means that $\mathbf{x}^{\mathbf{j}}(\mathbf{x}^{\mathbf{i}}\mu) = \nu$, and by 5.20 $\nu \in \mathcal{T}(\mu)$, i.e., $\mathcal{T}(I)\mu \subseteq \mathcal{T}(\mu)$. Conversely, let $\nu \in \mathcal{T}(\mu)$. Then $\nu = \theta^{\mathbf{t}}\nu$ for all $\mathbf{t} \in \mathfrak{P}(\mu)$ and we can choose $\mathbf{t} \in \mathfrak{P}(\mu)$ such that $\theta^{\mathbf{t}} = \varepsilon$. Therefore, $\nu = \varepsilon\nu$ and $\nu \in \mathcal{T}(I)\mu$ since $\nu = \theta^{\mathbf{l}}\mu$ for a suitable $\mathbf{l} \in \mathbf{N}_0^k$. Hence, (6.11) is true.

If $\mathbf{t} \in \mathfrak{P}(I)$, then $\varepsilon\theta^{\mathbf{t}} = \varepsilon$, $\varepsilon\theta^{\mathbf{t}}\mu = \varepsilon\mu$, and since $\varepsilon = \theta^{\mathbf{l}}$, we have $\mathbf{t} \in \mathfrak{P}(\mu)$, i.e., (6.12) is true.

If the sequence $\mathbf{x}^{\mathbf{l}}\mu$ is not reversible, i.e., $\mathbf{x}^{\mathbf{l}}\mu \in \mathcal{O}(\mu)\backslash\mathcal{T}(\mu)$, then $\varepsilon\theta^{\mathbf{l}}\mu \ne \varepsilon\mu$. Therefore, $\theta^{\mathbf{l}} \notin \mathcal{T}(I)$, and $D(\mu) \le D(I)$.

Note that $\mathcal{K}(\mu) = \{\delta \in \mathcal{T}(I) \mid \delta\mu = \mu\}$ is a subgroup of $\mathcal{T}(I)$ and, by (6.11), $|\mathcal{T}(\mu)| = |\mathcal{T}(I)/\mathcal{K}(\mu)|$. Hence $T(I) = T(\mu)|\mathcal{K}(\mu)|$, and (6.13) is true.

Under the condition $I = \mathrm{An}(\mu)$ for any $\mathbf{i}, \mathbf{j} \in \mathbf{N}_0^k$ the equality $\mathbf{x}^{\mathbf{i}}\mu = \mathbf{x}^{\mathbf{j}}\mu$ is equivalent to the equality $\theta^{\mathbf{i}} = \theta^{\mathbf{j}}$. Therefore, (6.14) is true. □

Now let R be a finite ring and I be a reversible ideal of $\mathcal{P}_k$ with operator ring S. Then S is a finite ring and according to 6.17(b)

$$\mathcal{T}(I) = \langle \theta_1, \ldots, \theta_k \rangle < S^*, \qquad T(I) \mid |S^*|$$

(see also (5.11)).

6.24. Definition. We call a reversible ideal $I \triangleleft \mathcal{P}_k$ over a finite ring R *full-cycle* if $I \cap R = 0$, $L_R(I)$ is a cyclic S-module, and $\mathcal{T}(I) = S^*$. A reversible recurrence $u \in L_R(I)$ with annihilator $I = \mathrm{An}(u)$ is called *full-cycle* if $L_R(I) = Su$ and I is a full-cycle ideal.

6.25. Proposition. *Let R be a finite ring and $I \triangleleft \mathcal{P}_k$ be a reversible ideal such that*

$$I \cap R = 0, \qquad L_R(I) = Su. \tag{6.15}$$

Then

$$\mathfrak{P}(u) = \mathfrak{P}(I), \tag{6.16}$$

and I is a full-cycle ideal iff

$$\forall\, v \in L_R(I)\ \ ((\mathfrak{P}(v) = \mathfrak{P}(I)) \Rightarrow (v \in \mathcal{T}(u))). \tag{6.17}$$

□ The equality (6.16) follows from (6.15). Let I be a full-cycle ideal. Then

$$\mathcal{T}(I) = \langle \theta_1, \ldots, \theta_k \rangle = S^*, \qquad \mathcal{T}(u) = S^*u. \tag{6.18}$$

Let $v \notin \mathcal{T}(u)$. Then, by (6.18), $v = \alpha u$, where $\alpha \in S^*$. We may suppose that $S \neq GF(2)$. Then there exists $\delta \in S^* \backslash e$ such that $\delta\alpha = \alpha$. By (6.18), $\delta = \theta^{\mathbf{t}}$, $\mathbf{t} \in \mathbf{N}_0^k \backslash \mathfrak{P}(u)$. But $\mathbf{t} \in \mathfrak{P}(v)$ since $\delta v = \delta\alpha u = \alpha u = v$. Therefore, $\mathfrak{P}(v) \neq \mathfrak{P}(u)$, and (6.17) is true.

Conversely, let (6.17) be true. If $\mathcal{T}(I) \neq S^*$, then there exists $\delta \in S^* \backslash \mathcal{T}(I)$. Let $v = \delta u$. Then $v \notin \mathcal{T}(u)$, but $\mathfrak{P}(v) = \mathfrak{P}(u)$, since for any $\mathbf{t} \in \mathbf{N}_0^k$ we have

$$\mathbf{t} \in \mathfrak{P}(v) \Leftrightarrow \theta^{\mathbf{t}} v = v \Leftrightarrow \theta^{\mathbf{t}}\delta u = \delta u \Leftrightarrow \theta^{\mathbf{t}} u = u \Leftrightarrow \mathbf{t} \in \mathfrak{P}(u). \quad \square$$

6.26. Proposition. *Let R, Q be finite quasi-Frobenius rings, $R < Q$. Then there exists a full-cycle recurrence u over R such that the ring S of operators of u is isomorphic to Q.*

□ Let $Q^* = \langle \alpha_1, \ldots, \alpha_k \rangle$. Then $Q = R[\alpha_1, \ldots, \alpha_k]$, and for some monic ideal $I \triangleleft \mathcal{P}_k$ there exists an isomorphism

$$\sigma :\ Q \to \mathcal{P}_k/I = S = R[\theta_1, \ldots, \theta_k], \qquad \sigma(\alpha_s) = \theta_s, \qquad s \in \overline{1,k}.$$

Since ${}_RR$ is a QF-module, we have, by 4.7 (for $Q = R$), $L_R(I) = Su$ is a cyclic S-module, and by 4.6, $\mathrm{An}(u) = I$. Now it is sufficient to note that I is a full-cycle ideal by the definition of I. □

The important special cases of full-cycle recurrences and k-maximal recurrences over Galois fields and rings will be investigated below in Sections 12 and 19.

7. The Cyclic Type of Reversible LRS-Families over a Finite Module

A. Decomposition of a family to the cycles [37, 44, 70, 139, 150].

7.1. Definition. A k-LRS-family $L_M(I)$ is called *reversible* if any sequence $\mu \in L_M(I)$ is reversible.

7.2. Proposition. *If $I \triangleleft \mathcal{P}_k$ is a reversible ideal, then $L_M(I)$ is a reversible family. If $L_M(I)$ is a reversible family and ${}_RM$ is a finitely generated module, then $I' = \mathrm{An}(L_M(I))$ is a reversible ideal of $\mathcal{P}_k$ and $L_M(I) = L_M(I')$.*

□ The first statement follows from 6.22. If $L_M(I) = \mathcal{P}_k\mu_1 + \ldots + \mathcal{P}_k\mu_t$ is a reversible family, then I' contains the reversible ideal $\mathrm{An}(\mu_1) \cap \ldots \cap \mathrm{An}(\mu_t)$. □

Define the relation $\sim$ on the k-LRS-family $L_M(I)$ by

$$\mu \sim \nu \Leftrightarrow \exists\, \mathbf{i} \in \mathbf{N}_0^k :\ \mathbf{x}^{\mathbf{i}}\mu = \nu \qquad (\mu, \nu \in L_M(I)).$$

7.3. Proposition. *The relation $\sim$ is an equivalence relation on $L_M(I)$ iff $L_M(I)$ is a reversible family* (see 5.20). □

7.4. Corollary. *Let $F_1(x_1), \ldots, F_k(x_k) \in \mathcal{P}_k$ be monic elementary polynomials, ${}_RM$ be a faithful f.g.-module. Then $\sim$ is an equivalence relation on $L_M(F_1, \ldots, F_k)$ iff the polynomials $F_1(x_1), \ldots, F_k(x_k)$ are reversible.* □

7.5. Proposition. *If $I \lhd \mathcal{P}_k$ is a reversible ideal, then the relation $\sim$ decomposes $L_M(I)$ into classes of equivalent sequences, and the class of $\mu \in L_M(I)$ is $\mathcal{T}(\mu) = \mathcal{T}(I)\mu$, i.e., the cycle of μ.* □

In what follows in this section, ${}_RM$ is a faithful f.g.-module over a finite ring R, $I \lhd \mathcal{P}_k$ is a reversible ideal. In this case $L_M(I)$ is a finite family. It can be characterized by the following parameters. For $t \in \mathbf{N}$ define $N_I^M(t)$ as the number of recurrences $\mu \in L_M(I)$ of the period $T(\mu) = t$; $C_I^M(t)$ — as the number of cycles of cardinality t in $L_M(I)$. Obviously, only a finite number of these parameters is not equal to 0, and $N_I^M(t) = C_I^M(t)t$.

B. The cyclic type of a reversible 1-LRS-family [48, 70, 150].

7.6. Definition. Let $I \lhd \mathcal{P} = \mathcal{P}_1$ be a reversible ideal. The polynomial

$$Z_I^M(y) = \sum_{t \geq 1} C_I^M(t) y^t$$

over $\mathbf{Z}$ is called the *cyclic type* of the finite reversible family $L_M(I)$.

7.7. Definition. The composition of polynomials $A(y) = \sum_{i \geq 1} a_i y^i$ and $B(y) = \sum_{i \geq 1} b_i y^i$ over $\mathbf{Z}$ is the polynomial $C(y) = \sum_{t \geq 1} c_t y^t$, where

$$c_t = \sum_{i,j \geq 1,\, [i,j]=t} a_i b_j (i,j), \qquad t \in \mathbf{N}.$$

Notation: $C(y) = A(y) * B(y)$.

It is easy to show that $y^i * y^j = (i,j) y^{[i,j]}$ and

$$C(y) = \sum_{i \geq 1} \sum_{j \geq 1} a_i b_j (i,j) y^{[i,j]} = \sum_{i,j \geq 1} a_i b_j y^i * y^j.$$

7.8. Proposition. *Let $\mathbf{Z}_1[y]$ be the set of all polynomials from $\mathbf{Z}[y]$ with zero constant term. Then $(\mathbf{Z}_1[y], +, *)$ is a commutative ring with unit y. If $B^{(s)}(y) = \sum_{t \geq 1} b_t^{(s)} y^t \in \mathbf{Z}_1[y]$ for $s \in \overline{1,r}$, then*

$$B^{(1)}(y) * \ldots * B^{(r)}(y) = \sum_{t \geq 1} \Big(\sum_{t_1, \ldots, t_r \geq 1} \frac{t_1 \ldots t_r}{[t_1, \ldots, t_r]} \cdot b_{t_1}^{(1)} \ldots b_{t_r}^{(r)} \Big) \cdot y^t.$$

7.9. Definition. The ring $(\mathbf{Z}_1[y], +, *)$ is called the *ring of cyclic types* (for 1-LRS-families).

The operation of composition of the cyclic types enables us to reduce the evaluation of cyclic types of reversible LRS-families to more simple families (see [48]).

7.10. Proposition. *If ${}_RM$ is a direct sum of submodules $M = M_1 \dot{+} \ldots \dot{+} M_r$, then*

$$Z_I^M(y) = Z_I^{M_1}(y) * \ldots * Z_I^{M_r}(y).$$

If an ideal $I \lhd \mathcal{P}$ is the product of comaximal ideals, $I = I_1 I_2 = I_1 \cap I_2$, $I_1 + I_2 = \mathcal{P}$, then

$$Z_I^M(y) = Z_{I_1}^M(y) * Z_{I_2}^M(y).$$

□ In both cases $L_M(I)$ is a direct sum, $L_M(I) = L_{M_1}(I) \dot{+} L_{M_2}(I)$ and $L_M(I) = L_M(I_1) \dot{+} L_M(I_2)$ respectively. Let $\mu = \mu_1 + \mu_2$ be the appropriate decomposition of a recurrence $\mu \in L_M(I)$. Then, by 5.8, $T(\mu) = [T(\mu_1), T(\mu_2)]$ and, depending on what case is considered,

$$N_I^M(t) = \sum_{[t_1,t_2]=t} N_I^{M_1}(t_1) N_I^{M_2}(t_2), \qquad N_I^M(t) = \sum_{[t_1,t_2]=t} N_{I_1}^M(t_1) N_{I_2}^M(t_2).$$

Therefore,

$$C_I^M(t) = N_I^M(t)/t = \sum_{[t_1,t_2]=t} (t_1, t_2) C_I^{M_1}(t_1) C_I^{M_2}(t_2)$$

or, respectively,

$$C_I^M(t) = \sum_{[t_1,t_2]=t} (t_1, t_2) C_{I_1}^M(t_1) C_{I_2}^M(t_2). \quad \square$$

In connection with these results, we formulate some open problems.

1. Describe indecomposable cyclic types in the *semigroup* $(\mathbf{Z}_1^+[y], *)$ *of cyclic types*, where $\mathbf{Z}_1^+[y]$ is the set of polynomials from $\mathbf{Z}_1[y]$ with nonnegative coefficients.

2. Describe linear cyclic types in $\mathbf{Z}_1^+[y]$, i.e., polynomials $Z(y) \in \mathbf{Z}_1^+[y]$ such that $Z(y) = Z_I^M(y)$ for some finite module ${}_RM$ and reversible ideal $I \triangleleft \mathcal{P}$.

3. Describe linear cyclic types which cannot be represented as a nontrivial composition of cyclic types.

These problems are connected with the investigation of the algebraic properties of the ring $(\mathbf{Z}_1[y], +, *)$. The last problem is interesting by itself.

The first result in this area can be formulated as follows.

7.11. Proposition. *A cyclic type $A(y) = a_0 y + a_1 y^t \in \mathbf{Z}_1^+[y]$ is indecomposable in $\mathbf{Z}_1[y]$ in the following cases.*

(a) *if $a_1 < t + 2\sqrt{a_0}$;*

(b) *if a_0 is a simple number and $a_1 < t + a_0 + 1$.*

If $a_0 = r^2$ and $a_1 = t + 2r$, $r \in \mathbf{N}$, then

$$A(y) = (ry + y^t) * (ry + y^t).$$

If $a_1 = t + a_0 + 1$, then

$$A(y) = (y + y^t) * (a_0 y + y^t).$$

□ If

$$A(y) = B(y) * C(y), \tag{7.1}$$

then $B(y) = b_0 y + b_1 y^t$, $C(y) = c_0 y + c_1 y^t$ and

$$b_0 c_0 = a_0, \tag{7.2}$$

$$b_0 c_1 + b_1 c_0 + b_1 c_1 t = a_1. \tag{7.3}$$

Thus, in the general case, the problem of the description of decompositions (7.1) of a cyclic type $A(y)$ reduces to the description of all decompositions (7.2), where b_0, $c_0 \in \mathbf{N}$, and to the solution of the appropriate Diophantine equation (7.3) in two unknowns b_1, $c_1 \in \mathbf{N}$. It remains to note that under the conditions (a), (b) the system (7.2), (7.3) has only a trivial solution. □

C. Reversible k-LRS-families. To obtain an analogue of 7.10 for k-LRS-families, we formulate the definition of the cyclic type in another way.

Let $\mathcal{H}_k$ be the set of all subgroups $\mathcal{G} < \mathbf{Z}^k$ of rank k such that $\mathcal{G}$ is generated by the set $\mathcal{G}^+$ of its nonnegative vectors.

7.12. Lemma. *$\mathcal{H}_k$ is a semigroup with respect to the operation $\cap$ of intersection of semigroups.*

□ Let $\mathcal{G}_1, \mathcal{G}_2 \in \mathcal{H}_k$ and $\mu_s \in M_s^{(k)}$ be sequences such that $\mathfrak{P}(\mu_s) = \mathcal{G}_s$, $s = 1, 2$ (see 5.12). Then the sequence $\mu = (\mu_1, \mu_2)$ over module $M = M_1 \oplus M_2$ satisfies $\mathfrak{P}(\mu) = \mathcal{G}_1 \cap \mathcal{G}_2$ (Proposition 5.28). Therefore, $\mathcal{G}_1 \cap \mathcal{G}_2 \in \mathcal{H}_k$. □

Denote $\mathbf{Z}[\mathcal{H}_k]$ to be the semigroup algebra of a semigroup $\mathcal{H}_k$ over $\mathbf{Z}$.

7.13. Definition. The *cyclic type* of a finite reversible k-LRS-family $L_M(I)$ is the element Z_I^M of the algebra $\mathbf{Z}[\mathcal{H}_k]$ of the form

$$Z_I^M = \sum_{\mathcal{G} \in \mathcal{H}_k} C_I^M(\mathcal{G})\mathcal{G},$$

where $C_I^M(\mathcal{G})$ is the number of cycles $T(\mu) \subseteq L_M(I)$ with $\mathfrak{P}(\mu) = \mathcal{G}$.

In the case $k = 1$, Definition 7.13, coincides, essentially, with 7.6. In fact, each subgroup $\mathcal{G} \in \mathcal{H}_1$ is generated by the number $t = [\mathbf{Z} : \mathcal{G}]$, and the cyclic type $Z_I^M = \sum_{t \geq 1} C_I^M(\langle t \rangle)\langle t \rangle$ from 7.13 is nothing else but the cyclic type $Z_I^M(y) = \sum_{t \geq 1} C_I^M(t) y^t$ from 7.6.

7.14. Definition. *The composition of elements* $A = \sum_{\mathcal{G} \in \mathcal{H}_k} a_{\mathcal{G}}\mathcal{G}$ and $B = \sum_{\mathcal{G} \in \mathcal{H}_k} b_{\mathcal{G}}\mathcal{G}$ of the ring $\mathbf{Z}[\mathcal{H}_k]$ is the element $C = \sum_{\mathcal{G} \in \mathcal{H}_k} c_{\mathcal{G}}\mathcal{G}$, where

$$c_{\mathcal{G}} = \sum_{\mathcal{G}_1 \cap \mathcal{G}_2 = \mathcal{G}} [\mathbf{Z}^k : \mathcal{G}_1 + \mathcal{G}_2] a_{\mathcal{G}_1} b_{\mathcal{G}_2} = \sum_{\mathcal{G}_1 \cap \mathcal{G}_2 = \mathcal{G}} \frac{[\mathbf{Z}^k : \mathcal{G}_1][\mathbf{Z}^k : \mathcal{G}_2]}{[\mathbf{Z}^k : \mathcal{G}]} \cdot a_{\mathcal{G}_1} b_{\mathcal{G}_2}.$$

7.15. Proposition. *The algebra* $(\mathbf{Z}[\mathcal{H}_k], +, *)$ *is a commutative ring with unit* $\mathbf{Z}^k$. *If* $B_s = \sum_{\mathcal{G} \in \mathcal{H}_k} b_{\mathcal{G}}^{(s)}\mathcal{G} \in \mathbf{Z}[\mathcal{H}_k]$ *for* $s \in \overline{1, r}$, *then*

$$B_1 * \ldots * B_r = \sum_{\mathcal{G} \in \mathcal{H}_k} \Big(\sum_{\mathcal{G}_1 \cap \ldots \cap \mathcal{G}_r = \mathcal{G}} \frac{[\mathbf{Z}^k : \mathcal{G}_1] \ldots [\mathbf{Z}^k : \mathcal{G}_r]}{[\mathbf{Z}^k : \mathcal{G}]} \cdot b_{\mathcal{G}_1}^{(1)} \ldots b_{\mathcal{G}_r}^{(r)} \Big) \mathcal{G}. \square$$

7.16. Definition. The ring $(\mathbf{Z}[\mathcal{H}_k], +, *)$ is called the *ring of cyclic types* for k-LRS-families.

7.17. Proposition. *Let* $L_M(I)$ *be a finite reversible* k*-LRS-family. If* $M = M_1 \dotplus M_2$ *is the direct sum of submodules, then* $Z_I^M = Z_I^{M_1} * Z_I^{M_2}$. *If* $I = I_1 I_2$ *is the product of comaximal ideals, then* $Z_I^M = Z_{I_1}^M * Z_{I_2}^M$. □

8. Extensions of 1-Sequences [46]

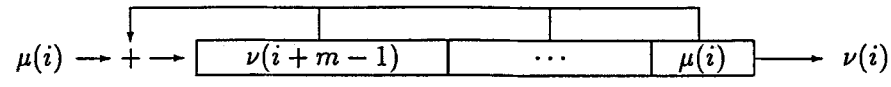
8.1. Definition. The sequence $\nu \in M^{(1)}$ is called an *extension* of the sequence $\mu \in M^{(1)}$ with the help of a polynomial $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0 \in \mathcal{P}$ and an initial vector $\alpha = (a_0, \ldots, a_{m-1}) \in M^m$ if $\nu(\overline{0, m-1}) = \alpha$, $F(x)\nu = \mu$, i.e.,

$$\nu(\overline{0, m-1}) = \alpha, \qquad \nu(i+m) = f_{m-1}\nu(i+m-1) + \ldots + f_0\nu(i) + \mu(i), \qquad i \in \mathbf{N}_0. \tag{8.1}$$

We write $\nu = (\alpha \frac{\mu}{F})$. If $\mu = (a, a, \ldots)$ is a constant sequence, then the sequence ν from (8.1) is called an *affine recurrence* of order m.

In particular, the congruent sequence from Example 1.4 is an affine recurrence, namely, the extension of sequence $(\delta, \delta, \ldots)$ by the polynomial $x - q$.

The sequence ν from (8.1) is an output of the following nonautonomous automaton:



LRS $F(x)$ over M

8.2. Proposition. *Under the condition* (8.1) *we have*

$$\mathrm{An}\,(\nu) = (An(\mu) : F(x)); \tag{8.2}$$

$$F(x) \cdot \mathrm{An}(\mu) \subseteq \mathrm{An}(\nu) \subseteq \mathrm{An}(\mu). \tag{8.3}$$

If $G(x) \in \mathcal{P}$ is a monic polynomial, then

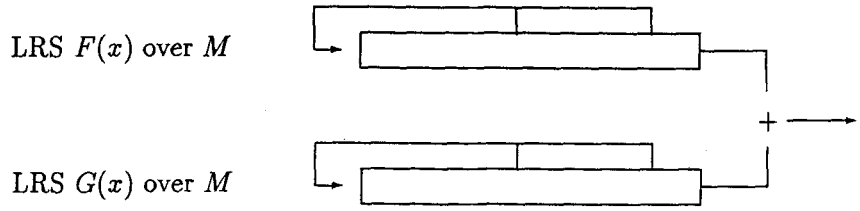
$$L_M(FG) = \{\nu \in M^{(1)} \mid F(x)\nu \in L_M(G)\}, \tag{8.4}$$

$$L_M(FG) = \left\{\left(\alpha \frac{\mu}{F}\right) \Big| \, \alpha \in M^m, \ \mu \in L_M(G)\right\}, \tag{8.5}$$

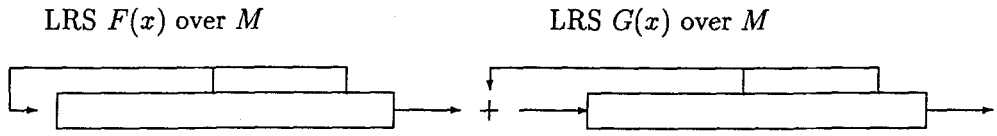
i.e., $L_M(FG)$ is the set of all extensions of sequences $\mu \in L_M(G)$ with help of the polynomial $F(x)$. □

8.3. Corollary. *A sequence ν of the form* (8.1) *is an LRS iff μ is an LRS. An affine recurrence of order m is an LRS of order $m+1$. If ${}_RM$ is a finite module, then ν is a periodic sequence iff μ is periodic, and $D(\nu) \geq D(\mu)$, $T(\mu) | T(\nu)$.* □

8.4. Remark. Propositions 4.2 and 4.3 imply that the set of all output sequences of the sum of two LRS



is $L_M((F) \cap (G)) \subseteq L_M(FG)$, and this set coincides with $L_M(FG)$ only if $(F, G) = (e)$. At the same time, Proposition 8.2 implies that the set of all output sequences of the composition of the same LRS



is an automaton with the set of output sequences $L_M(FG)$ independently of the properties of polynomials F and G.

Extensions of k-sequences are considered in Section 14.I.

9. Regular Extracts of a 1-LRS [7, 116, 138, 142]

Recall that, by Definition 5.13, for $l \in \mathbb{N}_0$, $d \in \mathbb{N}$ the *regular (l,d)-extract* of the sequence $\mu \in M^{(1)}$ is a sequence $\nu = \mu^{[l,d]}$ of the form

$$\nu(z) = \mu(l + dz). \tag{9.1}$$

We call ν a d-extract of μ (sometimes ν is also called a *decimated sequence* [142]). Recall that $S(F)$ is the accompanying matrix of a monic polynomial $F(x)$ (see 1.9).

9.1. Proposition. *Let ν be the regular (l,d)-extract from a recurrence $\mu \in L_M(F)$, and $B = S(F)^d$. Then ν is an LRS of order $m = \deg F(x)$ with characteristic polynomial $\chi_B(x)$. The annihilator of ν consists of all polynomials $H(x) \in \mathcal{P}$ satisfying the condition*

$$\mu(\overline{0, m-1})H(B)A_l = 0, \tag{9.2}$$

where $A_l = (\hat{S}_l, B\hat{S}_l, \ldots, B^{m-1}\hat{S}_l)$, $\hat{S}_l$ *is the first column of the matrix* $S(F)^l$.

□ Since $\mu(z) = \mu(\overline{0, m-1})\hat{S}_z$ (see (1.2)), from (9.1) we have

$$\nu(z) = \mu(\overline{0, m-1})B^z\hat{S}_l. \tag{9.3}$$

Then, for any $H(x) \in \mathcal{P}$, the sequence $\xi = H(x)\nu$ has the form

$$\xi(z) = \mu(\overline{0, m-1})H(B)B^z\hat{S}_l. \tag{9.4}$$

This implies the equality $\chi_B(x)\nu = 0$, and since $\deg \chi_B(x) = m$, we have $(H(x) \in \mathrm{An}\,(\mu)) \Leftrightarrow (\xi(\overline{0, m-1}) = 0) \Leftrightarrow$ (9.2). □

9.2. Remark. The equality (9.2), which describes the ideal $\mathrm{An}\,(\nu)$, cannot be substituted by the equality $\mu(\overline{0, m-1})H(B) = 0$ even if $M = R$ is a field. For example, let $R = \mathbf{Z}_3$ and $\mu = (0, 1, 2, 2, 0, 2, 1, 1, 0, 1, 2, \ldots)$ be the LRS with minimal polynomial $F(x) = x^2 - 2x - 1$. Then $\nu = \mu^{[0,4]}$ is a zero sequence; however $B = S(F)^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, and the minimal polynomial of the vector $\mu(\overline{0,1}) = (0, 1)$ with respect to the matrix B is equal to $x - 2$. Therefore, the polynomial $H(x) = 1 \in \mathrm{An}\,(\nu)$ does not satisfy the condition $\mu(\overline{0, m-1})H(B) = 0$.

Let us consider the set $L_M^{(d)}(F)$ of all regular d-extracts of recurrences of the family $L_M(F)$. For a square matrix B over the ring R, we define

$$\mathrm{An}\,(B) = \{H(x) \in \mathcal{P} |\ H(B) = 0\}.$$

If $B = S(F)^d$, then, according to Proposition 9.1,

$$L_M^{(d)}(F) \subseteq L_M(\mathrm{An}\,(B)). \tag{9.4}$$

This relation may be refined.

9.3. Proposition. (a) *If* ${}_RM$ *is a finitely generated* R*-module, then* $L_M^{(d)}(F)$ *is a finitely generated (over the ring* R*)* $\mathcal{P}$*-module, i.e.,* $L_M^{(d)}(F) \in \mathfrak{M}_1(M)$ (see Section 4B), *and*

$$\mathrm{An}\,(L_M^{(d)}(F)) = \mathrm{An}\,(B). \tag{9.6}$$

(b) *If* ${}_RM$ *is a QF-module* (see 4.5), *then*

$$L_M^{(d)}(F) = L_M(\mathrm{An}\,(B)). \tag{9.7}$$

(c) *If* $G(x)$ *is the minimal polynomial of the matrix* B *and* $\deg G(x) = n$, *then the equality*

$$L_R^{(d)}(F) = L_R(G) \tag{9.8}$$

holds iff the matrix $A_0 = (\hat{E}_1, B\hat{E}_1, \ldots, B^{m-1}\hat{E}_1)$ *is invertible on the left side. Under this condition* $\mathrm{An}\,(B) = \mathcal{P}G(x)$.

□ (a) $L_M^{(d)}(F)$ is a $\mathcal{P}$-module, since for any recurrence $\mu \in L_M(F)$ we have $x\mu^{[l,d]} = \mu^{[l+d,d]} \in L_M^{(d)}(F)$. By 2.2, $L_M(F) = R\mu_1 + \ldots + R\mu_s$ is an f.g.-R-module; hence $L_M^{(d)}(F) = \sum_{l=0}^{d-1}\sum_{t=1}^{s} R\mu_t^{[l,d]}$ is an f.g.-R-module. The family $L_M^{(d)}(F)$ is the set of all $(0, d)$-extracts from sequences of the family $L_M(F)$. Therefore, by 9.1, a polynomial $H(x) \in \mathcal{P}$ belongs to $\mathrm{An}\,(L_M^{(d)}(F))$ iff

$$\forall\, \alpha \in M^m \qquad (\alpha H(B)A_0 = 0), \tag{9.9}$$

where $A_0 = (\hat{E}_1, B\hat{E}_1, \ldots, B^{m-1}\hat{E}_1)$ is the matrix of the first columns of the matrices $E, B, \ldots, B^{m-1}$. The condition (9.9) is equivalent to the condition

$$H(B)\hat{E}_1 = 0. \tag{9.10}$$

Since $H(B) = H(S(F)^d)$ is a linear combination of the powers of the accompanying matrix, (9.10) is equivalent to the equality $H(B) = 0$, i.e., (9.6) holds.

(b) Since $L_M^{(d)}(F) \in \mathfrak{M}_k$, (9.7) follows from (9.6) and 4.6.

(c) It follows from (9.3) (for $l = 0$) that a sequence $\nu \in L_M(G)$ belongs to $L_M^{(d)}(F)$ iff

$$\nu(\overline{0, m-1}) = \mu(\overline{0, m-1})A, \text{ where } \mu \in L_M(F).$$

Hence (9.8) is equivalent to the condition $R^m A = R^n$, which means that the matrix A is invertible on the left side. In the last case, the system of columns of the matrix A is linearly independent over R, and therefore the matrix B is not annihilated by polynomials of degree less than n. Hence $\operatorname{An}(B) = \mathcal{P}G(x)$. □

9.4. Remark. In the general case, the inclusion (9.5) is not an equality. For example, let $R = \mathbb{Z}_2[x_1, x_2]/I$, where $I = (x_1^2, x_2^2, x_1x_2)$, and $\alpha_s = x_s + I \in R$, $s = 1, 2$. Let $F(x) = x^2 - \alpha_1 x - \alpha_2 \in \mathcal{P}$ and $d = 2$. Then $B = S(F)^2 = \begin{pmatrix} \alpha_2 & 0 \\ \alpha_1 & \alpha_2 \end{pmatrix}$, $\operatorname{An}(B) = (x^2, \alpha_1, \alpha_2)$, and the family $L_R(\operatorname{An}(B))$ consists of all sequences of the form $(\beta_0, \beta_1, 0, 0, \ldots)$, where $\beta_0, \beta_1 \in R\alpha_1 + R\alpha_2$. Then the inclusion (9.5), which has in the case under consideration the form $L_R^{(2)}(F) \subseteq L_R(\operatorname{An}(B))$, is strict. For example, the sequence $\nu = (0, \alpha_2, 0, 0, \ldots) \in L_R(\operatorname{An}(B))$ does not belong to $L_R^{(2)}(F)$. In fact, if $\nu \in L_R^{(2)}(F)$, then, by (9.3), the system of linear equations

$$(0, \alpha_2) = (y_1, y_2)\begin{pmatrix} e & \alpha_2 \\ 0 & \alpha_1 \end{pmatrix},$$

is solvable. But this is not true, since $\alpha_2 \notin R\alpha_1$.

9.5. Remark. The equality (9.8) may not be true even if (in the notation of Proposition 9.3) the matrix B has a unique minimal polynomial. For example, if $M = R = \mathbb{Z}$, $F(x) = x^2 - 2x - 2$, and $d = 2$, then $B = \begin{pmatrix} 2 & 4 \\ 2 & 6 \end{pmatrix}$ and $G(x) = \chi_B(x) = x^2 - 8x + 4$ is the unique minimal polynomial of B. But the LRS $e^G \in L_{\mathbb{Z}}(G)$ does not belong to $L_{\mathbb{Z}}^{(2)}(F)$.

9.6. Corollary. *Let $F(x)$ be a monic polynomial over the field P and $G(x)$ be the minimal polynomial of the matrix $B = S(F)^d$. Then*

$$L_P^{(2)}(F) = L_P(G). \tag{9.11}$$

□ The matrix B is not annihilated by polynomials of degrees less than $n = \deg G(x)$. Therefore, the system of columns of the matrix $A = (\hat{E}_1, B\hat{E}_1, \ldots, B^{n-1}\hat{E}_1)$ is linearly independent and A is invertible on the left side. Now (9.11) follows from Proposition 9.3(c). □

Chapter 2.

LINEAR RECURRING SEQUENCES OVER FIELDS

Here we state some results on the properties of an LRS over a field P. We keep the notations $\mathcal{P} = \mathcal{P}_1 = P[x]$, $\mathcal{P}_k = P[x_1, \ldots, x_k]$. Since the field P is a quasi-Frobenius ring, by Theorem 4.6, for any monic ideals I_1, $I_2 \triangleleft \mathcal{P}_k$ and for finitely generated $\mathcal{P}_k$-submodules $\mathcal{M}_1$, $\mathcal{M}_2 \in P^{(k)}$, the following equalities hold:

$$\operatorname{An}(L_P(I_1)) = I_1, \qquad L_P(\operatorname{An}(\mathcal{M}_1)) = \mathcal{M}_1,$$

$$L_P(I_1 \cap I_2) = L_P(I_1) + L_P(I_2), \qquad L_P(I_1 + I_2) = L_P(I_1) \cap L_P(I_2),$$

$$\operatorname{An}(\mathcal{M}_1 \cap \mathcal{M}_2) = \operatorname{An}(\mathcal{M}_1) + \operatorname{An}(\mathcal{M}_2), \qquad \operatorname{An}(\mathcal{M}_1 + \mathcal{M}_2) = \operatorname{An}(\mathcal{M}_1) \cap \operatorname{An}(\mathcal{M}_2).$$

Note that monic ideals of the ring $\mathcal{P}_k$ are exactly its ideals of zero dimension [13].

10. Bases of LRS-Families and Generating Systems of Their Annihilators

A. Monic and maximal ideals. As was noted in Section 1, an ideal $I \triangleleft \mathcal{P}_k$ is monic iff the ring

$$S = \mathcal{P}_k/I = P[\theta_1, \ldots, \theta_k], \text{ where } \theta_s = x_s + I, \tag{10.1}$$

associated *with this ideal*, is a finite-dimensional P-algebra; moreover,

$$I = \{H(x) \in \mathcal{P}_k |\ H(\theta) = 0\}. \tag{10.2}$$

10.1. Definition. The number

$$\deg I = \dim \mathcal{P}_k/I \tag{10.3}$$

is called the *degree of a monic ideal* $I \triangleleft \mathcal{P}_k$.

10.2. Proposition. *For a monic ideal* $I \triangleleft \mathcal{P}_k$ *there exists a finite subset* $\mathcal{F} \subset \mathbb{N}_0^k$ *such that*

(a) *if* $\mathrm{j} \in \mathcal{F}$, $\mathrm{i} \in \mathbb{N}_0^k$, $\mathrm{i} \le \mathrm{j}$, *then* $\mathrm{i} \in \mathcal{F}$;

(b) *the set* $\mathcal{B} = \{\theta^{\mathrm{i}} |\ \mathrm{i} \in \mathcal{F}\}$ *is a base of the vector space* S_P. □

10.3. Definition. Under the notation of Proposition 10.2, the set $\mathcal{F} \subset \mathbb{N}_0^k$ is called the *Ferre diagram of the ideal* I [71], and the base $\mathcal{B}$ is called the *Ferre base of the ring* S.

In general, the Ferre diagram of the ideal I is not unique. But if $I = (f_1(x_1), \ldots, f_k(x_k))$ is an elementary ideal, $\deg f_s(x_s) = m_s$, $s \in \overline{1,k}$, then $\deg I = m_1 \ldots m_k$ and the unique Ferre diagram of I is $\mathcal{F} = \Pi(\mathrm{m})$ (see Section 2.B).

10.4. Proposition. *Any monic ideal* I *contains a unique elementary ideal* $\mathcal{E}(I)$, *which contains all elementary ideals belonging to* I.

We call $\mathcal{E}(I)$ the *elementary ideal of the ideal* I.

□ $\mathcal{E}(I)$ is the sum of all elementary ideals belonging to I. □

In what follows, we shall concentrate mainly on maximal ideals of the ring $\mathcal{P}_k$. The following results are based on [13].

10.5. Proposition. *Each maximal ideal of the ring* $\mathcal{P}_k$ *is monic. For a monic ideal* $I \triangleleft \mathcal{P}_k$ *of degree* n, *the following conditions are equivalent:*

(a) *the ring* $S = \mathcal{P}_k/I$ *associated with the ideal* I (see (10.1)), *is a field;*

(b) *I is a maximal ideal;*

(c) *I is a prime ideal;*

(d) *there exists an extension $Q = P[\alpha_1, \dots, \alpha_k]$ of degree n of the field P such that*

$$I = \{H(\mathbf{x}) \in \mathcal{P}_k |\ H(\alpha) = 0\}. \tag{10.4}$$

Under the condition (d) *the following equality holds:*

$$\mathcal{E}(I) = (f_1(x_1), \dots, f_k(x_k)),$$

where $f_s(x) = \mu_{\alpha_s, P}(x)$ is the minimal polynomial of the element α_s over the field P. □

10.6. Corollary. *A maximal ideal $I \lhd \mathcal{P}_k$ of degree n has a generating system*

$$g_1(x_1), g_2(x_1, x_2), \dots, g_k(x_1, \dots, x_k) \tag{10.5}$$

such that each polynomial $g_s(x_1, \dots, x_s)$ is irreducible over P and is a monic (with respect to x_s) polynomial of degree n_s, where $n_1 \dots n_k = n$ and $\Pi(\mathbf{n})$ is a Ferre diagram of the ideal I.

□ Suppose that the conditions of Proposition 10.5(d) are fulfilled. Let

$$P_0 = P, \qquad P_s = P[\alpha_1, \dots, \alpha_s], \qquad n_s = [P_s : P_{s-1}], \qquad s \in \overline{1,k}. \tag{10.6}$$

The polynomial $\mu_{\alpha_s, P_{s-1}}(x)$ has the form

$$\mu_{\alpha_s, P_{s-1}}(x) = g_s(\alpha_1, \dots, \alpha_{s-1}, x), \tag{10.7}$$

where $g_s(x_1, \dots, x_s) \in \mathcal{P}_k$ is a polynomial of the form

$$g_s(x_1, \dots, x_s) = x_s^{n_s} - \sum_{i=0}^{n_s - 1} g_s^{(i)}(x_1, \dots, x_{s-1}) x_s^i.$$

It is evident that under the condition (10.7) the system (10.5) generates the ideal I. □

Note that the generating system (10.5) is a Groebner base of the ideal I [10, 36].

10.7. Corollary. *If P is a finite field, then for any $n \in \mathbf{N}$ there exists a maximal ideal of the ring $\mathcal{P}_k$ of degree n.* □

10.8. Definition. Under the condition (10.4), we call the row $\alpha = (\alpha_1, \dots, \alpha_k)$ a *common root* of the prime ideal $I \lhd \mathcal{P}_k$ in the field Q [13], and we say that Q is the *field of the root α of the ideal I.*

B. Bases of LRS-families.

10.9. Proposition. *Let I be a monic ideal of the ring $\mathcal{P}_k$ with the Ferre diagram $\mathcal{F} = \{\mathbf{j}_1, \dots, \mathbf{j}_d\}$. Then the family $L_P(I)$ is a space of dimension $\deg I = |\mathcal{F}|$ over P, and each LRS $u \in L_P(I)$ is uniquely defined by the polyhedron of values $u(\mathcal{F}) = (u(\mathbf{j}_1), \dots, u(\mathbf{j}_d))$. A system of recurrences $u_1, \dots, u_d \in L_P(I)$ is a base of the space $L_P(I)$ iff the matrix*

$$\begin{pmatrix} u_1(\mathbf{j}_1, \dots, \mathbf{j}_d) \\ \dots\dots\dots \\ u_d(\mathbf{j}_1, \dots, \mathbf{j}_d) \end{pmatrix}$$

is invertible. If Q is an extension of the field P, then any base of the family $L_P(I)$ is also a base of the family $L_Q(I)$.

□ According to Proposition 10.2, for each $\mathbf{j} \in \mathbf{N}_0^k$ there exists a unique polynomial $h^{(\mathbf{j})}(x) = \sum_{\mathbf{i} \in \mathcal{F}} h_{\mathbf{i}}^{(\mathbf{j})} \mathbf{x}^{\mathbf{i}} \in \mathcal{P}_k$ such that $\theta^{\mathbf{j}} = h^{(\mathbf{j})}(\theta)$. Then, for each k-LRS $u \in L_P(I)$, we have $u(\mathbf{j}) = \sum_{\mathbf{i} \in \mathcal{F}} h_{\mathbf{i}}^{(\mathbf{j})} u(\mathbf{i})$. □

Recall that by Theorem 2.20 and Definition 2.21 each k-LRS over the field P has an analytical representation over some finite algebraic extension of P (see also [90, 91]). Consider the following important special cases.

10.10. Proposition. *Let $I = (f_1(x_1), \dots, f_k(x_k))$ be an elementary ideal and $\deg f_r(x_r) = m_r$, $r \in \overline{1,k}$.*

(a) *If* $f_r(x) = (x - a_{r0}) \dots (x - a_{rm_r-1})$ *is a separable polynomial over* P *for any* $r \in \overline{1,k}$, *then the system of* k*-LRS*

$$\{a^{[0]}_{1s_1} \otimes \dots \otimes a^{[0]}_{ks_k} | \ \mathbf{s} \in \Pi(\mathbf{m})\} \qquad \text{(see 1.24)}$$

is a base of the family $L_P(I)$. *Moreover, if all roots* α_{rs} *are nonzero, then each recurrence* $u \in L_P(I)$ *can be uniquely represented in the form*

$$u(\mathbf{z}) = \sum_{\mathbf{s} \in \Pi(\mathbf{m})} c_{\mathbf{s}} a^{z_1}_{1s_1} \dots a^{z_k}_{ks_k}, \qquad c_{\mathbf{s}} \in P. \tag{10.8}$$

(b) *If* $f_r(x) = (x - e)^{m_r}$, $r \in \overline{1,k}$, *then*

$$\{e^{[s_1]} \otimes \dots \otimes e^{[s_k]} | \ \mathbf{s} \in \Pi(\mathbf{m})\}$$

is a base of the family $L_P(I)$. *Each recurrence* $u \in L_P(I)$ *has the unique representation*

$$u(\mathbf{z}) = \sum_{\mathbf{s} \in \Pi(\mathbf{m})} c_{\mathbf{s}} \binom{z_1}{s_1} \dots \binom{z_k}{s_k}, \qquad c_{\mathbf{s}} \in P. \square$$

10.11. Definition. If, for a sequence $u \in P^{\langle k \rangle}$, there exists a finite algebraic extension Q of the field P such that for some $\mathbf{m} \in \mathbb{N}_0^k$ the sequence u has the representation (10.8), where $c_{\mathbf{s}} \in Q$ and $a_{r0}, \dots a_{rm_r-1} \in Q^*$ are distinct elements for any $r \in \overline{1,k}$, then we say that u is an *exponentially represented sequence* [78]. The set of all such sequences is denoted by $\mathcal{E}P^{\langle k \rangle}$.

Obviously, $u \in \mathcal{E}P^{\langle k \rangle}$ iff $u \in L_P(f_1(x_1), \dots, f_k(x_k))$, where $f_1, \dots, f_k$ are separable polynomials with invertible constant coefficients.

Under the conditions of Proposition 10.10(b), we can construct another basis of the family $L_P(I)$. Let ε_s, $s \in \mathbb{N}_0$, be the following sequence over P:

if char $P = 0$, then $\varepsilon_s(i) = i^s e$, $i \in \mathbb{N}_0$;

if char $P = p > 0$, then $\varepsilon_s(i) = e \cdot \prod_{t \geq 0} i_t^{s_t}$, $i \in \mathbb{N}_0$, where $i = \sum i_t p^t$, $s = \sum s_t p^t$ are the p-ary decompositions of i and s.

10.12. Proposition. *The system of sequences* $\{\varepsilon_{s_1} \otimes \dots \otimes \varepsilon_{s_k} | \ \mathbf{s} \in \Pi(\mathbf{m})\}$ *is a basis of the family* $L_P((x_1 - e)^{m_1}, \dots, (x_k - e)^{m_k})$.

□ For $k = 1$, this was proved in [174]. For $k > 1$, this follows from the equality $L_P(f_1(x_1), \dots, f_k(x_k)) = L_P(f_1(x_1)) \otimes \dots \otimes L_P(f_k(x_k))$ (Example 1.25). □

The following proposition reduces the problem of the construction of a basis of the family $L_P(I)$ to the case where I is a primary ideal.

10.13. Proposition. *Any monic ideal* $I \triangleleft \mathcal{P}_k$ *is the intersection* $I = I_1 \cap \dots \cap I_r$ *of pairwise comaximal primary ideals, and*

$$L_P(I) = L_P(I_1) \dotplus \dots \dotplus L_P(I_r).$$

□ The first statement is the Lasker–Noether theorem [13]; the second follows from Proposition 4.3. □

C. The families of k-LRS with primary annihilators over finite fields. Let $P = GF(q)$, $I \triangleleft \mathcal{P}_k$ be a maximal ideal of degree n, which satisfies the conditions of Proposition 10.5(d) and the conditions (10.6). Then $Q = P[\alpha_1, \dots, \alpha_k] = GF(q^n)$. Let $\mathrm{tr} = \mathrm{tr}_P^Q$ be the trace from the field Q into the field P, $\mathrm{tr}(x) = x + x^q + \dots + x^{q^{n-1}}$. The following result refines proposition 10.9(a) and generalizes the known description [37, 173] of a 1-LRS with irreducible characteristic polynomial.

10.14. Theorem. *For any recurrence* $u \in L_P(I)$ *there exists a unique constant* $\xi \in Q$ *such that*

$$u(\mathbf{z}) = \mathrm{tr}(\xi \alpha^{\mathbf{z}}). \tag{10.9}$$

Any sequence of the form (10.9) *belongs to* $L_P(I)$, *and if* $\xi \neq 0$, *then*

$$L_P(I) = \mathcal{P}_k u = Su$$

(here S is the ring from (10.1)*, associated with I). Any recurrence $u \in L_P(I)$ is uniquely determined by the polyhedron of the initial values $u(\Pi(\mathbf{n}))$, where $\mathbf{n} = (n_1, \ldots, n_k)$ is the vector defined from* (10.6).

□ Let u be a sequence of the form (10.9). Since tr is a linear map from Q_P onto P_P, for any polynomial $H(\mathbf{x}) \in \mathcal{P}_k$ we get

$$H(\mathbf{x})u = v, \text{ where } v(\mathbf{z}) = \operatorname{tr}(\xi H(\alpha)\alpha^{\mathbf{z}}), \tag{10.10}$$

and, by (10.4), $u \in L_P(I)$. If $\xi \neq 0$, then $u \neq 0$ (since $\operatorname{tr}(\xi H(\alpha)) \neq 0$ for some $H(\alpha) \in Q$, and then $v \neq 0$). Therefore, the number of different recurrences of the form (10.9) is equal to $|Q| = q^n = |P|^{\deg I} = |L_P(I)|$. □

10.15. Corollary. *If $P = GF(q)$ and I is the maximal ideal of $\mathcal{P}_k$ of degree n, then for any nonzero recurrence $u \in L_P(I)$ we have $\mathfrak{P}(u) = \mathfrak{P}(I)$, $T(u) = T(I) \leq q^n - 1$.* □

For 1-LRS, Theorem 10.14 makes it possible to consider the case of an arbitrary primary ideal.

10.16. Theorem. *Let $g(x)$ be an irreducible polynomial of degree m over P, $Q = P[\alpha] = GF(q^m)$ be the splitting field of $g(x)$, $g(\alpha) = 0$. Then for any LRS $u \in L_P(g(x)^l)$ there exists a unique set of constants $\xi_0, \ldots, \xi_{l-1} \in Q$ such that*

$$u(z) = \operatorname{tr}(\xi_0\alpha^z) + \binom{z}{1}\operatorname{tr}(\xi_1\alpha^z) + \ldots + \binom{z}{l-1}\operatorname{tr}(\xi_{l-1}\alpha^z). \tag{10.11}$$

Any sequence (10.11) *belongs to $L_P(g(x)^l)$.*

□ Let $\alpha_0 = \alpha$, $\alpha_1 = \alpha^q, \ldots, \alpha_{m-1} = \alpha^{q^{m-1}}$. Then any sequence u of the form (10.11) can be written as

$$u = \sum_{r=0}^{l-1}\sum_{s=0}^{m-1} a_{sr}\alpha_s^{[r]},$$

where $\alpha_s^{[r]}$ is a binomial sequence (Definition 2.15) and $a_{sr} = \xi_r^{q^s}a_s^r$. By Theorem 2.18, $u \in L_P(g(x)^l)$, and different sets of the coefficients $\xi_0, \ldots, \xi_{l-1}$ give different recurrences u. It remains to note that the number of such sets is equal to $q^{ml} = |L_P(g(x)^l)|$. □

This theorem, together with Proposition 10.13, gives an appropriate method of investigating an arbitrary reversible 1-LRS over a finite field. It is interesting to obtain a generalization of Theorem 10.16 for k-LRS with the primary annihilator.

10.17. Corollary. *Under the condition* (10.11)*, if $u \neq 0$, then $M_u(x) = g(x)^\rho$, where $\rho = \max\{r \in \overline{0, l-1} \mid \xi_r \neq 0\}$.* □

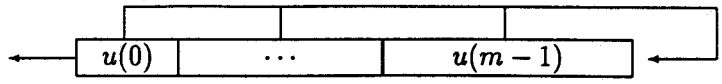
D. The Berlekamp–Massey algorithm [4, 37, 108, 112, 115, 117, 131, 159]. As was noted in Section 3.B, in order to construct the annihilator $\operatorname{An}(u)$ of a k-LRS $u \in P^{(k)}$ we must first construct the elementary ideal $\mathcal{E}(\operatorname{An}(u))$. The last problem can be reduced to construction of the minimal polynomial $M_u(x)$ of some 1-LRS $u \in P^{(1)}$. If the rank of u is known, then we can use the method of Section 3.A. But if the rank u is unknown, this method is manipulated with the Hankel matrix $\mathcal{G}_n(u)$ for increasing n. The Berlekamp–Massey algorithm [4, 131] has no such deficiency. With the help of this algorithm, we find the minimal polynomial of an LRS of rank m and obtain a method of solving a Hankel system of linear equations with complexity $O(m^2)$. We describe our version of the algorithm for 1-LRS.

10.18. Definition. We say that the monic polynomial $g(x) = x^m - c_{m-1}x^{m-1} - \ldots - c_0 \in \mathcal{P}$ *generates the segment $u(\overline{0, l-1})$ of the sequence u* of length l, if either $l \leq m$ or $l > m$ and

$$u(i+m) = c_{m-1}u(i+m-1) + \ldots + c_0u(i) \text{ for } i \in \overline{0, l-m-1}.$$

The algorithm, starting with a given $u(\overline{0, l-1})$, constructs the polynomial of least degree which generates this segment.

For an arbitrary monic polynomial $g(x) \in \mathcal{P}$, denote by $k_u(g)$ the number of zero elements in the beginning of the sequence $v = g(x)u$, and define $l_u(g) = k_u(g) + \deg g(x)$. Then $l_u(g)$ is the maximal length of the initial segment of the sequence u generated by the polynomial $g(x)$, i.e., by the register



LRS $g(x)$ over P.

10.19. Definition. The *rank of the segment* $u(\overline{0, l-1})$ of the sequence u is the minimum $m_u(l)$ of the degrees of monic polynomials that generate this segment:

$$m_u(l) = \min\{\deg g(x) : g(x) \in \mathcal{P},\ l_u(g) \geq l\}.$$

For a given $u \in P^{(1)}$, $l \in \mathbf{N}$, the Berlekamp–Massey algorithm constructs a monic polynomial $g(x) \in \mathcal{P}$ such that

$$l_u(g) \geq l, \qquad \deg g(x) = m_u(l). \tag{10.12}$$

10.20. Description of the algorithm. For given $u \in P^{(1)}$ and $l \in \mathbf{N}$, we construct the sequence of monic polynomials $g_0(x), g_1(x), \ldots, g_t(x), \ldots$ from $\mathcal{P}$ of degrees $m_0 = 0 < m_1 \leq m_2 \leq \ldots \leq m_t \leq \ldots$ by the following algorithm.

Step 0. Let $g_0(x) = e$, $m_0 = 0$. Evaluate $l - m_0 = l$ terms of the sequence $u_0 = g_0(x)u = u$. If $u_0(\overline{0, l-1}) = 0$, then $l_u(g_0) \geq l$ and $g(x) = g_0(x)$, $m_u(l) = m_0 = 0$. Otherwise, we have

$$u_0 = (0, \ldots, 0, u_0(k_0), \ldots), \qquad u_0(k_0) \neq 0, \qquad k_0 = k_u(g_0) < l - m_0.$$

Step 1. Let

$$g_1(x) = x^{k_0+1} - u_0(k_0+1)u_0(k_0)^{-1}x^{k_0}g_0(x), \qquad m_1 = k_0 + 1.$$

Evaluate $l - m_1$ terms of the sequence $u_1 = g_1(x)u$. If $u_1(\overline{0, l-m_1-1}) = 0$, then $l_u(g_1) \geq l$ and $g(x) = g_1(x)$, $m_u(l) = m_1$. Otherwise,

$$u_1 = (0, \ldots, 0, u_1(k_1), \ldots), u_1(k_1) \neq 0, \qquad k_1 = k_u(g_1) < l - m_1.$$

Suppose that we have already constructed the polynomials $g_0(x), \ldots, g_t(x)$ of degrees $m_0 = 0 < m_1 \leq \ldots \leq m_t$, and that for $j \in \overline{0,t}$

$$g_j(x)u = u_j = (0, \ldots, 0, u_j(k_j), \ldots), \qquad u_j(k_j) \neq 0, \qquad k_j = k_u(g_j) < l - m_j.$$

Step t+1. Define the parameter $s = s(t)$ such that

$$m_t = m_{t-1} = \ldots = m_{s+1} > m_s \tag{10.13}$$

(since $m_0 < m_1$, there exists such s). Let

$$\begin{gathered} g_{t+1}(x) = g_t(x) - x^{k_s-k_t}u_t(k_t)u_s(k_s)^{-1}g_s(x), \\ m_{t+1} = m_t, \text{ if } k_t \leq k_s; \\ g_{t+1}(x) = x^{k_s-k_t}g_t(x) - u_t(k_t)u_s(k_s)^{-1}g_s(x), \\ m_{t+1} = m_t + k_t - k_s, \text{ if } k_t > k_s. \end{gathered} \tag{10.14}$$

Evaluate $l - m_{t+1}$ terms of the sequence $u_{t+1} = g_{t+1}(x)u$. If $u^{t+1}(\overline{0, l-m_{t+1}-1}) = 0$, then $g(x) = g_{t+1}(x)$, $m_u(l) = m_{t+1}$. Otherwise,

$$u_{t+1} = (0, \ldots, 0, u_{t+1}(k_{t+1}), \ldots),$$
$$u_{t+1}(k_{t+1}) \neq 0, \qquad k_{t+1} = k_u(g_{t+1}) < l - m_{t+1},$$

and we go to the next step.

The proof of convergence of the algorithm is based on the following propositions.

10.21. Lemma. *If* $k_t + l_t < l$, *then*

$$l_u(g_{t+1}) = m_{t+1} + k_{t+1} > l_u(g_t) = m_t + k_t. \tag{10.15}$$

□ If $t = 0$, then (10.15) is obvious. By (10.14), $m_{t+1} \geq m_t$, and $(m_{t+1} = m_t) \Leftrightarrow (k_t \leq k_s)$.

If $m_{t+1} = m_t$, i.e., $k_t \leq k_s$, then $u_{t+1} = u_t - v$, where $v = x^{k_s - k_t} u_t(k_t) u_s(k_s)^{-1} u_s$ and $v(\overline{0, k_t}) = (0, \ldots, 0, u_t(k_t)) = u(\overline{0, k_t})$. Hence $u_{t+1}(\overline{0, k_t}) = \mathbf{0}$, i.e., $k_{t+1} > k_t$ and (10.15) holds.

If $m_{t+1} > m_t$, i.e., $k_t > k_s$, then u_{t+1} is the difference of the sequences $x^{k_s - k_t} u_t$ and $u_t(k_t) u_s(k_s)^{-1} u_s$ with coincident initial vectors of length $k_s + 1$. Therefore, $k_t > k_s + 1$ and $m_{t+1} + k_{t+1} = m_t + k_t - k_s + k_{t+1} \geq m_t + k_t + 1 > m_t + k_t$. □

10.22. Lemma. *If $k_t + l_t < l$, then*

$$m_{t+1} = \max\{m_t, k_t + 1\}. \tag{10.16}$$

□ Induction on t. For $t = 0$, (10.16) is obvious. If $t > 0$, then for the parameter s from (10.13), by the induction assumption, $m_{s+1} = \max\{m_s, k_s + 1\}$. Since $m_t = m_{s+1} > m_s$, we have $m_t = k_s + 1 > m_s$.

If $k_t \leq k_s$, then $m_{t+1} = m_t = k_s + 1 \geq k_t + 1$. If $k_t > k_s$, then $m_{t+1} = m_t + k_t - k_s > m_t$ and $m_{t+1} = k_s + 1 + k_t - k_s = k_t + 1$. □

10.23. Lemma. *Let $\lambda \in \mathbb{N}$, $m = m_u(\lambda)$, and $f(x) \in \mathcal{P}$ be a monic polynomial such that*

$$l_u(f) \geq \lambda, \qquad \deg f(x) = m.$$

Let $h(x) \in \mathcal{P}$ be a monic polynomial of degree n such that $l_u(h) > l_u(f)$. Then $n \geq \max\{m, k_u(f) + 1\}$.

□ Since $l_u(f) \geq \lambda$, we have $n \geq m_u(\lambda) = m$. It remains to show that $n \geq k_u(f) + 1$. Suppose that $n \leq k_u(f)$. Then the sequence $w = h(x)f(x)u$ begins with the series of exactly $k_u(f) - n$ zero elements. On the other hand, since $w = f(x)h(x)u$, the length of this series is equal to $k_u(h) - m$. Hence $l_u(h) = n + k_u(h) = m + k_u(f) = l_u(f)$. This contradicts the condition of our lemma. □

10.24. Proposition. *In the notation of* 10.20, *if $t \geq 0$ and $k_t < l - m_t$, then*

(a) $l_u(g_{t+1}) \geq l_u(g_t) + 1 = l_t + 1$;

(b) $g_{t+1}(x)$ *is a polynomial of the least degree which generates the segment $u(\overline{0, l_t})$, i.e.,*

$$m_u(l_t + 1) = m_{t+1}.$$

If $\tau = \min\{t \in \mathbb{N}_0 |\ m_t + k_t \geq l\}$, then the polynomial $g(x) = g_\tau(x)$ satisfies the conditions (10.12).

□ Induction on t with the use of Lemmas 10.21–10.23. □

In the general case, the polynomial $g(x)$ with properties (10.12) is not uniquely determined, but we can formulate

10.25. Proposition. *If $l \in \mathbb{N}$ is such that the rank of the segment $u(\overline{0, l-1})$ satisfies the condition*

$$m_u(l) = m \leq l/2, \tag{10.17}$$

then there exists a unique monic polynomial $g(x) \in \mathcal{P}$ such that

$$\deg g(x) = m, \qquad l_u(g) \geq l. \tag{10.18}$$

□ Let $v \in L_P(g)$ be the LRS with the initial vector $v(\overline{0, m-1}) = u(\overline{0, m-1})$. Then

$$v(\overline{0, l-1}) = u(\overline{0, l-1}) \tag{10.19}$$

and $g(x) = M_v(x)$ (otherwise, the segment $u(\overline{0, l-1})$ is generated by a polynomial of degree less than m.) If $f(x)$ is another monic polynomial satisfying (10.18), then by (10.19) and (10.17), we have $f(x)v = 0$. Hence $g(x) | f(x)$ and $f(x) = g(x)$. □

10.26. Theorem. *If $u \in P^{(1)}$ is an LRS of rank m, then the Berlekamp–Massey algorithm, described in 10.11, with not more than*

$$\tau = \min\{t \in \mathbb{N}_0 |\ m_t + k_t \geq 2m\}$$

steps, produces the minimal polynomial of the LRS u, i.e., $g_\tau(x) = M_u(x)$. Moreover, $\tau \leq 2m - k_0 - 1$.

□ By Proposition 10.24(b), $g_r(x)$ is the polynomial of the least degree which generates $u(\overline{0,2m-1})$. By Proposition 10.25, it coincides with $M_u(x)$. □

Under the conditions of Theorem 10.26, the Berlekamp–Massey algorithm produces the solution of the Hankel system of linear equations

$$\vec{x}\, G_m(u) = u(\overline{m,2m-1}).$$

The complexity $N_P(m)$ of the algorithm is estimated by the following number of the arithmetic operations of the field P:

$$N_P(m) \le 8m^2 - (4m+3)k_0 + \varkappa \le 10m^2(1+0(1)),$$

where $\varkappa = k_0 + k_1 + \ldots + k_r$. Thus, $N_P(m) = 0(m^2)$. Other modifications of the Berlekamp–Massey algorithm, in particular with the complexity $0(m \log m)$, and also the k-dimensional Berlekamp–Massey algorithms, can be found in [108, 112, 115, 117, 159].

11. Periodic Recurring Sequences over Fields

A. General criterion of the periodicity of a 1-LRS [37, 70, 100]. By 6.3 and 3.4, 3.5, it is sufficient to give a criterion of the periodicity of the minimal polynomial $f(x) = M_u(x)$ of a recurrence $u \in \mathcal{L}P^{(1)}$.

11.1. Theorem. *Let $f(x) \in P[x]$ be a monic polynomial with canonical decomposition over splitting field Q:*

$$f(x) = x^l(x-\alpha_1)^{l_1}\ldots(x-\alpha_r)^{l_r}. \tag{11.1}$$

Then $f(x)$ is a periodic polynomial if and only if the multiplicative orders of the roots of $f(x)$ in Q are finite,

$$\operatorname{ord}\alpha_s = t_s \in \mathbf{N}, \qquad s \in \overline{1,r}, \tag{11.2}$$

and if char $P = 0$, *then, in addition, all roots are simple,*

$$l_1 = \ldots = l_r = 1. \tag{11.3}$$

If char $P = 0$, *then, under the conditions* (11.1)–(11.3),

$$D(f) = l, \qquad T(f) = [t_1, \ldots, t_r]. \tag{11.4}$$

If char $P = p > 0$, *then, under the conditions* (11.1), (11.2),

$$D(f) = l, \qquad T(f) = [t_1, \ldots, t_r] \cdot p^{\lambda}, \tag{11.5}$$

where

$$\lambda =]\log_p(\max\{l_1, \ldots, l_r\})[. \quad \square \tag{11.6}$$

11.2. Corollary. *If $g(x)$ is an irreducible reversible polynomial over $P = GF(q)$ of degree m, then the period of $g(x)$ is equal to the order of its arbitrary root $\alpha \in Q = GF(q^m)$, and*

$$T(g) \mid q^m - 1, \qquad T(g) \nmid q^n - 1 \text{ for } n < m. \quad \square$$

11.3. Corollary. *Let $f(x) = x^l g_1(x)^{l_1}\ldots g_r(x)^{l_r}$ be the canonical decomposition of a monic polynomial $f(x)$ over $P = GF(q)$. Then $D(f) = l$, $T(f) = [T(g_1), \ldots, T(g_r)] \cdot p^{\lambda}$, where λ is defined by* (11.6). □

B. The cyclic type of a reversible 1-LRS-family over a finite field [37, 70, 139]. Let $f(x)$ be a reversible polynomial over $P = GF(q)$ with canonical decomposition $f(x) = g_1(x)^{l_1}\ldots g_r(x)^{l_r}$. By 7.10, the cyclic type $Z_f^P(y)$ of the family $L_P(f)$ is the composition of the cyclic types of the families $L_P(g_1(x)^{l_1}), \ldots, L_P(g_r(x)^{l_r})$. Thus, it is necessary to describe the cyclic types of reversible families with primary characteristic polynomials.

11.4. Theorem. *Let $f(x) = g(x)^l$, where $g(x) \in \mathcal{P}$ is an irreducible polynomial of degree m and period $T(g) = \tau$, and $p^{\lambda-1} < k \le p^\lambda$. Then*

$$Z_f^P(y) = y + \frac{q^m - 1}{\tau} \cdot y^\tau + \sum_{s=1}^{\lambda-1} \frac{q^{mp^s} - q^{mp^{s-1}}}{\tau p^s} \cdot y^{\tau p^s} + \frac{q^{ml} - q^{mp^{\lambda-1}}}{\tau p^\lambda} \cdot y^{\tau p^\lambda}. \tag{11.7}$$

□ $L_P(f)$ is the set of all sequences u of the form (10.11). If $u \ne 0$ and, in the notation of (10.11),

$$\xi_{\rho-1} \ne 0, \qquad \xi_\rho = \ldots = \xi_{l-1} = 0, \tag{11.8}$$

then, by 10.17, $M_u(x) = g(x)^\rho$, and, by 10.17, $T(u) = \tau p^s$, where $p^{s-1} < \rho \le p^s$. Thus, $T(u) = \tau p^s$ if and only if $\xi_{p^{s-1}}, \xi_{p^{s-1}+1}, \ldots, \xi_{l-1}$ are not all equal to 0 and $\xi_t = 0$ for $t \ge p^s$. It now follows that the number $N_f^P(\tau p^s)$ of recurrences $u \in L_P(f)$ of the period τp^s is given by

$$N_f^P(\tau p^s) = \begin{cases} q^{ml} - q^{mp^{\lambda-1}}, & \text{if } s = \lambda, \\ q^{mp^s} - q^{mp^{s-1}}, & \text{if } s < \lambda. \end{cases} \quad \square$$

12. Maximal Linear Recurring Sequences over Galois Fields

Let $P = GF(q)$, u be a reversible k-LRS over P, $I = \mathrm{An}(u)$, and $S = \mathcal{P}_k/I = P[\theta_1, \ldots, \theta_k]$ be the operator ring of u (see 1.18). Then, by 5.26, $T(u) \le |S^*| \le |S| - 1$.

12.1. Definition. A reversible k-LRS u over a Galois field P is called a *k-maximal recurrence* (*k-max-LRS*) if the operator ring S of u is a Galois field and

$$T(u) = |S^*| = |S| - 1. \tag{12.1}$$

If $S = GF(q^m)$, then we say that u is a *k-max-LRS* of rank m. In the case $k = 1$, we also say that u is an *LRS of maximal period.*

In view of Definition 6.24, a k-max-LRS over P is a full-cycle LRS such that its operator ring is a field.

Note that, by Theorem 5.26, condition (12.1) is equivalent to

$$S = GF(q^m), \qquad S^* = \langle \theta_1, \ldots, \theta_k \rangle. \tag{12.2}$$

The following description of k-maximal recurrences generalize the well-known characterization of 1-LRS of maximal period over a finite field [37, 70, 133], and make it possible to unify the special cases examined in [128, 144, 153, 154].

12.2. Theorem. *Let $Q = GF(q^m)$ be an extension of P of degree m, and elements $\alpha_1, \ldots, \alpha_k \in Q^*$ satisfy*

$$Q^* = \langle \alpha_1, \ldots, \alpha_k \rangle. \tag{12.3}$$

Then, for any $\xi \in Q^*$, the k-sequence $u \in \mathcal{P}^{(k)}$ defined by

$$u(\mathbf{z}) = \mathrm{tr}_P^Q(\xi \alpha^{\mathbf{z}}) \tag{12.4}$$

is a k-max-LRS of rank m. Conversely, for any k-maximal recurrence $u \in \mathcal{P}^{(k)}$ of rank m there exist elements $\xi, \alpha_1, \ldots, \alpha_k \in Q^*$ such that (12.3) and (12.4) hold.

□ By 10.14, under conditions (12.3), (12.4), the ideal $I = \mathrm{An}(u)$ is a maximal ideal of the form (10.4). The operator ring S is isomorphic to Q, and there exists an isomorphism over P which maps θ_s to α_s, $s \in \overline{1,k}$. Hence, (12.3) holds.

If u is a k-max-LRS of rank m over P, then, by Definition 12.1, the operator ring S satisfies (12.2). There exists a field isomorphism $\sigma : S \to Q$ over P. If $\sigma(\theta_s) = \alpha_s$, $s \in \overline{1,k}$, then (12.3) and (10.4) hold. Therefore, by 10.14, (12.4) holds for a suitable $\xi \in Q^*$. □

12.3. Definition. A maximal ideal $I \lhd \mathcal{P}_k$ is called an *ideal of maximal period* over $P = GF(q)$ if its operator ring S satisfies (12.2) for some $m \in \mathbf{N}$.

12.4. Theorem. *Let $I \lhd \mathcal{P}_k$ be an ideal of maximal period over $P = GF(q)$, and suppose that* (12.2) *holds. Then the group of periods of I has the form $\mathfrak{P}(I) = \{\mathbf{t} \in \mathbf{Z}^k |\ \theta^{\mathbf{t}} = e\}$, and $T(I) = q^m - 1$. The factor group $\mathbf{Z}^k/\mathfrak{P}(I)$ is a cyclic group of order $q^m - 1$. The cyclic type of the family $L_P(I)$* (see 7.13) *is given by*

$$Z_I^P = 1 \cdot \mathbf{Z}^k + 1 \cdot \mathfrak{P}(I). \tag{12.5}$$

□ The first part of the theorem follows from 6.21 and 6.22. By 10.14, for any $u \in L_P(I) \backslash 0$ we have $L_P(I) = Su$. Hence, by (12.2), all nonzero recurrences from $L_P(I)$ belong to the cycle $\mathcal{T}(u) = S^*u$ of u, i.e., (12.5) is true. □

12.5. Proposition. *Let u be a 1-LRS of maximal period $q^m - 1$ over $P = GF(q)$. Then the group of multipliers and the reduced period of u are given by*

$$\mathrm{Mult}\,(u) = P^*, \qquad T_r(u) = (q^m - 1)/(q - 1). \square$$

If u is a 1-LRS of maximal period $\tau = q^m - 1$ over $P = GF(q)$ and $f(x)$ is the minimal polynomial of u, then the root α of $f(x)$ in the extension $Q = GF(q^m)$ of P is a primitive element of Q. We now obtain some properties of regular extracts of u. For $k \in \overline{1, \tau}$, we set

$$m(k) = [P(\alpha^k) : P], \qquad f_k(x) = \mu_{\alpha^k, P}(x).$$

Then $f_k(x)$ is an irreducible polynomial over P of degree $m(k)$, and $m(k)|m$. The following theorem refines some results of Section 9.

12.6. Theorem [58, 70]. *In the previous notations, the following statements hold.*

(a) *Any (l, k)-extract v of u belongs to $L_P(f_k)$.*

(b) *Any nonzero sequence $v \in L_P(f_k)$ is an (l, k)-extract of u exactly for $q^{m-m(k)}$ different integers $l \in \overline{0, \tau - 1}$, and the zero sequence — exactly for $q^{m-m(k)} - 1$ different $l \in \overline{0, \tau - 1}$.*

(c) *Let $g(x) \in P[x]$ be a reversible irreducible polynomial of degree n, $n|m$, and let $v \in L_P(g)$, $v \neq 0$. Then exactly nq^{m-n} regular extracts of u are equal to v.* □

The statistical characteristics of k-maximal recurrences will be considered in Section 26.

13. The Algebra of Linear Recurring Sequences over a Field

The space $P^{(k)}$ of k-sequences over a field P is an associative commutative algebra, in which the sequences are multiplied as functions, i.e., if $u, v \in P^{(k)}$, then $uv = w$, where $w(z) = u(z)v(z)$. Subalgebras of $(P^{(k)}, +, \cdot)$ are the families $L_P(x_1^{l_1}(x_1^{t_1} - e), \ldots, x_k^{l_k}(x_k^{t_k} - e))$, where $l_1, \ldots, l_k \in \mathbf{N}_0$, $t_1, \ldots, t_k \in \mathbf{N}$, and the sets $\pi P^{(k)}$, $\mathcal{R}P^{(k)}$, $\mathcal{D}P^{(k)}$ of periodic, reversible, and degenerating k-sequences respectively. Moreover, $\mathcal{D}P^{(k)}$ is an ideal of $P^{(k)}$. If P is finite, then the set $\mathcal{L}P^{(k)}$ of all k-linear recurrences over P coincides with $\pi P^{(k)}$ and, therefore, is a subalgebra in $P^{(k)}$. It will be shown below that $\mathcal{L}P^{(k)}$ is a subalgebra in $P^{(k)}$ for arbitrary P.

A. Multiplication of k-LRS-families [37, 82, 83, 93, 109, 119, 152, 174]. Here we generalize some results of [174, 37] for the case of k-recurrences.

13.1. Definition. *Multiplication* of subspaces $\mathcal{M}, \mathcal{N} \subset_P P^{(k)}$ is defined as the subspace $\mathcal{MN}$, generated (over P) by uv for all $u \in \mathcal{M}$, $v \in \mathcal{N}$, i.e., $\mathcal{MN} =_P \{uv |\ u \in \mathcal{M}, v \in \mathcal{N}\}$.

13.2. Proposition. *The multiplication on the set $\tilde{P}^{(k)}$ of all subspaces of $P^{(k)}$ is associative, commutative, and distributive with respect to addition. If $\mathcal{M}_s \in \tilde{P}^{(k)}$, $\dim_P \mathcal{M}_s = m_s$, $s \in \overline{1, t}$, then*

$$\dim_P \mathcal{M}_1 \ldots \mathcal{M}_t \leq m_1 \ldots m_t. \tag{13.1}$$

The algebra $(\tilde{P}^{(k)}, +, \cdot)$ is a commutative semiring with unit $L_P(x_1 - e, \ldots, x_k - e)$ and zero $L_P(e) = 0$. □

13.3. Theorem. *For any monic ideals $I_1, \dots, I_t \triangleleft \mathcal{P}_k$, there exists a unique ideal $I \triangleleft \mathcal{P}_k$ such that*

$$L_P(I_1) \dots L_P(I_t) = L_P(I). \tag{13.2}$$

In addition,

$$\deg I \leq \deg I_1 \cdot \dots \cdot \deg I_t. \tag{13.3}$$

□ By 13.1 and 13.2, the set $\mathcal{M} = L_P(I_1) \dots L_P(I_t)$ is a finite-dimensional subspace in $P^{\langle k \rangle}$. Since $x_i \mathcal{M} \subseteq \mathcal{M}$ for $i \in \overline{1,k}$, $\mathcal{M}$ is a $\mathcal{P}_k$-submodule in $P^{\langle k \rangle}$. Therefore, by 2.12, $\mathcal{M} < \mathcal{L}P^{\langle k \rangle}$. Since a field is a QF-ring, we have, by 4.6, $\mathcal{M} = L_P(I)$, where $I = \operatorname{An}(\mathcal{M})$. The inequality (13.3) follows from (13.1) and 10.9. □

13.4. Definition. The monic ideal from (13.2) is called the *disjunction of ideals* $I_1, \dots, I_t$ and is denoted by

$$I = I_1 \vee \dots \vee I_t. \tag{13.4}$$

A monic polynomial $f(x) \in P[x]$ is called the *disjunction of monic polynomials* $f_1(x), \dots, f_t(x) \in P[x]$ of one indeterminate x if

$$L_P(f_1) \dots L_P(f_t) = L_P(f). \tag{13.5}$$

We denote it by

$$f = f_1 \vee \dots \vee f_t. \tag{13.6}$$

Associativity of the multiplication implies associativity of the disjunction.

13.5. Corollary. *The set $\mathcal{L}P^{\langle k \rangle}$ of a k-LRS over P is a subalgebra of the algebra $(P^{\langle k \rangle}, +, \cdot)$.* □

B. Properties of the disjunction. Definition (13.6) of the disjunction of polynomials depends on the field P (see (13.5)). Indeed, there is no dependence on P, and we have

13.6. Proposition. *Under the conditions of Theorem* 13.3, *let Q be an extension of P. Then, along with* (13.2),

$$L_Q(I_1) \dots L_Q(I_t) = L_Q(I). \tag{13.7}$$

□ By 13.3,

$$L_Q(I_1) \dots L_Q(I_t) = L_Q(J), \tag{13.8}$$

where $J \triangleleft Q[\mathrm{x}]$ is a monic ideal. Since $L_P(I_s) \subseteq L_Q(I_s)$, $s \in \overline{1,t}$, (13.2) and (13.8) imply that $L_P(I) \subseteq L_Q(J)$ and $L_Q(I) = Q \cdot L_P(I) \subseteq L_Q(J)$.

Any basis $\{u_1^{(s)}, \dots, u_{m_s}^{(s)}\}$ of the family $L_P(I_s)$ is also a basis of $L_Q(I_s)$ (Proposition 10.9). Hence, the system of sequences $\{u_{k_1}^{(1)} \dots u_{k_t}^{(t)} \mid k_s \in \overline{1,m_s}, s \in \overline{1,t}\}$ generates $L_P(I)$ over P and $L_Q(J)$ over Q. Therefore, $L_Q(J)$ is annihilated by each polynomial from I, and $L_Q(J) \subseteq L_Q(I)$. □

The disjunction of arbitrary monic ideals has not been described yet. For monic ideals the problem reduces to a description of the disjunction of polynomials of one indeterminate.

13.7. Proposition. *Let $I = (f_1(x_1), \dots, f_k(x_k))$, $J = (g_1(x_1), \dots, g_k(x_k))$ be elementary ideals of $\mathcal{P}_k$. Then*

$$I \vee J = (f_1 \vee g_1, \dots, f_k \vee g_k).$$

□ By 1.25, the subspaces $L_P(I)$, $L_P(J)$ are generated over P by sequences of the form

$$u = u_1 \otimes \dots \otimes u_k, \qquad u_s \in L_P(f_s), \qquad s \in \overline{1,k},$$

$$v = v_1 \otimes \dots \otimes v_k, \qquad v_s \in L_P(g_s), \qquad s \in \overline{1,k}$$

respectively. Then $L_P(I \vee J)$ is generated by sequences of the form $uv = u_1 v_1 \otimes \dots \otimes u_k v_k$. Here $u_s v_s \in L_P(f_s \vee g_s)$, and $L_P(f_s \vee g_s)$ are generated by all possible products $u_s v_s$. □

The disjunction of polynomials of one indeterminate is described by the following propositions.

13.8. Lemma. *For any t, $s \in \mathbf{N}_0$,*

$$x^t \vee x^s = x^m, \text{ where } m = \min\{t, s\}.$$

If $f(x) \in P[x]$ is a monic polynomial and $f(0) \neq 0$, then

$$x^t \vee f(x) = x^t. \quad \square$$

13.9. Lemma [174]. *If $g(x)$ is a separable polynomial over P, $\deg g > 0$, then for any $a \in \mathbf{N}$*

$$g(x) \vee (x-e)^a = g(x)^a. \square$$

13.10. Definition. Let $\operatorname{char} P = p$. Define the *disjunction $a \vee b$ of natural numbers a, b* [174]. If $p = 0$, then $a \vee b = a + b - 1$. If $p > 0$ and

$$a - 1 = \sum_{s \geq 0} a_s p^s, \qquad b - 1 = \sum_{s \geq 0} b_s p^s, \qquad 0 \leq a_s,\ b_s < p,$$

are the p-ary expansions of $a - 1$ and $b - 1$, then

$$a \vee b = p^\lambda + \sum_{s \geq \lambda} (a_s + b_s) p^s,$$

where $\lambda = \min\{r \geq 0 |\ a_t + b_t < p \text{ for } t \geq r\}$.

13.11. Lemma [174]. *For any $a, b \in \mathbf{N}$,*

$$(x-e)^a \vee (x-e)^b = (x-e)^{a \vee b}. \quad \square$$

13.12. Lemma [174]. *Let $f(x)$, $g(x)$ be monic separable polynomials over P, Q be their splitting field over P, and let the decompositions of $f(x)$, $g(x)$ over Q be given by*

$$f(x) = (x - \alpha_1) \ldots (x - \alpha_m), \qquad g(x) = (x - \beta_1) \ldots (x - \beta_n).$$

Then

$$f \vee g = \text{l.c.m.}[x - \alpha_s \beta_t,\ s \in \overline{1,m},\ t \in \overline{1,n}],$$

$$f^a \vee g^b = (f \vee g)^{a \vee b}, \qquad a, b \in \mathbf{N}. \quad \square$$

13.13. Theorem [174]. *Let $f(x)$, $g(x)$ be monic polynomials of positive degrees over P, and let Q be a purely nonseparable extension of P such that in the canonical decompositions of $f(x)$, $g(x)$ over Q,*

$$f = f_1^{a_1} \ldots f_m^{a_m}, \qquad g = g_1^{b_1} \ldots g_n^{b_n},$$

the polynomials f_s, g_t, $s \in \overline{1,m}$, $t \in \overline{1,n}$, are separable. Then

$$f \vee g = \text{l.c.m.}[f_s^{a_s} \vee g_t^{b_t},\ s \in \overline{1,m},\ t \in \overline{1,n}]. \quad \square$$

C. Subalgebras of the algebra of linear recurrences.

Let

$$L_P(\mathbf{f}^{\mathbf{a}}) = L_P(f_1(x_1)^{a_1}, \ldots, f_k(x_k)^{a_k}), \qquad L_P(\mathbf{f}^{\infty}) = \bigcup_{\mathbf{a} \in \mathbf{N}_0^k} L_P(\mathbf{f}^{\mathbf{a}}).$$

13.14. Lemma. *A subspace $L_P(\mathbf{f}^{\mathbf{a}})$, where $a_1, \ldots, a_k \in \mathbf{N} \cup \{\infty\}$, is a subalgebra of $\mathcal{L}P^{(k)}$ if and only if $L_P(f_s(x)^{a_s})$ are subalgebras in $\mathcal{L}P^{(1)}$ for any $s \in \overline{1,k}$.*

□ It is sufficient to use the relation (see 1.25)

$$L_P(\mathbf{f}^{\mathbf{a}}) = L_P(f_1(x)^{a_1}) \otimes \ldots \otimes L_P(f_k(x)^{a_k}). \quad \square$$

13.15. Proposition. *The set $L_P((\mathbf{x} - \mathbf{e})^{\infty})$ is a subalgebra in $\mathcal{L}P^{(k)}$. The family $L_P((\mathbf{x} - \mathbf{e})^{\mathbf{a}})$ is a subalgebra in $\mathcal{L}P^{(k)}$ if and only if*

$$\mathbf{a} = (1, \ldots, 1), \text{ if } \operatorname{char} P = 0;$$

$$a = (p^{\lambda_1}, \ldots, p^{\lambda_k}), \text{ if } \operatorname{char} P = p > 0.$$

□ This follows from 13.14 and 13.11. □

13.16. Remark. It is interesting to describe subalgebras in $\mathcal{L}P^{\langle k\rangle}$ which are also $\mathcal{P}_k$-submodules. From Proposition 14.20 it follows that such subalgebras coincide with bialgebras in the bialgebra $\mathcal{L}P^{\langle k\rangle}$, defined in Section 14. For $k = 1$ subbialgebras of $\mathcal{L}P^{\langle 1\rangle}$ are completely described in 14.36, 14.35. These results and Lemma 13.14 make it possible to enumerate some subbialgebras in $\mathcal{L}P^{\langle k\rangle}$ for $k > 1$, but their complete description is an open problem.

Define $\mathcal{R}P^{\langle k\rangle}_{\mathrm{irr}}$ as the set of all recurrences $u \in \mathcal{L}P^{\langle k\rangle}$ such that $u \in L_P(f_1(x_1), \dots, f_k(x_k))$, where $f_1(x), \dots, f_k(x)$ are irreducible reversible polynomials over P.

13.17. Theorem. *The algebra $\mathcal{L}P^{\langle k\rangle}$ of k-linear recurrences can be represented in the form*

$$\mathcal{L}P^{\langle k\rangle} = \mathcal{D}P^{\langle k\rangle} \dotplus \mathcal{R}P^{\langle k\rangle}_{\mathrm{irr}} \cdot L_P((\mathbf{x} - \mathbf{e})^\infty).$$

□ By 13.9, 13.7, for any monic polynomials $f_1(x), \dots, f_k(x)$ we have $L_P(\mathbf{f}) \cdot L_P((\mathbf{x} - \mathbf{e})^\infty) = L_P(\mathbf{f}^\infty)$. Hence, $\mathcal{R}P^{\langle k\rangle}_{\mathrm{irr}} \cdot L_P((\mathbf{x} - \mathbf{e})^\infty) = \mathcal{R}P^{\langle k\rangle}$, and our result follows from 5.27. □

Recall that P is called a *perfect field* if any irreducible polynomial over P is separable. If (and only if) P is perfect the subspace $\mathcal{R}P^{\langle k\rangle}_{\mathrm{irr}}$ is a subalgebra of $\mathcal{L}P^{\langle k\rangle}$. In this situation, $\mathcal{R}P^{\langle k\rangle}_{\mathrm{irr}}$ coincides with the set $\mathcal{E}P^{\langle k\rangle}$ of exponentially representable sequences (see 10.11), and the following result holds.

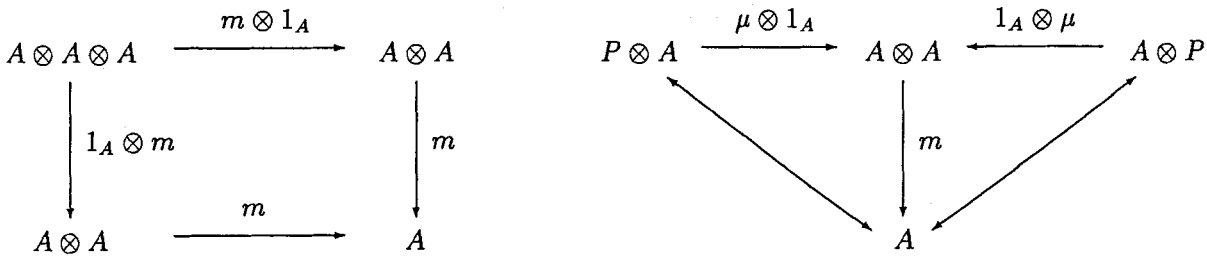
13.18. Corollary. *If P is perfect, then*

$$\mathcal{L}P^{\langle k\rangle} = \mathcal{D}P^{\langle k\rangle} \dotplus \mathcal{E}P^{\langle k\rangle} \cdot L_P((x_1 - e)^\infty, \dots, (x_k - e)^\infty). \quad \square$$

14. Hopf Algebras of Linear Recurring Sequences

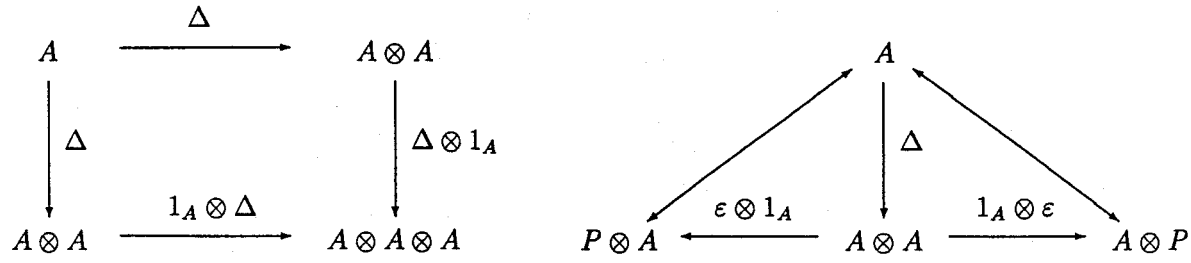
All linear spaces in this section are considered over a fixed field P. Let $\mathrm{Hom}(A, B)$ be the set of all linear mappings from the vector space A into B, $A^* = \mathrm{Hom}(A, P)$. If $\sigma \in \mathrm{Hom}(A, B)$, then σ^* denotes the dual mapping $\sigma^* : B^* \to A^*$, $\sigma^*(\varphi) = \varphi\sigma$. References: [3, 31, 32, 90, 91, 147, 163]; see also V. A. Artamonov *Structure of Hopf Algebras, Itogi Nauki i Tekhn. Algebra. Topologiya. Geometriya*, **29**, 3–63 VINITI (1991).

A. Hopf algebras. An *algebra* over the field P is a vector space A with a *multiplication map* $m : A \otimes A \to A$ and a *unit map* $\mu : P \to A$, such that the following diagrams are commutative:



A is commutative if $mT = m$, where $T : A \otimes A \to A \otimes A$, $T(a \otimes b) = b \otimes a$. We write $m(a \otimes b) = ab$. The element $1 = \mu(e)$ is the unit of the algebra A, where e is the unit of P. To define a coalgebra, we reverse the arrows in these diagrams.

14.1. Definition. A *coalgebra* is a vector space A with a *comultiplication* (or diagonalization) $\Delta : A \to A \otimes A$ and a *counit* $\varepsilon : A \to P$, such that the following diagrams are commutative:



Thus, if $a \in A$ and $\Delta a = \sum a_i \otimes a_i'$, then $\sum(\Delta a_i) \otimes a_i' = \sum a_i \otimes (\Delta a_i')$ and $\sum \varepsilon(a_i)a_i' = a = \sum a_i \varepsilon(a_i')$. This property expresses the *coassociativity* of Δ. A is *cocommutative* if $T\Delta = \Delta$. A subspace B is a *subcoalgebra* of A if $\Delta(B) \subseteq B \otimes B$. A *homomorphism of coalgebras* is a linear mapping $\sigma : A \to A'$ such that $(\sigma \otimes \sigma)\Delta = \Delta'\sigma$ and $\varepsilon'\sigma = \varepsilon$.

If A is an algebra and a coalgebra and Δ, ε are homomorphisms of algebras, i.e., $\Delta m(a \otimes b) = m\Delta(a) \otimes m\Delta(b)$, $\varepsilon m(a \otimes b) = \varepsilon(a)\varepsilon(b)$, then A is called a ***bialgebra***. A subalgebra B is called a *subbialgebra* if B is also a subcoalgebra. A *Hopf algebra* is a bialgebra A with an *antipode* map $S : A \to A$ such that if $a \in A$ and $\Delta a = \sum a_i \otimes a_i'$, then $\sum S(a_i)a_i' = \varepsilon(a)1 = \sum a_i S(a_i')$. A subbialgebra B is called a *Hopf subalgebra* if $S(B) \subseteq B$. A *homomorphism of Hopf algebras* is an algebra and coalgebra homomorphism $\sigma : A \to A'$ such that $S'\sigma = \sigma S$.

14.2. Example. The polynomial algebra $P[x_1, \ldots, x_k]$ is a Hopf algebra with comultiplication

$$\Delta f = f(\mathbf{x} \otimes \mathbf{1} + \mathbf{1} \otimes \mathbf{x}) = f(x_1 \otimes 1 + 1 \otimes x_1, \ldots, x_k \otimes 1 + 1 \otimes x_k),$$

counit $\varepsilon(f) = f(\mathbf{0})$, and antipode $S(f) = f(-\mathbf{x})$. We denote this Hopf algebra by $P[\mathbf{x}]$.

14.3. Example. The polynomial algebra $P[x_1, \ldots, x_k]$ is a bialgebra with $\Delta f = f(\mathbf{x} \otimes \mathbf{x})$, $\varepsilon(f) = f(\mathbf{1})$. We denote it by $\mathcal{B}_k$.

An element $a \neq 0$ of a coalgebra A such that $\Delta a = a \otimes a$ is called a *group-like element*. The set $G(A)$ of group-like elements of a Hopf algebra A is a group, $a^{-1} = S(a)$ for $a \in G(A)$ [163]. Since the element $x_1 \in G(\mathcal{B}_k)$ is not invertible in $\mathcal{B}_k$, then there does not exist an antipode in the bialgebra $\mathcal{B}_k$.

B. The continuous dual of the Hopf algebra. If (C, Δ, ε) is a coalgebra, then C^* is an algebra with the unit ε. The multiplication $*$ in C^* is called the *convolution* and is defined by $(u * v)(c) = (u \otimes v)\Delta c$, where $u, v \in C^*$, $c \in C$, i.e., if $\Delta c = \sum c_i \otimes c_i'$, then $(u * v)(c) = \sum u(c_i)v(c_i')$. Thus, the multiplication $*$ in C^* is obtained by dualization of Δ, i.e., by putting together $\Delta^* : (C \otimes C)^* \to C^*$ with the natural map

$$\varkappa : C^* \otimes C^* \to (C \otimes C)^*, \qquad (\varkappa(u \otimes v))(c \otimes d) = u(c)v(d).$$

The associativity of $*$ follows from the coassociativity of Δ. The algebra C^* is called the *dual of the coalgebra* C.

Now we define the coalgebra which is dual to the algebra (A, m, μ). Note that the dualization of the multiplication m is the map $m^* : A^* \to (A \otimes A)^*$, the image may not lie in $A^* \otimes A^*$ (if $\dim A = \infty$). But there exist subspaces A^0 in A^* such that $m^*(A^0) \subseteq A^0 \otimes A^0$, and our coalgebra is the largest of them (see [163]).

A subspace J in A is called *cofinite* if $\dim_P(A/J) < \infty$. Denote

$$A^0 = \{u \in A^* | \operatorname{Ker} u \text{ contains a cofinite } \textit{ideal} \text{ of } A\}.$$

Then the restriction of the injection $A^* \otimes A^* \to (A \otimes A)^*$ on $A^0 \otimes A^0$ appears to be an isomorphism between $A^0 \otimes A^0$ and $(A \otimes A)^0$ [163], and $\Delta^0 = m^*|A^0$ is a comultiplication in A^0. It is easy to check that $\Delta^0 u = \sum u_i \otimes u_i'$ (where u, u_i, $u_i' \in A^0$) if and only if $u(ab) = \sum u_i(a)u_i'(b)$ for any a, $b \in A$. The map $\varepsilon^0 = \mu^*|A^0 : A^0 \xrightarrow{\mu^*} P^* = P$ (dual to the unit μ of algebra A) is a count of the coalgebra A^0. We have $\varepsilon^0(u) = u(1)$. The coalgebra A^0 is called the *continuous dual of the algebra* A, or the *C-dual of* A.

If $(A, m, \mu, \Delta, \varepsilon)$ is a bialgebra, then A^0 is a coalgebra and A^* is an algebra, and A^0 is a subalgebra of A^*. It can be shown that A^0 is a bialgebra [163], called the *C-dual of the bialgebra* A. If A is a Hopf algebra with antipode S, then A^0 is a Hopf algebra with antipode

$$S^0 = S^*|A^0 : \ A^0 \xrightarrow{S^*} A^0, \qquad (S^0u)(a) = u(S(a)).$$

14.4. Definition. A^0 is called the *continuous dual of a Hopf algebra* A, or the *C-dual of* A.

C. Hopf algebras of k-linear recurring sequences. Let us turn to Examples 14.2, 14.3. Any linear map $u \in P[\mathbf{x}]^*$ is determined by its values $u(\mathbf{x}^{\mathbf{i}})$, $\mathbf{i} \in \mathbf{N}_0^k$. We identify u with the k-sequence, denoted also by u, putting $u(\mathbf{i}) = u(\mathbf{x}^{\mathbf{i}})$, $\mathbf{i} \in \mathbf{N}_0^k$. Then $u \in P[\mathbf{x}]^0$ if and only if $\mathrm{An}\,(u)$ contains a cofinite ideal, i.e., if u is a k-LRS. Thus, $P[\mathbf{x}]^0$ is the space of all k-LRS over the field P. Since we consider elements of $P[\mathbf{x}]^0$ as sequences, but not as mappings, some relations of item 14.B are written in another form. For example, the rule $\varepsilon^0(u) = u(1)$ of evaluation of the counit in the C-dual coalgebra is written in the form $\varepsilon^0(u) = u(1) = u(\mathbf{x}^{\mathbf{0}}) = u(\mathbf{0})$, where $1 \in P[\mathbf{x}]$, $\mathbf{0} \in \mathbf{N}_0^k$.

14.5. Proposition [91, 147]. *The C-dual $P[\mathbf{x}]^0$ of the Hopf algebra from Example* 14.2, *is a Hopf algebra of all k-LRS with the following operations:*

$$(u * v)(\mathbf{i}) = \sum_{\mathbf{j} \le \mathbf{i}} \binom{\mathbf{i}}{\mathbf{j}} u(\mathbf{j}) v(\mathbf{i} - \mathbf{j}), \ \textit{where} \ \binom{\mathbf{i}}{\mathbf{j}} = \binom{i_1}{j_1} \dots \binom{i_k}{j_k}$$

is the convolution (multiplication of sequences in $P[\mathbf{x}]^0$),

$$e^{\mathbf{x}} \ (\textit{where } e^{\mathbf{x}}(\mathbf{0}) = 1_P, \qquad e^{\mathbf{x}}(\mathbf{i}) = 0, \qquad \mathbf{i} \in \mathbf{N}_0^k \backslash \mathbf{0}, \ \text{see (2.13)})$$

is the unit sequence,

$$\Delta^0(u)(\mathbf{i} \otimes \mathbf{j}) = u(\mathbf{i} + \mathbf{j}) \ \textit{is the comultiplication,}$$

$$\varepsilon^0(u) = u(\mathbf{0}) \ \textit{is the counit,}$$

$$S^0(u)(\mathbf{i}) = (-1)^{i_1 + \dots + i_k} u(\mathbf{i}) \ \textit{is the antipode,}$$

where $u, v \in P[\mathbf{x}]^0$, $\mathbf{i}, \mathbf{j} \in \mathbf{N}_0^k$. □

14.6. Proposition [32]. *The C-dual $\mathcal{L}P^{\langle k \rangle}$ of the bialgebra from Example* 14.3 *is the bialgebra of all k-LRS with componentwise multiplication of sequences, unit sequence $e^{\mathbf{x}-1}$ (where $e^{\mathbf{x}-1}(\mathbf{i}) = 1_P$, $\mathbf{i} \in \mathbf{N}_0^k$), and coalgebra operations Δ^0, ε^0 as in $P[\mathbf{x}]^0$.* □

This bialgebra is denoted by $\mathcal{L}P^{\langle k \rangle}$ (but not $\mathcal{B}_k^0$), because the algebra of all k-LRS with componentwise multiplication of sequences was already denoted by $\mathcal{L}P^{\langle k \rangle}$ in Section 13 (see 13.5). The Hopf algebra $P[\mathbf{x}]^0$ and the bialgebra $\mathcal{L}P^{\langle k \rangle}$ are commutative and cocommutative. They are left $\mathcal{P}_k$-modules relative to the usual multiplication of a polynomial on a sequence (see (1.3)).

14.7. Remark. Let $u \in L_P(f)$, $v \in L_P(g)$, $\deg f = m$, $\deg g = n$, and $M(0)$ be the $(m \times n)$-matrix with the elements $M(0)_{ij} = u(i)v(j)$, $i \in \overline{0, m-1}$, $j \in \overline{0, n-1}$. Let

$$M(s+1) = S(f)^T M(s) + M(s) S(g), \qquad s \ge 0.$$

Then $(u * v)(s) = M(s)_{00}$, $s \ge 0$. Thus, the terms $(u * v)(s)$ of the convolution of the sequences u and v can be evaluated recursively. Thus, it is enough to keep in memory the matrix $M(s)$ of fixed size $m \times n$ instead of the segments $u(\overline{0, s})$, $v(\overline{0, s})$ of the sequences u, v.

Now we point out one of subbialgebras in $\mathcal{L}P^{\langle k \rangle}$ which is a Hopf algebra.

14.8. Definition. A function $\mu : \mathbf{Z}^k \to M$ is called a *k-bisequence* over a module ${}_RM$. Define the multiplication of a polynomial on a k-bisequence by the rule (1.3). Then the set of all k-bisequences is the left $R[\mathbf{x}]$-module. The *annihilator* of a k-bisequence μ is the ideal $\mathrm{An}\,(\mu) = \{F(\mathbf{x}) \in R[\mathbf{x}] \,|\, F(\mathbf{x})\mu = 0\}$. A k-bisequence μ is called a *k-linear recurring bisequence* (k-LRB) if $\mathrm{An}\,(\mu)$ contains a monic ideal.

14.9. Definition. A k-bisequence ν is called a *reverse* of the k-sequence μ if $\nu|\mathbf{N}_0^k = \mu$ and $\mathrm{An}(\nu) = \mathrm{An}(\mu)$.

14.10. Examples. The reverse of the k-arithmetical progression $\mu(\mathbf{i}) = \alpha_0 + \alpha_1 i_1 + \ldots + \alpha_k i_k$, $i \in \mathbf{N}_0^k$, where $\alpha_0, \alpha_1, \ldots, \alpha_k \in M$ (see 1.19), is the k-bisequence $\nu(\mathbf{i}) = \alpha_0 + \alpha_1 i_1 + \ldots + \alpha_k i_k$, $i \in \mathbf{Z}_0^k$. The unit $e^{\mathbf{x}}$ of the algebra $P[\mathbf{x}]^0$ (see 14.5) has no reverses. Let $R = \mathbf{Z}[y_1, y_2, \ldots, z_1, z_2, \ldots]/J$, where $J = (y_1 - 2y_2, y_2 - 2y_3, y_3 - 2y_4, \ldots, y_1 - 2z_2, z_2 - 2z_3, z_3 - 2z_4, \ldots)$. Then the sequence $\mu = (y_1, 2y_1, 4y_1, \ldots)$ has two reverses $(\ldots, y_3, y_2, y_1, 2y_1, \ldots)$ and $(\ldots, z_3, z_2, y_1, 2y_1, \ldots)$.

14.11. Proposition. (a) *If there exist elementary polynomials $F_1(x_1), \ldots, F_k(x_k)$ of a k-LRS $\mu \in M^{(k)}$ such that the elements $F_s(0)$, $s \in \overline{1,k}$, are invertible in R, then μ has a reverse.*

(b) *If R is an Artinian ring, then the converse of proposition* (a) *is true.*

(c) *If the condition* (a) *is satisfied, then the reverse of the k-LRS μ is uniquely determined.*

□ (a) Let $k = 1$, $\mu \in L_M(F)$, $m = \deg F$, $F^*(x) = F(0)^{-1}x^m F(1/x)$. Consider the sequence $\varkappa \in L_M(F^*)$ with initial vector $\varkappa(\overline{0, m-1}) = (\mu(m-1), \ldots, \mu(0))$. Then the k-bisequence ν defined by $\nu|\mathbf{N}_0 = \mu$, $\nu(-i) = \varkappa(i+m+1)$, $i \geq 1$, is a reverse of μ. For $k > 1$, the proof is analogous.

(b) A commutative Artinian ring is the direct sum of local rings, and it is sufficient to consider the case where R is a local Artinian ring with maximal ideal $\mathfrak{N}$. Let ν be a reverse of the k-LRS μ and $G_s(x_s) \in \mathrm{An}(\nu)$, $s \in \overline{1,k}$. For $s \in \overline{1,k}$ choose a monic polynomial $F_s(x) \in R[x]$ such that $F_s(x) \equiv G_s(x) \pmod{\mathfrak{N}[x]}$ and any nonzero coefficient of $F_s(x)$ is invertible. Then $G_s(x)$ divides $F_s(x)^n$, where n is the index of nilpotency of the ideal $\mathfrak{N}$, and, therefore, $F_s(x_s)^n \in \mathrm{An}(\nu)$. The polynomial $F_s(x)^n$ can be written in the form $F_s(x)^n = x^l H_s(x)$, where $H_s(0) \in R^*$. Then $H_s(x_s) \in \mathrm{An}(\nu) = \mathrm{An}(\mu)$. □

14.12. Remark. If R is not an Artinian ring, then the converse of Proposition 14.11(a) is not true. For example, let $R = \mathbf{Z}[y_1, y_2, \ldots]/J$, where $J = (y_1 - 2y_2, y_2 - 2y_3, \ldots)$. Then the sequence $\mu = (y_1, 2y_1, 4y_1, \ldots)$ has the reverse $(\ldots, y_3, y_2, y_1, 2y_1, \ldots)$, but μ does not satisfy the conditions 14.11(a) because $\mathrm{An}(\mu) = (x-2)$.

14.13. Corollary. *A periodic k-LRS over a module ${}_RM$ has a reverse if and only if it is reversible in the sense of Definition* 5.17.

□ This follows from 5.18(b) and 14.11(a). □

By Corollary 14.13, we can extend Definition 5.17 of a reversible sequence on the class of nonperiodic sequences.

14.14. Definition. A k-LRS μ over a module ${}_RM$ is said to be *reversible* if there exists a reverse of μ.

14.15. Proposition [32]. *The sets $\mathcal{D}P^{(k)}$ of degenerating and $\mathcal{R}P^{(k)}$ of reversible k-LRS are subbialgebras in the bialgebra $\mathcal{L}P^{(k)}$ of all k-LRS over the field P, and* (see also (5.15))

$$\mathcal{L}P^{(k)} = \mathcal{D}P^{(k)} \dotplus \mathcal{R}P^{(k)}.$$

Moreover, $\mathcal{R}P^{(k)}$ is a Hopf algebra with antipode $S^0(u)(\mathbf{i}) = \nu(-\mathbf{i})$, $\mathbf{i} \in \mathbf{N}_0^k$, where ν is the reverse of the k-LRS u. □

D. Comultiplication in the coalgebras $\mathcal{L}P^{(k)}$ and $P[\mathbf{x}]^0$.

Let $u \in \mathcal{L}P^{(k)}$. By definition, $\Delta^0 u$ is an element of $\mathcal{L}P^{(k)} \otimes \mathcal{L}P^{(k)}$, $\Delta^0 u = \sum u_t \otimes u'_t$, such that

$$\sum u_t(\mathbf{i}) u'_t(\mathbf{j}) = u(\mathbf{i}+\mathbf{j}) \text{ for } \mathbf{i}, \mathbf{j} \in \mathbf{N}_0^k. \tag{14.1}$$

Proposition 14.5 does not give an explicit description of the sequences u_t, u'_t. Now we give one such description.

14.16. Proposition. *Let $u \in \mathcal{L}P^{(k)}$ be a k-LRS with elementary characteristic polynomials $f_1(x_1), \ldots, f_k(x_k)$ of degrees $m_1, \ldots, m_k$. Then*

$$\Delta^0 u = \sum_{\mathbf{t} \leq \mathbf{m}-\mathbf{1}} (\mathbf{x}^{\mathbf{t}} u) \otimes e_{\mathbf{t}}^{\mathbf{F}},$$

where $\mathbf{m} = (m_1, \ldots, m_k)$ and $e_{\mathbf{t}}^{\mathbf{F}}$ is defined in (2.13).

□ We show that (14.1) holds. For $\mathbf{i}, \mathbf{j} \in \mathbf{N}_0^k$ we have

$$u(\mathbf{i}+\mathbf{j}) = (\mathbf{x}^{\mathbf{i}}u)(\mathbf{j}) = \Big(\sum_{\mathbf{t}\le\mathbf{m}-1} (\mathbf{x}^{\mathbf{i}}u)(\mathbf{t})\cdot e_{\mathbf{t}}^{\mathbf{F}}\Big)(\mathbf{j}) = \sum_{\mathbf{t}\le\mathbf{m}-1} (\mathbf{x}^{\mathbf{t}}u)(\mathbf{i})\cdot e_{\mathbf{t}}^{\mathbf{F}}(\mathbf{j}).\square$$

14.17. Example. Let $k=1$, $f(x)=x^2-x-1$, $u=(0,1,1,2,\ldots)\in L_P(f)$ be the Fibonacci sequence over P (see 1.5). Then $e_1^f = e^f = u$, $e_0^f = xu-u$; hence $\Delta^0 u = u\otimes(xu)+(xu)\otimes u - u\otimes u$.

14.18. Example. Let $u(\mathbf{i}) = \mathbf{a}^{\mathbf{i}}$, where $\mathbf{a}\in P^k\backslash\mathbf{0}$ (a k-geometric progression, see 1.19), or let $u=e^{\mathbf{x}}$ be the unit of the algebra $P[\mathbf{x}]^0$ (a k-geometric progression for $\mathbf{a}=\mathbf{0}$). Then $\Delta^0 u = u\otimes u$, i.e., $u\in G(\mathcal{L}P^{\langle k\rangle})$. It is easy to see that we have enumerated all group-like elements of the coalgebras $\mathcal{L}P^{\langle k\rangle}$ and $P[\mathbf{x}]^0$. Since $(\mathbf{a}^{\mathbf{i}})\cdot(\mathbf{b}^{\mathbf{i}}) = ((\mathbf{ab})^{\mathbf{i}})$, the group-like elements of the bialgebra $\mathcal{L}P^{\langle k\rangle}$ form a semigroup, isomorphic to the semigroup $(P,\cdot)$, and the group-like elements of the Hopf algebra $\mathcal{R}P^{\langle k\rangle}$ form a group, isomorphic to the multiplicative group of the field P. Since $(\mathbf{a}^{\mathbf{i}})*(\mathbf{b}^{\mathbf{i}}) = ((\mathbf{a}+\mathbf{b})^{\mathbf{i}})$, the group-like elements of the Hopf algebra $P[\mathbf{x}]^0$ form a group, isomorphic to the additive group of the field P. Thus,

$$(G(\mathcal{L}P^{\langle k\rangle}),\cdot)\cong(P,\cdot),$$
$$(G(\mathcal{R}P^{\langle k\rangle}),\cdot)\cong(P^*,\cdot),$$
$$(G(P[\mathbf{x}]^0),*)\cong(P,+).$$

In Proposition 14.16, $\Delta^0 u$ is expressed through the shifts of the sequence u and the sequences $e_{\mathbf{t}}^{\mathbf{F}}$. We can express $\Delta^0 u$ only through the shifts of u (as in Example 14.17) or only through $e_{\mathbf{t}}^{\mathbf{F}}$. In the more general case where B is a subcoalgebra of a coalgebra (C,Δ,ε) and $\{b_r|\ r\in\Omega\}$ is a basis of the vector space ${}_PB$, the coefficients $\lambda_{rst}\in P$, defined by $\Delta b_r = \sum_{s,t\in\Omega}\lambda_{rst}b_s\otimes b_t$, are called the *structure constants* of the comultiplication Δ with respect to the basis $\{b_r|\ r\in\Omega\}$. The structure constants of the subcoalgebras $L_P(f_1,\ldots,f_s)\subset\mathcal{L}P^{\langle k\rangle}$ with respect to different bases are obtained in [91, 147]. Note that the simplest constants are obtained with respect to the binomial basis (see Section 2.D):

$$\Delta^0(\mathbf{a}^{[\mathbf{l}]}) = \sum_{\mathbf{j}\le\mathbf{l}} \mathbf{a}^{[\mathbf{j}]}\otimes\mathbf{a}^{[\mathbf{l}-\mathbf{j}]},\ \text{where } \mathbf{a}^{[\mathbf{l}]}(\mathbf{i}) = \binom{\mathbf{i}}{\mathbf{l}}\mathbf{a}^{\mathbf{i}-\mathbf{l}},\qquad \mathbf{i}\in\mathbf{N}_0^k.$$

E. Subcoalgebras in $\mathcal{L}P^{\langle k\rangle}$ and $P[\mathbf{x}]^0$.

For a k-LRS $u\in\mathcal{L}P^{\langle k\rangle}$, define $C(u)$ as a minimal subcoalgebra in $\mathcal{L}P^{\langle k\rangle}$ such that $u\in C(u)$.

14.19. Proposition. *$C(u)$ is equal to the cyclic $\mathcal{P}_k$-module generated by u, i.e., $C(u)=\mathcal{P}_k u$.*

□ Let $\Delta^0 u = \sum u_t\otimes u_t'$, where $u_t, u_t'\in C(u)$. By (14.1), $\mathbf{x}^{\mathbf{i}}u = \sum u_t(\mathbf{i})u_t'\in\sum Pu_t'\subseteq C(u)$, $\mathbf{i}\in\mathbf{N}_0^k$. Hence $\mathcal{P}_k u\subseteq C(u)$.

Conversely, since u is a k-LRS, the space $\mathcal{P}_k u$ is finite-dimensional over P. Let $\{v_1,\ldots,v_n\}$ be its basis. We can find polynomials $g_1(\mathbf{x}),\ldots,g_n(\mathbf{x})\in\mathcal{P}_k$ such that $(g_s(\mathbf{x})v_t)(\mathbf{0}) = \delta_{st}$ (δ_{st} is the Kronecker delta). Denote $\psi_t(\mathbf{i})$ as a coefficient on v_t in the decomposition of $\mathbf{x}^{\mathbf{i}}u$ with respect to the basis $\{v_1,\ldots,v_n\}$:

$$\mathbf{x}^{\mathbf{i}}u = \sum_{t=1}^{n}\psi_t(\mathbf{i})v_t,\qquad \mathbf{i}\in\mathbf{N}_0^k. \tag{14.2}$$

Then ψ_s is a k-sequence, and

$$(g_s(\mathbf{x})u)(\mathbf{i}) = (g_s(\mathbf{x})\mathbf{x}^{\mathbf{i}}u)(\mathbf{0}) = \sum_{t=1}^{n}\psi_t(\mathbf{i})(g_s(\mathbf{x})v_t)(\mathbf{0}) = \psi_s(\mathbf{i}).$$

Hence $\psi_s = g_s(\mathbf{x})u\in\mathcal{P}_k u$. By (14.2),

$$u(\mathbf{i}+\mathbf{j}) = (\mathbf{x}^{\mathbf{i}}u)(\mathbf{j}) = \sum_{t=1}^{n}\psi_t(\mathbf{i})v_t(\mathbf{j}).$$

It follows that $\Delta^0 u = \sum \psi_t \otimes v_t \in \mathcal{P}_k u \otimes \mathcal{P}_k u$. Therefore, $\mathcal{P}_k u$ is a subcoalgebra and $C(u) \subseteq \mathcal{P}_k u$. □

Another proof is given in [91].

14.20. Proposition. *A subspace in $\mathcal{L}P^{\langle k\rangle}$ is a subcoalgebra if and only if it is a $\mathcal{P}_k$-submodule.*

□ B is a subcoalgebra $\Leftrightarrow \forall\, u \in B\ (C(u) \subseteq B) \Leftrightarrow \forall\, u \in B\ (\mathcal{P}_k u \subseteq B) \Leftrightarrow B$ is a $\mathcal{P}_k$-submodule. □

14.21. Corollary. *Finite-dimensional (over P) subcoalgebras in $\mathcal{L}P^{\langle k\rangle}$ are exactly k-LRS-families $L_P(I)$, where I is a monic ideal in $\mathcal{P}_k$.* □

Since $P[\mathrm{x}]^0 = \mathcal{L}P^{\langle k\rangle}$ as coalgebras, all results of this section are also true for the coalgebra $P[\mathrm{x}]^0$.

F. The convolution of LRS-families.

In Section 13.B, we described the product of LRS-families in the algebra $(\mathcal{L}P^{\langle 1\rangle}, +, \cdot)$. Here we consider an analogous problem for the algebra $(P[x]^0, +, *)$.

14.22. Definition. For subsets $U, V \subseteq P[\mathrm{x}]^0$, define the *convolution* $U * V$ as a subspace spanned by $u * v$, where $u \in U$, $v \in V$, i.e., $U * V =_P \{u * v |\ u \in U, v \in V\}$.

Since

$$x_s(u * v) = (x_s u) * v + u * (x_s v), \qquad s \in \overline{1,k}, \tag{14.3}$$

the convolution of k-LRS-families is a finite-dimensional $\mathcal{P}_k$-module and, therefore, it is a k-LRS-family (see the proof of Theorem 13.3). For $k = 1$, this means that for arbitrary monic polynomials $f(x), g(x) \in P[x]$ there exists a monic polynomial $h(x) \in P[x]$ such that $L_P(f) * L_P(g) = L_P(h)$. Our purpose is to describe the form of $h(x)$. Let $a \vee b$ be the disjunction of natural numbers a and b, defined in 13.10.

14.23. Definition. Let f, g be irreducible separable polynomials over the field P, $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ be the roots of these polynomials in the splitting field. Denote

$$f * g = \text{ l.c.m.}\,[x - (\alpha_s + \beta_t) |\ 1 \le s \le m,\ 1 \le t \le n], \tag{14.4}$$

$$f^a * g^b = (f * g)^{a \vee b}.$$

If $\operatorname{char} P = p > 0$, then polynomials f, g, irreducible over P, may be not separable. Then there exists a purely separable extension Q of P such that $f = \Phi^r$, $g = \Psi^s$, where Φ, Ψ are irreducible over Q and separable, r, s are powers of p. Define $f^a * g^b = \Phi^{ar} * \Psi^{bs}$. Finally, if f, g are arbitrary polynomials over P with canonical decompositions $f = f_1^{a_1} \ldots f_m^{a_m}$, $g = g_1^{b_1} \ldots g_n^{b_n}$, then we define

$$f * g = \text{ l.c.m.}\,[f_s^{a_s} * g_t^{b_t} |\ 1 \le s \le m,\ 1 \le t \le n].$$

We call $f * g$ the *convolution of polynomials* f and g. It is easy to see that $f * g$ is a polynomial over P.

Note that if in (14.4) we find an l.c.m. of the polynomials $x - \alpha_s \beta_t$ instead of $x - (\alpha_s + \beta_t)$, and keep without changes the rest of Definition 14.23, then we get exactly the disjunction $f \vee g$ of the polynomials f and g (see 13.12, 13.13). Thus, the convolution of polynomials may be considered as an additive analogue of the disjunction.

Recall that $\alpha^{[l]}$ denotes a binomial sequence of order $l + 1$ with root α (see Section 2.D).

14.24. Lemma. *If $\alpha, \beta \in P$, $a, b \ge 0$, then*

$$\alpha^{[a]} * \beta^{[b]} = \binom{a+b}{a} (\alpha + \beta)^{[a+b]}. \quad \square$$

14.25. Lemma. *If $\alpha, \beta \in P$, $a, b \ge 1$, then*

$$L_P((x - \alpha)^a) * L_P((x - \beta)^b) = L_P((x - \alpha - \beta)^{a \vee b}).$$

□ Let U and V be the left and right parts of the last equality. In the case $\operatorname{char} P = 0$, our lemma follows from 14.24. Let $\operatorname{char} P = p > 0$, $r = \sum r_i p^i < a$, $s = \sum s_i p^i < b$, where $0 \le r_i,\ s_i < p$. To prove the inclusion $U \subset V$, it is sufficient to check that $\alpha^{[r]} * \beta^{[s]} \in V$. By Lemma 14.24, $\alpha^{[r]} * \beta^{[s]} = \binom{r+s}{r} (\alpha+\beta)^{[r+s]}$. If $\binom{r+s}{r} \equiv 0$

$(\mathrm{mod}\, p)$, then everything is clear. Otherwise, by the Lucas theorem [4, Corollary 4.72], $r_i + s_i < p$, $i \geq 0$. Therefore, we have

$$\sum_{i\geq\lambda} r_i p^i \leq \sum_{i\geq\lambda} a_i p^i, \qquad \sum_{i\geq\lambda} s_i p^i \leq \sum_{i\geq\lambda} b_i p^i, \qquad \sum_{i<\lambda} (r_i + s_i) p^i < p^\lambda,$$

where λ is taken from Definition 13.10 of the disjunction of a and b. By summing these three inequalities, we get $r + s < a \vee b$. Therefore, by Lemma 2.16, $(\alpha + \beta)^{[r+s]} \in V$.

Conversely, let $m = \sum m_i p^i < a \vee b$. The definition of $a \vee b$ implies that there exist integers $r < a$, $s < b$ such that $r + s = m$ and $r_i + s_i = m_i$ for $i \geq 0$. Then, by Lemma 14.24, $\binom{m}{r}(\alpha + \beta)^{[m]} = \alpha^{[r]} * \beta^{[s]}$, and, by the Lucas theorem, $\binom{m}{r} \not\equiv 0 \ (\mathrm{mod}\, p)$. Therefore, $(\alpha + \beta)^{[m]} \in U$ for any $m < a \vee b$, and by Lemma 2.16 we see that $V \subset U$. □

14.26. Lemma. *If a polynomial $f(x) \in P[x]$ is separable, then $L_P(f^a) = L_P(f) * L_P(x^a)$.*

□ Let $\alpha_1, \ldots, \alpha_m$ be the roots of $f(x)$ in the splitting field Q. Then, by 13.6,

$$L_P(f^a) = P^\infty \cap L_Q(f^a) = P^\infty \cap \sum \oplus L_Q((x - \alpha_i)^a) =$$

$$P^\infty \cap \sum \oplus (L_Q(x - \alpha_i) * L_Q(x^a)) = P^\infty \cap (L_Q(f) * L_Q(x^a)) = L_P(f) * L_P(x^a).\square$$

14.27. Theorem [31]. *For arbitrary polynomials $f(x)$, $g(x)$ over the field P, we have $L_P(f) * L_P(g) = L_P(f * g)$.*

□ Lemmas 14.24–14.26 enable us to prove Theorem 14.27 analogously to the proof of Theorem 13.13 (see [174]). □

14.28. Remark. If P is a finite field and f, g are irreducible polynomials over P of coprime degrees m, n, then Definition 14.23 and Theorem 13.13 show that $f * g$ and $f \vee g$ are irreducible polynomials over P of degrees mn. Thus, we can use Theorems 13.13 and 14.27 to construct irreducible polynomials of large degrees over finite fields. Indeed, if $u \in L_P(f) \backslash 0$, $v \in L_P(g) \backslash 0$, then $f * g$ (correspondingly $f \vee g$) is the minimal polynomial of LRS $u * v$ (correspondingly uv), which can be found by means of the Berlekamp–Massey algorithm (see Section 10.C). Note that the polynomial $f \vee g$ is not primitive, but $f * g$ may be primitive (for example, when $P = \mathbb{F}_2$, $f(x) = x^2 + x + 1$, $g(x) = x^3 + x + 1$). Therefore, Theorem 14.27 makes it possible to construct primitive polynomials of large degrees.

14.29. Corollary. *Let $I = (f_1(x_1), \ldots, f_k(x_k))$ and $J = (g_1(x_1), \ldots, g_k(x_k))$ be elementary ideals of the ring $\mathcal{P}_k$. Then*

$$L_P(I) * L_P(J) = L_P(f_1 * g_1, \ldots, f_k * g_k). \quad \square$$

The open problems are as follows: give descriptions of the convolution, the product (see Section 13), and the E-convolution (see section 14.G below) of arbitrary k-LRS-families $L_P(I)$, $L_P(J)$ for $k > 1$.

G. The exponential convolution of k-sequences.

14.30. Definition. *The exponential convolution (E-convolution)* of k-sequences u, v is a k-sequence $u \bigtriangledown v$ such that

$$(u \bigtriangledown v)(\mathbf{i}) = \sum_{\mathbf{j}\leq\mathbf{i}} u(\mathbf{j}) v(\mathbf{i} - \mathbf{j}).$$

The E-convolution of subsets U, $V \subseteq P^{(k)}$ is the subspace $U \bigtriangledown V =_P \{u \bigtriangledown v |\ u \in U, v \in V\}$. The set $P^{(k)}$ of all k-sequences is an algebra with operations $+$, $\bigtriangledown$, isomorphic to the algebra of formal power series $P[[\mathbf{x}]]$ over the field P. The isomorphism is given by

$$\sigma : (P^{(k)}, +, \bigtriangledown) \to (P[[\mathbf{x}]], +, \cdot), \qquad u \to \mathfrak{G}_u(\mathbf{x}),$$

where $\mathfrak{G}_u(\mathbf{x})$ is the generating function of u (see Section 2.C).

14.31. Proposition [114]. *If $f(x)$, $g(x) \in P[x]$ are monic polynomials, then $L_P(f) \bigtriangledown L_P(g) \subset L_P(fg)$.*

□ By Proposition 2.14, the generating functions of the sequences $u \in L_P(f)$, $v \in L_P(g)$ have the form

$$\mathfrak{G}_u(x) = M(x)/f^*(x), \qquad \mathfrak{G}_v(x) = N(x)/g^*(x),$$

where $\deg M(x) < m = \deg f(x)$, $\deg N(x) < n = \deg g(x)$. Therefore,

$$\mathfrak{G}_{u \nabla v} = \mathfrak{G}_u(x)\mathfrak{G}_v(x) = M(x)N(x)/(fg)^*(x),$$

and, by 2.14, $u \nabla v \in L_P(fg)$. □

In this proposition the inclusion is proper: the proof implies that

$$L_P(f) \nabla L_P(g) = P \cdot xe^{fg} + P \cdot x^2 e^{fg} + \ldots + P \cdot x^{m+n-1} e^{fg},$$

and we know that $L_P(fg) = Pe^{fg} + P \cdot xe^{fg} + \ldots + P \cdot x^{m+n-1}e^{fg}$.

14.32. Corollary. *Under the conditions of Corollary* 14.29, *we have*

$$L_P(I) \nabla L_P(J) \subset L_P(f_1 \nabla g_1, \ldots, f_k \nabla g_k). \square$$

It follows from 14.32 that the E-convolution of k-recurrences is a k-LRS. Therefore, $(\mathcal{L}P^{\langle k \rangle}, +, \nabla)$ is a subalgebra in the algebra $(P^{\langle k \rangle}, +, \nabla)$. Let $P_{\mathrm{rat}}[[\mathrm{x}]]$ be the subalgebra in $P[[\mathrm{x}]]$ consisting of all rational functions, described in Proposition 2.14. Then the restriction of the isomorphism $\sigma : P^{\langle k \rangle} \to P[[\mathrm{x}]]$ on $\mathcal{L}P^{\langle k \rangle}$ is an algebra isomorphism between $(\mathcal{L}P^{\langle k \rangle}, +, \nabla)$ and $(P_{\mathrm{rat}}[[\mathrm{x}]], +, \cdot)$.

H. The structure of algebras of linear recurring sequences.

Let $p = \operatorname{char} P$ (p is arbitrary), Ω be the set of all irreducible polynomials from $P[x]$, $\hat{P}$ be the algebraic closure of P, $e(f)$ be the multiplicity of the roots of polynomial $f(x) \in \Omega$. For a subset $\mathcal{G} \subseteq \Omega$ denote $K(\mathcal{G}) = \{\alpha \in \hat{P} |\ f(\alpha) = 0 \text{ for some } f(x) \in \mathcal{G}\}$. We define $0^0 = p^0 = 1$, $0^\infty = p^\infty = \infty$. We say "$\infty$ divides n" if $n = \infty$. As in Section 13, $a \vee b$ is the disjunction of integers a and b and $L_P(f^\infty) = \cup_{n \geq 1} L_P(f^n)$.

14.33. Theorem [32]. (a) *Any nonzero subcoalgebra of the Hopf algebra* $P[x]^0$ *has the form*

$$C = \sum_{g \in \mathcal{G}} \oplus L_P(g^{n_g}), \text{ where } \mathcal{G} \subseteq \Omega, \qquad n_g \in \mathbb{N} \cup \{\infty\}.$$

(b) C *is a subbialgebra if and only if* $K(\mathcal{G})$ *is a submonoid in* $(\hat{P}, +)$ *and*

$$\forall f, g \in \mathcal{G}\ \ \forall \alpha \in K(f)\ \ \forall \beta \in K(g) \quad (n_h e(h) \geq n_f e(f) \vee n_g e(g)),$$

where $h(x) = \mu_{P,\alpha+\beta}(x)$ *is the minimal polynomial of the element* $\alpha + \beta$ *over the field* P. *In particular, it follows that there exists* $s \in \mathbb{N} \cup \{0, \infty\}$ *such that* $n_x = p^s$ *and* p^s *divides* n_g *for any* $g \in \mathcal{G}$.

(c) C *is a Hopf subalgebra if and only if* $K(\mathcal{G})$ *is a subgroup in* $(\hat{P}, +)$ *and there exists* $s \in \mathbb{N} \cup \{0, \infty\}$ *such that* $n_g = p^s$ *for any* $g \in \mathcal{G}$.

□ (a) follows from 14.19. Let P be algebraically closed. Then each subcoalgebra in $P[x]^0$ is of the form

$$C = \sum_{a \in K} \oplus L_P((x-a)^{n_a}), \text{ where } K \subseteq P, \qquad n_a \in \mathbb{N} \cup \{\infty\}.$$

(b) Let C be a subbialgebra. Then C possesses the unit sequence $e^x = (1, 0, 0, \ldots)$; hence $L_P(x) \subseteq C$ and $0 \in K$. Since

$$L_P((x-a)^{n_a}) * L_P((x-b)^{n_b}) = L_P((x-a-b)^{n_a \vee n_b}) \qquad (a, b \in K),$$

K is a submonoid in $(\hat{P}, +)$ and $n_a \vee n_b \leq n_{a+b}$. Conversely, if these conditions hold, then the coalgebra C possesses the unit sequence and C is closed under the convolution of sequences, i.e., C is a subbialgebra.

Since $L_P(x^{n_0}) * L_P(x^{n_0}) = L_P(x^{n_0 \vee n_0}) \subseteq C$, we have $n_0 \vee n_0 \leq n_0$; hence $n_0 = p^s$. Since $L_P(x^{n_0}) * L_P((x-a)^{n_a}) = L_P((x-a)^{n_0 \vee n_a}) \subseteq C$, we have $n_0 \vee n_a = p^s \vee n_a \leq n_a$. Therefore, p^s divides n_a for all $a \in K$.

(c) Let subbialgebra C be a Hopf subalgebra. For $U \subseteq P[x]^0$ denote $S^0(U) = \{S^0(u) |\ u \in U\}$. Obviously, $S^0(L_P((x-a)^{n_a})) = L_P((x+a)^{n_a})$. Hence, if $a \in K$, then $-a \in K$, i.e., K is a subgroup of $(\hat{P}, +)$, and $n_{-a} = n_a$. Further,

$$L_P((x-a)^{n_a}) * L_P((x+a)^{n-a}) = L_P(x^{n_a \vee n_{-a}}) \subseteq C.$$

Therefore, $n_a \vee n_a \leq n_0 = p^s$, and since n_a is divided by p^s by (b), we have that $n_a = p^s$ for any $a \in K$. Conversely, if K is a subgroup in $(\hat{P}, +)$ and $n_a = p^s$ for any $a \in K$, then C is a subbialgebra and $S^0(C) \subseteq C$, i.e., C is a Hopf subalgebra.

The case where P is not algebraically closed is reduced to the case where P is algebraically closed. □

Theorem 14.33 implies that $\mathcal{D}P^{\langle 1 \rangle} = L_P(x^\infty)$ is a Hopf subalgebra in $P[x]^0$. Therefore, the set $\mathcal{D}P^{\langle k \rangle} = L_P(\mathrm{x}^\infty)$ of degenerating k-recurrences is a Hopf subalgebra in $P[\mathrm{x}]^0$. Define $\mathcal{L}P^{\langle k \rangle}_{\mathrm{irr}}$ as the subspace of k-recurrences u such that $\mathrm{Ann}\,(u)$ contains an elementary ideal $(f_1(x_1), \ldots, f_k(x_k))$, where $f_s(x)$ is a product of distinct polynomials irreducible over P, $s \in \overline{1,k}$. Then the following analogue of Theorem 13.17 holds.

14.34. Theorem (V. Kurakin, 1993). *The Hopf algebra $P[\mathrm{x}]^0$ of all k-recurrences is the convolution of the subcoalgebra $\mathcal{L}P^{\langle k \rangle}_{\mathrm{irr}}$ and the Hopf subalgebra $\mathcal{D}P^{\langle k \rangle}$ of all degenerating k-recurrences:*

$$P[\mathrm{x}]^0 = \mathcal{L}P^{\langle k \rangle}_{\mathrm{irr}} * \mathcal{D}P^{\langle k \rangle}.$$

The subcoalgebra $\mathcal{L}P^{\langle k \rangle}_{\mathrm{irr}}$ is a subbialgebra if and only if P is a perfect field, and in this case $\mathcal{L}P^{\langle k \rangle}_{\mathrm{irr}}$ is a Hopf subalgebra. □

14.35. Theorem [32]. (a) *Any nonzero subcoalgebra of the Hopf algebra $\mathcal{R}P^{\langle k \rangle}$ has the form*

$$C = \sum_{g \in \mathcal{H}} \oplus L_P(g^{n_g}), \text{ where } \mathcal{H} \subseteq \Omega \backslash \{x\}, \qquad n_g \in \mathbb{N} \cup \{\infty\}.$$

(b) *C is a subbialgebra if and only if $K(\mathcal{H})$ is a submonoid in $(\hat{P}^*, \cdot)$ and*

$$\forall f, g \in \mathcal{H}\ \forall \alpha \in K(f)\ \forall \beta \in K(g) \qquad (n_h e(h) \geq n_f e(f) \vee n_g e(g)),$$

where $h(x) = \mu_{P,\alpha\beta}(x)$. In particular, there exists $s \in \mathbb{N} \cup \{0, \infty\}$ such that $n_{x-1} = p^s$ and p^s divides n_g for any $g \in \mathcal{H}$.

(c) *C is a Hopf subalgebra if and only if $K(\mathcal{H})$ is a subgroup in $(\hat{P}^*, \cdot)$ and there exists $s \in \mathbb{N} \cup \{0, \infty\}$ such that $n_g = p^s$ for any $g \in \mathcal{H}$.*

□ By 13.9–13.12,

$$L_P((x-a)^{n_a}) \cdot L_P((x-b)^{n_b}) = L_P((x-ab)^{n_a \vee n_b}).$$

In all other respects the proof repeats the proof of 14.33. □

14.36. Theorem [32]. *Any subcoalgebra (subbialgebra) of the bialgebra $\mathcal{L}P^{\langle 1 \rangle}$ is of the form $L_P(x^n) \oplus C$, where $n \in \mathbb{N} \cup \{0, \infty\}$ and C is a subcoalgebra (correspondingly subbialgebra) of $\mathcal{R}P^{\langle 1 \rangle}$.* □

Consider the decomposition from Theorem 13.17:

$$\mathcal{L}P^{\langle k \rangle} = \mathcal{D}P^{\langle k \rangle} \dot{+} \mathcal{R}P^{\langle k \rangle},$$

where

$$\mathcal{D}P^{\langle k \rangle} = L_P(\mathrm{x}^\infty), \qquad \mathcal{R}P^{\langle k \rangle} = \mathcal{R}P^{\langle k \rangle}_{\mathrm{irr}} \cdot L_P((\mathrm{x}-\mathrm{e})^\infty).$$

Theorems 14.35, 14.36 imply that the set $\mathcal{D}P^{\langle k \rangle} = L_P(\mathrm{x}^\infty)$ of degenerating k-recurrences and the set $\mathcal{R}P^{\langle k \rangle}$ of reversible k-recurrences are subbialgebras of the bialgebra $\mathcal{L}P^{\langle k \rangle}$, $L_P((\mathrm{x}-\mathrm{e})^\infty)$ is a Hopf subalgebra of $\mathcal{R}P^{\langle k \rangle}$, $\mathcal{R}P^{\langle k \rangle}_{\mathrm{irr}}$ is a subcoalgebra of $\mathcal{R}P^{\langle k \rangle}$, and $\mathcal{R}P^{\langle k \rangle}_{\mathrm{irr}}$ is a Hopf subalgebra of $\mathcal{R}P^{\langle k \rangle}$ if and only if P is a perfect field.

I. Extensions of k-recurrences as solutions of the Cauchy problem. By (14.3), the multiplication of k-sequences on the polynomial x_s, $s \in \overline{1,k}$, is a derivation of the algebra $P[\mathbf{x}]^0$. Therefore, the relation

$$f(\mathbf{x})u = v \tag{14.5}$$

is a linear partial differential equation. The set of all solutions of (14.5) is the set of all extensions of the sequence v by the polynomial $f(\mathbf{x})$ (see Section 8). The condition $u(\mathbf{i}) = \alpha$, where $\alpha \in P$, is equivalent to the condition $(\mathbf{x}^{\mathbf{i}}u)(0) = \alpha$, which may be interpreted as the initial condition for a solution of the differential equation (14.5). In this terminology, the extension $(\alpha\frac{v}{f})$ of a 1-LRS v by a polynomial $f(x)$ of degree m and a vector $\alpha = (\alpha_0, \ldots, \alpha_{m-1})$ is a solution of the *Cauchy problem*

$$f(x)u = v, \qquad (u(0), (xu)(0), \ldots, (x^{m-1}u)(0)) = \alpha,$$

and the set of all extensions of LRS v by the polynomial $f(x)$ is the *integral of the sequence* v [136].

14.37. Definition. Let P be a field of characteristic 0. The *exponential generating function* of a k-sequence $u \in P^{(k)}$ is defined as the formal power series

$$\mathcal{E}_u(\mathbf{z}) = \sum_{\mathbf{i} \in \mathbb{N}_0^k} \frac{u(\mathbf{i})}{\mathbf{i}!} \cdot \mathbf{z}^{\mathbf{i}}, \text{ where } \mathbf{z} = (z_1, \ldots, z_k).$$

The multiplication of sequences u on x_s corresponds to the derivation of $\mathcal{E}_u(\mathbf{z})$ with respect to z_s. Therefore, for $f(\mathbf{x}) \in P[\mathbf{x}]$ we have

$$\mathcal{E}_{f(\mathbf{x})u}(\mathbf{z}) = f\Big(\frac{\partial}{\partial \mathbf{z}}\Big)\mathcal{E}_u(\mathbf{z}), \text{ where } \frac{\partial}{\partial \mathbf{z}} = \Big(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_k}\Big),$$

and the equality (14.5) may be written in the form

$$f\Big(\frac{\partial}{\partial \mathbf{z}}\Big)\mathcal{E}_u(\mathbf{z}) = \mathcal{E}_v(\mathbf{z}). \tag{14.6}$$

Thus, if $\operatorname{char} P = 0$, then all extensions of a k-LRS v by polynomial $f(\mathbf{x})$ are exactly all k-recurrences u such that $\mathcal{E}_u(\mathbf{z})$ satisfies the linear differential equation (14.6).

It is straightforward to check that the mapping $\varkappa : u \to \mathcal{E}_u(\mathbf{z})$ is an algebra isomorphism from $(P^{(k)}, +, *)$ onto $(P[[\mathbf{z}]], +, \cdot)$. Let $P_{\mathrm{der}}[[\mathbf{z}]] < P[[\mathbf{z}]]$ be the subalgebra of all series $G(\mathbf{z}) = \sum g_{\mathbf{i}}\mathbf{z}^{\mathbf{i}}$ such that $f_1\Big(\frac{\partial}{\partial z_1}\Big)G = \ldots = f_k\Big(\frac{\partial}{\partial z_k}\Big)G = 0$ for some monic polynomials $f_1(x), \ldots, f_k(x) \in P[x]$. Define the comultiplication, counit, and antipode on the algebra $P_{\mathrm{der}}[[\mathbf{z}]]$ by

$$\Delta G = \sum_{\mathbf{i},\mathbf{j}} \binom{\mathbf{i}+\mathbf{j}}{\mathbf{i}} g_{\mathbf{i}+\mathbf{j}}\mathbf{z}^{\mathbf{i}} \otimes \mathbf{z}^{\mathbf{j}}, \qquad \varepsilon(G) = G(\mathbf{0}), \qquad S(G) = G(-\mathbf{z}).$$

14.38. Proposition. *Let P be a field of characteristic 0. Then the map $\varkappa : u \to \mathcal{E}_u(\mathbf{z})$ is an isomorphism of the Hopf algebras $P[\mathbf{x}]^0$ and $P_{\mathrm{der}}[[\mathbf{z}]]$.* □

J. k-Recurrences as the Hopf algebra of the representative functions. Let $(G, +)$ be a commutative monoid, P^G be the algebra of all functions $u : G \to P$ with pointwise operations. For $g \in G$, $u \in P^G$ define gu to be the function from P^G such that

$$(gu)(h) = u(g + h), \qquad h \in G.$$

14.39. Definition. A function $u \in P^G$ is called a *representative function* if the subspace of P^G spanned by $\{gu \mid g \in G\}$ is finite-dimensional over P. The set $R(G)$ of all representative functions is a P-subalgebra of P^G [3, 147].

Define the comultiplication Δ and the counit ε in $R(G)$ by

$$\Delta u = \sum u_t \otimes u'_t, \text{ if } u(g+h) = \sum u_t(g)u'_t(h) \text{ for any } g, h \in G,$$

$$\varepsilon(u) = u(0).$$

Then $R(G)$ is a bialgebra [3]. If G is a group, then the map $S: R(G) \to R(G)$, $(S(u))(g) = u(-g)$, is an antipode, and $R(G)$ is a Hopf algebra [3].

Let $G = (\mathbf{N}_0^k, +)$. Then P^G is exactly the set $P^{\langle k \rangle}$ of all k-sequences. A sequence (i.e., a function) $u \in P^G$ is representative if and only if the subspace ${}_P\{\mathbf{x}^{\mathbf{i}}u | \ \mathbf{i} \in \mathbf{N}_0^k\}$ is finite-dimensional, i.e., if u is a k-LRS. It can be readily shown that the above-introduced operations in the bialgebra $R(\mathbf{N}_0^k)$ are identical to the operations in the bialgebra $\mathcal{L}P^{\langle k \rangle}$ introduced in 14.6. Therefore, we have

14.40. Proposition. *The bialgebra $R(\mathbf{N}_0^k)$ of representative functions on the monoid $(\mathbf{N}_0^k, +)$ coincides with the bialgebra $\mathcal{L}P^{\langle k \rangle}$ of k-linear recurring sequences over P* (see Proposition 14.6). □

If $G = (\mathbf{Z}^k, +)$, then P^G is the set of all k-bisequences over P, and $R(\mathbf{Z}^k)$ coincides with the set of all k-linear recurring bisequences over P.

14.41. Proposition. *The Hopf algebra $R(\mathbf{Z}^k)$ of representative functions on the group $(\mathbf{Z}^k, +)$ is isomorphic to the Hopf algebra $\mathcal{R}P^{\langle k \rangle}$ of all reversible k-LRS* (see Proposition 14.15).

□ The isomorphism $R(\mathbf{Z}^k) \to \mathcal{R}P^{\langle k \rangle}$ is given by $\nu \to \nu|\mathbf{N}_0^k$. □

Chapter 3.

LINEAR RECURRING SEQUENCES OVER ARTINIAN AND FINITE RINGS

In this chapter, except for Section 15.A and Section 19.D, we study the properties of 1-recurrences and of polynomials of one variable.

15. Reduction to Local Rings and Primary Annihilators

A. Componentwise properties of ideals and modules. Recall that a (commutative) ring R is called *local* if it has a unique maximal ideal, which we denote in this case by $\mathfrak{N}(R)$. An Artinian ring R is local iff the set of all of its zero divisors is a subgroup of the additive group $(R,+)$. This subgroup for a local Artinian ring coincides with $\mathfrak{N}(R)$, and $\mathfrak{N}(R)^n = 0$ for some $n \in \mathbf{N}$. The least n with such property is called the index of nilpotency of the ideal $\mathfrak{N}(R)$ and is denoted by ind $\mathfrak{N}(R)$. The maximal ideal $\mathfrak{N}(R)$ of a local Artinian ring is equal to the Jacobson radical or to the nilradical of this ring [2]. We call it the *radical* of the ring R.

An arbitrary Artinian ring R can be uniquely (up to a permutation of summands) represented as a direct sum

$$R = R^{(1)} \dotplus \ldots \dotplus R^{(t)}, \tag{15.1}$$

where $R^{(s)}$ is a local Artinian ring with unit e_s, $s \in \overline{1,t}$. Moreover, $R^{(s)} = Re_s$, $e = e_1 + \ldots + e_t$, and the ring $\mathcal{P}_k = R[\mathrm{x}]$, any R-module M, and any ideal $I \lhd \mathcal{P}_k$ satisfy the following equalities:

$$\mathcal{P}_k = \mathcal{P}_k^{(1)} \dotplus \ldots \dotplus \mathcal{P}_k^{(t)}, \qquad \mathcal{P}_k^{(s)} = e_s\mathcal{P}_k = R^{(s)}[x_1, \ldots, x_k]; \tag{15.2}$$

$$M = M^{(1)} \dotplus \ldots \dotplus M^{(t)}, \qquad M^{(s)} = e_sM \text{ is an } R^{(s)}\text{-module}; \tag{15.3}$$

$$I = I^{(1)} \dotplus \ldots \dotplus I^{(t)}, \qquad I^{(s)} = e_sI \lhd \mathcal{P}_k^{(s)}. \tag{15.4}$$

We say that some property of the ideal I (of the module M) is *componentwise* if it is fulfilled for each component of the decomposition (15.4) (respectively (15.3)).

15.1. Proposition. *Under the above conditions for the ideal $I \lhd \mathcal{P}_k$, the following properties are componentwise: being a monic ideal; periodicity; reversibility; being a principal ideal. If I is a monic ideal, then*

$$L_M(I) = L_{M^{(1)}}(I^{(1)}) \dotplus \ldots \dotplus L_{M^{(t)}}(I^{(t)}), \tag{15.5}$$

where $L_{M^{(s)}}(I^{(s)}) = e_sL_M(I)$, $s \in \overline{1,t}$. If I is a periodic ideal, then its group of periods satisfies the equality

$$\mathfrak{P}(I) = \mathfrak{P}(I^{(1)}) \cap \ldots \cap \mathfrak{P}(I^{(t)}), \tag{15.6}$$

Its orbital semigroup $\mathcal{O}(I)$ and its cyclic group $\mathcal{T}(I)$ are subdirect products of semigroups $\mathcal{O}(I^{(s)}) = e_s\mathcal{O}(I)$ and of groups $\mathcal{T}(I^{(s)}) = e_s\mathcal{T}(I)$ respectively. The family $L_M(I)$ is finite and reversible iff all of its components in (15.5) *have the same properties, and in this case the cyclic types satisfy*

$$Z_I^M = Z_{I^{(1)}}^{M^{(1)}} * \ldots * Z_{I^{(t)}}^{M^{(t)}}. \square$$

15.2. Corollary. *Under the conditions* (15.1), (15.4) *if* $k = 1$ *and* $I \lhd \mathcal{P}$ *is a periodic ideal, then*

$$D(I) = \max\{D(I^{(1)}), \ldots, D(I^{(t)})\}, \qquad T(I) = [T(I^{(1)}), \ldots, T(I^{(t)})].\square$$

B. Primary decompositions of polynomial ideals over local Artinian rings. Let R be an Artinian ring and $\mathfrak{N} = \mathfrak{N}(R)$ be its radical. Then $\overline{R} = R/\mathfrak{N}$ is a field, and the canonical epimorphism $R \to \overline{R}$ has a natural extension up to the epimorphism $\mathcal{P} = R[x] \to \overline{\mathcal{P}} = \overline{R}[x]$, which maps the polynomial $F(x) = \sum f_i x^i$ into the polynomial $\overline{F}(x) = \sum \overline{f}_i x^i$. The kernel of the last epimorphism is the nilpotent ideal $\mathfrak{N}[x]$. It follows that the multiplicative group of the ring $\mathcal{P}$ has the form $\mathcal{P}^* = R^* + x\mathfrak{N}[x]$.

15.3. Theorem (W. Krull). *Any polynomial* $H(x) \in \mathcal{P}$ *such that* $\overline{H}(x) \neq \overline{0}$ *can be uniquely represented as a product* $H(x) = U(x)F(x)$ *where* $U(x) \in \mathcal{P}^*$ *and* $F(x)$ *is a monic polynomial.*

□ W. Krull, "Algebraische theorie der ringe. II," *Math. Ann.*, **91**, 1–46 (1923). □

15.4. Proposition. *Polynomials* $F(x)$, $G(x) \in \mathcal{P}$ *are comaximal iff* $(\overline{F}, \overline{G}) = \overline{e}$. □

The reduction to the polynomial ring $\overline{\mathcal{P}}$ over the field $\overline{R}$ is one of the main methods of studying the properties of polynomials and ideals of $\mathcal{P}$ and of linear recurrences over the ring R.

15.5. Theorem (Hensel lemma, [13, 135]). *Let* $F(x)$, $G_0(x)$, $H_0(x) \in \mathcal{P}$ *be monic polynomials such that* $\overline{F}(x) = \overline{G}_0(x)\overline{H}_0(x)$, $(\overline{G}_0(x), \overline{H}_0(x)) = \overline{e}$. *Then there exists a unique pair of monic polynomials* $G(x)$, $H(x) \in \mathcal{P}$ *such that* $F(x) = G(x)H(x)$, $\overline{G}(x) = \overline{G}_0(x)$, $\overline{H}(x) = \overline{H}_0(x)$. □

15.6. Definition. We call a polynomial $F(x) \in \mathcal{P}$ *primary* if $\overline{F}(x) = g(x)^k$, where $g(x) \in \overline{\mathcal{P}}$ is an irreducible polynomial.

15.7. Corollary. *Any monic polynomial* $F(x) \in \mathcal{P}$ *can be represented as the product*

$$F(x) = F_1(x) \ldots F_l(x) \tag{15.7}$$

of monic pairwise comaximal primary polynomials. Such a representation is unique up to permutation of factors. □

15.8. Definition. We call the decomposition (15.7) the *canonical decomposition* of the polynomial $F(x)$ over the ring R.

15.9. Proposition. *Let* $I \lhd \mathcal{P}$ *be a monic ideal and* $F(x)$ *be a monic polynomial of least degree from the ideal* I. *Then*

$$I = \mathcal{P}F(x) + \mathfrak{N}(I), \text{ where } \mathfrak{N}(I) = I \cap \mathfrak{N}[x]. \tag{15.8}$$

The ideal I *is primary (principal) iff* $F(x)$ *is a primary polynomial (iff* $I = \mathcal{P}F(x)$*).* □

15.10. Definition. A monic polynomial $F(x)$ from (15.8) will be called the *main generator of the monic ideal* I.

15.11. Proposition. *Any monic ideal* $I \lhd \mathcal{P}$ *can be represented as the intersection of primary pairwise comaximal ideals. Such a representation is unique up to permutation of components. If the main generator* $F(x)$ *of* I *has the canonical decomposition* (15.7), *then this representation has the form*

$$I = I^{(1)} \cap \ldots \cap I^{(l)}, \qquad I^{(s)} = \mathcal{P}F_s(x) + \mathfrak{N}(I), \qquad s \in \overline{1,l}. \tag{15.9}$$

15.12. Definition. Under the conditions of Proposition 15.11, we call the decomposition (15.9) the *canonical primary decomposition* of the ideal I.

As in 15.2, we may state that the consideration of periodic properties of a monic ideal I is reduced to the study of periodic properties of its primary components $I^{(s)}$ from (15.9), and if $L_M(I)$ is a finite reversible LRS-family, then

$$Z_I^M = Z_{I^{(1)}}^M * \ldots * Z_{I^{(l)}}^M.$$

16. Canonical Systems of Generators of Monic Ideals and 1-LRS-Families over Local Principal Ideal Rings

A. Canonical generating system of an ideal. Let R be a local Artinian principal ideal ring. Then the lattice of its ideals is a chain of length $n = \operatorname{ind}\mathfrak{N}(R)$:

$$R \supset \mathfrak{N}(R) \supset \ldots \supset \mathfrak{N}(R)^{n-1} \supset \mathfrak{N}(R)^n = 0,$$

and for any $\pi \in \mathfrak{N}(R)\backslash\mathfrak{N}(R)^2$ we have $\mathfrak{N}(R)^s = \pi^s\mathfrak{N}(R)$, $s \in \overline{0,n}$ [2].

16.1. Definition. The *norms* of an element $r \in R$, a polynomial $G = G(x) = g_0 + g_1x + \ldots + g_mx^m \in \mathcal{P}$, and a subset $S \subseteq \mathcal{P}$ are defined by

$$\|r\| = \max\{i \in \overline{0,n} \mid r \in \pi^iR\}, \qquad \|G\| = \min\{\|g_j\| : j \in \overline{0,m}\},$$

$$\|S\| = \min\{\|G\| : G \in S\}.$$

We say that a polynomial $G(x)$ is *correct* if $\|g_m\| = \|G\|$.

16.2. Lemma. *A correct polynomial $G = G(x) = \sum_{i=0}^m g_ix^i$ divides a polynomial $F = F(x) = \sum f_jx^j$ with a remainder iff $\|f_j\| \geq \|g_m\|$ for all $j \geq m$. Moreover, the remainder* $\operatorname{Res}(F/G)$ *is uniquely defined.* □

From the Krull theorem (see 15.3) we have

16.3. Lemma. *A polynomial $F(x) \in \mathcal{P}\backslash 0$ can be represented as a product of an invertible (in the ring $\mathcal{P}$) polynomial and a correct polynomial $G(x)$. The latter is defined uniquely up to a factor from R^* and satisfies the relations $\|G\| = \|F\|$, $\deg G \leq \deg F$.* □

16.4. Definition. We say that $G(x)$ *divides* $F(x)$ *modulo* π^d, if $F = QG + \pi^dH$ for some Q, $H \in \mathcal{P}$.

The initial version of the following theorem (for ideals of $\mathbb{Z}[x]$) belongs essentially to Kronecker [122].

16.5. Theorem. *Let $I \lhd \mathcal{P}$ be a nonzero ideal and $\|I\| = a_0$. Then I contains a system of $t+1 < n - a_0$ correct polynomials*

$$G_0(x), \ldots, G_t(x), \qquad \|G_s\| = a_s, \qquad \deg G_s = m_s, \qquad s \in \overline{0,t} \tag{16.1}$$

with the following properties:

(C1) $\|I\| = a_0 < a_1 < \ldots < a_t < n = a_{t+1}$;

(C2) $m_0 > m_1 > \ldots > m_t \geq 0$;

(C3) *if $F \in I$ and $\deg F(x) < m_s$, $s \geq 0$, then $F(x) = 0$ for $s = t$ and $\|F(x)\| \geq a_{s+1}$ for $s < t$.*

Any such system of polynomials also has the following properties:

(C4) *if $F \in I$ and $\|F\| > a_s$, then*

$$G_s(x) | F(x) \bmod \pi^{a_{s+1}} \text{ and } F \in (G_s, \ldots, G_t);$$

(C5) $I = (G_0, G_1, \ldots, G_t)$;

(C6) *if $a_s \leq a < a_{s+1}$, then $I \cap \pi^a\mathcal{P} = (\pi^{a-a_s}G_s, G_{s+1}, \ldots, G_t)$,*

$$(I : \pi^a) = (F_s(x), \pi^{a_{s+1}-a}F_{s+1}(x), \ldots, \pi^{a_t-a}F_t(x), \pi^{n-a}),$$

where $F_0, \ldots, F_t$ are polynomials with invertible leading coefficients such that

$$G_s(x) = \pi^{a_s}F_s(x), \qquad s \in \overline{0,t}; \tag{16.2}$$

(C7) *under the conditions* (16.2), *any polynomial $H(x) \in \mathcal{P}$ is uniquely represented in the form*

$$H(x) = H(x)F_0(x) + \ldots + H_t(x)F_t(x) + H_{t+1}(x),$$

where $\deg H_sF_s < m_{s-1}$ for $s \in \overline{1,t}$, $\deg H_{t+1} < m_t$, and $H \in I$ if and only if $\|H_s\| \geq a_s$ for $s \in \overline{0,t+1}$.

□ The polynomial $G_0(x)$ is the polynomial of the least degree m_0 from I with norm $a_0 = \|I\|$. If $I = (G_0(x))$, then the proof is completed. Otherwise, the ideal I_1 generated by the set $\operatorname{Res}(I/G_0)$ has the

norm $a_1 > a_0$ ($a_1 < n$). Choose a polynomial $G_1(x) \in I_1$ with norm a_1 of the least degree m_1. It is clear that $m_1 < m_0$. If $I_1 = (G_1)$, then $I = (G_0, G_1)$ and the proof is complete. Otherwise, we consider the ideal $I_2 = (\mathrm{Res}\,(I_1/G_1))$, etc.. For a more detailed proof, see in [46]. □

16.6. Definition. The system (16.1) of generators of the ideal I with properties (C1)–(C3) will be called a *canonical generating system* (CGS) of the ideal I.

Note that a CGS is an analogue of a standard base (Groebner base) of polynomial rings over a field [10, 36].

16.7. Corollary. *A monic ideal I of the ring $\mathcal{P}$ has a CGS of the form*

$$F_0(x), \pi^{a_1}F_1(x), \ldots, \pi^{a_t}F_t(x), \tag{16.3}$$

where $F_s(x)$ is a monic polynomial of degree m_s, $s \in \overline{1,t}$, $m_0 > m_1 > \ldots > m_t \geq 0$, $0 < a_1 < \ldots < a_t < n$, and

$$\pi^{a_{s+1}}F_s(x) \in (\pi^{a_{s+1}}F_{s+1}, \ldots, \pi^{a_t}F_t) \text{ for } s \in \overline{0,t-1}. \tag{16.4}$$

Moreover, if $\overline{R} = R/\mathfrak{N}(R) = GF(q)$ then $S = \mathcal{P}/I$ is a finite ring and

$$|S| = q^r, \text{ where } r = (m_0 - m_1)a_1 + \ldots + (m_{t-1} - m_t)a_t + m_t. \tag{16.5}$$

□ The proof of the last equality is reduced to the calculation of $[\mathcal{P} : I]$ with the help of the property (C7):

$$[\mathcal{P} : I] = \prod_{s=1}^{t} [R^{m_{s-1}-m_s} : \pi^{a_s}R^{m_{s-1}-m_s}] \cdot |R|^{m_t}. \quad \square$$

If we have some CGS of a monic ideal I, we can construct the primary decomposition of I and the CGS of each of the primary components of I.

16.8. Proposition. *An ideal $I \lhd \mathcal{P}$ with the CGS (6.3) is primary iff $F_0(x)$ is a primary polynomial. If the polynomial $\overline{F}_0(x) \in \overline{\mathcal{P}}$ is a product of two coprime polynomials over the field $\overline{R}$,*

$$\overline{F}_0(x) = k(x)h(x), \qquad (k(x), h(x)) = \overline{e}, \tag{16.6}$$

then for each $s \in \overline{0,t}$ the polynomial $F_s(x)$ from (16.3) can be uniquely represented as the product

$$F_s(x) = K_s(x)H_s(x) \tag{16.7}$$

of monic polynomials $K_s(x)$, $H_s(x) \in \mathcal{P}$ such that

$$\overline{K}_s(x) | k(x), \qquad \overline{H}_s(x) | h(x). \tag{16.8}$$

Moreover,

$$I = \mathcal{K} \cap \mathcal{H}, \tag{16.9}$$

where

$$\mathcal{K} = (K_0, \pi^{a_1}K_1, \ldots, \pi^{a_t}K_t), \qquad \mathcal{H} = (H_0, \pi^{a_1}H_1, \ldots, \pi^{a_t}H_t). \tag{16.10}$$

The canonical generating system of the ideal $\mathcal{K}$ can be obtained from the generating system $K_0(x)$, $\pi^{a_1}K_1(x), \ldots, \pi^{a_t}K_t(x)$ by deletion of all polynomials $\pi^{a_s}K_s$ such that $s \geq 1$, $\deg K_s = \deg K_{s-1}$.

□ Since $\overline{F}_s | \overline{F}_0$, we have from (16.6) that $\overline{F}_s(x) = (\overline{F}_s(x), k(x)) \cdot (\overline{F}_s(x), h(x))$. Using the Hensel lemma (see 15.5), we obtain (16.7) and (16.8). Proposition 15.11 implies the equality (16.9), where $\mathcal{K} = \mathcal{P}K_0(x) + \mathfrak{N}(I) = (K_0, \pi^{a_1}F_1, \ldots, \pi^{a_t}F_t)$, $\mathcal{H} = \mathcal{P}H_0(x) + \mathfrak{N}(I) = (H_0, \pi^{a_1}F_1, \ldots, \pi^{a_t}F_t)$. Furthermore, since $(K_0(x), H_s(x)) = (e)$, we have $\pi^{a_s}K_s \in \mathcal{K}$, because for suitable polynomials U, $V \in \mathcal{P}$ we have $\pi^{a_s}K_s = \pi^{a_s}K_sUK_0 + \pi^{a_s}K_sVH_s = (\pi^{a_s}K_sU)K_0 + V\pi^{a_s}F_s$. To prove the last statement it is sufficient to note that

$$\pi^{a_s}K_{s-1} \in (\pi^{a_s}K_s, \ldots, \pi^{a_t}K_t) \text{ for } s \in \overline{1,t} \text{ (see [46])}. \quad \square$$

16.9. Corollary. *Let an ideal $I \lhd \mathcal{P}$ have the CGS* (16.3)*, and let the canonical decomposition of the polynomial $F_0(x)$ have the form $F_0(x) = F_0^{(1)}(x) \dots F_0^{(k)}(x)$. Then each of the polynomials $F_s(x)$ can be represented as the product $F_s(x) = F_s^{(1)}(x) \dots F_s^{(k)}(x)$, where $F_s^{(i)}(x) | F_0^{(i)}(x)$ for $i \in \overline{1,k}$, and I is the intersection of the following primary pairwise comaximal ideals: $I = I^{(1)} \cap \dots \cap I^{(k)}$, where $I^{(j)} = (F_0^{(j)}, \pi^{a_1} F_1^{(j)}, \dots, \pi^{a_t} F_t^{(j)})$, $j \in \overline{1,k}$.* □

B. Generating systems of LRS-families. Here we fix a monic ideal $I \lhd \mathcal{P}$ with CGS (16.3). By Proposition 2.5, the elementary method of describing the family $L_R(I)$ is connected with the solution of the system of linear equations

$$(x_0, \dots, x_{m-1})(\pi^{a_1} F_1(S(F_0)), \dots, \pi^{a_t} F_t(S(F_0))) = 0. \tag{16.11}$$

Methods of solution of such systems over a principal ideal ring are wellknown (see Section 18 below). Thus, we can obtain a generating system of the family $L_R(I)$ over the ring R.

Now we give a description of some "more economical" systems of generators of the family $L_R(I)$ over the ring $\mathcal{P}$. In view of condition (16.4), we state that for any $i \in \overline{0,t-1}$, $j \in \overline{i+1,t}$,

$$F_i(x) = Q_{i,i+1}(x)F_{i+1}(x) - \pi^{a_{i+2}-a_{i+1}} Q_{i,i+2}(x)F_{i+2}(x) - \dots - \pi^{a_j - a_{i+1}} Q_{ij}(x)F_j(x) - \pi^{a_{j+1}-a_{i+1}} B_{ij}(x),$$

where $\deg Q_{is}(x)F_s(x) < m_{s-1}$, $\deg B_{ij}(x) < m_j$. Then

$$\overline{Q}_{i,i+1}(x) = \overline{F}_i(x)/\overline{F}_{i+1}(x),$$

$$\pi^{a_{j+1}-a_{i+1}} B_{ij}(x) = \operatorname{Res}(F_i/F_{i+1}, \dots, F_j), \tag{16.12}$$

$$\overline{B}_{i,i+1}(x) = \overline{Q}_{i,i+2}(x)\overline{F}_{i+2}(x) \text{ for } i \in \overline{0,t-2}.$$

16.10. Theorem [46]. *The family $L_R(I)$ is the set of all sequences $w \in R^{(1)}$ of the form*

$$w = u_t + \pi^{n-a_t} u_{t-1} + \dots + \pi^{n-a_1} u_0, \tag{16.13}$$

such that $u_0, \dots, u_t$ are sequences with the properties

$$F_t u_t = 0, \qquad F_i u_i = B_{i,i+1}u_{i+1} + \dots + B_{it}u_t, \qquad i \in \overline{0,t-1}. \tag{16.14}$$

Here

$$\overline{F}_s(x)\overline{F}_{s+1}(x)\overline{u}_s = 0 \text{ for } s \in \overline{0,t-1}. \tag{16.15}$$

The family $L_R(I)$ contains a system of recurrences

$$\alpha_t, \pi^{n-a_t}\alpha_{t-1}, \dots, \pi^{n-a_1}\alpha_0 \tag{16.16}$$

such that $\operatorname{An}(\overline{\alpha}_s) = (\overline{F}_s)$, $s \in \overline{0,t}$, and every such system generates $L_R(I)$ over $\mathcal{P}$.

If the family $L_R(I)$ contains a sequence w of the form (16.14) *such that*

$$\operatorname{An}(\overline{u}_t) = (\overline{F}_t), \qquad \operatorname{An}(\overline{u}_s) = (\overline{F}_s\overline{F}_{s+1}), \qquad s \in \overline{0,t-1}, \tag{16.17}$$

then $L_R(I) = \mathcal{P}w$ is a cyclic $\mathcal{P}$-module. □

16.11. Theorem [46]. *Let I be a primary ideal. Then $L_R(I)$ is a cyclic $\mathcal{P}$-module iff polynomials* (16.12) *satisfy the conditions*

$$(\overline{B}_{t-1,t}(x), \overline{F}_0(x)) = \overline{e}, \qquad (\overline{Q}_{i,i+2}(x), \overline{F}_0(x)) = \overline{e}, \qquad i \in \overline{0,t-2}. \tag{16.18}$$

16.12. Corollary. *Let I be a primary ideal. Then the ring $\mathcal{P}/I$ is quasi-Frobenius iff condition* (16.18) *holds.*

□ Since R is a quasi-Frobenius ring, this result follows from Theorems 4.7 and 16.11. □

It is interesting to extend Theorem 16.11 on arbitrary monic ideals and to obtain analogues of Theorems 16.5, 16.10 and 16.11 for an arbitrary local QF-ring.

17. Periods of Monic Polynomials and Ideals over Local Finite Rings

Here R is a finite (commutative) local ring, $\overline{R} = R/\mathfrak{N}(R) = GF(q)$, $p = \operatorname{char}\overline{R}$, $q = p^r$, $n = \operatorname{ind}\mathfrak{N}(R)$. We keep the notations of Sections 6 and 15.

A. General estimations of periods and defects [52, 53, 79, 80, 103, 104, 113, 118, 129, 167, 168]. All monic polynomials $F(x) \in \mathcal{P}$ and ideals I of the ring $\mathcal{P}$ are periodic. Moreover, in contrast to the general case (Remark 6.12), we have

17.1. Proposition. *A monic polynomial $F(x) \in \mathcal{P}$ can be uniquely represented as the product*

$$F(x) = F_{\deg}(x)F_{\mathrm{rev}}(x) \tag{17.1}$$

of some degenerating and reversible polynomials. If I is a monic ideal with the main generator $F(x)$, then its degenerating and reversible components (see 6.11) *are*

$$I_{\deg} = \mathcal{P}F_{\deg} + \mathfrak{N}(I), \qquad I_{\mathrm{rev}} = \mathcal{P}F_{\mathrm{rev}} + \mathfrak{N}(I).$$

□ The decomposition (17.1) is obtained from

$$\overline{F}(x) = x^k f_1(x), \text{ where } f_1(0) \in \overline{R}^*, \tag{17.2}$$

with the help of the Hensel lemma (see 15.5). □

17.2. Proposition. *The period and defect of a monic ideal I with the main generator $F(x)$ satisfy the relations*

$$D(\overline{F}) \le D(I) \le D(F) \le nD(\overline{F}) \le n \cdot \deg F(x), \tag{17.3}$$

$$T(\overline{F})|T(I), \qquad T(I)|T(F). \tag{17.4}$$

□ By 17.1 and 6.8, it is sufficient to prove (17.3) for a degenerating ideal and to prove (17.4) for a reversible ideal. The first two inequalities in (17.3) follow from the implications

$$x^\lambda \in I \Rightarrow \overline{F}(x)|\overline{x}^\lambda; \qquad F(x)|x^\lambda \Rightarrow x^\lambda \in I.$$

If $\overline{F}(x)|\overline{x}^\lambda$, then $x^\lambda \equiv \alpha(x) \pmod{F(x)}$, where $\alpha(x) \in \mathfrak{N}(R)[x]$. Therefore, $\alpha(x)^n = 0$, $F(x)|x^{n\lambda}$, and the third inequality in (17.3) is proved. Finally, (17.4) follows from the implications

$$x^t - e \in I \Rightarrow \overline{F}(x)|x^t - \overline{e}; \qquad F(x)|x^t - e \Rightarrow x^t - \overline{e} \in I. \quad \square$$

Further estimation of the parameter $T(I)$ is connected with the following characterization of the ring R. Let $\nu =]\log_P n[$ be the minimal integer which is greater than or equal to $\log_P n$, $\operatorname{char}(\mathfrak{N}(R)^{p^s}) = p^{d_s}$ for $s \in \overline{0,\nu}$, and

$$\omega(R) = \max\{s + d_s |\ s \in \overline{0,\nu}\}. \tag{17.5}$$

17.3. Proposition. *The period of a reversible ideal I with main generator $F(x)$ is given by*

$$T(I) = T(\overline{F})p^{\alpha(I)}, \tag{17.6}$$

where

$$\alpha(I) \le \omega(R) \le d_0 + \nu - 1. \tag{17.7}$$

□ Let $S = \mathcal{P}/I = R[\theta]$, $\theta = x + I$. By Propositions 6.17(b) and 6.4, $\theta \in S^*$ and $T(I) = \operatorname{ord}\theta$. Let $T(\overline{F}) = t$. Then, by (17.4), $t|\operatorname{ord}\theta$ and $\theta^t = e + a$, where $a \in \mathfrak{N}(R)S$. For $l \in \mathbb{N}_0$ denote

$$J_l = \mathfrak{N}(R)^{p^l} + p\mathfrak{N}(R)^{p^{l-1}} + \ldots + p^l\mathfrak{N}(R).$$

Induction on l gives (see [48])

$$(e + a)^{p^l} = e + a_l, \text{ where } a_l \in J_l S.$$

Since $J_l = 0$ for $l \geq \omega(R)$, we have $(e+a)^{p^{\omega(R)}} = e$. Hence $\operatorname{ord}\theta | tp^{\omega(R)}$, i.e., $T(I) | T(\overline{F})p^{\omega(R)}$. This implies (17.6) and (17.7). □

We can give the exact value of the parameter $\omega(R)$ if R satisfies the following additional condition.

17.4. Definition. We say that a local ring R is *balanced* if $pR = \mathfrak{N}(R)^{\varepsilon}$ for some $\varepsilon \in \mathbf{N}$. The minimal ε with this property is called the *ramification index* of the ring R. Notation: $\varepsilon = \varepsilon(R)$.

The class of balanced rings is rather large. It includes all finite local rings of characteristic p (for such rings $\varepsilon(R) = n$) and local principal ideal rings [42, 132].

17.5. Proposition [48]. *If R is a balanced ring with ramification index ε, then*

$$w(R) = \left]\frac{n-p^b}{\varepsilon}\right[+ b, \text{ where } b = \left]\log_p \frac{\varepsilon}{p-1}\right[. \square$$

It follows from (17.6) that the evaluation of the period of the reversible ideal I can be reduced to the evaluation of the period $T(\overline{F})$ of the polynomial $\overline{F}(x)$ over the ring $\overline{R}$ and to the evaluation of the parameter $\alpha(I)$ as the minimal $\alpha \in \mathbf{N}$ with the property

$$\operatorname{Res}\left(x^{T(\overline{F})p^{\alpha}} - e/F(x)\right) \in I.$$

Below we propose a more suitable method for evaluation of $\alpha(I)$.

B. Distinguished polynomials [21, 48].

17.6. Definition. We call a reversible polynomial $D(x) \in \mathcal{P}$ *distinguished* if $T(D) = T(\overline{D})$. We say that $D(x)$ is a distinguished polynomial corresponding to the polynomial $G(x) \in \mathcal{P}$ (or to the polynomial $g(x) \in \overline{\mathcal{P}}$) if $\overline{D}(x) = \overline{G}(x)$ (respectively $\overline{D}(x) = g(x)$). A polynomial $G(x) \in \mathcal{P}$ is called *separable* if $(G(x), G(x)') = (e)$ (i.e., $(\overline{G}(x), \overline{G}(x)') = (\overline{e})$; here the bar denotes the derivative).

17.7. Proposition. *For any reversible separable polynomial $G(x) \in \mathcal{P}$, there exists a unique distinguished polynomial $G_*(x) \in \mathcal{P}$ corresponding to $G(x)$. The product of coprime distinguished polynomials is a distinguished polynomial.*

□ Let $T(\overline{G}) = \tau$. Then $(\tau, p) = 1$ and $K(x) = x^{\tau} - e$ is a separable polynomial. Since $\overline{G}(x) | \overline{K}(x)$, according to the Hensel lemma there exists a unique monic polynomial $G_*(x) \in \mathcal{P}$ such that $G_* | K$ and $\overline{G}_* = \overline{G}$. □

The Hensel lemma gives us an algorithm of constructing of a distinguished polynomial corresponding to a given separable polynomial, but this algorithm is rather complicated, since the degree of polynomial $x^{\tau} - e$ is large. We propose a simpler algorithm.

There exists an extension $R[\xi]$ of the ring R such that

$$x^p - e = (x-e)(x-\xi)\dots(x-\xi^{p-1}). \tag{17.8}$$

For example, if $p = 2$, then $\xi = -1$ and $R[\xi] = R$. Note that $R[\xi]$ is a local ring, since $x^p - \overline{e} = (x-\overline{e})^p$ is a primary polynomial.

17.8. Lemma. *For any separable reversible polynomial $G(x) \in \mathcal{P}$ of the degree m, we have*

$$(-1)^{m(p-1)} \cdot \prod_{i=0}^{p-1} G(\xi^i x) = G^{[1]}(x^p), \tag{17.9}$$

where $G^{[1]}(x)$ is a monic polynomial from $\mathcal{P}$ with the property

$$\overline{G}^{[1]}(x^p) = \overline{G}(x)^p.$$

□ There exists a Galois extension S [132] of the ring R such that $G(x) = \prod_{i=1}^{m}(x-\alpha_i)$, where $\alpha_1, \dots, \alpha_m \in S$. Then $\prod_{j=0}^{p-1}(\xi^j x - \alpha_i) = (-1)^{p-1}(x^p - \alpha_i^p)$, and the left part of the equality (17.9) is equal to $(x^p - \alpha_1^p)\dots(x^p -$

α_m^p). The last polynomial has the required form and belongs to $R[x]$, since the set of its roots is invariant under any automorphism of the ring S over R. □

17.9. Proposition. *Let $G(x)$ be a separable reversible polynomial of degree m and let the polynomials $G^{[0]}(x), G^{[1]}(x), \ldots \in \mathcal{P}$ be defined by*

$$G^{[0]}(x) = G(x),$$

$$G^{[k+1]}(x) = (-1)^{m(p-1)} \prod_{i=0}^{p-1} G^{[k]}(\xi^i x), \qquad k \in \mathbf{N}_0. \tag{17.10}$$

Let $\overline{R} = GF(q)$, $q = p^r$, $\varkappa =]\omega(R)/r[$. Then

$$G_*(x) = G^{[\varkappa r]}(x), \tag{17.11}$$

and $G(x)$ is a distinguished polynomial iff

$$G^{[r]}(x) = G(x). \tag{17.12}$$

□ In the notations from the proof of Lemma 17.8, we have

$$G^{[\varkappa r]}(x) = (x - \alpha_1^{q^k}) \ldots (x - \alpha_m^{q^k}).$$

Moreover, $\overline{\alpha}_i^{q^k} = \overline{\alpha}_i$ and $\operatorname{ord} \alpha_i^{q^k} = \operatorname{ord} \overline{\alpha}_i$. Hence, $\overline{G}^{[\varkappa r]} = \overline{G}$ and $T(\overline{G}^{[\varkappa r]}) = T(\overline{G})$, i.e., (17.11) is true. The polynomial $G(x)$ is distinguished iff $\alpha_i^q = \alpha_i$, $i \in \overline{1,m}$. The last condition is equivalent to (17.12), since $G^{[r]}(x) = (x - \alpha_1^q) \ldots (x - \alpha_m^q)$. □

In the important special case where $p = 2$ and $q = 2^r$, formulas (17.10) can be substantially simplified. The polynomials $G^{[k]}(x)$ can be represented in the form $G^{[k]}(x) = G_{(0)}^{[k]}(x^2) + xG_{(1)}^{[k]}(x^2)$ and calculated in the following way.

17.10. Lemma. *If $p = 2$, $q = 2^r$, then under the conditions* 17.9

$$G^{[k+1]}(x^2) = (-1)^m G^{[k]}(x) G^{[k]}(-x),$$

$$G^{[k+1]}(x) = (-1)^m (G_{(0)}^{[k]}(x)^2 - xG_{(1)}^{[k]}(x)^2).$$

Moreover,

$$(-1)^m G^{[k]}(-x) = G^{[k]}(x) + 2\Delta_G^{[k]}(x),$$

where

$$\overline{\Delta}_G^{[k]}(x) \equiv \overline{G}_{(0)}^{[k]}(x^2) \equiv x\overline{G}_{(1)}^{[k]}(x^2) \equiv x\overline{G}^{[k]}(x)' \pmod{\overline{G}^{[k]}(x)}.\square$$

C. Calculation of periods of reversible ideals with the help of distinguished polynomials.

17.11. Definition. The *radical* of the reversible polynomial $F(x) \in \mathcal{P}$ is the distinguished polynomial $\operatorname{rad} F(x)$ corresponding to the product of all monic factors, irreducible over $\overline{R}$, of the polynomial $\overline{F}(x) \in \overline{\mathcal{P}}$.

This definition is concordant with the definition of the radical of an ideal. Namely, if I is an ideal of $\mathcal{P}$ with main generator $F(x)$, then its radical $\operatorname{rad} I$ is an ideal with main generator $\operatorname{rad} F(x)$.

Note that $\operatorname{rad} F(x)$ is a separable polynomial. To construct it, it is sufficient to know only the polynomial $\operatorname{rad} \overline{F}(x)$. The last polynomial can be calculated with the help of the operations of differentiation, evaluation of g.c.d., and arithmetical operations over polynomials, but without the decomposition of $\overline{F}(x)$ into irreductible factors over the field $\overline{R}$.

17.12. Theorem. *Let I be a reversible ideal with main generator $F(x)$, $G(x) = \operatorname{rad} F(x)$, k be the maximum of multiplicities of the irreductible factors of $\overline{F}(x)$ over $\overline{R}$, and $p^{a-1} < k \leq p^a$. Then*

$$T(I) = T(\overline{G})p^{a+\alpha(I)} = T(\overline{G})p^{\beta(I)}, \tag{17.13}$$

where $\beta(I)$ is the minimal $b \in \mathbb{N}_0$ such that

$$G^{[b]}(x^{p^b}) \in I. \tag{17.14}$$

□ Let $\tau = T(\overline{G})$. Then $T(\overline{F}) = \tau p^a$ (see Theorem 11.1), and (17.13) follows from (17.6). The parameter $\beta(I)$ is the least $b \in \mathbb{N}_0$ such that $x^{\tau p^b} - e \in I$. The last condition is equivalent to (17.14), since

$$x^{\tau p^b} - e = G^{[b]}(x^{p^b})H(x^{p^b}),$$

where $\overline{G}^{[b]}(x^{p^b}) = \overline{G}(x)^{p^b}$, and hence $(H(x^{p^b})) + I = \mathcal{P}$. □

This algorithm of calculation of the parameter $\alpha(I)$ in (17.6) has the simplest form in the case where R is a *Galois ring*, i.e., it is a local principal ideal ring with $\mathfrak{N}(R) = pR$. Such a ring is uniquely defined (up to isomorphism) by its cardinality and characteristic. In the above notations, these parameters have the form $|R| = q^n$, $\operatorname{char} R = p^n$ [42, 132]. We denote such a ring by $R = GR(q^n, p^n) = GR(p^{rn}, p^n)$ (another notation $GR(r, p^n)$ [132]). In particular, $GF(q) = GR(q, p)$, $\mathbf{Z}_{p^n} = GR(p^n, p^n)$.

If $R = GR(q^n, p^n)$, then by Corollary 16.7 a reversible ideal $I \lhd \mathcal{P}$ has a CGS of the form

$$F(x) = F_0(x), p^{a_1}F_1(x), \ldots, p^{a_t}F_t(x). \tag{17.15}$$

Let $G(x) = \operatorname{rad} F_0(x)$ and let parameters τ, k, a be the same as in Theorem 17.11. For any $b \in \mathbb{N}_0$, we denote

$$U_b(x) = \operatorname{Res}(G^{[b]}(x^{p^b})/F(x)) \tag{17.16}$$

and suppose that the decomposition of $U_b(x)$ in the system of radices $F_1(x), \ldots, F_t(x)$ has the form

$$U_b(x) = U_{b1}(x)F_1(x) + \ldots + U_{bt}(x)F_t(x) + U_{b,t+1}(x), \tag{17.17}$$

$\deg U_{bi}(x)F_i(x) < \deg F_{i-1}(x)$, $i \in \overline{1, t+1}$. Let

$$n_{bi} = \|U_{bi}(x)\|, \qquad i \in \overline{1, t+1}; \qquad n_b = \min\{n_{b1}, \ldots, n_{b,t+1}\};$$

$$d_b(I) = \max\{a_1 - n_{b1}, \ldots, a_t - n_{b,t}, n - n_{b,t+1}\}. \tag{17.18}$$

17.13. Theorem (A. Nechaev, 1982). *Under the above suppositions, $T(I) = T(\overline{F})p^{\alpha(I)}$, where*

$$\alpha(I) = \begin{cases} d_a(I), & \text{if } p^{n_a} > 2, \text{ or } p^{n_a} = 2,\ d_a(I) \le 1; \\ d_{a+1}(I) + 1, & \text{if } p^{n_a} = 2,\ d_a(I) \ge 1. \end{cases}$$

□ From (17.17) and (17.18), by Theorem 16.5 we get $n_b = \|U_b(x)\|$. Hence

$$U_b(x) = p^{n_b}V_b(x), \qquad n_b \in \overline{0, n}, \qquad \overline{V}_b(x) \neq \overline{0}. \tag{17.19}$$

By Theorem 17.12, $\alpha(I)$ is the least $d \in \mathbb{N}_0$ such that

$$x^{\tau p^{a+d}} - e \in I. \tag{17.20}$$

Since $\overline{F}(x) | \overline{G}(x)^{p^a}$ and $\overline{G}(x)^{p^a} = \overline{G}^{[a]}(x^{p^a})$, we have

$$x^{\tau p^a} \equiv e + p^{n_a}V_a(x)W_0(x) \pmod{I}, \text{ where } n_a \ge 1; \tag{17.21}$$

moreover $\mathcal{P}W_0(x) + I = \mathcal{P}$. If $p^{n_a} > 2$, then for any $d \in \mathbb{N}_0$

$$x^{\tau p^{a+d}} \equiv e + p^{n_a+d}V_a(x)W_d(x) \pmod{I},$$

where $\overline{W}_d(x) = \overline{W}_0(x)$, and hence the condition (17.20) is equivalent to the condition $p^{n_a+d}V_a(x) \in I$, i.e., to the condition

$$p^d U_a(x) \in I. \tag{17.22}$$

By Theorem 16.5(C7), it follows from (17.17) and (17.18) that (17.22) is equivalent to the system of inequalities

$$d + n_{b_s} \geq a_s \text{ for } s \in \overline{1, t+1} \ \ (a_{t+1} = n).$$

Therefore, the minimal d with the property (17.20) is $d = d_a(I)$, i.e., $\alpha(I) = d_a(I)$.

If $p^{n_a} = 2$, then $p = 2$, $n_a = 1$, and, squaring both parts of (17.21), we get

$$x^{\tau 2^{a+1}} \equiv e + 2^{n_{a+1}} V_{a+1}(x) W_1(x) \pmod{I},$$

where $n_{a+1} > 1$ and $\mathcal{P}W_1(x) + I = \mathcal{P}$. Now the proof is completed analogously to the case $p^{n_a} > 2$. □

The following results generalize the results of [113, 166], where the case $R = \mathbb{Z}_{p^n}$ was considered.

17.14. Corollary. *Let $F(x)$ be a reversible polynomial of degree m over the ring $R = GR(q^n, p^n)$, $n > 1$, $G(x) = \operatorname{rad} F(x)$ and τ, k, a are the same as above. Then*

(a) *for some $n_a \in \overline{1, n}$*

$$\operatorname{Res}(G^{[a]}(x^{p^a})/F(x)) = p^{n_a} V_a(x), \qquad \overline{V}_a(x) \neq \overline{0}, \tag{17.23}$$

and if $p^{n_a} > 2$, or if $p^{n_a} = 2$, $n = 2$, or if $p^{n_a} = 2$, $n > 2$ and

$$\overline{V}_a(x)(\overline{V}_a(x) + (x\overline{G}(x)')^{2^a}) \not\equiv \overline{0} \pmod{\overline{F}(x)}, \tag{17.24}$$

then

$$T(F) = T(\overline{F}) p^{n-n_a}; \tag{17.25}$$

(b) *if $p^{n_a} = 2$, $n > 2$, and (17.24) does not hold, then for some $n_{a+1} \in \overline{3, n}$*

$$\operatorname{Res}(G^{[a+1]}(x^{2^{a+1}})/F) = 2^{n_{a+1}} V_{a+1}(x), \qquad \overline{V}_{a+1}(x) \neq \overline{0}, \tag{17.26}$$

and then we have

$$T(F) = T(\overline{F}) p^{n-n_{a+1}+1} < T(\overline{F}) p^{n-n_a}. \tag{17.27}$$

Moreover,

$$T(F) \leq (q^m - 1) p^{n-1}. \tag{17.28}$$

□ Let $I = \mathcal{P}F(x)$. Then $T(F) = T(I)$, and (17.23) follows from (17.16), (17.19), (17.21). In the case considered, $d_a(I) = n - n_a$, and if $p^{n_a} > 2$ or $p^{n_a} = n = 2$, then, by Theorem 17.13, $\alpha(I) = d_a(I)$, and (17.25) is true.

If $p^{n_a} = 2$, $n > 2$, then for some $n_{a+1} \in \overline{2, n}$ the relation (17.26) holds. In this case, $d_{a+1}(I) = n - n_{a+1}$, and, by Theorem 17.13, we get $\alpha(I) = d_{a+1}(I) + 1$, i.e., the equality in (17.27) is true. In this case, (17.25) is true iff $n_{a+1} = 2$. By 17.10, the polynomial $U_{a+1}(x) = \operatorname{Res}(G^{[a+1]}(x^{2^{a+1}})/F)$ has the form

$$U_{a+1}(x) \equiv U_a(x) \cdot \operatorname{Res}(G^{[a]}(-x^{2^a})/F) \equiv 4W(x) \pmod{F(x)},$$

where

$$\overline{W}(x) \equiv \overline{V}_a(x)(\overline{V}_a(x) + (x\overline{G}(x)')^{2^a}) \pmod{F(x)}.$$

Now it follows from (17.26) that the equality $n_{a+1} = 2$ is equivalent to $\overline{W}(x) \not\equiv \overline{0}$, i.e., to (17.24).

The inequality (17.28) follows from the inequality $T(\overline{F}) \leq q^m - 1$ (see Proposition 6.7). □

Note that in the case $R = \mathbb{Z}_{p^n}$ the conditions (17.23), (17.26) are substantially simplified, since $G^{[a+1]}(x) = G^{[a]}(x) = G(x)$, and Corollary 17.14 gives an algorithm for the calculation of the period of the polynomial $F(x)$ which is simpler than the algorithms from [113,166].

D. Polynomials of maximal period over the Galois ring [21, 48]. In connection with (17.28) we formulate

17.15. Definition. A reversible polynomial $F(x)$ of degree m over a Galois ring $R = GR(q^n, p^n)$ is said to be a *polynomial of maximal period* (MP-polynomial) if

$$T(F) = (q^m - 1) p^{n-1}. \tag{17.29}$$

17.16. Theorem (A. Nechaev, 1982, see [48]). *A reversible polynomial $F(x)$ of degree m over the ring $R = GR(q^n, p^n)$ is a polynomial of maximal period iff the following conditions hold:*

(a) *$\overline{F}(x)$ is a polynomial of maximal period over the field $\overline{R}$;*

(b) *if $F_*(x)$ is the distinguished polynomial corresponding to $F(x)$, then*

$$F(x) = F_*(x) + pV(x), \tag{17.30}$$

where

$$\overline{V}(x) \neq \overline{0}, \tag{17.31}$$

and if $p = 2 < n$, then, in addition,

$$\overline{V}(x) \not\equiv x\overline{F}(x)' \pmod{F(x)}. \tag{17.32}$$

Under the condition (a), *the condition* (b) *is equivalent to the condition*

(c) *if $\tau = q^m - 1$, then*

$$x^\tau \equiv e + p\Phi(x) \pmod{F(x)}, \qquad \deg \Phi(x) < m, \qquad \overline{\Phi}(x) \neq \overline{0}, \tag{17.33}$$

and in the case $p = 2 < n$, in addition,

$$\overline{\Phi}(x) \neq \overline{e}. \tag{17.34}$$

□ The equality (17.29) is equivalent to the pair of equalities $T(\overline{F}) = q^m - 1$, $T(F) = T(\overline{F})p^{n-1}$. The first of these equalities is equivalent to the condition (a), and the second one, in view of Corollary 17.14, is equivalent to (b). Now we prove the second part of the theorem. Under the notations of Theorem 17.13 and Corollary 17.14 we have $G(x) = F_*(x)$, $\tau = q^m - 1$, $k = 1$, $a = 0$, $V_a = V_0 = V(x)$. Therefore, by (17.21), the relation (17.33) is equivalent to (17.31). Further, let $p = 2 < n$. In this case, (17.29) is equivalent to (17.33) with the additional condition

$$x^{2\tau} \equiv e + 2^2\Phi_2(x) \pmod{F(x)}, \qquad \deg \Phi_2(x) < m, \qquad \overline{\Phi}_2(x) \neq \overline{0}. \tag{17.35}$$

Since $\Phi_2(x) \equiv \Phi(x)(\Phi(x) + e) \pmod{F(x)}$, then (17.35) is equivalent to (17.33) and (17.34). Thus, (b) $\Leftrightarrow$ (c). □

17.17. Corollary. *An MP-polynomial of degree m over the ring $R = GR(q^n, p^n)$ exists iff $q^m > 2$ or $q^m = 2 = n$. Under these conditions for any MP-polynomial $f(x) \in \overline{R}[x]$ of degree m there exists an MP-polynomial $F(x) \in R[x]$ with $\overline{F}(x) = f(x)$, and the number of such polynomials is equal to*

$$\begin{array}{ll} (q^m - 1)q^{(n-2)m}, & \text{if } p > 2 \text{ or } p = 2 = n; \\ (q^m - 2)q^{(n-2)m}, & \text{if } p = 2 < n. \end{array}$$

□ The set of all MP-polynomials $F(x) \in \mathcal{P}$ with $\overline{F} = f$ coincides with the set of all polynomials of the form (17.30) with the properties (17.31), (17.32), where $F_*(x)$ is the distinguished polynomial corresponding to $f(x)$. A unique case, where in (17.30) we cannot choose $V(x)$ with the properties (17.31), (17.32), is the case $m = 1$, $R = \mathbf{Z}_{2^n}$, $n > 2$. □

17.18. Corollary. *A reversible polynomial $F(x)$ of degree m over a Galois ring $R = GR(q^n, p^n)$, $q = p^r$, is an MP-polynomial iff $T(\overline{F}) = q^m - 1$ and the polynomial $W(x)$ defined from the relation $F(x) - F^{[r]}(x) = pW(x)$ satisfies the conditions*

$$\overline{W}(x) \neq \overline{0}, \text{ and if } p = 2 < n, \ \overline{W}(x) \not\equiv x\overline{F}(x)' \pmod{\overline{F}(x)}. \tag{17.36}$$

□ By 17.9, $F^{[r]}(x) \equiv F_*(x) \pmod{p^2}$. Therefore, $\overline{W}(x) = \overline{V}(x)$, where $V(x)$ is the polynomial from (17.30). □

The above results make it possible to simplify the algorithm of construction of MP-polynomials over $\mathbf{Z}_{p^n}$ with the help of the table of MP-polynomials over $\mathbf{Z}_p$ and some combinatorical conditions on the coefficients of polynomials.

17.19. Corollary (A. Kuzmin, 1986, see [21]). *Let $F(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ be a reversible polynomial over $\mathbf{Z}_{p^n}$, $p > 2$, such that $T(\overline{F}) = p^m - 1$. Then $F(x)$ is an MP-polynomial iff*

$$\sum_{j_0,\ldots,j_{m-1}\in A} \frac{p!}{j_0!\ldots j_{m-1}!} \prod_{s=0}^{m} (a_s x^s)^{j_s} \not\equiv F(x^p) \pmod{p^2},$$

where $a_m = e$, A is the set of all rows $(j_0, \ldots, j_m)$ of the numbers from $\overline{0, p-1}$ such that

$$j_0 + j_1 + \ldots + j_m = p, \qquad j_1 + 2j_2 + \ldots + mj_m \equiv 0 \pmod{p}.$$

In particular, $F(x)$ is an MP-polynomial when

$$a_0^p \not\equiv a_0 \pmod{p^2},$$

or when

$$F(x) = x^m + a_k x^k + a_0, \qquad m \geq p - 2. \quad \square$$

17.20. Corollary (A. Nechaev, 1982). *Let $F(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ be a reversible polynomial over $\mathbf{Z}_{2^n}$ such that $T(\overline{F}) = 2^m - 1$. Then $F(x)$ is an MP-polynomial in the following cases:*

(a) *m is even, $a_0 \equiv e \pmod 4$;*

(b) *m is odd and*

$$a_1 \underset{4}{\equiv} \begin{cases} e + 2a_0a_2 & \text{if } \overline{a}_1 = \overline{e}; \\ 2(e + a_0a_2) & \text{if } \overline{a}_1 = \overline{0}; \end{cases}$$

(c) *$F(x) = x^m + a_k x^k + a_0$, $a_k, a_0 \in \{-e, e\}$, $(m, a_0) \neq (2k, e)$.* $\square$

18. The Cyclic Type of a Finite Reversible LRS-Family

A. LRS-families over a finite module [48, 53, 79, 80, 103]. Let R be a finite (commutative) ring, M be a faithful f.g.-R-module, I be a reversible ideal of the ring $\mathcal{P} = R[x]$. According to the results of Section 15, the description of the cyclic type of the family $L_M(I)$ is reduced to the case where R is a local ring and I is a primary ideal; we suppose this in what follows.

Let I be a primary ideal with the main generator $F(x)$ and with the generating system $F(x)$, $G_1(x), \ldots, G_t(x)$. Let $\deg F(x) = m$ and

$$\overline{F}(x) = g(x)^k, \tag{18.1}$$

where $g(x)$ is an irreducible polynomial over the field $\overline{R}$,

$$T(g(x)) = \tau, \qquad p^{a-1} < k \leq p^a. \tag{18.2}$$

Then $\operatorname{rad} F(x) = G(x)$ is a distinguished polynomial corresponding to $g(x)$, and by 17.12, $T(I) = \tau p^{\beta(I)}$.

For an $(m \times l)$-matrix B over R, let $\mathcal{K}_M(B)$ be the R-module of all solutions $(\mu_1, \ldots, \mu_m) \in M^m$ of the system of linear equations $(x_1, \ldots, x_m)B = (0, \ldots, 0)$. Denote

$$B_s = (G^{[s]}(S), G_1(S), \ldots, G_t(S))_{m \times m(t+1)}, \qquad s \geq 0,$$

where $G^{[s]}(x)$ is the polynomial defined in (17.10), and $S = S(F)$ is the accompanying matrix of the polynomial $F(x)$.

18.1. Proposition [48]. *Under the above assumptions, the cyclic type of the family $L_M(I)$ is given by*

$$Z_I^M(y) = y + \sum_{s=0}^{\beta(I)} c_I^M(\tau p^s) y^{\tau p^s}, \tag{18.3}$$

where

$$c_I^M(\tau) = \frac{1}{\tau}(|\mathcal{K}_M(B_0)| - 1), \tag{18.4}$$

$$c_I^M(\tau p^s) = \frac{1}{\tau p^s}(|\mathcal{K}_M(B_s)| - |\mathcal{K}_M(B_{s-1})|), \qquad s \in \overline{1, \beta(I)}. \tag{18.5}$$

If ${}_RM$ is a QF-module or $I = \mathcal{P}F(x)$ is a principal ideal, then $c_I^M(\tau p^{\beta(I)}) \neq 0$, i.e., there exists a recurrence $\mu \in L_M(I)$ such that $T(\mu) = T(I)$.

□ The period of any recurrence $\mu \in L_M(I)$ is equal to the minimal $T \in \mathbf{N}$ with $\mu(\overline{0, m-1})(S(F)^T - E) = 0$. As was shown in [48], if $\mu \neq 0$, then $T = \tau p^s$ for some $s \in \mathbf{N}_0$. Therefore, the cyclic type of the family $L_M(I) \subseteq L_M(F)$ is given by (18.3). By Proposition 2.5, if $\mu \in L_M(F)$, then

$$\mu \in L_M(I) \Leftrightarrow \mu(\overline{0, m-1})(G_1(S), \ldots, G_t(S)) = 0.$$

Hence, for each $s \in \overline{0, \beta(I)}$ the number $K(\tau p^s)$ of recurrences $\mu \in L_M(I)$ with $T(\mu) | \tau p^s$ is equal to the number of solutions in M^m of the system of linear equations

$$(x_1, \ldots, x_m)(S(F)^{\tau p^s} - E, G_1(S), \ldots, G_t(S)) = 0. \tag{18.6}$$

Since $S(F)^{\tau p^s} - E = G^{[s]}(S^{p^s})U_s$, where U_s is an invertible matrix (see the proof of Theorem 17.12), the system (18.6) is equivalent to the system $(x_1, \ldots, x_m)B_s = 0$, and $K(\tau p^s) = |\mathcal{K}_M(B_s)|$. Now (18.4), (18.5) follow from the equalities

$$c_I^M(\tau) = \frac{1}{\tau}(K(\tau) - 1),$$

$$c_I^M(\tau p^s) = \frac{1}{\tau p^s}(K(\tau p^s) - K(\tau p^{s-1})) \text{ for } s \in \overline{1, \beta(I)}.$$

Let $b \in \overline{0, \beta(I)}$ be the maximal number such that $c_I^M(\tau p^b) \neq 0$. Then the period of any recurrence $\mu \in L_M(I)$ divides τp^b, hence

$$x^{\tau p^b} - e \in \mathrm{An}\,(L_M(I)). \tag{18.7}$$

If M is a QF-module, then $\mathrm{An}\,(L_M(I)) = I$, and it follows from (18.7) that $T(I) | \tau p^b$, i.e., $b = \beta(I)$. If $I = \mathcal{P}F(x)$ is a principal ideal, then (18.7) means that $(\mu_1, \ldots, \mu_m)(S(F)^{\tau p^b} - E) = 0$ for all $(\mu_1, \ldots, \mu_m) \in M^m$. Since M is a faithful R-module, $S(F)^{\tau p^b} = E$. Therefore, $T(F) | \tau p^b$, i.e., $T(I) | \tau p^b$ and $b = \beta(I)$. □

18.2. Corollary. *Let M be a faithful finite R-module over a finite ring R and I be a reversible ideal of $\mathcal{P}$. Then the length of any cycle of the family $L_M(I)$ divides the maximum of the lengths of cycles of this family. If M is a QF-module or I is a principal ideal, then there exists an LRS $\mu \in L_M(I)$ with $T(\mu) = T(I)$.*

□ In view of results of Section 15, this statement follows from 18.1 and from the properties of the operation of composition of the cyclic types. □

Conjecture: there always exists an LRS $\mu \in L_M(I)$ with $T(\mu) = T(I)$.

B. LRS-families over a local principal ideal ring. The usage of formulas (18.4), (18.5) is not convenient because do not have a good theory which makes it possible to evaluate the number of solutions of a system of linear equations over an arbitrary local ring R [11, 12]. But such a theory exists for a principal ideal ring R, and it substantially simplifies the calculations. In what follows, we assume that R is a finite local principal ideal (commutative) ring, satisfying the conditions formulated at the beginning of Section 16.A, and such that

$$\overline{R} = R/\mathfrak{N}(R) = GF(q), \qquad q = p^r, \qquad p = \mathrm{char}\,\overline{R}, \qquad pR = \mathfrak{N}(R)^e.$$

In this case, if $m \leq l$, then each $(m \times l)$-matrix B over R is equivalent to the unique diagonal matrix (see [8])

$$B \sim D = \mathrm{diag}\,(\pi^{d_1}, \ldots, \pi^{d_m}), \qquad 0 \leq d_1 \leq \ldots \leq d_m \leq n. \tag{18.8}$$

18.3. Definition. We say that the matrix D from (18.8) is the *canonical form* of the matrix B, the vector $\operatorname{sign} B = [d_1, \ldots, d_m]$ is the *signature* of B, and $\operatorname{def} B = d_1 + \ldots + d_m$ is the *defect* of B.

Under the condition (18.8) the module $\mathcal{K}_R(B)$ of the solutions in R^m of the system of linear equations $(x_1, \ldots, x_m)B = 0$ satisfies the condition

$$\mathcal{K}_R(B) \cong R/(\pi^{d_1}) \oplus \ldots \oplus R/(\pi^{d_m}), \qquad |\mathcal{K}_R(B)| = q^{\operatorname{def} B}.$$

18.4. Proposition. *Let R be a principal ideal ring, $I \lhd \mathcal{P}$ be a primary reversible ideal with the main generator satisfying the conditions* (18.1), (18.2), *and let matrices B_s be the same as in Proposition* 18.1. *Let*

$$\operatorname{def} B_s = d(s) \text{ for } s \geq 0.$$

Then the cyclic type of the family $L_R(I)$ is given by

$$Z_I^R(y) = y + \sum_{s=0}^{\beta(I)} c_I^R(\tau p^s) y^{\tau p^s}, \tag{18.9}$$

where

$$c_I^R(\tau) = \frac{1}{\tau}(q^{d(0)} - 1), \tag{18.10}$$

$$c_I^R(\tau p^s) = \frac{1}{\tau p^s}(q^{d(s)} - q^{d(s-1)}), \qquad s \in \overline{1, \beta(I)}; \tag{18.11}$$

moreover, $c_I^R(\tau p^{\beta(I)}) \neq 0$.

□ This follows from 18.1. □

If I is a principal ideal, we obtain some simplifications in the calculation of the cyclic type of $L_R(I)$.

18.5. Theorem (A. Nechaev, 1982, see [48]). *Let R be a finite local principal ideal ring with ramification index ε and with the index of nilpotency of its radical n. Let $F(x)$ be a primary reversible polynomial over R satisfying the conditions* (18.1), (18.2), *$G(x) = \operatorname{rad} F(x)$, and for $s \geq 0$*

$$\operatorname{sign} G^{[s]}(S^{p^s}) = [d_1(s), \ldots, d_m(s)],$$
$$d(s) = d_1(s) + \ldots + d_m(s). \tag{18.12}$$

Let s_1 be the least $s \in \mathbb{N}_0$ such that

$$d_1(s) > \frac{\varepsilon}{2}, \text{ if } p > 2;$$
$$d_1(s) > \varepsilon, \text{ if } p = 2,\ n > \varepsilon; \tag{18.13}$$
$$d_1(s) = n, \text{ if } p = 2,\ n = \varepsilon.$$

Then

$$T(F) = \tau p^{\sigma}, \text{ where } \sigma = s_1 + \left]\frac{n - d_1(s_1)}{\varepsilon}\right[, \tag{18.14}$$

and the family $L_R(F)$ has the cyclic type

$$Z_F^R(y) = y + \sum_{s=0}^{\sigma} c_F^R(\tau p^s) y^{\tau p^s},$$

where the coefficients $c_F^R(\tau p^s)$ are defined by (18.10), (18.11). *Moreover, for each $s > s_1$ the parameters $d(s)$ in* (18.11) *can be expressed with the help of $[d_1(s_1), \ldots, d_m(s_1)]$ in the form*

$$d_j(s) = \nu(d_j(s_1) + (s - s_1)\varepsilon), \qquad j \in \overline{1, m}, \tag{18.15}$$

where $\nu(x) = \min\{n, x\}$. The parameter s_1 satisfies the inequality

$$s_1 \leq b(d_1(a)) + a + 1, \tag{18.16}$$

where a is defined in (18.2), $b(x) = \max\{0, \log_p \frac{e}{x(p-1)}\}$.

□ The form of the polynomial $Z_F^R(y)$ is described in Propositions 18.1 and 18.4. The simplifications connected with the parameter s_1 are based on the following properties. Since $pR = \mathfrak{N}(R)^e$, under the condition (18.8) we have $\operatorname{sign} pB = [\nu(d_1+\varepsilon), \dots, \nu(d_m+\varepsilon)]$. Therefore, by (18.12), in order to prove (18.15) it is sufficient to show that if $s \geq s_1$, then

$$G^{[s+1]}(S^{p^{s+1}}) \sim pG^{[s]}(S^{p^s}), \text{ where } S = S(F).$$

Since $G^{[s]}(S^{p^s}) \sim S^{\tau p^s} - E$, it is sufficient to prove that

$$S^{\tau p^{s+1}} - E \sim p(S^{\tau p^s} - E). \tag{18.17}$$

Let $S^{\tau p^s} = V$. Then $V = E + \pi^d C$, where $d = d_1(s)$, and $S^{\tau p^{s+1}} - E = V^p - E = (V-E)(V^{p-1} + \dots + V + E)$, where

$$(V^{p-1} + \dots + V + E) \equiv pE + \frac{p(p-1)}{2}\pi^d C \pmod{\mathfrak{N}(R)^{2d}}. \tag{18.18}$$

Since $s \geq s_1$, the number $d = d_1(s)$ satisfies (18.13), and hence

$$\frac{p(p-1)}{2}\pi^d R \subseteq \mathfrak{N}(R)^{e+1} = p\mathfrak{N}(R), \qquad \mathfrak{N}(R)^{2d} \subseteq p\mathfrak{N}(R).$$

Now it follows from (18.18) that $V^{p-1} + \dots + V + E = pW$, where W is an invertible matrix, because $\overline{W} = \overline{E}$. Therefore, $V^p - E \sim p(V-E)$, i.e., we get (18.17). For the proof of (18.16), see [48]. □

19. Linear Recurring Sequences over Galois Rings

Here $R = GR(q^n, p^n)$ is a Galois ring (see Section 17C), $q = p^r$, $F(x)$ is a monic polynomial from $\mathcal{P} = R[x]$ of degree m.

A. Linear recurrences of maximal period and families of them [8, 15, 45, 47, 48, 52, 53, 77, 102, 103, 113, 118, 166]. It follows from 6.3 and 17.3 that if $u \in R^{(1)}$ is an LRS of rank m, then $T(u) \leq (q^m-1)p^{n-1}$.

19.1. Definition. We say that a sequence $u \in R^{(1)}$ is a *linear recurring sequence of maximal period* (MP-*recurrence*) over a Galois ring R if for some $m \in \mathbb{N}$

$$\operatorname{rang} u = m \text{ and } T(u) = (q^m - 1)p^{n-1}. \tag{19.1}$$

Denote by $\overline{u}$ the image of a sequence $u \in R^{(1)}$ under the natural homomorphism $R \to \overline{R}$: $\overline{u} = (\overline{u}(0), \overline{u}(1), \dots) \in \overline{R}^{(1)}$.

19.2. Proposition. *An LRS $u \in R^{(1)}$ with minimal polynomial $F(x)$ is an MP-recurrence iff $F(x)$ is an MP-polynomial over R and $\overline{u} \neq \overline{0}$.*

□ The necessity of the condition $T(F) = (q^m - 1)p^{n-1}$ is obvious. The condition $\overline{u} \neq \overline{0}$ is equivalent to the condition $(\Phi_u(x), F(x)) = e$, which is equivalent to the equality $T(u) = T(F)$. □

The following results can be found in [26, 42, 45, 132, 148].

If $F(x)$ is an MP-polynomial over R, then its operator ring $S = \mathcal{P}/(F(x))$ is a Galois ring: $S = GR(q^{mn}, p^n)$. Let $Q = GR(q^{mn}, p^n)$ be a Galois extension of R. The polynomial $F(x)$ has exactly m roots in Q and has the form $F(x) = (x - \alpha^{(0)}) \dots (x - \alpha^{(m-1)})$, where $\alpha^{(s)} \in Q^*$, $\operatorname{ord} \alpha^{(s)} = T(F) = (q^m - 1)p^{n-1}$ and $Q = R[\alpha^{(s)}]$ for $s \in \overline{0, m-1}$. The group $\operatorname{Aut}(Q/R)$ of automorphisms of S over R is a cyclic group of order m: $\operatorname{Aut}(Q/R) = \langle\rho\rangle = \{e, \rho, \dots, \rho^{m-1}\}$. The roots of $F(x)$ can be enumerated in such a way that $\alpha^{(s)} = \rho^s(\alpha^{(0)})$ for $s \in \overline{0, m-1}$, i.e.,

$$F(x) = (x - \alpha)(x - \rho(\alpha)) \dots (x - \rho^{m-1}(\alpha)), \qquad \alpha = \alpha^{(0)}. \tag{19.2}$$

The trace $\mathrm{Tr} : {}_RQ \to {}_RR$, $\mathrm{Tr}(x) = \mathrm{Tr}_R^Q(x)$ from Q into R, defined by

$$\mathrm{Tr}_R^Q(x) = x + \rho(x) + \ldots + \rho^{n-1}(x), \tag{19.3}$$

is an epimorphism of modules.

19.3. Theorem [45, 47]. *Let $F(x)$ be an MP-polynomial. Then, keeping the previous notations, for any $u \in L_R(F)$ there exists a unique constant $\xi \in Q$ such that*

$$u(z) = \mathrm{Tr}_R^Q(\xi a^z). \tag{19.4}$$

Moreover, u is an MP-recurrence iff $\xi \in Q^*$, i.e., $\overline{\xi} \neq \overline{0}$. Any sequence (19.4) *belongs to $L_R(F)$.*

□ The proof is analogous to the proof of 10.14, 10.15 (see [45]). □

This result easily implies

19.4. Theorem. *Under the assumptions of* 19.3, *if $u \neq 0$, then*

$$T(u) = \tau p^{n-1-s}, \tag{19.5}$$

where $\tau = q^m - 1$, $s = \|\xi\| = \max\{i \in \overline{0,n} | \ \xi \in p^i Q\}$. The cyclic type of the family $L_R(F)$ is given by

$$Z_F(y) = y + \sum_{s=0}^{n-1} p^{(rm-1)s} y^{\tau p^s}. \quad \square \tag{19.6}$$

We suppose in what follows that $F(x)$ is a fixed MP-polynomial with the parameters defined above. The set of all MP-recurrences from $L_R(F)$ is denoted by $L_R^*(F)$. By 19.4, $L_R^*(F)$ is the union of $N = p^{(rm-1)(n-1)}$ cycles of length τp^{n-1}.

19.5. Definition. The system of polynomials

$$\mathbb{C}_F = \{C_i(x) | \ i \in \overline{1,N}\} \tag{19.7}$$

is called an *enumerator of cycles for the MP-polynomial* $F(x)$ if for any MP-recurrence $u \in L_R^*(F)$ the set $\{C_i(x)u | \ i \in \overline{1,N}\}$ is a system of representatives of all cycles of maximal length in $L_R(F)$.

19.6. Theorem (A. Nechaev, 1982, see [48]). *For any MP-polynomial $F(x)$, there exists an enumerator of cycles.*

□ Let $\Phi(x)$ be a polynomial from (17.33). Since $\overline{R}$ is an r-dimensional space over $GF(p)$, there exist polynomials $\Phi_1(x) = \Phi(x)$, $\Phi_2(x), \ldots, \Phi_{rm}(x)$ of degrees less than m and such that the system of polynomials $\{\overline{\Phi}_i(x) | \ i \in \overline{1,rm}\}$ is linearly independent over $GF(p)$ and for $p = 2$, in addition, $\overline{\Phi}_{rm}(x) = \overline{e}$ (see (17.34)). If $p = 2$, then there exists a polynomial $B(x) \in R[x]$ such that there are no solutions in $\overline{R}[x]$ of the comparison $Y^2 + Y \equiv \overline{B}(x) \pmod{\overline{F}(x)}$. Denote

$$U_i(x) = e + p\Phi_i(x) \text{ for } i \in \overline{1,rm}, \qquad V(x) = e + 4B(x).$$

Then the following system is an enumerator of cycles (19.7) for $F(x)$: if $p > 2$ or $p = 2 = n$, then this system consists of the polynomials

$$U_2(x)^{k_2} \ldots U_{rm}(x)^{k_{rm}}, \qquad 0 \leq k_i \leq p^{n-1} - 1, \qquad i \in \overline{2,rm}; \tag{19.8}$$

if $p = 2 < n$, then this system consist of the polynomials

$$U_2(x)^{k_2} \ldots U_{rm-1}(x)^{k_{rm-1}} V(x)^k (-1)^l, \tag{19.9}$$

where $0 \leq k_i \leq 2^{n-1}$ for $i \in \overline{1,rm-1}$, $0 \leq k \leq 2^{n-2} - 1$, $l \in \overline{0,1}$.

This statement follows from the fact that, by [148] (see also [132]), under these conditions, the set $\mathbb{C}_F(\alpha) = \{C_i(\alpha) | \ i \in \overline{1,N}\}$ is a subgroup of the group Q^*, belonging to its congruence subgroup $e + pQ$

and such that $Q^* = \langle\alpha\rangle \times \mathbf{C}_F(\alpha)$. If u is an MP-recurrence of the form (19.4), then $C_i(x)u = u_i$, where $u_i(z) = \mathrm{Tr}\,(\xi C_i(\alpha)\alpha^z) \in L_R^*(F)$. Moreover, if $C_j(x) \neq C_i(x)$, then the sequences u_i and u_j belong to different cycles, since $C_j(\alpha)C_i(\alpha)^{-1} \notin \langle\alpha\rangle$. □

B. The coordinate sequences of MP-recurrences [18, 25, 26, 45, 47, 95, 123].

19.7. Definition. A subset $\mathcal{B} = \{b_0 = 0, b_1, \ldots, b_{q-1}\}$ of a Galois ring R is called a *coordinate set of* R if the mapping $\nu : \mathcal{B} \to \overline{R}$, $\nu(\beta) = \overline{\beta}$, is a bijection.

Any element $a \in R$ is uniquely represented in the form

$$a = a_0 + pa_1 + \ldots + p^{n-1}a_{n-1}, \qquad a_s \in \mathcal{B}, \qquad s \in \overline{0, n-1}, \tag{19.10}$$

called the *decomposition of* a *in the coordinate set* $\mathcal{B}$. We say that the n functions

$$\gamma_s^{\mathcal{B}} : R \to \mathcal{B}, \qquad \gamma_s^{\mathcal{B}}(a) = a_s, \qquad s \in \overline{0, n-1}, \tag{19.11}$$

are the *coordinate functions* in the coordinate set $\mathcal{B}$. If u is a sequence over R, then the sequences $w_s = \gamma_s^{\mathcal{B}}(u)$ over $\mathcal{B}$, defined by $w_s(i) = \gamma_s^{\mathcal{B}}(u(i))$, $i \in \mathbf{N}_0$, are called the *coordinate sequences* of u in the coordinate set $\mathcal{B}$.

Examples of coordinate sets are *the p-adic coordinate set* $\Gamma(R) = \{\beta \in R |\ \beta^q = \beta\}$ of a Galois ring R and *the p-ary coordinate set* $\mathcal{B}_p = \{0, e, 2e, \ldots, (p-1)e\}$ of $\mathbf{Z}_{p^n}$. The decompositions of elements of R in these sets are called *p-adic* and *p-ary decompositions* respectively. Coordinate functions in the p-adic and p-ary (for $R = \mathbf{Z}_{p^n}$) coordinate sets are denoted by γ_s and δ_s:

$$\gamma_s = \gamma_s^{\Gamma(R)}, \qquad \delta_s = \gamma_s^{\mathcal{B}_p}, \qquad s \in \overline{0, n-1}. \tag{19.12}$$

Note that $\gamma_s = \delta_s$ for $s \in \overline{0, n-1}$ iff $R = \mathbf{Z}_{2^n}$.

Define the operations $\oplus$, $\otimes$ on the coordinate set $\mathcal{B}$ by the rule $a \oplus b = \gamma_0^{\mathcal{B}}(a+b)$, $a \otimes b = \gamma_0^{\mathcal{B}}(ab)$, a, $b \in \mathcal{B}$. Then $(\mathcal{B}, \oplus, \otimes) = GF(q)$, and the bijection $\nu : \mathcal{B} \to \overline{R}$ is a field isomorphism. If we define the multiplication of an element $b \in \mathcal{B}$ on element $\overline{c} \in \overline{R}$ by $\overline{c}b = \gamma_0^{\mathcal{B}}(cb)$, then $\mathcal{B}$ becomes an $\overline{R}$-algebra. Thus, we may investigate any sequence $w \in \mathcal{B}^{\langle 1\rangle}$ as a sequence over the field $\overline{R}$.

For an MP-recurrence $u \in L_R^*(F)$, denote

$$u_s = \gamma_s(u), \qquad v_s = \delta_s(u), \qquad w_s = \gamma_s^{\mathcal{B}}(u), \qquad s \in \overline{0, n-1}. \tag{19.13}$$

We would like to study the period $T(w_s)$ of w_s, its minimal polynomial $M_{w_s}(x)$ over $\overline{R}$, and the rank of w_s. Sometimes it is appropriate to study the p-ary and p-adic coordinate sequences u_s and v_s.

19.8. Theorem (A. Nechaev, 1982; A. Kuzmin, 1986 [26, 123]). *Let* $F(x)$ *be an MP-polynomial and* $f(x) = \overline{F}(x) \in \overline{\mathcal{P}} = \overline{R}[x]$. *Then*

$$M_{w_0}(x) = f(x), \tag{19.14}$$

and for each $s \in \overline{1, n-1}$

$$M_{w_s}(x) = f(x)^{p^{s-1}+1} f_{s1}(x)^{p^{s-1}} \ldots f_{sk}(x)^{p^{s-1}-k+1} \ldots f_{s,p^{s-1}}(x), \tag{19.15}$$

where $f_{sk}(x)$ *is a separable polynomial over* $\overline{R}$, $\deg f_{sk}(x) \geq 0$, *and*

$$f(x) f_{s1}(x) \ldots f_{s,p^{s-1}}(x) | x^\tau - e, \qquad \tau = q^m - 1. \tag{19.16}$$

Moreover, $T(w_0) = \tau$, $\mathrm{rank}\, w_0 = m$, *and for* $s \in \overline{1, n-1}$

$$T(w_s) = \tau p^s, \qquad \mathrm{rank}\, w_s \geq m(p^{s-1}+1). \tag{19.17}$$

If $R = \mathbf{Z}_{p^n}$, *then the polynomials* $f_{s1}, \ldots, f_{s,p^t}$ *for* $t \leq s-2$ *are uniquely determined by the sequences* $v_0, \ldots, v_{t+1}$, *and*

(a) *if* $p = 2$, *then*

$$f_{sj} = f_{4j} \text{ for } s \geq 4,\ j \in \overline{1,2}; \qquad f_{sj} = f_{lj} \text{ for } s \geq l \geq 5,\ 1 \leq j \leq 2^{l-2} - 2;$$

(b) *if* $p > 2$, *then*

$$f_{sj} = f_{lj} \text{ for } s \geq l \geq 3,\ 1 \leq j \leq (p-1)p^{l-2} - 2.$$

The proof is based on the following results. Let

$$\tau_t = \tau p^t = (q^m - 1)p^t.$$

19.9. Lemma. *For* $t \in \overline{0, n-1}$, *there exists a polynomial* $\Phi^{(t+1)}(x)$ *over* R *such that*

$$x^{\tau_t} - e \equiv p^{t+1} \cdot \Phi^{(t+1)}(x) \pmod{F(x)}, \text{ where } \deg \Phi^{(t+1)}(x) < m,\ \overline{\Phi}^{(t+1)}(x) \neq \overline{0}. \tag{19.18}$$

If $p = 2$, *then*

$$\overline{\Phi}^2(x) \equiv \overline{\Phi}^{(1)}(x) + \overline{\Phi}^{(1)}(x)^2 \pmod{\overline{G}(x)},$$
$$\Phi^{(t+1)}(x) \equiv \Phi^{(t)}(x) \pmod{2^{t-1}} \text{ for } t \geq 2; \tag{19.19}$$

if $p > 2$, *then*

$$\Phi^{(t+1)}(x) \equiv \Phi^{(t)}(x) \pmod{p^t} \text{ for } t \geq 1. \quad \square \tag{19.20}$$

The sequence $u^{(t)} = \Phi^{(t)}(x)u$ is called the *t-th derivative sequence* of the sequence u. Denote

$$u_s^{(t)} = \gamma_s(u^{(t)}), \qquad v_s^{(t)} = \delta_s(u^{(t)}), \qquad w_s^{(t)} = \gamma_s^{\mathcal{B}}(u^{(t)}), \qquad s, t \in \overline{0, n-1}. \tag{19.21}$$

Then $u^{(t)} \in L_R^*(F)$ and by (19.19), (19.20),

$$\text{if } p = 2, \text{ then } w_0^{(t)} = w_0^{(2)} \text{ for } t \geq 2,\ w_1^{(t)} = w_1^{(3)} \text{ for } t \geq 3; \tag{19.22}$$

$$\text{if } p > 2, \text{ then } w_0^{(t)} = w_0^{(1)} \text{ for } t \geq 1,\ w_1^{(t)} = w_1^{(2)} \text{ for } t \geq 2. \tag{19.23}$$

The function $\Delta : \mathcal{B} \times \mathcal{B} \to \mathcal{B}$, defined by $\Delta(x, y) = \gamma_1^{\mathcal{B}}(x + y)$, will be called the *carry function* into the first digit in the case of summation of elements of the coordinate set $\mathcal{B}$. Let

$$\chi_{\mathcal{B}}(x) = x(x - b_1) \ldots (x - b_{q-1})$$

be the *characteristic polynomial of the coordinate set* $\mathcal{B}$ and $\chi^*(x)$ be a polynomial of degree $\leq q - 1$ such that

$$\chi_{\mathcal{B}}(x) = x^q - x + p\chi^*(x).$$

19.10. Lemma. *For any* $a, b \in \mathcal{B}$

$$\gamma_1^{\mathcal{B}}(\gamma_0(a)) \equiv \chi^*(\gamma_0(a)) \pmod{p}, \qquad a \in R,$$

$$\Delta(a, b) \underset{p}{\equiv} \sum_{j=1}^{p-1} \frac{(-1)^j}{j} a^{p^{r-1}j} b^{p^{r-1}(p-j)} - \chi^*(a + b) + \chi^*(a) + \chi^*(b). \square \tag{19.24}$$

In the case $R = \mathbb{Z}_{p^n}$, for $s \geq 2$, $t \in \overline{0, s-2}$, define

$$v_{s,t} = (x^\tau - \overline{e})^{p^s - p^t} v_s.$$

19.11. Lemma. *The following relations hold:*

$$(x^{\tau_{s-1}} - \overline{e})w_s = w_0^{(s)} \text{ for } s \geq 1, \tag{19.25}$$

$$(x^{\tau_{s-2}} - \overline{e})w_s = w_1^{(s)} + \Delta(w_{s-1}, w_0^{(s-1)}) \text{ for } s \geq 2. \tag{19.26}$$

If $R = \mathbf{Z}_{2^n}$, *then for* $t \geq 1$

$$v_{s,t} = \begin{cases} v_0^{(2)} v_{t+1} \oplus v_1^{(t+1)}, & \text{if } s = t+2, \\ v_0^{(2)}(v_{t+1} \oplus v_1^{(t+1)}), & \text{if } s > t+2; \end{cases} \tag{19.27}$$

$$v_{s,t} = \begin{cases} v_0^{(1)} v_1 \oplus v_1^{(1)}, & \text{if } s = 2, \\ v_0^{(2)}(v_0^{(1)} v_1 \oplus v_1^{(1)}) \oplus \overline{\Phi}^{(1)}(x) v_0^{(2)}, & \text{if } s = 3, \\ v_0^{(2)}(v_0^{(1)} v_1 \oplus v_1^{(1)} \oplus \overline{\Phi}^{(1)}(x) v_0^{(2)}), & \text{if } s \geq 4. \end{cases} \tag{19.28}$$

If $R = \mathbf{Z}_{p^n}$, $p \geq 3$, *then*

$$(x^{\tau_0/2} + \overline{e})v_1 = -v_0^{p-1} \ominus \frac{1}{2} v_0^{(1)}, \tag{19.29}$$

and for $s \geq 2$, $t \in \overline{0, s-2}$,

$$v_{s,t} = (v_0^{(1)})^{p-1} v_{t+1} \oplus \frac{1}{2}((v_0^{(1)})^{p-1} \oplus v_0^{(1)}) \oplus z_{s,t}, \tag{19.30}$$

where

$$z_{s,t} = \begin{cases} (v_0^{(1)})^{p-1} \cdot (\overline{\Phi}^{(1)}(x)^2 v_0), & \text{if } p = 3,\ t = 0,\ s > 2, \\ \overline{\Phi}^{(1)}(x)^2 v_0, & \text{if } p = 3,\ t = 0,\ s = 2, \\ 0 & \text{otherwise.} \end{cases} \tag{19.31}$$

□

Now, Theorem 19.8 is proved according to the following scheme. Since $F(x)u = 0$, then $F(x)w_0 = 0$, and (19.14) is true. It follows from (19.25) that

$$M_{w_s}(x)/(M_{w_s}(x), x^{\tau_{s-1}} - \overline{e}) = f(x). \tag{19.32}$$

Also taking into account the relation $x^{\tau_{s-1}} - \overline{e} = (x^{\tau} - \overline{e})^{p^{s-1}}$, we get (19.15), (19.16), and (19.17). The definition of $v_{s,t}$ and (19.15) imply that

$$M_{v_{s,t}}(x) = M_{v_s}(x)/(M_{v_s}(x), (x^{\tau} - \overline{e})^{p^{s-1}-p^t}) = f(x)^{p^t+1} f_{s1}(x)^{p^t} \ldots f_{s,p^t}(x).$$

Moreover, by (19.22), (19.23) and (19.27)–(19.31), if $s \geq t+2$, then $v_{s,t} = v_{t+2,t}$. This implies statements (a) and (b). □

C. The study of the coordinate sequences with the help of the trace function. The representation (19.4) makes it possible to get some interesting results about the properties of the coordinate sequences w_t by means of studying the coordinate functions $\gamma_t(\mathrm{Tr}_R^Q(x))$. For M, $N \in \mathbf{N}$ we denote

$$I(M, N) = \{(k_0, \ldots, k_{M-1}) \in \mathbf{N}^M : \ k_0, \ldots, k_{M-1} \in \overline{0, p-1},\ k_0 + \ldots + k_{M-1} = N\}.$$

For $r = \log_p q$ and $t \leq \log_p(m(p-1))$ define the polynomial $\Psi_t^{(r)}(x)$ over the field $\Gamma(R) = GF(q)$ by

$$\Psi_t^{(r)}(x) = \sum_{(k_0,\ldots,k_{m-1}) \in I(m,p^t)} \oplus \frac{1}{k_0! \ldots k_{m-1}!} \cdot x^{p^{r-1}(k_0 + k_1 q + \ldots + k_{m-1} q^{m-1})}. \tag{19.33}$$

If $r = 1$ (i.e., if $q = p$), then $\Psi_t^{(r)}(x)$ is denoted by $\Psi_t(x)$.

For a natural number $k = \sum k_s p^s$, $0 \leq k_s < p$, define the *p-ary weight* $w(k) = \sum k_s$. The *index of nonlinearity* of the polynomial

$$A(x_1, \ldots, x_t) = \sum a_{i_1 \ldots i_t} x_1^{i_1} \ldots x_t^{i_t}$$

is defined by

$$\partial(A) = \max\{w(i_1) + \ldots + w(i_t) |\ a_{i_1 \ldots i_t} \neq 0\}.$$

Then $\partial(\Psi_t^{(r,j)}) = p^t$. Let $\mathrm{tr}\,(x) = \mathrm{tr}_{\Gamma(R)}^{\Gamma(Q)}(x) = x \oplus x^q \oplus \ldots \oplus x^{q^{m-1}}$ be the trace from the field $\Gamma(Q)$ into the field $\Gamma(R)$, where $Q = GR(q^{mn}, p^n)$.

19.12. Theorem (A. Nechaev, 1982; A. Kuzmin, 1986 [26, 45, 47, 123]). *Let $R = GR(q^n, p^n)$, $q = p^r$, $R < Q = GR(q^{mn}, p^n)$ and $\mathrm{Tr}\,(x) = \mathrm{Tr}_R^Q(x)$. Then*

$$\gamma_0(\mathrm{Tr}\,(x)) = \mathrm{tr}\,(\gamma_0(x)), \tag{19.34}$$

$$\gamma_1(\mathrm{Tr}\,(x)) = \Psi_1^{(r)}(\gamma_0(x)) \oplus \mathrm{tr}\,(\gamma_1(x)). \tag{19.35}$$

If $R = \mathbb{Z}_{p^n}$ (i.e., $q = p$, $r = 1$), then for $1 \le t \le \log_p(m(p-1))$ there exists a polynomial $h_t(x_0, \ldots, x_{t-1})$ over R such that $\partial(h_t) < p^t$ and

$$\delta_t(\mathrm{Tr}\,(x)) \underset{p}{\equiv} \Psi_t(\gamma_0(x)) + h_t(\gamma_0(x), \ldots, \gamma_{t-1}(x)) + \mathrm{tr}\,(\gamma_t(x)) \tag{19.36}$$

□ The equality (19.34) follows from the fact that the group $\mathrm{Aut}\,(Q/R)$ is generated by the following automorphism:

$$\rho(x) = \gamma_0(x)^q + p\gamma_1(x)^q + \ldots + p^{n-1}\gamma_{n-1}(x)^q \tag{19.37}$$

(see [42,45]). Since the proof of (19.36) is rather long (see [123]), we only illustrate its idea, proving (19.35).

It follows from (19.37) that

$$\gamma_1(\mathrm{Tr}\,(x)) = \gamma_1(\mathrm{Tr}\,(\gamma_0(x))) \oplus \mathrm{tr}\,(\gamma_1(x)). \tag{19.38}$$

For an arbitrary $\beta \in \Gamma(Q)$ denote

$$\beta_s = \beta^{q^s}, \qquad s \in \overline{0, m-1}; \qquad b = \beta_0 + \ldots + \beta_{m-1},$$

$$\vec{\beta} = (\beta_0, \ldots, \beta_{m-1}), \qquad \vec{\beta}^t = (\beta_0^t, \ldots, \beta_{m-1}^t). \tag{19.39}$$

Then $\mathrm{Tr}\,(\beta) = b$, and, by (19.38), in order to prove (19.35), it is sufficient to prove that

$$\gamma_1(b) = \Psi_1^{(r)}(\beta). \tag{19.40}$$

Consider the following polynomials over R:

$$\omega_0(x_0, \ldots, x_{m-1}) = x_0 + \ldots + x_{m-1},$$

$$\omega_1(x_0, \ldots, x_{m-1}) = \sum_{(k_0,\ldots,k_{m-1}) \in I(m,p)} \frac{1}{k_0! \ldots k_{m-1}!} \cdot x_0^{k_0} x_1^{k_1} \ldots x_{m-1}^{k_{m-1}}.$$

Then $b = \omega_0(\vec{\beta})$, and (19.40) is equivalent to

$$\gamma_1(b) \equiv \omega_1(\vec{\beta}^{p^{r-1}}) \pmod p.$$

To prove it, let us raise the equality $b = \omega_0(\vec{\beta})$ to the p-th power. We get $b^p = \omega_0(\vec{\beta}^p) + p!\omega_1(\vec{\beta})$. By step-by-step raising to the p-th power, we get

$$b^{p^2} \equiv \omega_0(\vec{\beta}^p)^p \equiv \omega_0(\vec{\beta}^{p^2}) + p!\omega_1(\vec{\beta}^p) \pmod{p^2},$$

$$\ldots\ldots\ldots$$

$$b^{p^r} \equiv \omega_0(\vec{\beta}^{p^r}) + p!\omega_1(\vec{\beta}^{p^{r-1}}) \pmod{p^r}.$$

The last relation with the relations

$$b^{p^r} = b^q \equiv \gamma_0(b) \pmod{p^2}, \qquad \omega_1(\vec{\beta}^{p^{r-1}}) = \omega_1(\vec{\beta}) = b,$$

mean that $\gamma_0(b) \equiv b + p!\omega_1(\vec{\beta}^{p^{r-1}}) \pmod{p^2}$, and since $b - \gamma_0(b) = p\gamma_1(b)$, we have

$$\gamma_1(b) \equiv -(p-1)!\omega_1(\vec{\beta}^{p^{r-1}}) \equiv \omega_1(\vec{\beta}^{[r-1}) \pmod{p}.\square$$

Applying Theorem 19.12 to the relation (19.4), we can describe the properties of the analytical representation of the coordinate sequences and estimate the degree of the polynomial $f_{s,p^s-1}(x)$ from (19.15). Denote

$$\xi_t = \gamma_t(\xi), \qquad \alpha_t = \gamma_t(\alpha), \qquad c = \alpha_1\alpha_0^{-1}, \qquad \zeta_t(z) = \operatorname{tr}(\gamma_t(\xi\alpha^z)).$$

19.13. Theorem (A. Nechaev, 1982; A. Kuzmin, 1986 [26,45, 123]). *Let u be an MP-recurrence of the form* (19.4). *Then*

$$w_0(z) \underset{p}{\equiv} u_0(z) = \operatorname{tr}(\xi_0\alpha_0^z), \qquad \operatorname{rank} w_0 = m. \tag{19.41}$$

$$u_1(z) = \Psi_1^{(r)}(\xi_0\alpha_0^z) \oplus \operatorname{tr}(\xi_1\alpha_0^z) \oplus z \cdot \operatorname{tr}(\xi_0 c\alpha_0^z). \tag{19.42}$$

If $R = \mathbf{Z}_{p^n}$ and $1 \le t \le \log_p(m(p-1))$, then

$$v_t(z) \underset{p}{\equiv} \Psi_t(\xi_0\alpha_0^z) + G_t(\alpha_0^z, z) + \zeta_t(z), \tag{19.43}$$

where $G_t(x,y) \in \Gamma(Q)[x,y]$, $\partial_x(G_t(x,y)) < p^t$, $\deg_y G_t(x,y) < p^{t-1}$. Moreover, $M_{\zeta_t}(x) = f(x)^{p^{t-1}+1}$.

□ By (19.4), the relations (19.41) follow from (19.34). Since $u(z) \equiv \operatorname{Tr}((\xi_0 + p\xi_1)(\alpha_0 + p\alpha_1)^z) \pmod{p^2}$, we have

$$u_1(z) = \gamma_1(\operatorname{Tr}(\xi_0\alpha_0^z)) \oplus \operatorname{tr}(\xi_1\alpha_0^z) \oplus z \cdot \operatorname{tr}(\xi_0 c\alpha_0^z).$$

Now (19.42) follows from (19.35) and from the relations

$$\gamma_0(\xi_0\alpha_0^z) = \xi_0\alpha_0^z, \qquad \gamma_1(\xi_0\alpha_0^z) = 0.$$

The proof of (19.43) can be found in [123]. □

Theorem 19.13 makes it possible to estimate the ranks of the sequences u_1 and v_t. In particular,

$$\operatorname{rank} u_1 = \binom{m+p-1}{p} + m, \qquad \operatorname{rank} v_1 \ge \binom{m+p-1}{p} + \binom{m+p-2}{p-1} + m.$$

More profound results will be obtained in Chapter 4.

D. k-maximal recurring sequences over a Galois ring. Analogously to the definition 12.1, we give

19.14. Definition. An exact reversible k-LRS u over a Galois ring $R = GR(q^n, p^n)$ is called a *k-maximal recurrence* if its operator ring $S = \mathcal{P}_k/\operatorname{An}(u)$ is a Galois ring, and

$$T(u) = |S^*|, \tag{19.44}$$

i.e., if u is a full-cycle recurrence over R (see 6.24), and its operator ring is a Galois ring. If here $S = GR(q^{mn}, p^n)$, then we say that u is a *k-max-LRS of rank m.*

By Theorem 5.26, (19.44) is equivalent to the conditions

$$S = GR(q^{mn}, p^n), \qquad S^* = \langle\theta_1, \dots, \theta_k\rangle, \tag{19.45}$$

where $\theta_s = x_s + I$, $s \in \overline{1,k}$.

The existence of these recurrences follows from

19.15. Theorem (A. Nechaev, 1993). *Let $Q = GR(q^{mn}, p^n)$ be a Galois extension of the Galois ring R, and let elements $\alpha_1, \dots, \alpha_k \in Q^*$ be such that*

$$Q^* = \langle\alpha_1, \dots, \alpha_k\rangle. \tag{19.46}$$

Then for any $\xi \in Q^*$ the k-sequence $u \in R^{(k)}$ of the form

$$u(\mathbf{z}) = \mathrm{Tr}_R^Q(\xi\alpha^{\mathbf{z}}) \tag{19.47}$$

is a k-max-LRS of rank m over R with period

$$T(u) = (q^m - 1)q^{m(n-1)}. \tag{19.48}$$

□ It follows from (19.46) that

$$Q = R[\alpha_1, \ldots, \alpha_k]. \tag{19.49}$$

Therefore, for a given $\eta \in Q$, the k-sequence $v(\mathbf{z}) = \mathrm{Tr}_R^Q(\eta\alpha^{\mathbf{z}})$ is equal to 0 iff $\eta = 0$. It follows that, under the condition (19.47),

$$\mathrm{An}\,(u) = \{H(\mathbf{x}) \in \mathcal{P}_k | H(\alpha) = 0\}, \tag{19.50}$$

since $H(\mathbf{x})u(\mathbf{z}) = \mathrm{Tr}_R^Q(H(\alpha)\xi\alpha^{\mathbf{z}})$. Furthermore, we see from (19.49) and (19.50) that the ring of operators $S = \mathcal{P}_k/\mathrm{An}\,(u) = R[\theta_1, \ldots, \theta_k]$ (see 1.18) is isomorphic to Q, and there exists an isomorphism $\varphi : S \to Q$ over R such that $\varphi(\theta_s) = \alpha_s$, $s \in \overline{1,k}$. By (19.46), this implies (19.45), and, according to 19.14, u is a k-max-LRS of rank m over R with period (19.48). □

Now we are going to show that Theorem 19.15 describes all k-maximal recurrences over R. Let u satisfy the conditions of Definition 19.14. Note that S_R is a free module of rank m over a Galois ring. Hence, the system $\delta_1, \ldots, \delta_t \in S$ generates S_R iff the system $\overline{\delta}_1, \ldots, \overline{\delta}_t$ generates $\overline{S}_{\overline{R}}$ over $\overline{R}$ [2, 132, 135]. Therefore, it follows from (19.45) that the basis of S_R can be chosen in the form

$$\mathcal{B} = \{\theta^{\mathbf{j}} | \, \mathbf{j} \in \mathcal{F}\}, \tag{19.51}$$

where $\mathcal{F}$ is a subset of $\mathbb{N}_0^k$ of cardinality m. Moreover, the basis (19.51) can be chosen in such way that $\mathcal{F}$ is a Ferre diagram (see 10.3).

19.16. Definition. A basis $\mathcal{B}$ of the module S_R of the form (19.51) and such that $\mathcal{F}$ is a Ferre diagram is called a *Ferre basis*, and $\mathcal{F}$ is called a *Ferre diagram* of the linear recurrence u (and of the ideal $I = \mathrm{An}\,(u)$).

19.17. Lemma. *Any k-maximal linear recurrence of rank m over a Galois ring R is uniquely determined by the ideal $I = \mathrm{An}\,(u)$ and by the polyhedron of values $u(\mathcal{F})$ on an arbitrary set $\mathcal{F} \subset \mathbb{N}_0^k$ such that the system of elements $\mathcal{B}$ of the form* (19.51) *is a basis of the operator ring S over R. In this case, for any polyhedron of values $a(\mathcal{F}) \in R^{\mathcal{F}}$, there exists a unique recurrence $v \in L_R(I)$ with $v(\mathcal{F}) = a(\mathcal{F})$.*

□ See the proof of Proposition 10.9. □

19.18. Theorem (A. Nechaev, 1993). *Let u be a k-max-LRS over $R = GR(q^n, p^n)$ of rank m. Then the extension $Q = GR(q^{mn}, p^n)$ of R contains invertible elements ξ, $\alpha_1, \ldots, \alpha_k$ such that the equalities* (19.46), (19.47) *hold.*

□ By (19.45), there exists an isomorphism $\varphi : S \to Q$ over R. Let $\alpha_s = \varphi(\theta_s)$, $s \in \overline{1,k}$. Then (19.45) implies (19.46) and (19.49). Choose a basis $\mathcal{B}$ of the module S_R in the form (19.51). Then the system of elements $\mathcal{A} = \{\alpha^{\mathbf{j}} | \, \mathbf{j} \in \mathcal{F}\}$ is the basis of Q_R, and the system of linear equations

$$\mathrm{Tr}_R^Q(x\alpha^{\mathbf{j}}) = u(\mathbf{j}), \qquad \mathbf{j} \in \mathcal{F},$$

has the unique solution $\xi \in Q$. Moreover, $\xi \in Q^*$ because u is an exact sequence over R, and, therefore, $\overline{u}(\mathcal{F}) \neq \overline{0}$. By Theorem 19.15, the sequence $v(\mathbf{z}) = \mathrm{Tr}_R^Q(\xi\alpha^{\mathbf{z}})$ is a k-max-LRS of rank m with annihilator $\mathrm{An}\,(v) = \mathrm{An}\,(u)$. Since $v(\mathcal{F}) = u(\mathcal{F})$, we have, by 19.17, that $u = v$, i.e., (19.47) holds. □

Note that we can construct a k-max-LRS of rank m over a finite field for any k, $m \in \mathbb{N}$. In the case of Galois ring this is not true. If $R = GR(q^n, p^n)$, $q = p^r$, then there exists a k-max-LRS of rank m over R if and only if

$$k \geq mr, \text{ if } p > 2 \text{ or } p = n = 2;$$

$$k \geq mr + 1, \text{ if } p = 2 < n.$$

These restrictions on k follow from (19.45) [132, 148].

19.19. Definition. We call a reversible ideal $I \triangleleft \mathcal{P}_k$ an *ideal of maximal period* over a Galois ring R if its operator ring S satisfies (19.45) for some $m \in \mathbf{N}$.

19.20. Theorem (A. Nechaev, 1993). *Let I be an ideal of maximal period over $R = GR(q^n, p^n)$. Suppose that* (19.45) *holds. Then the group of periods of I is $\mathfrak{P}(I) = \{\mathbf{t} \in \mathbf{Z}^k | \ \theta^{\mathbf{t}} = e\}$, and*

$$T(I) = (q^m - 1)q^{m(n-1)}, \qquad \mathbf{Z}^k/\mathfrak{P}(I) \cong GR(q^{mn}, p^n)^*.$$

The cyclic type of the family $L_R(I)$ is given by

$$Z_I^R = 1 \cdot \mathbf{Z}^k + 1 \cdot \mathfrak{P}(I_1) + \ldots + 1 \cdot \mathfrak{P}(I_{n-1}) + 1 \cdot \mathfrak{P}(I),$$

where $I_s = I + p^s\mathcal{P}_k$, $s \in \overline{1, n-1}$. Moreover, $\mathcal{T}(I_s) \cong GR(q^{ms}, p^s)^*$.

□ The family $L_R(I)$ is the set of all recurrences of the form $v(\mathbf{z}) = \operatorname{Tr}_R^Q(\eta\alpha^{\mathbf{z}})$, $\eta \in Q$, because $|L_R(I)| = |S| = |Q|$. The equality $v = 0$ is equivalent to $\eta = 0$. If $v \neq 0$, then $\eta \in p^tQ \backslash p^{t+1}Q$ for some $t \in \overline{0, n-1}$, i.e., $\eta = p^t\xi$, $\xi \in Q^*$. In this case

$$v(\mathbf{z}) = p^t \cdot \operatorname{Tr}_R^Q(\xi\alpha^{\mathbf{z}}),$$

$\operatorname{An}(v) = I + p^{n-t}\mathcal{P}_k = I_{n-t}$, and $\mathcal{P}_k/\operatorname{An}(v) = S/p^{n-t}S = GR(q^{m(n-t)}, p^{n-t})$. By (19.45), $(\mathcal{P}_k/\operatorname{An}(v))^* = \langle\tilde{\theta}_1, \ldots, \tilde{\theta}_k\rangle$, where $\tilde{\theta}_s = x_s + I_{n-t}$. Therefore,

$$T(v) = |GR(q^{m(n-t)}, p^{n-t})^*| = (q^m - 1)q^{m(n-t-1)},$$

all recurrences from $L_R(I)$ with the annihilator I_{n-1} belong to the cycle $\mathcal{T}(v)$ and have the group of periods $\mathfrak{P}(I_{n-t})$. This implies (19.52). □

Chapter 4.

REPRESENTATIONS OF LINEAR RECURRING SEQUENCES

Definition. Let R, S be commutative rings with unit, u be a sequence over R, and $\sigma : R \to S$ be a map of the set R into the set S. The sequence $\sigma(u)$ over the ring S, defined by $\sigma(u)(i) = \sigma(u(i))$, $i \geq 0$, is called a *representation of the sequence u over the ring S* or an *S-representation of the sequence u*. The map σ is also called a representation.

If u is an LRS over R, then $\sigma(u)$ is not necessarily an LRS over S (for example, $R = S = \mathbb{Z}$, $u(i) = i$, $\sigma(2^n) = 1$, $\sigma(i) = 0$ if $i \neq 2^n$). If u is periodic (for example, if R is a finite ring), with period T and defect λ, then $\sigma(u)$ is an LRS over S with characteristic polynomial $x^{T+\lambda} - x^{\lambda}$. But we may have characteristic polynomials of $\sigma(u)$ of degree less than $T + \lambda$. The description of the annihilators of representations of a given sequence gives useful information about this sequence. It is also possible to use this description for a comparison of properties of different rings S. Note that in Section 30.C we use the GF(2)-representations of linear recurring sequences over $\mathbb{Z}_4$ for the construction of the Kerdoc code in a cyclic form.

In this chapter, u is an LRS of maximal period over a finite field or over a Galois ring. The main results concern the descriptions of the annihilators, of characteristic and minimal polynomials, and of ranks (or the estimates of ranks) of representations of the sequence u over different rings S. References: [23, 24, 26, 27, 28, 30, 33, 34, 45, 47, 83, 92, 93, 95, 107, 109, 119, 123, 164].

20. S-Representations of MP-Recurrences over Finite Fields

Let U be an LRS of maximal period over the field $GF(q)$ with a minimal polynomial $f(x)$ of degree m, and let

$$T = T(U) = q^m - 1, \qquad \tau = T/(q-1), \qquad \beta = (-1)^m f(0).$$

Since $f(x)$ is a polynomial of maximal period, β is a primitive element of $GF(q)$, and by 12.5, (12.4), $U(i+\tau) = \beta U(i)$ for $i \geq 0$. The sequence $u(i) = \beta^i$, $i \geq 0$, is an LRS of maximal period $T(u) = q - 1$ over $GF(q)$ with minimal polynomial $x - \beta$.

Let S be a commutative ring with unit e such that qe is non-zero divisor, and $\sigma : GF(q) \to S$, $\sigma(0) = 0$. Let (K) be an ideal generated by a subset $K \subseteq S[x]$.

20.1. Theorem [34]. $\operatorname{An}(\sigma(U)) = (G(x^\tau) |\ G(x) \in \operatorname{An}(\sigma(u)))$.

In the case where $S = GF(2)$, q is odd, this result was obtained in [92].

20.2. Corollary. *A polynomial $G(x)$ is a minimal polynomial of $\sigma(u)$ if and only if $G(x^\tau)$ is a minimal polynomial of $\sigma(U)$.* □

20.3. Corollary. *The following equality holds:* $\operatorname{rank}\sigma(U) = \tau \cdot \operatorname{rank}\sigma(u)$. *In particular, if $\sigma \neq 0$, then* $\operatorname{rank}\sigma(U) \geq \tau$. □

20.4. Corollary. *If $q = 2$, $\sigma \neq 0$, then* $\operatorname{An}(\sigma(U)) = (x^T - e)$ *and* $\operatorname{rank}\sigma(U) = T$. □

Thus, to find the annihilator, minimal polynomials, and the rank of the sequence $\sigma(U)$ for an MP-recurrence U of rank m, it is sufficient to find them for the MP-recurrence u of rank 1. Note that, by [70] (or by 26.2), the segment $u(\overline{0, q-2})$ is a permutation of $q - 1$ nonzero elements of $GF(q)$. Therefore, $\sigma(u)$ can be *any* sequence over the ring S of period $q - 1$ (depending on σ).

20.5. Remark. If $\sigma(0) = c \neq 0$ and $\tilde{\sigma} = \sigma - c$, then

$$\operatorname{rank}\tilde{\sigma}(U) - 1 \leq \operatorname{rank}\sigma(U) \leq rank\tilde{\sigma}(U) + 1.$$

Thus, the rank of $\sigma(u)$ can be determined up to ± 1.

To prove Theorem 20.1, define $\beta^0 = e$, $\beta^\infty = 0$ and $x^\infty v = 0$ for an arbitrary sequence v. Let $e(i)$, $i \geq 0$, be an element of the set $\{0, 1, \ldots, q-2, \infty\}$ such that $U(i) = \beta^{e(i)}$.

20.6. Lemma. *If* $G(x) = g_0 + g_1 x + \ldots \in S[x]$, $i, j \geq 0$, *then*

$$(G(x^\tau)\sigma(U))(i + \tau j) = (G(x)x^{e(i)}\sigma(u))(j).\square$$

20.7. Corollary. *If* $G(x)\sigma(u) = 0$, *then* $G(x^\tau)\sigma(U) = 0$. □

20.8. Lemma. *If* $H(x)\sigma(U) = 0$ *and*

$$H(x) = H_0(x^\tau) + xH_1(x^\tau) + \ldots + x^{\tau-1}H_{\tau-1}(x^\tau), \tag{20.1}$$

then $H_0(x)\sigma(u) = 0$.

□ By Lemma 20.6, for i, $j \geq 0$ we have

$$(H(x)\sigma(U))(i + \tau j) = \Big(\sum_{k=0}^{\tau-1} H_k(x)x^{e(i+k)}\sigma(u)\Big)(j) = 0. \tag{20.2}$$

Let us sum these relations for integers $i \in \overline{0, T-1}$ such that $e(i) = 0$. By [70] (or by 26.2), the number of integers $i \in \overline{0, T-1}$ such that $e(i) = 0$ (i.e., $U(i) = e$) is equal to q^{m-1}, and for arbitrary $k \in \overline{1, \tau-1}$, $a \in \{0, 1, \ldots, q-2, \infty\}$ the number of integers $i \in \overline{0, T-1}$ such that $(e(i), e(i+k)) = (0, a)$ is equal to q^{m-2}. Therefore, the result of the summation of (20.2) is

$$q^{m-1}H_0(x)\sigma(u) + q^{m-2} \cdot \sum_{k=1}^{\tau-1} H_k(x)(e + x + \ldots + x^{q-2})\sigma(u) = 0.$$

An analogous summation of (20.2) for integers $i \in \overline{0, T-1}$ such that $e(i) = \infty$ gives

$$q^{m-2} \cdot \sum_{k=1}^{\tau-1} H_k(x)(e + x + \ldots + x^{q-2})\sigma(u) = 0.$$

Therefore, $q^{m-1}H_0(x)\sigma(u) = 0$, and since qe is not a zero divisor, $H_0(x)\sigma(u) = 0$. □

20.9. Corollary. *If* (20.1) *holds and* $H(x)\sigma(U) = 0$, *then*

$$H_0(x)\sigma(u) = H_1(x)\sigma(u) = \ldots = H_{\tau-1}(x)\sigma(u) = 0.$$

□ By Lemmas 20.6 and 20.8, $H_0(x^\tau)\sigma(U) = 0$. Therefore,

$$(xH_1(x^\tau) + \ldots + x^{\tau-1}H_{\tau-1}(x^\tau))\sigma(U) = (H(x) - H_0(x^\tau))\sigma(U) = 0.$$

Since $\sigma(U)$ is reversible, we have $(H_1(x^\tau) + \ldots + x^{\tau-2}H_{\tau-1}(x^\tau))\sigma(U) = 0$. By Lemma 20.8, $H_1(x)\sigma(u) = 0$. The proof is completed by induction. □

□ Proof of Theorem 20.1. The inclusion $\operatorname{An}(\sigma(U)) \supseteq (G(x^\tau) | G(x) \in \operatorname{An}(\sigma(u)))$ follows from 20.7; the inverse inclusion follows from 20.9. □

By 20.3, if $\sigma \neq 0$, then $\tau \leq \operatorname{rank}\sigma(U) \leq T$. A representation $\sigma \neq 0$ is called *minimal* (*maximal*) if $\operatorname{rank}\sigma(U) = \tau$ ($\operatorname{rank}\sigma(U) = T$).

20.10. Example. A mapping σ such that $\sigma(GF(q)^*) = c \in S\backslash 0$ is minimal. A mapping σ, which is equal to 0 for every point except for some $\lambda_0 \in GF(q)\backslash 0$, is maximal.

20.11. Proposition. *A mapping* $\sigma : GF(q) \to S$ *is minimal if and only if there exist elements* $a \in S$, $c \in S\backslash 0$ *such that* $ca^{q-1} = c$ *and*

$$\sigma(0) = 0, \qquad \sigma(e) = c, \qquad \sigma(\beta^i) = ca^i, \qquad i \in \overline{1, q-2}.\square$$

21. $GF(q)$-Representations of MP-Recurrences over $GF(q)$

Let u be an LRS of maximal period over the field $P = GF(q)$, $q = p^r$, with minimal polynomial $f(x)$ of degree m. Any mapping $\sigma : P \to P$ is defined by the polynomial $\Lambda(x) = \lambda_{q-1}x^{q-1} + \ldots + \lambda_1 x + \lambda_0 \in P[x]$ such that $\sigma(a) = \Lambda(a)$, $a \in P$. Denote $I = \{l \in \overline{0,q-1} \mid \lambda_l \neq 0\}$.

For $k \in \mathbb{N}_0$, let

$$k = \sum_{s\geq 0} p^s \nu_s(k) = \sum_{s\geq 0} q^s N_s(k), \qquad \nu_s(k) \in \overline{0,p-1}, \qquad N_s(k) \in \overline{0,q-1},$$

$$w(k) = \sum_{s\geq 0} \nu_s(k), \qquad W(k) = \sum_{s\geq 0} N_s(k).$$

We write the sum $k = k_1 + \ldots + k_t$ of integers $k_1, \ldots, k_t \in \mathbb{N}_0$ in the form $k = k_1 \dot{+} \ldots \dot{+} k_t$ if $\nu_s(k) = \nu_s(k_1) + \ldots + \nu_s(k_t)$ for $s \geq 0$. Let $\theta \in GF(q^m)$ be a root of the polynomial $f(x)$ and $T = q^m - 1$. For $l \in \overline{1,q-1}$ denote

$$f^{(0)}(x) = x - e,$$

$$f^{(l)}(x) = \prod\{x - \theta^k \mid k \in \overline{1,T},\ W(k) = l,\ l = N_0(k) \dot{+} \ldots \dot{+} N_{m-1}(k)\}.$$

These polynomials are pairwise coprime, they belong to $P[x]$, and

$$\deg f^{(l)}(x) = \prod_{s=0}^{r-1} \binom{m + \nu_s(l) - 1}{\nu_s(l)}, \qquad l \in \overline{1,q-1},$$

where $r = \log_p q$. If $q = p$, then these formulas can be simplified:

$$f^{(l)}(x) = \prod\{x - \theta^k \mid k \in \overline{1,T},\ w(k) = l\}, \qquad l \geq 1,$$

$$deg f^{(l)}(x) = \binom{m + l - 1}{l}, \qquad l \in \overline{1,p-1}.$$

21.1. Theorem. *The following relations hold:*

$$M_{\sigma(u)}(x) = \prod_{l\in I} f^{(l)}(x), \qquad \operatorname{rank}\sigma(u) = \sum_{l\in I} \prod_{s=0}^{r-1} \binom{m + \nu_s(l) - 1}{\nu_s(l)},$$

where $I = \{l \in \overline{0,q-1} \mid \lambda_l \neq 0\}$.

□ By Theorem 12.2, $u(i) = \operatorname{tr}(c\theta^i)$, $i \geq 0$, where tr is the trace from $GF(q^m)$ to $GF(q)$, $c \in GF(q^m)\backslash 0$. Then for $l \in \overline{1,q-1}$:

$$u(i)^l = \sum_{\substack{j_0+\ldots+j_{m-1}=l \\ 0\leq j_t\leq l}} \frac{l!}{j_0! \ldots j_{m-1}!} \cdot (c\theta^i)^{j_0 + q j_1 + \ldots + q^{m-1} j_{m-1}}.$$

By Lucas' theorem [4], p does not divide the polynomial coefficient in the last relation if and only if $l = j_0 \dot{+} \ldots \dot{+} j_{m-1}$. Therefore, the minimal polynomial of the LRS u^l is equal to $f^{(l)}(x)$, $l \in \overline{0,q-1}$. Now the theorem follows from the equality $\sigma(u) = \Lambda(u) = \sum_{l\in I} \lambda_l u^l$. □

21.2. Corollary. *We have* $\operatorname{rank}\sigma(u) \leq \binom{m+p-1}{m}^r$, *and this inequality becomes an equality if and only if* $I = \overline{0,q-1}$, *i.e., if all coefficients of the polynomial* $\Lambda(x)$ *are not equal to* 0. □

22. $\mathbf{Z}_{p^n}$-Representations of MP-Recurrences over $GF(p)$

Let u be an LRS of maximal period over the field $P = GF(p)$ (p is prime) with minimal polynomial $f(x)$ of degree m, $R = \mathbf{Z}_{p^n}$, and let $\sigma : P \to R$ be a mapping. To simplify the formulations, we consider only the case $\sigma(0) = 0$. The general case is considered in [27].

A. The polynomial corresponding to σ. Let e_p, e be the units of the field P and the ring R respectively, $\Gamma(R) = \{\beta_0 = 0, \beta_1, \ldots, \beta_{p-1}\}$ be the p-adic coordinate set of R (see Section 19.B), $\beta_t \equiv te \pmod p$, $t \in \overline{0, p-1}$. We define the *norm* of a mapping $\sigma : P \to R$ as $\|\sigma\| = \max\{t \in \overline{0,n} | \sigma(P) \subseteq p^t R\}$ (see also 16.1).

22.1. Proposition. *There exists the unique polynomial $\Psi_\sigma(x) = \psi_{p-1}x^{p-1} + \ldots + \psi_1 x$ over R such that*

$$\Psi_\sigma(\beta_t) = \sigma(te_P), \qquad t \in \overline{0, p-1}. \tag{22.1}$$

The following equations are satisfied: $\|\Psi_\sigma(x)\| = \|\sigma\|$,

$$\Psi_\sigma(x) = \frac{x}{p-1} \cdot \sum_{t=1}^{p-1} \sigma(te_P)(x^{p-2} + x^{p-3}\beta_t + \ldots + x\beta_t^{p-3} + \beta_t^{p-2}). \tag{22.2}$$

□ The system of linear equations (22.1) of the variables $\psi_1, \ldots, \psi_{p-1}$ has a unique solution because its determinant is the Vandermonde determinant. The equality (22.1) for the polynomial (22.2) can be proved by direct evaluations. □

B. The annihilator of the sequence $\sigma(u)$. Let $\varkappa : P \to \overline{R}$ be the isomorphism of the fields $P = GF(p)$ and $\overline{R} = GF(p)$. Let $F_*(x) \in R[x]$ be the distinguished polynomial corresponding to the polynomial $\varkappa(f)$ (see 17.6): $F_*(x) | x^T - e$, $\overline{F}_*(x) = \varkappa(f(x))$, where $T = T(f) = T(u) = p^m - 1$. Let θ be a root of the polynomial $F_*(x)$, θ belonging to the Galois extension $S = GR(p^{mn}, p^n)$ of the Galois ring R. Let

$$F_*^{(r)}(x) = \prod\{x - \theta^k \mid 1 \le k \le T,\ w(k) = r\}, \qquad r \ge 1,$$

where $w(k)$, $\nu_s(k)$ are defined as in Section 21. It is easy to see that $F_*^{(r)}(x) \in R[x]$ and $F_*^{(r)}(x) = e$ for $r > (p-1)m$. The degree of the polynomial $F_*^{(r)}(x)$ is equal to the number $\left\{ {m \atop r} \right\}$ of combinations of r identical balls into m boxes under the condition that each box contains less than or equal to $p-1$ balls. By [59, p. 215]

$$\left\{ {m \atop r} \right\} = \sum_{j \ge 0} (-1)^j \binom{m}{j} \binom{r + m - pj - 1}{m - 1}, \qquad r \ge 1. \tag{22.3}$$

If $p = 2$, then $\left\{ {m \atop r} \right\} = \binom{m}{r}$. For $s \in \overline{0, n-1}$, let

$$F_s(x) = \prod_{l=1}^{p-1} (F_*^{(l)}(x) \cdot F_*^{(l+p-1)}(x) \cdot \ldots \cdot F_*^{(l+(s-\|\psi_l\|)(p-1))}(x)).$$

22.2. Theorem [27]. *Let $\|\sigma\| = r \in \overline{0, n-1}$. Then*

$$\mathrm{An}(\sigma(u)) = (F_{n-1}(x), pF_{n-2}(x), \ldots, p^{n-r-1}F_r(x), p^{n-r}).$$

In particular, $F_{n-1}(x)$ is a minimal polynomial of $\sigma(u)$.

Note that if $\deg F_s(x) = \deg F_t(x)$ for some $0 \le t < s \le n-1$, then $F_s(x) = F_t(x)$. In this situation we may exclude $p^{n-t-1}F_t(x)$ from the generating set of $\mathrm{Ann}(\sigma(u))$. After all such exclusions, we get the canonical system of generators (i.e., Groebner base) of the ideal $\mathrm{Ann}(\sigma(u))$ (see Section 16.A).

Denote $F_*^{(r)}(x) = F_*^{(1)}(x) \cdot \ldots \cdot F_*^{(r)}(x)$.

22.3. Corollary. *For any $s \in \overline{0, n-1}$ the polynomial $p^{n-s-1} \cdot F_*^{((p-1)(s+1))}(x)$ annihilates LRS $\sigma(u)$. In particular, $F_*^{((p-1)n)}(x)$ is a characteristic polynomial of $\sigma(u)$.* □

□ Proof of Theorem 22.2. The characteristic polynomial $x^T - e$ of the sequence $\sigma(u)$ is the product of pairwise coprime polynomials $(x-\theta)(x-\theta^2)\dots(x-\theta^T)$. Therefore, by 2.18,

$$\sigma(u)(i) = \sum_{k=1}^{T} c_k \theta^{ki}, \qquad i \geq 0, \tag{22.4}$$

where $c_k \in S$ are uniquely determined coefficients. By 2.19,

$$\operatorname{An}(\sigma(u)) = \prod_{k=1}^{T} \operatorname{An}(c_k \theta^{ki}) = \prod_{k=1}^{T} (x - \theta^k, p^{n-\|c_k\|}) \tag{22.5}$$

To find $\|c_k\|$, we write the LRS $\varkappa(u) \in L_{\overline{R}}(\overline{F}_*(x))$ in the form $\varkappa(u)(i) = \operatorname{tr}(\overline{c\theta}^i)$, $c \in S$, $i \geq 0$, $\operatorname{tr} = \operatorname{tr}_p^{p^m}$ (see 10.16). Let $i \geq 0$ and let $s \in \overline{0, p-1}$ be an integer such that $u(i) = se_p$. Then $\varkappa(u)(i) = s\overline{e} = \overline{\beta}_s = \operatorname{tr}(\overline{c\theta}^i)$, hence $\beta_s = (\operatorname{tr}(c\theta^i))^{p^{n-1}}$, and

$$\sigma(u)(i) = \sigma(se_p) = \Psi_\sigma(\beta_s) = \Psi_\sigma((\operatorname{tr}(c\theta^i))^{p^{n-1}}) = \sum_{l=1}^{p-1} \psi_l \cdot (c\theta^i + (c\theta^i)^p + \dots + (c\theta^i)^{p^{m-1}})^{p^{n-1}l}. \tag{22.6}$$

By Theorem 2.18, the coefficients of the binomial sequence $\{\theta^{ki}\}$ in (22.4) and (22.6) are equal. This leads to the relations

$$c_k \equiv \frac{(-p)^t \cdot c^k \cdot l!}{\nu_0(k)! \dots \nu_{m-1}(k)!} \cdot \psi_l \pmod{p^{t+\|\psi_l\|+1}}, \qquad 1 \leq k \leq T,$$

where l is the residue of $w(k)$ modulo $p-1$ in the set $\overline{1, p-1}$, $t = (w(k) - l)/(p-1)$, ψ_l is the coefficient of the polynomial $\Psi_\sigma(x)$, and $w(k)$, $\nu_r(k)$ are defined in Section 21. Therefore,

$$\|c_k\| = \min\{t + \|\psi_l\|, n\}.$$

Now the theorem follows from (22.5) and from the definition of $F_s(x)$. □

C. The rank of the sequence $\sigma(u)$.

22.4. Proposition [27]. *The rank of the LRS $\sigma(u)$ depends only on the representation σ and on the rank m of the LRS u over the field P_0 and can be evaluated by the formula* $\operatorname{rank}\sigma(u) = r(\sigma, m)$, *where*

$$r(\sigma, m) = \sum_{l=1}^{p-1} \left(\left\{ \begin{matrix} m \\ l \end{matrix} \right\} + \left\{ \begin{matrix} m \\ l + p - 1 \end{matrix} \right\} + \dots + \left\{ \begin{matrix} m \\ l + (n - 1 - \|\psi_l\|)(p-1) \end{matrix} \right\} \right). \tag{22.7}$$

If p, n are fixed, $m \to \infty$, then $r(\sigma, m) = \binom{m+t-1}{t}(1 + 0(\frac{1}{m}))$, where $t = (p-1)(n - \|\sigma\| - 1) + l(\sigma)$, $l(\sigma) = \max\{l \in \overline{1, p-1} \mid \|\psi_l\| = \|\sigma\|\}$.

□ By Theorem 22.2, $r(\sigma, m) = \deg F_{n-1}(x)$, and (22.7) follows from the definition of $F_{n-1}(x)$. The equality $\|\Psi_\sigma(x)\| = \|\sigma\|$ (see 22.1) shows that the definition of $l(\sigma)$ is correct. The asymptotic formula follows from (22.7) and from the relation $\left\{ \begin{matrix} m \\ r \end{matrix} \right\} = \binom{m+r-1}{r}\left(1 + 0\left(\frac{1}{m}\right)\right)$. □

22.5. Corollary. *If $p = 2$, then*

$$r(\sigma, m) = \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{n - \|\sigma\|}.$$ □

Now we are going to describe representations σ such that the $\operatorname{rank}\sigma(u)$ is maximal or minimal. Denote

$$R(m) = \left\{ \begin{matrix} m \\ 1 \end{matrix} \right\} + \left\{ \begin{matrix} m \\ 2 \end{matrix} \right\} + \left\{ \begin{matrix} m \\ 3 \end{matrix} \right\} + \dots + \left\{ \begin{matrix} m \\ (p-1)n \end{matrix} \right\},$$

$$r(m) = \left\{ \begin{matrix} m \\ 1 \end{matrix} \right\} + \left\{ \begin{matrix} m \\ p \end{matrix} \right\} + \left\{ \begin{matrix} m \\ 2p-1 \end{matrix} \right\} + \ldots + \left\{ \begin{matrix} m \\ 1+(p-1)(n-1) \end{matrix} \right\}.$$

22.6. Definition. A representation σ is called *maximal* if $r(\sigma, m) = R(m)$ for any $m \geq 1$, and *minimal*, if $\|\sigma\| = 0$ and $r(\sigma, m) = r(m)$ for any $m \geq 1$.

Note that if $\|\sigma\| = t > 0$, then $\sigma : P \to p^t R$, and σ may be considered as a representation over $\mathbf{Z}_{p^{n-t}}$ instead of $R = \mathbf{Z}_{p^n}$. This explains the condition $\|\sigma\| = 0$ in the definition of a minimal representation. Formula (22.7) implies

22.7. Proposition [27]. *If $m \geq 1$, then $r(\sigma, m) \leq R(m)$. A representation σ is maximal if and only if $\|\psi_1\| = \ldots = \|\psi_{p-1}\| = 0$.* □

For example, let $\sigma(0) = \sigma(2e_P) = \ldots = \sigma((p-1)e_P) = 0$, $\sigma(e_P) = (p-1)e$. Then $\Psi_\sigma(x) = x^{p-1} + \ldots + x$ and σ is maximal.

22.8. Proposition [27]. *If $\|\sigma\| = 0$, $m \geq 1$, then $r(\sigma, m) \geq r(m)$. The following conditions are equivalent:*

(a) *σ is minimal;*

(b) *coefficients of the polynomial $\Psi_\sigma(x)$ satisfy $\|\psi_1\| = 0$, $\psi_2 = \ldots = \psi_{p-1} = 0$;*

(c) *there exists an element $\psi_1 \in R \backslash pR$ such that $\sigma(te_P) = \psi_1 \beta_t$, $t \in \overline{0, p-1}$, where $\{\beta_0, \ldots, \beta_{p-1}\} = \Gamma(R)$.*

□ The inequality $r(\sigma, m) \geq r(m)$ and the equivalence (a) $\Leftrightarrow$ (b) follows from (22.7). The equivalence (b) $\Leftrightarrow$ (c) follows from 22.1. □

22.9. Definition. The representation $\sigma : P \to R$ of the form $\sigma(te_P) = \beta_t$, $t \in \overline{0, p-1}$, is called *p-adic*. The representation σ_p of the form $\sigma_p(te_P) = te$, $t \in \overline{0, p-1}$, is called *p-ary*.

D. The p-ary representation σ_p [28].

22.10. Lemma. *Let elements $b_t = \sigma(te_p)$ satisfy the conditions $b_t \equiv te \pmod p$, $t \in \overline{0, p-1}$. Then the polynomial $\Psi_\sigma(x)$ from 22.1 is compared with x modulo p. Let*

$$\chi(x) = x(x - b_1) \ldots (x - b_{p-1}) = x^p + h_{p-1}x^{p-1} + \ldots + h_1 x$$

and let $\Psi^*(x)$, $\chi^*(x)$ be polynomials of degree $p-1$ over R such that

$$\Psi_\sigma(x) = x + p\Psi^*(x), \qquad \chi(x) = x^p - x + p\chi^*(x).$$

(see also Lemma 19.10). *Then $\Psi^*(x) \equiv \chi^*(x) \pmod p$.*

□ Since $b_t \equiv te \equiv \beta_t \pmod p$, $b_t^p \equiv \beta_t \pmod{p^2}$ and

$$b_t = b_t + \chi(b_t) = b_t^p + p \cdot \chi^*(b_t) \equiv \beta_t + p \cdot \chi^*(\beta_t) \pmod{p^2}.$$

On the other hand, by Proposition 22.1,

$$b_t = \Psi_\sigma(\beta_t) = \beta_t + p \cdot \Psi^*(\beta_t), \qquad t \in \overline{0, p-1},$$

and our lemma follows from the uniqueness of the polynomial $\Psi_\sigma(x)$. □

Denote $\mathrm{r}_k(p) = 1^k + 2^k + \ldots + (p-1)^k$. Then

$$p | \mathrm{r}_k(p), \qquad 1 \leq k \leq p-2; \qquad p^2 \nmid \mathrm{r}_1(p); \qquad p^2 | \mathrm{r}_{2a+1}(p), \qquad 3 \leq 2a+1 \leq p-2.$$

22.11. Definition. A pair $(p, 2a)$, $2 \leq 2a \leq p-3$, is called *regular* if $p^2 \nmid \mathrm{r}_{2a}(p)$. Otherwise, this pair is called *irregular* [6]. The number of irregular pairs is called the *index of irregularity of p* and is denoted by $ii(p)$. If $ii(p) = 0$, then the prime number p is called *regular*.

For example, there are three irregular $p < 100$, namely 37, 59, and 67. Our definition of a regular number is equivalent to other definitions; see [6]. Note that a pair $(p, 2a)$ is regular if and only if the numerator of the Bernoulli number B_{2a} is not divisible by p. Denote

$$Q_1 = \sum_{t=0}^{n-1} \left\{ \begin{matrix} m \\ 1+(p-1)t \end{matrix} \right\}, \qquad Q_l = \sum_{t=0}^{n-2} \left\{ \begin{matrix} m \\ l+(p-1)t \end{matrix} \right\}, \qquad l \in \overline{2, p-1}.$$

22.12. Theorem [28]. *Let u be an LRS of maximal period of rank m over the field $P = GF(p)$, $p \geq 3$. Then*

$$Q_1 + \sum_{l \in \mathcal{L}} Q_l + Q_{p-1} \leq \operatorname{rank} \sigma_p(u) \leq \sum_{\substack{1 \leq l \leq p-2 \\ l \text{ is odd}}} Q_l + Q_{p-1}, \tag{22.8}$$

where $\mathcal{L} = \{l \in \overline{3, p-2} \mid l \text{ is odd}, (p, p-l) \text{ is a regular pair}\}$.

□ Since $\Psi_{\sigma_p}(x) \equiv x \pmod p$,

$$\psi_2 \equiv \psi_3 \equiv \ldots \equiv \psi_{p-1} \equiv 0 \pmod p.$$

Using (22.2), it is possible to prove that

$$\psi_2 = \psi_4 = \ldots = \psi_{p-3} = 0, \qquad \psi_{p-1} = \frac{1}{2} \cdot p.$$

The second inequality in (22.8) follows from these relations and from (22.7). Let $\mathbf{s}_k(p) = \mathbf{s}_k(1, 2, \ldots, p-1)$, where $\mathbf{s}_k(x_1, \ldots, x_{p-1})$ is the symmetric function in $p-1$ variables of degree k. Applying Lemma 22.10 and the Newton formulas, which connect $\mathbf{s}_k$ and $\mathbf{r}_k$, we get

$$\psi_l \equiv h_l = (-1)^{p-l} \mathbf{s}_{p-l}(p) \equiv \frac{1}{l} \cdot \mathbf{r}_{p-l}(p) \pmod{p^2}, \tag{22.9}$$

$l \in \overline{2, p-1}$. Therefore, $\|\psi_l\| = 1$ for $l \in \mathcal{L}$, and $\|\psi_1\| = 0$, $\|\psi_{p-1}\| = 1$. The first inequality in (22.8) follows from these relations and from (22.7). □

22.13. Corollary. *Let $p \geq 3$. Then*

$$\operatorname{rank} \sigma_p(u) = \sum_{\substack{1 \leq l \leq p-2 \\ l \text{ is odd}}} Q_l + Q_{p-1}$$

if and only if p is a prime regular number. □

22.14. Corollary. *If $p = 2$, then the p-ary representation σ_p is minimal and maximal. If $p = 3$, then σ_p is maximal. If $p \geq 5$, then σ_p is not minimal and not maximal.* □

22.15. Examples. We give the values of the ranks of sequences $\sigma(u)$ for minimal, p-ary, and maximal representation σ. The last column contains the period $T = p^m - 1$ of $\sigma(u)$.

p	n	m	$r(m)$	$r(\sigma_p, m)$	$R(m)$	T
2	4	11	205	205	205	561
2	8	11	1980	1980	1980	2047
5	4	11	$7.6 \cdot 10^5$	$1.5 \cdot 10^6$	$6 \cdot 10^7$	$4.9 \cdot 10^7$
5	8	11	$1.2 \cdot 10^7$	$3.5 \cdot 10^7$	$4.8 \cdot 10^7$	$4.9 \cdot 10^7$
11	4	5	$1.5 \cdot 10^4$	$8.2 \cdot 10^4$	$1.59 \cdot 10^5$	$1.61 \cdot 10^5$
11	8	5	$1.6 \cdot 10^4$	$9.7 \cdot 10^4$	T	$1.61 \cdot 10^5$

23. The First Coordinate Sequences of MP-Recurrences over a Galois Ring

Let $R = GR(q^n, p^n)$, $q = p^r$, $\mathcal{B} = \{b_0 = 0, b_1, \ldots, b_{q-1}\}$ be the coordinate set of the ring R, $\Gamma(R) = \{\beta_0 = 0, \beta_1, \ldots, \beta_{q-1}\}$ be the p-adic coordinate set (see Section 19.B). We suppose that the elements of all coordinate sets are enumerated in such a way that $b_t \equiv \beta_t \pmod p$, $t \in \overline{0, q-1}$, and if $R = \mathbb{Z}_{p^n}$, then $b_t \equiv te \pmod p$, $t \in \overline{0, p-1}$.

By Proposition 22.1, there exists the uniquely defined polynomial

$$\Psi(x) = \Psi_{\mathcal{B}}(x) = \psi_{q-1} x^{q-1} + \ldots + \psi_1 x \in R[x]$$

such that $\Psi_{\mathcal{B}}(\beta_t) = b_t$, $t \in \overline{0, q-1}$. Let

$$\chi_{\mathcal{B}}(x) = x(x-b_1)\dots(x-b_{q-1}) = \sum h_l x^l$$

be the characteristic polynomial of the coordinate set $\mathcal{B}$.

23.1. Lemma. *If $a \in R$, then $\gamma_0(a) = a^{q^{n-1}}$, $\gamma_0^{\mathcal{B}}(a) = \Psi_{\mathcal{B}}(\gamma_0(a))$.*

□ It is easy to prove by induction that $\gamma_0(a) \equiv a^{q^{k-1}} \pmod{p^k}$. □

Let $G(x)$ be a polynomial of maximal period of degree $m \geq 2$ over R, ξ be a root of $G(x)$, $\xi \in Q = GR(q^{mn}, p^n) > R$ and $T = q^m - 1$. As in Section 21, we define the polynomials

$$\overline{G}^{(l)}(x) = \prod\{x - \overline{\xi}^k \mid k \in \overline{1,T},\ W(k) = l,\ l = N_0(k) \dot{+} \dots \dot{+} N_{m-1}(k)\},$$

where $l \in \overline{1, q-1}$, and

$$\overline{G}^{(q)}(x) = \prod\{x - \overline{\xi}^d \mid 1 \leq d \leq q^m - 1,\ W(d) = q,\ (q/p) | N_s(d) \text{ for } s \geq 0\}$$

of degree $\deg \overline{G}^{(q)}(x) = \binom{m+p-1}{p} - m$. The polynomials $\overline{G}^{(l)}(x)$, $l \in \overline{1, q}$, are pairwise coprime and belong to $\overline{R}[x]$. Denote

$$\mathcal{L} = \mathcal{L}_{\mathcal{B}} = \{l \in \overline{2, q-1} \mid \psi_l \not\equiv \pmod{p^2}\} = \{l \in \overline{2, q-1} \mid h_l \not\equiv 0 \pmod{p^2}\}.$$

The last equality follows from Lemma 22.10.

23.2. Theorem [28, 33]. *Let u be an LRS of maximal period over a Galois ring $R = GR(q^n, p^n)$, $q = p^r$, with minimal polynomial $G(x)$ of degree m, and let $u_1 = \gamma_1^{\mathcal{B}}(u)$ be the first coordinate sequence of u in the coordinate set $\mathcal{B}$. Then*

$$M_{\overline{u}_1}(x) = \overline{G}(x)^2 \cdot \prod_{l \in \mathcal{L}} \overline{G}^{(l)}(x) \cdot \overline{G}^{(q)}(x),$$

$$\operatorname{rank} u_1 = m + \sum_{l \in \mathcal{L}} \prod_{s=0}^{r-1} \binom{m + \nu_s(l) - 1}{\nu_s(l)} + \binom{m+p-1}{p}.$$

□ Let $\Psi_{\mathcal{B}}(x) = \psi_1 x + p\Phi(x)$. By Lemma 23.1,

$$u_0 = \gamma_0^{\mathcal{B}}(u) \equiv \Psi_{\mathcal{B}}(u^q) \equiv \psi_1 u^q + p\Phi(u) \pmod{p^2}.$$

It follows that $pu_1 \equiv u - u_0 \equiv u - \psi_1 u^q - p\Phi(u) \pmod{p^2}$. Let y be a sequence over R such that $u - \psi_1 u^q \equiv py \pmod{p^2}$. Then $\overline{u}_1 = \overline{y} - \overline{\Phi}(\overline{u})$. By Theorem 21.1, the minimal polynomial of the LRS $\overline{\Phi}(\overline{u})$ is equal to $\prod_{l \in \mathcal{L}} \overline{G}^{(l)}(x)$. If we represent u by the trace function, $u(i) = \operatorname{Tr}_R^S(a\xi^i)$ (Theorem 19.3) and investigate the analytical representation of y, we get $M_{\overline{y}}(x) = \overline{G}(x)^2 \overline{G}^{(q)}(x)$. It follows that the minimal polynomials of the sequences $\overline{y}$ and $\overline{\Phi}(\overline{u})$ are coprime. Therefore, the minimal polynomial of $\overline{u}_1$ is equal to the product of these polynomials. □

In particular, if $\gamma_1(u)$ is the first coordinate sequence of the LRS u in the p-adic coordinate set, then $\operatorname{rank} \gamma_1(u) = m + \binom{m+p-1}{p}$. This result was proved by A. Nechaev for $p = 2$ in 1982 and by A. Kuzmin for $p \geq 3$ in 1986 (see [123]).

23.3. Corollary. *The following inequalities hold:*

$$m + \binom{m+p-1}{p} \leq \operatorname{rank} \gamma_1^{\mathcal{B}}(u) \leq \binom{m+p-1}{p-1}^r + \binom{m+p-1}{p} - 1. \quad \square$$

23.4. Corollary. *If $R = \mathbb{Z}_{2^n}$, then the minimal polynomial of the sequence $\overline{\gamma}_1^{\mathcal{B}}(u)$ is equal to $\overline{G}(x)^2 \overline{G}^{(2)}(x)$, and $\operatorname{rank} \gamma_1^{\mathcal{B}}(u) = m(m+3)/2$.* □

We call a coordinate set $\mathcal{B}$ *minimal* (*maximal*) if the first (second) inequality of Corollary 23.3 becomes an equality. It follows from Theorem 23.2 that $\mathcal{B}$ is minimal if and only if $\mathcal{L} = \varnothing$, i.e., $\Psi(x) \equiv \psi_1 x \pmod{p^2}$, i.e., if $\mathcal{B} \equiv \psi_1 \Gamma(R) \pmod{p^2}$ for some $\psi_1 \in e + pR$. For example, the p-adic coordinate set $\Gamma(R)$ is minimal. On the other hand, $\mathcal{B}$ is maximal if and only if $\mathcal{L} = \overline{2, q-2}$. For example, $\mathcal{B} = \{0, \beta_1 + pe, \beta_2, \dots, \beta_{q-1}\}$ is maximal.

23.5. Theorem [28, 33]. *Let $R = \mathbf{Z}_{p^n}$, u be an LRS of maximal period over R with minimal polynomial $G(x)$ of degree m, and let $\delta_1(u)$ be the first coordinate sequence of u in the p-ary coordinate set $\mathcal{B}_p$. Then*

$$M_{\delta_1(u)} = \overline{G}(x)^2 \cdot \prod_l \overline{G}^{(l)}(x) \cdot \overline{G}^{(p-1)}(x) \cdot \overline{G}^{(p)}(x),$$

$$\operatorname{rank} \delta_1(u) = m + \sum_l \binom{m+l-1}{l} + \binom{m+p-2}{p-1} + \binom{m+p-1}{p},$$

where the product and the sum are taken over odd numbers $l \in \overline{3, p-2}$ such that $(p, p-l)$ is a regular pair.

□ This theorem follows from 23.2 and (22.9). □

The tables of irregular pairs can be found, for example, in [6].

23.6. Corollary. *The p-ary coordinate set is minimal for $p = 2$, maximal for $p = 3$, and not minimal and not maximal for $p \geq 5$.* □

23.7. Corollary. *Under the conditions of Theorem* 23.5,

$$\operatorname{rank} \delta_1(u) \leq m + \sum_{\substack{3 \leq l \leq p-2 \\ l \text{ is odd}}} \binom{m+l-1}{l} + \binom{m+p-2}{p-1} + \binom{m+p-1}{p}, \tag{23.1}$$

and this inequality becomes an equality if and only if p is a prime regular number. □

The estimation (23.1) was proved by A. Kuzmin [123]. V. Kurakin [28, 33] determined when the inequality (23.1) becomes an equality.

By formulas for the sums of squares and quadrics,

$$\mathbf{r}_2(p) = \frac{1}{6} \cdot p(p-1)(2p-1), \qquad \mathbf{r}_4(p) = \frac{1}{30} \cdot p(2p-1)(3p^2 - 3p - 1).$$

Since these expressions are not divisible by p^2, the pairs $(p, 2)$, $(p, 4)$ for $p \geq 7$ are regular. This implies

23.8. Corollary. *Under the conditions of Theorem* 23.5, *if $p \geq 7$, then*

$$\operatorname{rank} \delta_1(u) \geq m + \sum_{\substack{3 \leq l \leq p-2i-6 \\ l \text{ is odd}}} \binom{m+l-1}{l} + \binom{m+p-5}{p-4} + \binom{m+p-3}{p-2} + \binom{m+p-2}{p-1} + \binom{m+p-1}{p},$$

where $i = ii(p)$ is the index of irregularity of p. In particular,

$$\operatorname{rank} \delta_1(u) \geq m + \binom{m+p-5}{p-4} + \binom{m+p-3}{p-2} + \binom{m+p-2}{p-1} + \binom{m+p-1}{p}. \quad \square$$

The formulas of the 6th, 8th, etc. powers (or the tables of the Bernoulli numbers) make it possible to find other regular pairs and to make more precise estimations of $\operatorname{rank} \delta_1(u)$.

Note that $ii(p) \ll p$. The tables in [6] show that if $p < 125,000$, then $ii(p) \leq 5$. So, for $p < 125,000$, the rank of the sequence $\delta_1(u)$ is very close to the upper estimate from Corollary 23.7. The same is also true for the upper estimate from Theorem 22.12.

23.9. Example. Let $R = \mathbf{Z}_{p^n}$, $p = 5$, $m = 11$. Then the ranks of the first coordinate sequences of LRS u in minimal, p-ary, and maximal coordinate sets are equal to

$$\operatorname{rank} \gamma_1(u) = 3014, \qquad \operatorname{rank} \delta_1(u) = 4301, \qquad \operatorname{rank} \gamma_1^{\mathcal{B}\max}(u) = 4367$$

respectively. If $p = 11$, $m = 5$, then the ranks are equal to 1370, 3577, and 4367 correspondingly.

24. Coordinate Sequences of MP-Recurrences over $\mathbf{Z}_{p^n}$

A. The main results. Let u be an LRS of maximal period over the ring $R = \mathbf{Z}_{p^n}$ with the minimal polynomial $G(x)$ of degree $m \geq 2$. Denote by $u_s = \gamma_s^{\mathcal{B}}(u)$, $s \in \overline{0, n-1}$, the s-th coordinate sequence of u in the arbitrary coordinate set $\mathcal{B}$ of the ring R (note that we have used another notation in Section 19.B,C; see (19.13)). Let ξ be a root of $G(x)$, ξ belong to the Galois extension $Q = GR(p^{mn}, p^n)$ of the ring R, and denote

$$\overline{G}^{(N)}(x) = \prod\{x - \overline{\xi}^d \mid d \in \overline{1,\tau},\ w(d) = N\}, \qquad N \geq 1, \qquad \tau = p^m - 1.$$

It is easy to see that $\deg \overline{G}^{(N)}(x) = \left\{ \begin{matrix} m \\ N \end{matrix} \right\}$ (see (22.3)). For $k, l \in \mathbf{N}$ denote

$$b(k,0) = k,$$

$$b(k,l) = 0, \text{ if } k < pl,$$

and in other cases

$$b(k,l) = k - pl + \begin{cases} \lambda, & \text{if } p \geq 3, \text{ where } \lambda \in \overline{1,p-1},\ \lambda \equiv l \pmod{p-1}, \\ 1, & \text{if } p = 2,\ l \text{ is even or } l = 1, \\ 2, & \text{if } p = 2,\ l \text{ is odd } l \geq 3. \end{cases}$$

24.1. Theorem [26, 30]. *The polynomial*

$$\overline{\mathcal{H}}(x) = \prod_{l=0}^{p^{s-1}} \Big(\prod_{N=b(l+1)+1}^{b(l)} \overline{G}^{(N)}(x) \Big)^{l+1}, \tag{24.1}$$

where $b(l) = b(p^s, l)$, is a characteristic polynomial of the sequence u_s, and

$$\operatorname{rank} u_s \leq \sum_{l=0}^{p^{s-1}} (l+1) \cdot \sum_{N=b(l+1)+1}^{b(l)} \left\{ \begin{matrix} m \\ N \end{matrix} \right\}. \tag{24.2}$$

In some special cases these estimations can be strengthened.

24.2. Theorem [30]. *Let $u_s = \gamma_s(u)$, $s \in \overline{0, n-1}$, be the coordinate sequences of u in the p-adic coordinate set. Then Theorem* 24.1 *remains true if the index N in the formulas* (24.1), (24.2) *satisfies the condition $N \equiv 1 \pmod{p-1}$.*

24.3. Theorem (A. Kuzmin [123]). *Let $u_s = \delta_s(u)$, $s \in \overline{0, n-1}$, be the coordinate sequences of u in the p-ary coordinate set, $p \geq 5$. Then Theorem* 24.1 *remains true if the index N in the formulas* (24.1), (24.2) *satisfies the condition $N \equiv 1 \pmod 2$ or $N \equiv 0 \pmod{p-1}$.*

Let $\Phi^{(s)}(x) \in R[x]$ be the polynomials from Lemma 19.9 and $u^{(s)} = \Phi^{(s)}(x)u$ be the s-th derivative sequence of u (see Section 19.B). Denote $\mathcal{L}_0 = \{0, p^{s-1}\}$,

$$\mathcal{L}_t = \{l \mid 1 \leq l \leq p^{s-1} - 1,\ l \equiv t \pmod{p-1}\}, \qquad t \in \overline{1,p-1}, \text{ if } p \geq 3,$$

$$\mathcal{L}_1 = \{1\} \cup \{l \mid 2 \leq l \leq 2^{s-1} - 2,\ l \text{ is even},\ 2^s - 2l + 1 < m\}, \text{ if } p = 2,$$

$$\mathcal{L}_2 = \{l \mid 3 \leq l \leq 2^{s-1} - 1,\ l \text{ is odd},\ 2^s - 2l + 2 < m\}, \text{ if } p = 2,$$

$$\mathcal{R}_t = \sum_{l \in \mathcal{L}_t} (l+1) \cdot \left\{ \begin{matrix} m \\ b(l) \end{matrix} \right\}, \text{ where } b(l) = b(p^s, l).$$

24.4. Theorem [23, 30]. (a) $\operatorname{rank} u_s \geq \mathcal{R}_0$.

(b) *If polynomial $G(x)$ is chosen in such way that the polynomials $\overline{\Phi}^{(1)}(x)^{p^\alpha}$, $\alpha \in \overline{0, m-1}$, are linearly independent over the field $\overline{R}$ modulo the polynomial $\overline{G}(x)$, then*

$$\operatorname{rank} u_s \geq \mathcal{R}_0 + \mathcal{R}_1 + \frac{m}{m+p} \cdot \mathcal{R}_2.$$

(c) *If the linear rank of the system of polynomials* $\operatorname{Res}(\overline{\Phi}^{(2)}(x)^\alpha / \overline{G}(x))$, $\alpha \in \overline{0, m-1}$, *is equal to $h > p$, then*

$$\operatorname{rank} u_s \geq \mathcal{R}_0 + \frac{h-p}{h} \cdot \mathcal{R}_1.$$

(d) *If* $\deg \overline{\Phi}^{(2)}(x) = 0$ (*i.e.*, $h = 1$), *then*

$$\operatorname{rank} u_s \geq \mathcal{R}_0 + \mathcal{R}_1 + \ldots + \mathcal{R}_{p-1}.$$

Note that, by (19.20), if $p \geq 3$, then $\overline{\Phi}^{(2)}(x) = \overline{\Phi}^{(1)}(x)$.

24.5. Remark. Theorems 24.1 and 24.4 complete the following series of earlier results. For example, under the condition (b) of Theorem 24.4, if $p = 2$, $s \in \overline{3, n-1}$, then

$$\operatorname{rank} \delta_s(u) \geq (2^{s-1}+1)m + \left(\binom{m}{4} 2^{s-1}\right) + \sum_{k=2}^{s-2} (2^{s-1} - 2^k + 1) \binom{m}{2^{k+1}+1} + \binom{m}{2^s}, \tag{24.3}$$

and if $p \geq 3$, $s \in \overline{2, n-1}$, then

$$\operatorname{rank} \delta_s(u) \geq (p^{s-1}+1)m + \sum_{k=2}^{t-2} (p^{s-1} - p^k + 1) \left\{ \begin{matrix} m \\ p^{k+1} + p - 1 \end{matrix} \right\} + \left\{ \begin{matrix} m \\ p^s \end{matrix} \right\}. \tag{24.4}$$

The presence of the summand in (24.3), noted by $*$, has not been proved in the general case, but the hypothesis was confirmed for $m \leq 14$ and $m = 20$. The lower estimations of $\operatorname{rank} \delta_s(u)$ for $p = 2$ are also given in [95]; these estimations do not contain the first and second summands of (24.3). Estimations (24.3) were obtained by A. Nechaev in 1982 in connection with the investigation of the function $\operatorname{Tr}(x)$ (see [47] and Section 19.C). Estimations (24.4) were obtained by A. Kuzmin in 1986. Theorems 24.1 and 24.4 were proved by A. Kuzmin for $\mathcal{B} = \mathcal{B}_p$ and by V. Kurakin for the arbitrary coordinate set $\mathcal{B}$ [23, 26, 30].

B. Methods of proofs. The method of sections.

24.6. Lemma. *Let y be a linear recurrence over a field P, $b(x) \in P[x]$, $z = b(x)y$. If an element γ of some expansion of P is a root of $M_z(x)$ of multiplicity $k > 0$ and a root of $b(x)$ of multiplicity $l \geq 0$, then γ is a root of $M_y(x)$ of multiplicity $k + l$.*

□ $M_z(x) = M_y(x)/(b(x), M_y(x))$. □

In what follows, an element which is not a root of a polynomial is called a root of multiplicity 0. We say that the sequence $z = b(x)y$ is the *section* of the sequence y by the polynomial $b(x)$. The method of sections consists in the following. We multiply a sequence y on some (well-chosen) polynomial $b(x)$. Then information about the roots of the polynomial $M_z(x)$ gives us some information about the roots of the polynomial $M_y(x)$.

Denote $\tau = p^m - 1$, $\tau_s = \tau p^s$, $s = \overline{0, n-1}$.

24.7. Proposition. *If $s \in \overline{0, n-1}$, then $T(u_s) = \tau_s$.*

□ Since $T(u \bmod p^{t+1}) | \tau_t$, by 6.3 and 17.3, $T(u_s) | \tau_s$ and

$$(x^{\tau_{s-1}} - e)u \equiv (x^{\tau_{s-1}} - e)p^s u_s \pmod{p^{s+1}}.$$

On the other hand, $(x^{\tau_{s-1}} - e)u = p^s u^{(s)}$ (by the definition of $u^{(s)}$). Hence

$$(x^{\tau_{s-1}} - e)u_s \equiv u^{(s)} \pmod{p}. \tag{24.5}$$

Therefore, $T(\overline{u}^{(s)}) = \tau | T(u_s)$, $T(u_s) / \tau_{s-1} = \tau p^{s-1}$ and, as was noted above, $T(u_s) | \tau_s = \tau p^s$. It follows then that $T(u_s) = \tau_s$. □

The polynomial complexity of a sequence. Consider a more general situation. Let R be a commutative Artinian principal ideal ring with residue field $\overline{R} = R/\mathfrak{N}(R)$, v be an LRS over R, $F(x) \in R[x]$ be a monic polynomial, and let Q be a Galois extension of R such that $\overline{F}(x) = (x - \overline{\theta}_1)^{a_1} \dots (x - \overline{\theta}_N)^{a_N}$ for some elements $\theta_1, \dots, \theta_N \in Q$, pairwise distinct modulo radical $\mathfrak{N}(Q)$. Let $F^{\langle r \rangle}(x)$ be monic polynomial over Q such that

$$\overline{F}^{\langle r \rangle}(x) = \text{ l.c.m.}[x - \overline{\theta}_{i_1} \dots \overline{\theta}_{i_k} | \ 1 \le k \le r, \ 1 \le i_1, \dots, i_k \le N].$$

Then the following conditions are equivalent:

(1) v is the sum of binomial sequences (see 2.15) with coefficients in Q such that the roots of these binomial sequences are products of not more than r elements from $\{\theta_1, \dots, \theta_N\}$;

(2) some power of the polynomial $F^{\langle r \rangle}(x)$ annihilates the LRS v;

24.8. Definition. The least $r \in \mathbf{N}$ such that the conditions (1), (2) are satisfied is called the *polynomial complexity* $\rho(F|v)$ of the sequence v with respect to the polynomial $F(x)$; if there does not exist such an integer r, we define $\rho(F|v) = \infty$. We also set $\rho(F|0) = 0$.

It is clear that if $\overline{F}(x) = \overline{H}(x)$, then $\rho(F|v) = \rho(H|v)$; but if $\overline{v} = \overline{w}$, then not necessarily $\rho(F|v) = \rho(F|w)$. Polynomial complexity is defined, in particular, for sequences over a field. Obviously, $\rho(\overline{F}|\overline{v}) \le \rho(F|v)$.

24.9. Example. If $v \in L_R(F) \cdot \dots \cdot L_R(F)$ (r times), then $\rho(F|v) \le r$. The converse is not true. For example, if $\rho(F|v) = 1$, then it is not necessary that $v \in L_R(F)$. We can only state that $v \in L_R(F^n)$ for some n (in particular, for $n = \operatorname{ind} \mathfrak{N}(R)$, the index of nilpotency of the radical $\mathfrak{N}(R)$).

The following properties are direct consequences of Definition 24.8:

$$\rho(F|v + w) \le \max\{\rho(F|v), \rho(F|w)\},$$

$$\rho(F|vw) \le \rho(F|v) + \rho(F|w). \tag{24.6}$$

The polynomial complexity of the sequences u_s. Now we return to the notations introduced at the beginning of the section. Let $\xi_0 = \gamma_0(\xi) \in \Gamma(Q)$, where $\Gamma(Q)$ is the p-adic coordinate set of the ring $Q = GR(p^{mn}, p^n)$ (see Section 19.B). Since the roots of the polynomial $\overline{G}(x)$ are $\overline{\xi}, \overline{\xi}^p, \dots, \overline{\xi}^{p^{m-1}}$, then $\rho(G|v) \le r$ if and only if the sequence $v \in Q^{\langle 1 \rangle}$ is the sum of binomial sequences with roots ξ^d (or ξ_0^d), where $d \in \overline{1, \tau}$, $w(d) \le r$, and r is the least natural number with this property (here $w(d)$ is the p-ary weight of d; see Section 21). For $v \in Q^{\langle 1 \rangle}$ we set

$$\rho(v) = \rho(G|v); \qquad \rho(\overline{v}) = \rho(\overline{G}|\overline{v}); \qquad \rho(v \bmod p^t) = \rho(p^{n-t}v);$$

$$v_{[s]} = v_s + pv_{s+1} + \dots + p^{n-s+1}v_{n-1} \text{ (where } v_s = \gamma_s^{\mathcal{B}}(v)), \qquad s \in \overline{0, n-1}.$$

24.10. Lemma. *For $s \in \overline{0, n-1}$, we have $\rho(\overline{u}_s) \le p^s$.*

□ By induction on s we get a stronger property:

$$\rho(\overline{u}_{[s]}) \le p^s; \qquad \rho(u_{[s]} \bmod p^{t+1}) < p^{s+t}, \qquad t \ge 1. \tag{24.7}$$

Since, by Theorem 19.3, $u_{[0]}(i) = u(i) = \operatorname{Tr}_R^Q(a\xi^i)$, we have $\rho(u_{[0]}) = 1$, so that (24.7) is proved for $s = 0$. Let (24.7) be true for some $s \in \overline{0, n-2}$. Then $u_{[s]} \equiv y \pmod p$, $\rho(y) \le p^s$. By Lemma 23.1,

$$pu_{[s+1]} = u_{[s]} - u_s = u_{[s]} - \gamma_0^{\mathcal{B}}(y) = u_{[s]} - \Psi_{\mathcal{B}}(y^{p^{n-1}}).$$

Let $\Psi^*(x)$ be a polynomial of degree $\le p-1$ such that $\Psi_{\mathcal{B}}(x) = x + p\Psi^*(x)$ (see Lemma 22.10). Then

$$pu_{[s+1]} = u_{[s]} - y^{p^{n-1}} - p\Psi^*(y^{p^{n-1}}). \tag{24.8}$$

it follows then that

$$pu_{[s+1]} \equiv u_{[s]} - y^p - p\Psi^*(y) \pmod{p^2}.$$

By the induction assumption, $\rho(u_{[s]} \bmod p^2) < p^{s+1}$. By (24.6), $\rho(y^l) \le \rho(y)l \le p^s l \le p^{s+1}$ for $l \le p$. Hence $\rho(pu_{[s+1]} \bmod p^2) \le p^{s+1}$, i.e., $\rho(\overline{u}_{[s+1]}) \le p^{s+1}$. From (24.8) it follows that

$$pu_{[s+1]} \equiv u_{[s]} - y^{p^{t+1}} - p\Psi^*(y^{p^t}) \pmod{p^{t+2}}, \qquad t \ge 1.$$

Using the induction assumption and (24.6), we get $\rho(pu_{[s+1]} \bmod p^{t+2}) < p^{s+t+1}$, i.e., $\rho(u_{[s+1]} \bmod p^{t+1}) < p^{s+1+t}$, $t \ge 1$. □

The method of extraction of the main term. By Lemma 24.10, $\overline{u}_s$ is the sum of binomial sequences with roots of the form ξ^d, $d \in \overline{1,\tau}$, $w(d) \le p^s$. Therefore, $\overline{u}_s = \overline{y} + \overline{\eta}$, where $\overline{y}$ is the sum of binomial sequences for which $w(d) = p^s$ and $\overline{\eta}$ is the sum of the rest of the binomial sequences, $\rho(\overline{\eta}) < p^s$. We call the sequence $\overline{y}$ the (*formal*) *main term* of the sequence $\overline{u}_s$ (it is possible that $\overline{y} = 0$). In this section we describe its analytical representation.

By Theorem 19.3, there exists a constant $a \in Q^*$ such that $u(i) = \operatorname{Tr}_R^Q(a\xi^i)$, $i \ge 0$. For $N \ge 0$, define the sequences $y[N]$ over the ring Q by

$$y[N](i) = \sum_{\substack{1 \le d \le \tau \\ w(d) = N}} E(d)\xi_0^{di}, \qquad i \ge 0,$$

where

$$E(d) = E_a(d) = \frac{a^d}{\nu_0(d)! \cdot \nu_1(d)! \cdot \ldots \cdot \nu_{m-1}(d)!}, \qquad d = \sum p^s \nu_s(d).$$

In particular, $y[0] = (e, e, e, \ldots)$. This definition gives the analytical representation of the sequence $y[N]$. It follows from the definition that $\rho(y[N]) \le N$ for $N \ge 0$.

24.11. Proposition. *If M, $N \in \mathbf{N}_0$, then*

$$y[M] \cdot y[N] \underset{p}{\equiv} \binom{M+N}{M} \cdot y[M+N] + \eta, \text{ where } \rho(\eta) < M + N.$$

If M, N are divisible on p, or if $M + N < p$, then this comparison is true modulo p^2. □

24.12. Theorem. *For $s \in \overline{0, n-1}$, we have*

$$u_s \equiv y[p^s] + \eta \pmod{p}, \text{ where } \rho(y[p^s]) \le p^s, \qquad \rho(\eta) < p^s.$$

Note that if the coordinate sequences of u are taken in the p-ary coordinate set, then this result follows from (19.43).

□ If $s = 0$, then our theorem follows from the relations

$$u_0(i) \underset{p}{\equiv} u(i) = \operatorname{Tr}_R^Q(a\xi^i) \underset{p}{\equiv} \operatorname{tr}_1^m(a\xi^i) = y[1](i). \tag{24.9}$$

Let the theorem be true for some $s \in \overline{0, n-2}$. By Lemma 23.1,

$$u_s \equiv \Psi_B((y[p^s] + \eta)^p) \equiv (y[p^s] + \eta)^p + p\Psi^*(y[p^s] + \eta) \pmod{p^2}.$$

Therefore, by (24.6), $u_s \equiv y[p^s]^p + \zeta \pmod{p^2}$, $\rho(\zeta) < p^{s+1}$, and by Proposition 24.11, $u_s \equiv (-p) \cdot y[p^{s+1}] + \pi \pmod{p^2}$, where $\rho(\pi) < p^{s+1}$. Hence

$$pu_{s+1} \equiv pu_{[s+1]} = u_{[s]} - u_s = u_{[s]} + p \cdot y[p^{s+1}] - \pi \pmod{p^2}.$$

Now the theorem for the parameter s+1 follows from (24.7) (for $t = 1$). □

Thus, we have extracted the main term $y[p^s]$ of the sequence u_s. Since $y[p^s] = 0$ for $p^s > m(p-1)$, Theorem 24.12 gives some information on the sequence u_s only for small s. To get more information on u_s, we use the method of sections.

The formal polynomial complexity. We say that a sequence $y \in R^{(1)}$ *is expressed via the sequences* $y_1, \dots, y_t \in R^{(1)}$ if y is the sum of products of these sequences with coefficients from R. Denote

$$\mathfrak{M}_0 = \{v_s |\ v \in L_R(G),\ \overline{v} \neq \overline{0},\ s \in \overline{0, n-1}\} \cup \{0\},$$

$$\mathfrak{M} = \{cy_1 \dots y_t |\ c \in R,\ t \in \mathbf{N},\ y_1, \dots, y_t \in \mathfrak{M}_0\}.$$

We define the *formal polynomial complexity* of sequences from $\mathfrak{M}_0$ by the following relations:

$$\tilde{\rho}(0) = 0, \qquad \tilde{\rho}(v_s) = p^s, \qquad s \in \overline{0, n-1}.$$

A sequence $y \in \mathfrak{M} \backslash 0$ can be written in the form

$$y = c \cdot y_1^{a_1} \dots y_t^{a_t}, \qquad c \in R \backslash 0, \qquad a_1, \dots, a_t \geq 1,$$

where $y_1, \dots, y_t$ are distinct sequences from $\mathfrak{M}_0$. Let

$$\tilde{\rho}(y) = \tilde{\rho}(y_1)\lambda_1 + \dots + \tilde{\rho}(y_t)\lambda_t,$$

where $\lambda_j \in \overline{1, p-1}$, $\lambda_j \equiv a_j \pmod{p-1}$. This definition is constructed in such a way that if $y, y' \in \mathfrak{M}$, $y \equiv y' \pmod{p}$, then $\tilde{\rho}(y) = \tilde{\rho}(y')$. For example, $\tilde{\rho}(u_s^p) = \tilde{\rho}(u_s) = p^s$.

We say that the *formal polynomial complexity* of a sequence $y \in R^{(1)}$ is equal to N, $\tilde{\rho}(y) = N$, if y is the sum of sequences from $\mathfrak{M}$ of the formal polynomial complexities $\leq N$, and N is the least nonnegative integer with this property. We write $\tilde{\rho}(y) = \infty$ if there exists no such N. The relation $\tilde{\rho}(y) \leq 0$ means, by definition, that $y = 0$. It follows from the definition that

$$\tilde{\rho}(y_1 + y_2) \leq \max(\tilde{\rho}(y_1), \tilde{\rho}(y_2)), \qquad \tilde{\rho}(y_1 y_2) \leq \tilde{\rho}(y_1) + \tilde{\rho}(y_2). \tag{24.10}$$

By Lemma 24.10, for any sequence $y \in R^{(1)}$,

$$\rho(\overline{y}) \leq \tilde{\rho}(y). \tag{24.11}$$

The value $\tilde{\rho}(y \bmod p^t) = \tilde{\rho}(p^{n-t}y)$ is called the *formal polynomial complexity of* y *modulo* p^t.

Sections of the sequences u_s. Let $k = \sum_{s=0}^{n-1} p^s \nu_s(k) \in \overline{1, p^n - 1}$. Denote

$$u^{[k]} = \prod_{s=0}^{n-1} u_s^{\nu_s(k)}, \qquad u^{[0]} = (e, e, e, \dots), \qquad u^{[-1]} = u^{[-2]} = \dots = 0.$$

The definitions imply that $\tilde{\rho}(u^{[k]}) = k$, $k \in \mathbf{Z}$.

24.13. Lemma. *If* $k \in \overline{1, p^n - 1}$, $l \in \mathbf{N}$, *then*

$$(x^\tau - e)^l \cdot u^{[k]} \equiv (cu^{[k-pl]} + \eta)\omega + \zeta \pmod{p},$$

where $c \in R \backslash pR$, $\tilde{\rho}(\eta) \leq k - pl - (p-1)$, $\tilde{\rho}(\zeta) \leq k - pl - p(p-1)$,

$$\omega = \begin{cases} (u_0^{(1)})^\lambda, & \text{if } p \geq 3 \text{ or } p = 2,\ l = 1, \\ u_0^{(2)}, & \text{if } p = 2,\ l \text{ is even}, \\ u_0^{(2)} u_0^{(1)}, & \text{if } p = 2,\ l \text{ is odd},\ l \geq 3, \end{cases}$$

$$\lambda \in \overline{1, p-1}, \qquad \lambda \equiv l \pmod{p-1},$$

and the sequence η *can be expressed via* $u_0, \dots, u_{s-1}, u_0^{(r+1)}$.

□ This theorem is proved in three steps: (1) $l = p^r$, $k = p^s$; (2) $l = p^r$, k is arbitrary; (3) l, k are arbitrary. To prove (2), it is necessary to use the equality $u^{[k]} = \prod_{s=0}^{n-1} \prod_{i=1}^{\nu_s(k)} u^{[p^s]}$ and the case (1). To prove (3), it is necessary to use the relation $(x^\tau - e)^l \equiv \prod_{r=0}^{n-1} \prod_{i=1}^{\nu_r(l)} (x^\tau - e)^{p^r} \pmod p$ and the case (2). We give more a detailed proof only in the case (1). By (19.22), (19.23), it is sufficient to show that

$$(x^{\tau_r} - e)u_s \equiv ((-1)^{s-r+1} u_{s-1}^{p-1} \dots u_{r+1}^{p-1} + \eta) u_0^{(r+1)} + \zeta \pmod p,$$

where $\tilde\rho(\eta) \le p^s - 2p^{r+1} + 1$, $\tilde\rho(\zeta) \le p^s - p(p^{r+1} - 1)$. This property is a direct consequence of the following lemma.

24.13′. Lemma. *Let $0 \le r \le s - 1 \le n - 2$. Then*

$$(x^{\tau_r} - e) \cdot p^s u_{[s]} = p^s (-1)^{s-r+1} (u_{s-1}^{p-1} \dots u_{r+1}^{p-1} \cdot u_0^{(r+1)})^{p^{n-2}} + p^s \eta u_0^{(r+1)} + p^s \zeta, \tag{24.12}$$

where

$$\tilde\rho(p^s \eta \bmod p^{t+1}) \le p^t - 2p^{r+1} + 1,$$

$$\tilde\rho(p^s \zeta \bmod p^{t+1}) \le p^t - p(p^{r+1} - 1), \qquad t \in \overline{s, n-1}, \tag{24.13}$$

and the sequence η can be expressed via $u_0, \dots, u_{s-1}, u_0^{(r+1)}$.

□ We use induction by s. Let $s = r + 1$. Then

$$(x^{\tau_r} - e) \cdot p^{r+1} u_{[r+1]} = (x^{\tau_r} - e)u = p^{r+1} u^{(r+1)} = p^{r+1} u_0^{(r+1)} + p^{r+2} u_{[1]}^{(r+1)}.$$

By Lemma 23.1, $p u_0^{(r+1)} = p \Psi_B((u_0^{(r+1)})^{p^{n-2}})$. Therefore,

$$(x^{\tau_r} - e) \cdot p^{r+1} u_{[r+1]} = p^{r+1} ((u_0^{(r+1)})^{p^{n-2}} + \eta u_0^{(r+1)} + \zeta),$$

where

$$p\eta u_0^{(r+1)} = (\psi_1 - e)(u_0^{(r+1)})^{p^{n-2}} + \sum_{l=2}^{p-1} \psi_l (u_0^{(r+1)})^{p^{n-2} l},$$

$$\zeta = p u_{[1]}^{(r+1)}.$$

Since $\Psi_B(x) \equiv x \pmod p$ by Lemma 22.10, we have $\psi_1 \equiv e \pmod p$, $\psi_l \equiv 0 \pmod p$, $l \ge 2$. Now one can check that the sequences $p^{r+1} \eta u_0^{(r+1)}$, $p^{r+1} \zeta$ satisfy conditions (24.13) for $s = r + 1$. Thus, our lemma is proved for $s = r + 1$.

Suppose that the lemma is proved for some $s \in \overline{r+1, n-2}$. Let

$$Y = (-1)^{s-r+1} u_{s-1}^{p-1} \cdot \dots \cdot u_{r+1}^{p-1} \cdot u_0^{(r+1)}.$$

By (24.12), $x^{\tau_r} u_s \equiv u_s + Y + \eta u_0^{(r+1)} + \zeta \pmod p$. By Lemma 23.1,

$$x^{\tau_r} u_s = \Psi_B((u_s + Y + \eta u_0^{(r+1)} + \zeta)^{p^{n-1}}).$$

Therefore, by (24.12),

$$(x^{\tau_r} - e) \cdot p^{s+1} u_{[s+1]} = (x^{\tau_r} - e) \cdot p^s u_{[s]} - (x^{\tau_r} - e) \cdot p^s u_s =$$

$$p^s (Y + \eta u_0^{(r+1)} + \zeta + u_s - \Psi_B((u_s + Y + \eta u_0^{(r+1)} + \zeta)^{p^{n-1}})) =$$

$$p^s (u_s - \Psi_B(u_s^{p^{n-1}})) + p^s (Y - \Psi_B(Y^{p^{n-1}})) +$$

$$p^s (\eta u_0^{(r+1)} - \Psi_B((\eta u_0^{(r+1)})^{p^{n-1}})) + p^s (\zeta - \Psi_B(\zeta^{p^{n-1}})) -$$

$$p^s \cdot \sum_{l=1}^{p-1} \psi_l \cdot \sum_{\substack{a+b+c+d=p^{n-1}l \\ 0\le a,b,c,d<p^{n-1}l}} \frac{(p^{n-1}l)!}{a!b!c!d!} \cdot u_s^a Y^b (\eta u_0^{(r+1)})^c \zeta^d.$$

Choose the summand of this sum with the indexes

$$(l,a,b,c,d) = (1, p^{n-2}(p-1), p^{n-2}, 0, 0).$$

We divide the other summands into two groups. Let $p^{s+1}\eta' u_0^{(r+1)}$ be the sum of the summands which have $u_0^{(r+1)}$ as a multiplier and which do not have ζ as a multiplier, and $p^{s+1}\zeta'$ be the sum of the rest of the summands. Then

$$(x^{\tau_r} - e) \cdot p^{s+1} u_{[s+1]} = -p^s \psi_1 \binom{p^{n-1}}{p^{n-2}} (u_s^{p-1} Y)^{p^{n-2}} +$$

$$p^{s+1}\eta' u_0^{(r+1)} + p^{s+1}\zeta' = -p^{s+1}(-1)^{s-r+1}(u_s^{p-1}Y)^{p^{n-2}} + p^s c (u_s^{p-1}Y)^{p^{n-2}} + p^{s+1}\eta' u_0^{(r+1)} + p^{s+1}\zeta',$$

where

$$c = p(-1)^{s-r+1} - \psi_1 \binom{p^{n-1}}{p^{n-2}} ((-1)^{s-r+1})^{p^{n-2}} \equiv p(-1)^{s-r+1} - \psi_1 p (-1)^{s-r+1} \equiv 0 \pmod p.$$

Let $p^{s+1}\eta'' u_0^{(r+1)} = p^s c (u_s^{p-1}Y)^{p^{n-2}} + p^{s+1}\eta' u_0^{(r+1)}$. Then

$$(x^{\tau_r} - e) \cdot p^{s+1} u_{[s+1]} = p^{s+1}(-1)^{s-r+2} \cdot (u_s^{p-1} \dots u_{r+1}^{p-1} \cdot u_0^{(r+1)})^{p^{n-2}} + p^{s+1}\eta'' u_0^{(r+1)} + p^{s+1}\zeta'.$$

Direct (but rather long) evaluations (based on the divisibility of the polynomial coefficients by the power of the prime number p, see [37, Lemma 6.39]), show that the sequences $p^{s+1}\eta'' u_0^{(r+1)}$, $p^{s+1}\zeta'$ satisfy the conditions (24.13) in which s is changed to $s+1$. Thus, we get the relation (24.12) for the parameter $s+1$. □

24.14. Corollary. *In the notations of Lemma* 24.13,

$$\overline{u}^{[k]} = \overline{dy}[k] + \overline{\xi}, \ \textit{where } k \ge 0, \ \overline{d} \ne \overline{0}, \ \rho(\overline{\xi}) < k;$$

$$(x^\tau - \overline{e})^l \cdot \overline{u}^{[k]} = \overline{0}, \ \textit{if } 0 \le k < pl;$$

$$(x^\tau - \overline{e})^l \cdot \overline{u}^{[k]} = \overline{cy}[k-pl]\overline{\omega} + \overline{\pi}, \ \textit{if } k \ge pl > 0,$$

where $\overline{c} \ne \overline{0}$, $\rho(\overline{y}[k-pl]\overline{\omega}) \le b(k,l)$, $\rho(\overline{\pi}) < b(k,l)$, *and* $b(k,l)$ *are defined in the beginning of the section.*

□ The first relation follows from 24.12 and 24.11. The second and the third relations follow from Lemma 24.13, the first relation, and (24.11). □

C. The proofs of the main theorems. Let $\overline{M}_s(x)$ be the minimal polynomial of the sequence $\overline{u}_s$ over the field $\overline{R}$.

□ Proof of Theorem 24.1. Let $\overline{\gamma}$ be a root of $\overline{M}_s(x)$ of multiplicity $A \ge 1$. It is sufficient to prove that $\overline{\gamma}$ is a root of the polynomial $\overline{\mathcal{H}}(x)$ of multiplicity $B \ge A$. By Lemma 24.10,

$$\overline{\gamma} = \overline{\xi}^d, \qquad d \in \overline{1,\tau}, \qquad 1 \le w(d) \le p^s.$$

Since $0 = b(p^{s-1}+1) < b(p^{s-1}) < \dots < b(0) = p^s$, there exists a unique integer $l \in \overline{0, p^{s-1}}$ such that $b(l+1) < w(d) \le b(l)$. The definition of $\overline{\mathcal{H}}(x)$ implies that $B = l+1$. Thus, it is sufficient to prove that $A \le l+1$. By Corollary 24.14, $\rho((x^\tau - \overline{e})^{l+1}\overline{u}_s) \le b(l+1)$. By the definition of $\rho(\overline{y})$, the last inequality means that the element $\overline{\gamma} = \overline{\xi}^d$ is not a root of the minimal polynomial of the sequence $(x^\tau - \overline{e})^{l+1}\overline{u}_s$. Therefore, by Lemma 24.6, $A \le l+1$. □

□ Proof of Theorem 24.2. It is sufficient to prove that any root of the polynomial $\overline{M}_s(x)$ has the form $\overline{\xi}^d$, $w(d) \equiv 1 \pmod{p-1}$, or, equivalently, the form $\overline{\xi}^d$, $d \equiv 1 \pmod{p-1}$. To prove this, it is sufficient to show that the sequence $u_{[s]}$ is the sum of binomial sequences over Q with roots

$$\xi_0^d, \qquad d \equiv 1 \pmod{p-1}, \ \text{where } \xi_0 = \gamma_0(\xi) \in \Gamma(Q). \tag{24.14}$$

We use induction on $s \geq 0$. The relations $u = \operatorname{Tr}_R^Q(a\xi^i)$, $i \geq 0$, imply that the LRS $u_{[0]} = u$ is the sum of binomial sequences with roots $\xi_0^{p^r}$. Let our property be true for some s. By Lemma 23.1,

$$u_s = \gamma_0(u_{[s]}) = (u_{[s]})^{p^{n-1}}.$$

Since the product of elements of the form (24.14) is an element of the form (24.14), u_s is the sum of binomial sequences with roots of the form (24.14). Hence, this property is true also for the sequence $pu_{[s+1]} = u_{[s]} - u_s$. □

□ Proof of Theorem 24.3. It is sufficient to consider the case $s = n-1$. The equalities $u(i) = \operatorname{Tr}_R^Q(a\xi^i)$ imply that

$$u\Big(i + \frac{\tau_n - 1}{p-1}\Big) = \beta u(i), \qquad i \geq 0, \tag{24.15}$$

where $\beta \in \Gamma(R)$ is an element of order $p-1$. Then the sequence $\overline{\omega} = (x^{\tau_{n-1}/2} + \overline{e})\overline{u}_{n-1}$ satisfies

$$\overline{\omega}(i) = \begin{cases} -1, & \text{if } u(i) \not\equiv 0 \pmod{p^{n-1}}, \\ 0, & \text{if } u(i) \equiv 0 \pmod{p^{n-1}}, \ i \geq 0. \end{cases}$$

Therefore, by (24.15), $T(\overline{\omega})|\frac{\tau_{n-1}}{p-1}$. Thus,

$$\overline{M}_{n-1}(x)|(x^{\tau_{n-1}/(p-1)} - \overline{e})(x^{\tau_{n-1}/2} + \overline{e}) = ((x^{\tau/(p-1)} - \overline{e})(x^{\tau/2} + \overline{e}))^{p^{n-1}}.$$

Hence, if $\overline{\xi}^d$ is a root of $\overline{M}_{n-1}(x)$, then either $\overline{\xi}^{d\tau/2} = -\overline{e}$ or $\overline{\xi}^{d\tau/(p-1)} = \overline{e}$. In the first case, $d \equiv 1 \pmod 2$; in the second case, $d \equiv 0 \pmod{p-1}$. □

□ Proof of Theorem 24.4. (a) By Theorem 24.12, $\overline{M}_s(x)$ is divided by the minimal polynomial of the sequence $\overline{y}[p^s]$, i.e., by $\overline{G}^{(p^s)}(x)$. By (24.5) and Lemma 24.6, $\overline{M}_s(x)$ is divided by $\overline{G}(x)^{p^{s-1}+1}$. Since the polynomials $\overline{G}^{(N)}(x)$, $N \geq 1$, are pairwise coprime, $\overline{M}_s(x)$ is divided by $\overline{G}^{(p^s)}(x) \cdot \overline{G}(x)^{p^{s-1}+1}$. Therefore, $\operatorname{rank} u_s \geq \mathcal{R}_0$.

(d) If $\deg \overline{\Phi}^{(2)}(x) = 0$, then by 24.14, (19.22), (19.23), 24.11,

$$(x^\tau - \overline{e})^l \cdot \overline{u}_s = \overline{c} \cdot \overline{y}[p^s - pl] \cdot \overline{u}_0 + \overline{\pi} = \overline{d} \cdot \overline{y}[p^s - pl + 1] + \overline{\pi},$$

where $\overline{c}, \overline{d} \neq \overline{0}$, $\rho(\overline{\pi}) < p^s - pl + 1 = b(l)$, $1 \leq l \leq p^{s-1} - 1$, and if $p = 2$, then $l \in \mathcal{L}_1$. Therefore, by Lemma 24.6, $\overline{M}_s(x)$ is divided by the polynomials $\overline{G}^{(b(l))}(x)^{l+1}$ for the above-mentioned l. Since these polynomials are pairwise coprime, $\overline{M}_s(x)$ is divided by the product of these polynomials. Putting this together with (a), we get (d).

By Corollary 24.14,

$$(x^\tau - \overline{e})^l \cdot \overline{u}_s = \overline{c} \cdot \overline{y}[p^s - pl] \cdot (\overline{u}_0^{(1)})^t + \overline{\pi}, \text{ if } p \geq 3, \ l \in \mathcal{L}_t,$$

$$(x^\tau - \overline{e})\overline{u}_s = \overline{c} \cdot \overline{y}[2^s - 2] \cdot \overline{u}_0^{(1)} + \overline{\pi}, \text{ if } p = 2, \ l = 1,$$

$$(x^\tau - \overline{e})^l \cdot \overline{u}_s = \overline{c} \cdot \overline{y}[2^s - 2l] \cdot \overline{u}_0^{(2)} + \overline{\pi}, \text{ if } p = 2, \ l \in \mathcal{L}_1 \backslash \{1\},$$

$$(x^\tau - \overline{e})^l \cdot \overline{u}_s = \overline{c} \cdot \overline{y}[2^s - 2l] \cdot \overline{u}_0^{(2)}\overline{u}_0^{(1)} + \overline{\pi}, \text{ if } p = 2, \ l \in \mathcal{L}_2,$$

where $\overline{c} \neq \overline{0}$, $\rho(\overline{\pi}) < b(l)$. Let $\gamma = \Phi^{(1)}(\xi)$ (where $\xi \in Q$ is the root of the polynomial $G(x)$). By (24.9),

$$\overline{u}^{(1)}(i) = \operatorname{tr}_1^m(\overline{a\gamma}\overline{\xi}^i), \qquad i \geq 0,$$

and if $p = 2$, then by (19.19), we have

$$\overline{u}^{(2)}(i) = \operatorname{tr}_1^m(\overline{a}(\overline{\gamma} + \overline{\gamma}^2)\overline{\xi}^i), \qquad i \geq 0.$$

These relations and the definition of $y[N]$ show that:
if $p \geq 3$, $l \in \mathcal{L}_t$, or if $p = 2$, $l = 1$ (then we put $t = 1$), then

$$(x^\tau - \overline{e})^l \overline{u}_s(i) = \overline{c} \cdot \sum_d \overline{E}(d)\overline{Q}_t(d)\overline{\xi}^{di} + \overline{\lambda}(i), \tag{24.16}$$

if $p = 2$, $l \in \mathcal{L}_1 \backslash \{1\}$, then

$$(x^\tau - \overline{e})^l \overline{u}_s(i) = \overline{c} \cdot \sum_d \overline{E}(d)(\overline{Q}_1(d) + \overline{Q}_1(d)^2)\overline{\xi}^{di} + \overline{\lambda}(i), \tag{24.17}$$

if $p = 2$, $l \in \mathcal{L}_2$, then

$$(x^\tau - \overline{e})^l \overline{u}_s(i) = \overline{c} \cdot \sum_d \overline{E}(d)\overline{R}(d)\overline{\xi}^{di} + \overline{\lambda}(i), \qquad i \geq 0, \tag{24.18}$$

where $\overline{c} \neq \overline{0}$, $\rho(\overline{\lambda}) < b(l)$, the summation in these formulas goes over integers $d \in \overline{1, \tau}$ such that $w(d) = b(l)$, the coefficients $E(d)$ are defined in 24.B, and

$$Q_t(d) = \sum_{\substack{1 \leq r \leq d \\ w(r) = t}} \binom{d}{r} \gamma^r, \qquad R(d) = \sum_{\substack{j \neq k \\ 0 \leq j, k \leq m-1}} \nu_j(d)\nu_k(d)\gamma^{2^j}\gamma^{2^{k+1}}.$$

Denote $V_N = \{d \in \overline{1, \tau} |\ w(d) = N\}$, $N \geq 1$. Since $\overline{E}(d) \neq \overline{0}$, the element $\overline{\xi}^d$, $d \in V_{b(l)}$, is a root of the minimal polynomial of the sequence (24.16) (respectively (24.17), (24.18)) if and only if $\overline{Q}_t(d) \neq \overline{0}$ (respectively $\overline{Q}_1(d) + \overline{Q}_1(d)^2 \neq \overline{0}$, $\overline{R}(d) \neq \overline{0}$). To get an estimation of rank u_s, it is sufficient to estimate the number of such d.

(b) Let $p \geq 3$. Suppose that the conditions of (b) are fulfilled. Then the elements $\overline{\gamma}^{p^\alpha}$, $\alpha \in \overline{0, m-1}$, are linearly independent over the field $\overline{R}$. Hence, $\overline{Q}_1(d) \neq \overline{0}$, $d \in \overline{1, \tau}$. Therefore, if $l \in \mathcal{L}_1$, then the minimal polynomial of the sequence (24.16) is divided by $\overline{G}^{(b(l))}(x)$, and, by 24.6, $\overline{M}_s(x)$ is divided by $\overline{G}^{(b(l))}(x)^{l+1}$, $l \in \mathcal{L}_1$. It follows that the rank $u_s \geq \mathcal{R}_0 + \mathcal{R}_1$.

Now let $l \in \mathcal{L}_2$. We are going to estimate the number of integers $d \in V_{b(l)}$ such that $\overline{Q}_2(d) \neq \overline{0}$. Divide the set V_N into the following classes. Two integers belong to one class iff they have the same p-ary digits; the order of the digits may be different. Let d, $d' \in V_{b(l)}$ be different integers from one class such that d turns into d' by permutation of the j-th and k-th digits of d. We have

$$Q_2(d) - Q_2(d') = \Big(\sum_{\substack{t=0 \\ t \neq k,\, t \neq j}}^{m-1} \nu_t(d)\gamma^{p^t} \Big) \cdot (\nu_k(d) - \nu_j(d))(\gamma^{p^k} - \gamma^{p^j}) + (\gamma^{2p^k} - \gamma^{2p^j}) \left(\binom{\nu_k(d)}{2} - \binom{\nu_j(d)}{2} \right)$$

Since the elements $\overline{\gamma}^{p^\alpha}$, $\alpha \in \overline{0, m-1}$, are linearly independent and $w(d) = b(l) \equiv 2 \pmod p$, then $\overline{Q}_2(d) \neq \overline{0}$ or $\overline{Q}_2(d') \neq \overline{0}$.

24.15. Lemma. *Let $\Omega = \{0, 1, \ldots, p-1\}$, $\beta_0 + \ldots + \beta_{p-1} = m$. Let A be the set of all vectors of length m over Ω such that β_j of the components of each vector is equal to j, $j \in \Omega$. Suppose that $B \subseteq A$ and there are no two vectors in B such that one of them is a permutation of two coordinates of another. Then*

$$|A| \geq |B|(1 + \max\{\beta_j;\ j \in \Omega\}) \geq |B| \cdot \frac{m+p}{p}. \quad \square$$

Applying this lemma for $A = V_{b(l)}$, $B = \{d \in V_{b(l)} |\ \overline{Q}_2(d) = \overline{0}\}$, we find that the number of integers $d \in V_{b(l)}$ such that $\overline{Q}_2(d) \neq \overline{0}$ is not less than $|A| - |B| \geq |A|\big(1 - \frac{p}{m+p}\big) = \left\{ \begin{matrix} m \\ b(l) \end{matrix} \right\} \cdot \frac{m}{m+p}$. This implies the estimation $\operatorname{rank} u_s \geq \mathcal{R}_0 + \mathcal{R}_1 + \frac{m}{m+p} \cdot \mathcal{R}_2$ for $p \geq 3$.

Now let $p = 2$. Then, in addition to the relations $\overline{Q}_1(d) \neq \overline{0}$, $d \in \overline{1,\tau}$, we have $\overline{Q}_1(d) + \overline{Q}_1(d)^2 \neq \overline{0}$, $d \in \overline{1,\tau-1}$. This and (24.16), (24.17) imply that $\operatorname{rank} u_s \geq \mathcal{R}_0 + \mathcal{R}_1$. The complete proof of (b) for $p = 2$ is based on (24.18) and is analogous to the case $p \geq 3$ with substitution of $R(d)$ instead of $Q_2(d)$.

(c) Under the condition (c), the element $\overline{\gamma}$ is a root of an irreducible polynomial of degree h over the field $\overline{R}$. Let $l \in \mathcal{L}_1$, and let d, $d' \in V_{b(l)}$ be chosen as in (b). Then

$$Q_1(d) - Q_1(d') = (\nu_k(d) - \nu_j(d))(\gamma^{p^k} - \gamma^{p^j}).$$

Therefore, $\overline{Q}_1(d) = \overline{Q}_1(d') = \overline{0}$ if and only if $h|k-j$. Hence, by Lemma 24.15, the equality $\overline{Q}_1(d) = \overline{0}$ is true not more than for the $\frac{m}{h} \cdot \frac{p}{m+p}$-th part of all integers $d \in V_{b(l)}$. Therefore,

$$\operatorname{rank} u_s \geq \mathcal{R}_0 + \Big(1 - \frac{m}{h} \cdot \frac{p}{m+p}\Big)\mathcal{R}_1 \geq \mathcal{R}_0 + \frac{h-p}{h} \cdot \mathcal{R}_1. \quad \square$$

24.16. Corollary. *If $m \to \infty$, then the* $\operatorname{rank} u_s = \binom{m}{p^s}(1 + 0(\frac{1}{m}))$. $\square$

Note that, in the notation of Theorem 24.4, the polynomial $G(x)$ can be chosen in such a way that the polynomial $\overline{\Phi}^{(1)}(x)$ (which depends only on $G(x)$) is an arbitrary polynomial satisfying (19.18), in particular, in such a way that the conditions of Theorem 24.4 are satisfied.

24.17. Examples. Let $p = 2$ and let the conditions of Theorem 24.4(b) be satisfied. Then, by Theorems 24.1 and 24.4, we have

if $m = 3$, then $15 \leq \operatorname{rank} u_3 \leq 31$, $195 \leq \operatorname{rank} u_7 \leq 451$;

if $m = 11$, then $3383 \leq \operatorname{rank} u_3 \leq 5340$, $59,703 \leq \operatorname{rank} u_7 \leq 128,430$;

if $m = 31$, then $1.37 \cdot 10^7 \leq \operatorname{rank} u_3 \leq 1.53 \cdot 10^7$, $6 \cdot 10^{10} \leq \operatorname{rank} u_7 \leq 10^{11}$.

Now let the conditions of Theorem 24.4(d) be satisfied. Then

if $p = 5$, $m = 3$, then $328 \leq \operatorname{rank} u_3 \leq 3093$, $2 \cdot 10^5 \leq \operatorname{rank} u_7 \leq 2 \cdot 10^6$;

if $p = 5$, $m = 11$, then $2 \cdot 10^8 \leq \operatorname{rank} u_3 \leq 10^9$, $10^{11} \leq \operatorname{rank} u_7 \leq 8 \cdot 10^{11}$;

if $p = 11$, $m = 5$, then $10^6 \leq \operatorname{rank} u_3 \leq 2 \cdot 10^7$, $2 \cdot 10^{10} \leq \operatorname{rank} u_7 \leq 3 \cdot 10^{11}$.

25. $GF(p)$-Representations of MP-Recurrences over $\mathbb{Z}_{p^n}$

We use the notation of Section 24. Consider $\overline{R}$-representations (i.e., $GF(p)$-representations) of the sequence u. For any mapping $\sigma : R \to \overline{R}$ there exists a unique polynomial $H_\sigma(x_0, \ldots, x_{n-1})$ over the field $\overline{R}$ such that $\deg_{x_i} H_\sigma \leq p-1$ for $i \in \overline{0,n-1}$ and

$$\sigma(a) = H_\sigma(\overline{a}_0, \ldots, \overline{a}_{n-1}), \qquad a \in R,$$

where $a_s = \gamma_s(a)$, $s \in \overline{0,n-1}$ are the p-adic coordinates of the element a (see Section 19.B). For a monomial $\mu = x_0^{k_0} \ldots x_{n-1}^{k_{n-1}}$, $0 \leq k_j \leq p-1$, denote $\tilde{\rho}(\mu) = k_0 + pk_1 + \ldots + p^{n-1}k_{n-1}$. Let $\tilde{\rho}(H_\sigma)$ be the maximal value of $\tilde{\rho}(\mu)$, where μ runs over all monomials of the polynomial H_σ with nonzero coefficients. For $p \geq 3$, define $J = J(\sigma)$ to be the set of all integers $j \in \overline{0,p-2}$ such that the polynomial H_σ contains a monomial μ with $\tilde{\rho}(\mu) = \tilde{\rho}(H_\sigma) - j$, and denote

$$\delta(k,l,N) = \begin{cases} l+1, & \text{if } N \in b(k,l) - J \text{ or } N \leq b(k,l) - p + 1, \\ l, & \text{otherwise,} \end{cases}$$

where $b(k,l)$ is defined in Section 24, $t - J = \{t - j \mid j \in J\}$. For $p = 2$, we set $\delta(k,l,N) = l+1$. Let $[x]$ be the largest integer less than or equal to x.

25.1. Theorem [30]. *Let u be an LRS of maximal period over the ring $R = \mathbb{Z}_{p^n}$ with minimal polynomial $G(x)$ of degree m, $\sigma : R \to \overline{R}$ be an arbitrary mapping, and $k = \tilde{\rho}(H_\sigma) > 1$. Then the polynomial*

$$\prod_{\substack{l \\ 0 \le pl \le k}} \Big(\prod_{N=b(l+1)+1}^{b(l)} \overline{G}^{(N)}(x)^{\delta(k,l,N)} \Big),$$

where $b(l) = b(k,l)$, is a characteristic polynomial of the sequence $\sigma(u)$ over the field $\overline{R}$, and

$$\operatorname{rank} \sigma(u) \le \sum_{\substack{l \\ 0 \le pl \le k}} \Big(\sum_{N=b(l+1)+1}^{b(l)} \left\{ \begin{matrix} m \\ N \end{matrix} \right\} \cdot \delta(k,l,N) \Big).$$

25.2. Theorem [30]. *Under the conditions of Theorem* 25.1, *let $p \ge 3$. Then*

$$\operatorname{rank} \sigma(u) \ge \sum_{N \in k-J} \left\{ \begin{matrix} m \\ N \end{matrix} \right\} + ([k/p]+1) \left\{ \begin{matrix} m \\ \varkappa \end{matrix} \right\}^*,$$

where $\varkappa \in \overline{1, p-1}$, $\varkappa \equiv [k/p] \bmod (p-1)$, and $*$ means that the second summand is present only if $k \ge p$ and the set $k - J$ contains an element $j \equiv 0 \pmod p$. If the polynomial $G(x)$ satisfies the condition 24.4(b), *then*

$$\operatorname{rank} \sigma(u) \ge \sum_{N \in k-J} \left\{ \begin{matrix} m \\ N \end{matrix} \right\} + \sum_{\substack{l : 0 \le pl \le k \\ l \equiv 1 \pmod{p-1}}} (l+1) \cdot \sum_{\substack{N \in b(l)-J \\ N > 0}} \left\{ \begin{matrix} m \\ N \end{matrix} \right\} + ([k/p]+1) \left\{ \begin{matrix} m \\ \varkappa \end{matrix} \right\}^* \cdot \Delta,$$

where $\Delta = 0$ if $\varkappa = 1$, and $\Delta = 1$ if $\varkappa \ne 1$.

25.3. Theorem [30]. *Under the conditions of Theorem* 25.1, *let $p = 2$. Then*

$$\operatorname{rank} \sigma(u) \ge \binom{m}{k} + \Big(\frac{k}{2} + 1\Big) m^*,$$

where $*$ means that the second summand is present only if $4 | k$. If the condition 24.4(b) *is satisfied, then*

$$\operatorname{rank} \sigma(u) \ge \binom{m}{k} + 2\binom{m}{k-1} + \sum_{\substack{l \text{ is even} \\ 4 \le 2l \le k,\, k-2l+1 < m}} (l+1) \binom{m}{k-2l+1}.$$

If $\overline{\Phi}^{(2)}(x) = \overline{e}$, then

$$\operatorname{rank} \sigma(u) \ge \binom{m}{k} + 2\binom{m}{k-1} + \sum_{\substack{l \text{ is even} \\ 4 \le 2l \le k}} (l+1) \binom{m}{k-2l+\varepsilon},$$

where $\varepsilon = 1$ if k if even, and $\varepsilon = 0$ if k is odd.

□ The proofs of Theorems 25.1–25.3 are analogous to the proofs of Theorems 24.1 and 24.4. □

25.4. Corollary. *Under the conditions of Theorem* 25.1, *let $m \to \infty$. Then the* $\operatorname{rank} \sigma(u) = \binom{m}{k}(1 + 0(\frac{1}{m})) \sim \binom{m}{k}$. □

Chapter 5.

STATISTICAL PROPERTIES OF LINEAR RECURRING SEQUENCES

26. Statistical Properties of Linear Recurring Sequences over Finite Fields

Let u be an LRS over the field $P = GF(q)$. For a set of nonnegative integers $\mathbf{k} = (k_0, \ldots, k_{s-1})$, $0 = k_0 < k_1 < \ldots < k_{s-1} = L$, and a row $\mathbf{a} = (a_0, \ldots, a_{s-1})$, $a_t \in P$, we define the frequency $\nu_u^N\binom{\mathbf{k}}{\mathbf{a}}$ of appearance of $\mathbf{a}$ in $u(\overline{0, N+L-1})$ as the number of integers $i \in \overline{0, N-1}$ such that

$$u(i + k_t) = a_t, \qquad t \in \overline{0, s-1}. \tag{26.1}$$

We would like to get estimations of $\nu_u^N\binom{\mathbf{k}}{\mathbf{a}}$, and, if possible, to define the exact value of $\nu_u^N\binom{\mathbf{k}}{\mathbf{a}}$ for various classes of LRS with some conditions on N, $\mathbf{k}$.

Some algebraic methods have been applied mainly to LRS of maximal period in the case $N = T(u)$. Under these conditions, the main problem is to determine the number of solutions of special systems of equations over a finite field [35, 37, 70].

Let u be an LRS of the maximal period $\tau = q^m - 1$ over the field P with the minimal polynomial $g(x)$ of degree m. Then $g(x)$ is a polynomial of maximal period over P, and the order of its root α in the multiplicative group of the field $Q = GF(q^m)$ is equal to τ. In this chapter, by a cycle of a periodic LRS u we also mean a segment of u of length $T(u)$ (cf. 5.23).

26.1. Theorem. *If the system of elements $\alpha^{k_0}, \ldots, \alpha^{k_{s-1}}$ of the field Q is linearly independent over P, then the frequency $\nu_u^\tau\binom{\mathbf{k}}{\mathbf{a}}$ of the appearance of $\mathbf{a}$ on a cycle of u is equal to q^{m-s}, if $\mathbf{a} \neq \mathbf{0}$, and $q^{m-s} - 1$, if $\mathbf{a} = \mathbf{0}$.*

□ Under these conditions, $\nu_u^\tau\binom{\mathbf{k}}{\mathbf{a}}$ is equal to the number of nonzero solutions in Q of the system of linear equations

$$\operatorname{tr}_P^Q(\alpha^{k_t} x) = a_t, \qquad t \in \overline{0, s-1}. \tag{26.2}$$

This number depends only on the dimension of the linear space spanned by $\alpha^{k_0}, \ldots, \alpha^{k_{s-1}}$ over P. □

If the system of elements $\alpha^{k_0}, \ldots, \alpha^{k_{s-1}}$ is linearly dependent over P, then system (26.2) has no solutions for some $\mathbf{a}$. But if (26.2) is solvable, then it has q^{m-r} solutions, where $r = \dim_P\{\alpha^{k_0}, \ldots, \alpha^{k_{s-1}}\}$.

It is possible to generalize the results of [35, 37, 70] on the properties of LRS of maximal period over $P = GF(q)$ to the case of k-maximal recurrences.

Let u be a k-max-LRS over P of rank m, and (12.3) be valid. Then the period of u is $T(u) = \tau = q^m - 1$. We can choose $\mathbf{i}_0, \ldots, \mathbf{i}_{\tau-1} \in \mathbf{N}_0^k$ such that the cycle of LRS u is described by

$$\mathcal{T}(u) = \{\mathbf{x}^{\mathbf{i}_0} u, \ldots, \mathbf{x}^{\mathbf{i}_{r-1}} u\} = \{\theta^{\mathbf{i}_0} u, \ldots, \theta^{\mathbf{i}_{r-1}} u\} \tag{26.3}$$

(see 5.23, 6.23, 12.4). Let

$$J = \{\mathbf{j}_1, \ldots, \mathbf{j}_l\} \subset \mathbf{N}_0^k, \qquad \mathbf{j}_1 \preceq \ldots \preceq \mathbf{j}_l, \tag{26.4}$$

be a finite set of vectors, and

$$\mathfrak{A}(J) = (a(\mathbf{j}_1), \ldots, a(\mathbf{j}_l)) \tag{26.5}$$

be the polyhedron of values in P^J (see Section 2B). Define $\nu_u(J/\mathfrak{A}(J))$ as the number of solutions $s \in \overline{0,\tau-1}$ of the equation

$$u(\mathbf{i}_s + J) = \mathfrak{A}(J). \tag{26.6}$$

26.2. Theorem. *Let vectors* (26.4) *be chosen in such a way that, in the notations of Section* 12, *the system of elements* $\alpha^{j_1},\dots,\alpha^{j_l}$ *of the field* Q *is linearly independent over* P. *Then* $l \le m$ *and*

$$\nu_u(J/\mathfrak{A}(J)) = \begin{cases} q^{m-l}, & \text{if } \mathfrak{A}(J) \neq 0, \\ q^{m-l}-1, & \text{if } \mathfrak{A}(J) = 0. \end{cases}$$

□ By (12.3) and (12.2), $\nu_u(J/\mathfrak{A}(J))$ is the number of nonzero solutions in Q of the system of linear equations

$$\operatorname{tr}_P^Q(\xi\alpha^{j_t}x) = a(\mathbf{j}_t), \qquad t \in \overline{1,l}.$$

The rank of this system is equal to l, so the desired result follows. □

In the particular cases where $k = 2,3$ and $J = \Pi(\mathbf{n})$ is the Ferre diagram of the ideal $I = \operatorname{An}(u)$ (see 10.6), this result has been obtained in [128, 145, 146, 153] and has been called the *window effect* (the window J, moving on the cycle $\mathcal{T}(u)$ of the LRS u, shows all nonzero polyhedrons $\mathfrak{A}(J) \in P^J$ for the same number of times).

Algebraic methods make it possible to get the exact values of the frequencies of appearance of rows on the cycle of an LRS. But they are connected with strong restrictions on the parameters of the LRS and on the length of the segment of a sequence.

The method of trigonometric sums gives informative results about $\nu_u^N\binom{\mathbf{k}}{\mathbf{a}}$ for recurrences with arbitrary characteristic polynomials [19, 20, 37, 54–57, 60, 73–75]. But the length N of the segment of a sequence must be large. The most of the known estimations of $\nu_u^N\binom{\mathbf{k}}{\mathbf{a}}$ are nontrivial for $N^2 > T(u)$. Here we give only one result, obtained in [60].

26.3. Theorem. *Let* u *be a LRS over the field* $GF(p)$, p *prime, with the irreducible minimal polynomial* $g(x)$ *of degree* m, *and let* α *be a root of* $g(x)$ *in the field* $GF(p^m)$. *If the system of elements* $\alpha^{k_0},\dots,\alpha^{k_{s-1}}$ *is linearly independent over* $GF(p)$, *then*

$$\left|\nu_u^N\binom{\mathbf{k}}{\mathbf{a}} - \frac{N}{p^s}\right| \le \frac{p^s-1}{p^s}(3(Np^m - N^2))^{1/3}.\square$$

There is another method of investigation of the statistical properties of LRS, consisting in construction of recurrences with given statistical characteristics. The most well-known representatives of this class are *uniformily distributed sequences*, i.e., recurrences u such that all elements of the field have the same frequency of appearance on the cycle of u [15, 168]. These works mainly deal with LRS of small ranks and with some class of LRS with minimal polynomials of special types.

More complete review of the statistical properties of LRS over finite fields is given in [37].

27. Statistical Properties of Linear Recurring Sequences over Residue Rings

In [18, 37, 110, 168] recurrences of small orders and uniformly distributed LRS (ULRS) have been studied. The difficulties in the study of the statistical characteristics of linear recurrences over residue rings are connected with the fact that the available algebraic methods and the method of trigonometric sums are only slightly effective in this case (in comparison with the case of LRS over finite fields).

Let $R = \mathbf{Z}_{p^n}$, p prime, and let $G(x) \in R[x]$ be a polynomial of degree m of maximal period $T = T(G) = (p^m-1)p^{n-1}$, u be an LRS of maximal period from $L_R(G)$, $T(u) = T$. Consider the frequencies $\nu_u(a) = \nu_u^T\binom{0}{a}$ of the appearance of elements $a \in R$ on the cycle of LRS u.

Let $\Phi^{(r)}(x)$, $r \in \overline{1, n-1}$, be the polynomials defined in Lemma 19.9. We say that the polynomial $G(x)$ satisfies the property (K_r) if $\deg \overline{\Phi}^{(r)}(x) > 0$.

27.1. Theorem [22]. *The frequencies of the appearance of elements of the ring R on the cycle of LRS u satisfy the following relations: if $p \geq 3$ and $G(x)$ satisfies (K_1), then*

$$\nu_u(a) \geq \frac{p-1}{p} \cdot \frac{T}{|R|} \text{ for any } a \in R;$$

if $p \geq 3$ and $G(x)$ does not satisfy (K_1), then

$$\nu_u(a) = p^{m-1} \text{ for } a \in R^*;$$

if $p = 2$ and $G(x)$ satisfies (K_2), then

$$\nu_u(a) \geq \frac{1}{4} \cdot \frac{T}{|R|} \text{ for any } a \in R;$$

if $p = 2$ and $G(x)$ does not satisfy (K_2), then

$$\nu_u(a) \geq \frac{1}{2} \cdot \frac{T}{|R|} \text{ for } a \in R^*.$$

□ Let $u^{(r)} = \Phi^{(r)}(x)u$ be the derivative sequence of LRS u (see Section 19.B). If $\overline{u}^{(1)}(i) \neq \overline{0}$, $\overline{u}^{(2)}(i) \neq \overline{0}$ for some i, then (24.5) implies that

$$\{u(i + \tau j) | \ 0 \leq j \leq p^{n-1} - 1\} = u(i) + pR, \text{ where } \tau = p^m - 1.$$

With regard to (19.22), (19.23), the desired results can now be obtained by means of the enumeration of integers $i \in \overline{0, \tau - 1}$ such that $\overline{u}^{(1)}(i) \neq \overline{0}$, $\overline{u}^{(2)}(i) \neq \overline{0}$, $u(i) = a$. □

In the case $R = \mathbb{Z}_4$, we have a complete classification of all possible types of distribution of elements on the cycle of u.

27.2. Theorem (A. Nechaev, 1983). *Let u be an MP-recurrence over $\mathbb{Z}_4$ with minimal polynomial $G(x)$ of degree m. Then, for a suitable ε, $\delta \in \{-1, 0, 1\}$, the distribution of elements on the cycle of LRS u is described by the following table:*

Conditions on m	$\nu_u(0)$	$\nu_u(1)$	$\nu_u(2)$	$\nu_u(4)$	Conditions on ε, δ
$m = 2\lambda$	$2^{m-1} - 2 - 2^\lambda\delta$	$2^{m-1} - 2^\lambda\varepsilon$	$2^{m-1} + 2^\lambda\delta$	$2^{m-1} + 2^\lambda\varepsilon$	$\varepsilon\delta = 0$
	$2^{m-1} - 2 - 2^{\lambda-1}\delta$	$2^{m-1} - 2^{\lambda-1}\varepsilon$	$2^{m-1} + 2^{\lambda-1}\delta$	$2^{m-1} + 2^{\lambda-1}\varepsilon$	$\varepsilon\delta \neq 0$
$m = 2\lambda + 1$	$2^{m-1} - 2 - 2^\lambda\delta$	$2^{m-1} - 2^\lambda\varepsilon$	$2^{m-1} + 2^\lambda\delta$	$2^{m-1} + 2^\lambda\varepsilon$	$\lvert\varepsilon\rvert = \lvert\delta\rvert$
	$2^{m-1} - 2 - 2^{\lambda-1}\delta$	$2^{m-1} - 2^{\lambda-1}\varepsilon$	$2^{m-1} + 2^{\lambda-1}\delta$	$2^{m-1} + 2^{\lambda-1}\varepsilon$	$\lvert\varepsilon\rvert \neq \lvert\delta\rvert$

□ Let θ be a root of the polynomial $\overline{G}(x)$ in the field $Q = GF(2^m)$, and let tr be the trace function from Q into $\overline{R}$. By (19.41), (19.42), the coordinate sequences of u can be represented by the trace function. Since we are interested in the distribution of elements on the cycle of u, we may suppose without loss of generality that

$$u_0(i) = \mathrm{tr}\,(\theta^i), \qquad u_1(i) = \mathrm{tr}\,(b\theta^i) + i\,\mathrm{tr}\,(c\theta^i) + \sigma_2(\theta^i), \qquad i \geq 0,$$

where $b \in Q$ is a constant depending on the initial vector of u, $c \in Q$ is a constant determined by properties of the polynomial $G(x)$, and $\sigma_2(x) = \sum_{0 \leq j < k < m} x^{2^j + 2^k}$. Since θ is a primitive element of Q, the frequency $\nu_u(a)$ of appearance of the element $a = a_0 + 2a_1$, $a_0, a_1 \in \{0, 1\}$, on the cycle of u is equal to the sum of the number of nonzero solutions over Q of the system of equations

$$\mathrm{tr}\,(x) = a_0, \qquad \mathrm{tr}\,(bx) + \sigma_2(x) = a_1$$

and of the number of nonzero solutions over Q of the system

$$\mathrm{tr}\,(x) = a_0, \qquad \mathrm{tr}\,((b+c)x) + \sigma_2(x) = a_1.$$

The first system corresponds to the terms $u(i)$ with even i, and the second to the terms with odd i. Thus, the problem is to evaluate the weights of the quadric quantics of the form $\mathrm{tr}\,(bx) + \sigma_2(x)$ over Q and the weights of their restrictions to the set $\{x \in Q |\ \mathrm{tr}\,(x) = 0\}$. It follows from the theory of quadrics over a field of characteristic 2 [9, 39] that for this purpose it is sufficient to evaluate the ranks and defects of the appropriate quadrics (see also Section 30 below). Straightforward evaluations lead to the stated results. □

This approach also makes it possible to estimate the frequencies of appearances of vectors on the cycle of an LRS u over $\mathbf{Z}_4$.

27.3. Theorem [22]. *Let u be an LRS over $\mathbf{Z}_4$ of maximal period $T = 2(2^m - 1)$ with minimal polynomial $G(x)$ of degree m. Let $s \le m/4$, $0 = k_0 < k_1 < \ldots < k_{s-1}$, and let the system of residues of the polynomials $x^{k_0}, \ldots, x^{k_{s-1}}$ modulo $\overline{G}(x)$ be linearly independent over $\overline{R} = GF(2)$. Then for any vector $\mathbf{a} \in \mathbf{Z}_4^s$*

$$\left| \nu_u^T \begin{pmatrix} \mathbf{k} \\ \mathbf{a} \end{pmatrix} - \frac{T}{4^s} \right| < \sqrt{T}. \quad \square$$

Applying probabilistic methods, it has been shown in [1] that if an LRS u is randomly chosen from $L_R(G)$, where $R = \mathbf{Z}_{2^n}$ and $G(x)$ is an MP-polynomial of degree m, then the distribution of vectors of length $t \le m$ on the segment of length N of the sequence u is close to the distribution of vectors on the segment of random sequence over $R = \mathbf{Z}_{2^n}$.

But all these results tell nothing about the presence of all elements of the ring on the cycle of an MP-recurrence.

27.4. Theorem [22]. *Let u be an LRS of maximal period of rank m over $R = \mathbf{Z}_{p^n}$. If $m(p-1) > p^n$, then $\nu_u(a) > 0$ for any $a \in R$. If $m(p-1) \ge (p^n - 1)$, then $\nu_u(a) > 0$ for any $a \in R^*$.*

□ Let $v = -u$ and $u_s = \delta_s(u)$, $v_s = \delta_s(v)$ be the p-ary coordinate sequences of the sequences u and v (see Section 19.B). It is necessary to prove that each nonzero element of R appears on the cycle of LRS $u \bmod p^{n-1}$. Suppose the contrary. Then $\overline{u}_{n-1} + \overline{v}_{n-1} = \overline{\varepsilon}$, where $\overline{\varepsilon}$ is the sequence of units of the field $\overline{R} = R/pR$. Let $G(x)$ be the minimal polynomial of u and let $\overline{\xi}$ be a root of $\overline{G}(x)$ in $GF(p^m)$. Since $\overline{\varepsilon}(i) = \overline{\xi}^{\tau i}$, $i \ge 0$, where $\tau = p^m - 1$, the polynomial complexity of $\overline{\varepsilon}$ with respect to $\overline{G}(x)$ is equal to $m(p-1)$ (see Definition 24.8). On the other hand, by Lemma 24.10 and by (24.6), $\rho(\overline{G}(x) | \overline{u}_{n-1} + \overline{v}_{n-1}) \le p^{n-1}$, and so we have a contradiction with the condition $m(p-1) > p^{n-1}$.

Now, to prove that any nonzero element $a \in \mathbf{Z}_{p^n}$ appears on the cycle of $u \bmod p^{n-1}$, it is necessary to consider the coordinate sequences of the recurrences u' and v' (instead of u, v), where $u'(i) = u(i) - a$, $i \ge 0$, $v' = -u'$. □

In contrast to MP-recurrences over residue rings, a k-maximal recurrence u of rank m over a Galois ring $R = GR(q^n, p^n)$ (see Section 19.D) has statistical characteristics which are similar to the characteristics of a k-maximal recurrence over a finite field. In this case

$$T(u) = T = (q^m - 1)q^{m(n-1)}, \tag{27.1}$$

and the cycle of u is described by

$$\mathcal{T}(u) = \{\mathbf{x}^{i_0}u, \ldots, \mathbf{x}^{i_{T-1}}u\} \tag{27.2}$$

(cf. (26.3)). Let $\mathfrak{A}(J) \subset R^J$ be the polyhedron of values of the form (26.5), and let $\nu_u(J/\mathfrak{A}(J))$ be the number of solutions $s \in \overline{0, T-1}$ of Eq. (26.6).

27.5. Theorem. *Let the k-maximal recurrence u of rank m over a Galois ring R satisfy the conditions of Theorem* 19.25, *and let the system* (26.4) *of vectors be such that $\{\alpha^{j_1}, \ldots, \alpha^{j_l}\}$ is a free system of elements of the module Q_R. Then $l \le m$ and*

$$\nu_u(J/\mathfrak{A}(J)) = \begin{cases} q^{m-l}q^{m(n-1)}, & \text{if } \overline{\mathfrak{A}}(\overline{J}) \ne \overline{0}, \\ (q^{m-l} - 1)q^{m(n-1)}, & \text{if } \overline{\mathfrak{A}}(\overline{J}) = \overline{0} \end{cases}$$

□ By (19.47) and (19.46), $\nu_u(J/\mathfrak{A}(J))$ is equal to the number of solutions in Q^* of the system of linear equations

$$\mathrm{Tr}_P^Q(\xi\alpha^{j_t}x) = a(j_t), \qquad t \in \overline{1,l}.$$

Since $\{\alpha^{j_1},\dots,\alpha^{j_l}\}$ is a free system, this system of equations has $q^{m-l}q^{m(n-1)}$ solutions in Q. If $\overline{\mathfrak{A}}(\overline{J}) \neq \overline{0}$, then each solution belongs to Q^*. If $\overline{\mathfrak{A}}(\overline{J}) = \overline{0}$, then exactly $q^{m(n-1)}$ solutions belong to $pQ = Q\backslash Q^*$. □

28. Uniformly Distributed Linear Recurring Sequences over Residue Rings

A reversible (i.e., purely periodic) sequence u over a ring R such that the elements of R have the same frequencies of appearance on the cycle of u is called a *uniformly distributed* LRS (ULRS) [15, 168]. Here we consider only two aspects of the investigation of ULRS: how does one construct a ULRS over a residue ring and what is the maximum of periods of a ULRS of a given order k?

Let $R = \mathbb{Z}_{p^n}$, p prime, and let w be a ULRS over R with characteristic polynomial $H(x)$ of degree k. Then

$$p^n|T(w)|T(H)|T(\overline{H})p^{n-1},$$

and therefore $p|T(\overline{H})$. Define $T(R,k)$ as the maximum of periods of ULRS over R of the given order k.

28.1. Theorem. *Let $R = \mathbb{Z}_{p^n}$. Then*

$$T(R,2) \leq (p-1)p^n \text{ and } T(R,k) \leq (p^{k-2}-1)p^n \text{ for } k > 2.$$

□ If w is a ULRS with minimal polynomial $H(x)$, then $T(w) = T(H) \leq T(\overline{H})p^{n-1}$, $p|T(\overline{H})$, and the polynomial $\overline{H}(x)$ is reversible. Now, it is sufficient to note that if $h(x)$ is a reversible polynomial over $GF(p)$ of degree k such that $p|T(h)$, then $T(h) \leq p(p-1)$ for $k = 2$ and $T(h) \leq p(p^{k-2}-1)$ for $k > 2$. □

Since the residue ring $\mathbb{Z}_N$ is the direct sum of primary residue rings, Theorem 28.1 makes it possible to estimate $T(\mathbb{Z}_N, k)$ for arbitrary $N \geq 2$.

ULRS of order 2 over $\mathbb{Z}_{p^n}$ are completely described in [168]. This article also contains a review on this subject. We now formulate some results of [168] in a form convenient for us.

28.2. Theorem. *Let u be an LRS over $R = \mathbb{Z}_{p^n}$ with characteristic polynomial $H(x)$ of degree 2 and with generator $\Phi_u(x)$. Then u is uniformly distributed if and only if the following conditions hold:*

(a) $\overline{H}(x) = (x-\overline{a})^2$, $a \in R^*$;

(b) *if $p = 2$, $n > 1$, then $H(x) \equiv (x-e)^2 \pmod 4$;*

if $p = 3$, $n > 1$, then $T(H) = T(\overline{H}) \cdot 3^{n-1}$.

(c) $(H(x), \Phi_u(x)) = e$. □

Let $L_R^0(H)$ be the set of all recurrences $u \in L_R(H)$ such that the generator of u is coprime with $H(x)$.

28.3. Theorem (A. Nechaev, 1986). *Let $H(x) = F(x)G(x)$ be a polynomial of degree $k \geq 4$ over $R = \mathbb{Z}_{p^n}$, where $F(x)$ satisfies conditions* (a) *and* (b) *of Theorem* 28.2, *and let $G(x)$ be a reversible polynomial of degree $m = k-2$ such that $\overline{G}(x)$ is an MP-polynomial over the field $\overline{R}$, i.e., $T(\overline{G}) = p^m - 1 = \tau$. Then for any $w \in L_R^0(H)$*

(a) *there exist uniquely defined sequences $u \in L_R^0(F)$, $v \in L_R^0(G)$ such that $w = u + v$;*

(b) *w is a ULRS of order k and period $T(w) = \tau p^n$;*

(c) *for any $i \in \mathbb{N}_0$, the sequence $w(i), w(i+\tau), \dots, w(i+\tau(p^n-1))$ is a permutation of elements of R.*

□ (a) The desired result follows from the condition $(F(x), G(x)) = e$ and from the equality $L_R(FG) = L_R(F) \dotplus L_R(G)$.

(b) Since $T(F) = \lambda p^n$, $T(G) = \tau p^d$, where $\lambda|\tau$, $d \in \overline{0,n-1}$, we have

$$T(w) = T(H) = [T(G), T(F)] = [\tau p^d, \lambda p^n] = \tau p^n.$$

The uniformity of w follows from (c).

(c) It is sufficient to prove that if $j \in \mathbf{N}$, $(j,p) = 1$, and $r \in \overline{0,n-1}$, then

$$\|w(i + \tau j p^r) - w(i)\| = r, \tag{28.1}$$

where $\|x\|$ is the norm of $x \in R$ (see 16.1). Let $w = u + v$ be the decomposition from (a). By (19.25), $T(v \bmod p^{r+1}) | \tau p^r$, hence $\|v(i+\tau j p^r) - v(i)\| \geq r+1$. Theorem 28.2 implies that $T(u \bmod p^{r+1}) = (\operatorname{ord} \overline{a}) \cdot p^{r+1}$, hence $\|u(i + \tau j p^r) - u(i)\| = r$. This implies (28.1). □

28.4. Corollary. *If $R = \mathbf{Z}_{p^n}$, $p^{k-2} > 2$, then*

$$T(R,k) = p^n(p^{k-2} - 1). \quad \square$$

The concept of an extension of a sequence (Section 8) proves to be useful for constructing a ULRS. If $R = \mathbf{Z}_{p^n}$ and $H(x) = (x-e)^2 G(x)$, then each LRS $w \in L_R^0(H)$ is an extension of the congruent sequence $v(i) = ai + b$, $a \in R^*$, $b \in R$ (see 1.4) by polynomial $G(x)$ and vector $w(\overline{0,m-1})$ (see (8.5)). This gives a simple method of realizing such a ULRS.

One can generalize this method to ULRS over an arbitrary residue ring. For example, let $R = \mathbf{Z}_{(pq)^n}$, where p, q are distinct primes. Let z be the sequence over $S = \mathbf{Z}_{(pq)^{n+\nu}}$ given by

$$z(i) = ai + b, \text{ where } a \equiv e \pmod p, \quad b \in S^*, \text{ and if } p = 2, \text{ then } a \equiv e \pmod 4,$$

and let $v(i) = [z(i)/(pq)^\nu]$, where the square brackets mean the integral part. We suppose that a reversible polynomial $G(x) \in R[x]$ of degree $m \geq 2$ and numbers M, $N \in \mathbf{N}_0$ satisfy the following conditions:

$$T(G \bmod p) = p^m - 1, \qquad T(G \bmod q) = q^m - 1, \qquad q^M | p^m - 1, \qquad p^N | q^m - 1,$$

$$((p^m - 1)/q^M, q) = 1, \qquad ((q^m - 1)/p^N, p) = 1, \qquad \max\{1, M, N\} \leq \nu.$$

28.5. Proposition (A. Kuzmin, 1986). *Under our previous hypotheses, let w be an extension of LRS v by the polynomial $G(x)$ and arbitrary vector $w(\overline{0,m-1})$. Then w is a ULRS over R.*

□ The proof is analogous to the proof of 28.3(b). □

We now state a result which shows that uniformly distributed sequences have some interesting analytical properties.

28.6. Theorem (A. Kuzmin and A. Nechaev, 1990). *Let $R = \mathbf{Z}_{p^n}$, w be a ULRS from $L_R(H)$. Suppose that the following conditions hold:*

(a) $H(x) = (x-e)^2 G(x)$, $\deg G(x) = m \geq 2$, $T(\overline{G}) = p^m - 1$;

(b) $T(w) = T(H) = p^n(p^m - 1)$.

Then, the minimal polynomials $M_t(x)$, $t \in \overline{0,n-1}$, of the coordinate sequences $\delta_t(w)$ of w in the p-ary coordinate set satisfy the following relations: if $p \geq 3$, then

$$M_t(x) = (x - \overline{e})^{p^t+1} \cdot \prod_{\substack{1 \leq N \leq p^t \\ N < m(p-1)}} \overline{G}^{(N)}(x)^{p^t - N + 1},$$

and if $p = 2$, then $M_t(x)$ divides on

$$(x - \overline{e})^{2^t+1} \cdot \prod_{\substack{1 \leq N \leq 2^t \\ N < m, 2 | N}} \overline{G}^{(N)}(x)^{2^t - N + 1},$$

where $\overline{G}^{(N)}(x)$ are the polynomials defined in Section 24.A. □

Chapter 6.

SOME APPLICATIONS IN CODING THEORY

29. LRS-Families and Linear Cyclic Codes

Let R be a finite ring and let M be an exact R-module.

A. 1-codes over modules. We transfer the standard terminology of the theory of codes over fields [4, 39]. An arbitrary subset $\mathcal{K} \subseteq M^N$ is called a *code of length N over the module ${}_RM$*. $\mathcal{K}$ is a *linear* (*R-linear*) *code* if $\mathcal{K}$ is a submodule of M.

The *Hamming weight* $\mathrm{Wt}(\alpha)$ of a vector $\alpha = (\alpha_0, \ldots, \alpha_{N-1}) \in M^N$ is the number of nonzero components of α. The *distance* between $\alpha, \beta \in M^N$ is defined by $d(\alpha, \beta) = \mathrm{Wt}(\alpha - \beta)$. The *code distance* of a code $\mathcal{K}$ is defined by $d(\mathcal{K}) = \min\{d(\alpha, \beta) |\ \alpha, \beta \in \mathcal{K},\ \alpha \neq \beta\}$. If $\mathcal{K}$ is a linear code, then

$$d(\mathcal{K}) = \min\{\mathrm{Wt}(\alpha) :\ \alpha \in \mathcal{K} \backslash 0\}. \tag{29.1}$$

A code $\mathcal{K}$ *detects r mistakes* if $d(\mathcal{K}) > r$, and *corrects t mistakes* if $d(\mathcal{K}) \geq 2t + 1$.

An $(N \times l)$-matrix H over R is called the *check matrix of a linear code* $\mathcal{K}$ if $\mathcal{K} = \{\alpha \in M^N |\ \alpha H = 0\}$. The system $H_1, \ldots, H_r$ of rows of the matrix H is said to be free over M if $a_1 H_1 + \ldots + a_r H_r = 0$, where $a_1, \ldots, a_r \in M$, implies $a_1 = \ldots = a_r = 0$.

29.1. Proposition. *If $\mathcal{K} < M^N$ is a linear code with check matrix H, then $d(\mathcal{K}) = r + 1$, where r is the maximal number such that any system of r rows of H is free over M.* □

Note that there exists an example of a linear code which has no check matrix.

29.2. Proposition [49, 137]. *Any linear code $\mathcal{K} < M^N$ has a check matrix over R if and only if M is a QF-module.* □

Recall that in Section 4 a method of constructing a QF-module over an arbitrary finite (commutative) ring R was given.

If $I \lhd \mathcal{P}$ is a monic ideal, then the set

$$L_M^{(N)}(I) = \{\mu(\overline{0, N-1}) |\ \mu \in L_M(I)\} \tag{29.2}$$

is a linear code of length N over M. If M is a QF-module, then the check matrix of this code can be easily written out if a system of generators of I is given. But not every linear code $\mathcal{K}$ can be represented in the form $\mathcal{K} = L_M^{(N)}(I)$ for a suitable I (even when M is a QF-module). The situation is completely different when $\mathcal{K}$ is a cyclic code.

We define the cyclic shift operator on M^N by $\bigtriangledown\alpha = (\alpha_1, \ldots, \alpha_{N-1}, \alpha_0)$, $\alpha \in M^N$. A code $\mathcal{K}$ is called *cyclic* if $\bigtriangledown\mathcal{K} = \mathcal{K}$.

29.3. Theorem. *Let M be a QF-module and let $I \lhd \mathcal{P}$ be a monic ideal. A code*

$$\mathcal{K} = L_M^{(N)}(I) \tag{29.3}$$

is cyclic if and only if I is a reversible ideal and $T(I)|N$. Any cyclic code $\mathcal{K} < M^N$ has the form (29.3) *for a suitable I.*

□ Let $\mathcal{K} < M^N$ be a linear cyclic code and $\mathcal{M} \subseteq M^{(1)}$ be the set of sequences μ of the form

$$\mu = (a_0, a_1, \ldots, a_{N-1}, a_0, a_1, \ldots, a_{N-1}, a_0, \ldots)$$

such that $\mu(\overline{0,N-1}) \in \mathcal{K}$. Obviously, $\mathcal{M}$ is a finitely generated R-submodule in $M^{(1)}$, and also a $\mathcal{P}$-submodule, since, by the definition of a cyclic code, $x\mu \in \mathcal{M}$ for $\mu \in \mathcal{M}$. Therefore, $\mathcal{M} = L_M(I)$, where $I = \mathrm{An}(\mathcal{M})$ (see 4.6), and (29.2) holds. The definition of $\mathcal{M}$ implies that $x^N - e \in I$, i.e., I is a reversible ideal and $T(I)|N$. □

29.4. Example. Let $g(x)$ be a polynomial of maximal period $\tau = q^m - 1$ over $P = GF(q)$, $\deg g(x) = m$. Then $L_P^{(\tau)}(g)$ is a linear cyclic code of length τ and dimension m, with code distance $d = (q-1)q^{m-1}$, and the weight of each nonzero vector from $L_P^{(\tau)}(g)$ is equal to d (see Section 26). Such a code is called a *symplectic code of maximal length* [39].

29.5. Example. Let $R = GR(q^n, p^n)$ be a Galois ring, and let $G(x) \in R[x]$ be the distinguished polynomial of degree m corresponding to a polynomial $g(x) \in \overline{R}[x]$ of maximal period $\tau = q^m - 1$ (Section 17.B). Then $L_R^{(\tau)}(G)$ is a linear cyclic code of length τ and dimension m over R (i.e., a free R-module of rank m). It consists of q^{mn} elements and has code distance $d(L_R^{(\tau)}(G)) = (q-1)q^{m-1}$.

29.6. Example. Let $R = GR(q^n, p^n)$ be a Galois ring, $F(x) \in R[x]$ be a polynomial of degree m of maximal period $N = (q^m - 1)p^{n-1}$. Then $L_R^{(N)}(F)$ is a linear cyclic code of dimension m over R and with code distance $d(L_R^{(N)}(F)) = p^{n-1}(q-1)q^{m-1}$.

B. k-Linear cyclic codes. Let $N_1, \ldots, N_k$ be natural numbers and M^{Π} be an R-module, where $\Pi = \Pi(\mathbf{N})$ (see Section 2.B). An R-submodule $\mathcal{K} < M^{\Pi}$ is called a *k-linear code over M of volume $N_1 \times \ldots \times N_k$*. Obviously, $\mathcal{K}$ is isomorphic to some linear code over M of length $N = N_1 \ldots N_k$. The Hemming weight of a code vector $\mu(\Pi) \in \mathcal{K}$ and the code distance $d(\mathcal{K})$ of $\mathcal{K}$ are defined analogously to the case of 1-linear codes.

If $I \lhd \mathcal{P}_k$ is a monic ideal, then the set $L_M^{(\mathbf{N})}(I) = \{\mu(\Pi) | \ \mu \in L_M(I)\}$ is a linear code over M of volume $N_1 \times \ldots \times N_k$.

We define k cyclic shift operators $\bigtriangledown_1, \ldots, \bigtriangledown_k$ on M^{Π} by the rule $\bigtriangledown_s(\mu(\Pi)) = \nu(\Pi)$ for $\mu(\Pi) \in M^{\Pi}$, where $\nu(z_1, \ldots, z_k) = \mu(z_1, \ldots, z_s \underset{s}{\oplus} 1, \ldots, z_k)$ and $\underset{s}{\oplus}$ is the addition modulo N_s. A code $\mathcal{K} < M^{\Pi}$ is called k-cyclic if $\bigtriangledown_s \mathcal{K} = \mathcal{K}$ for $s \in \overline{1,k}$.

29.7. Theorem. *Let M be a QF-module and let $I \lhd \mathcal{P}_k$ be a monic ideal. The code*

$$\mathcal{K} = L_M^{(\mathbf{N})}(I) \tag{29.4}$$

is k-cyclic if and only if

$$x_1^{N_1} - e, \ldots, x_k^{N_k} - e \in I. \tag{29.5}$$

Any cyclic code $\mathcal{K} < M^{\Pi}$ has the form (29.4), *where I satisfies* (29.5).

□ Let $\mathcal{K}$ be a cyclic code in M^{Π}. Let $\mathcal{M}$ be the subset of all recurrences $\mu \in L_M(x_1^{N_1} - e, \ldots, x_k^{N_k} - e)$ such that $\mu(\Pi) \in \mathcal{K}$. Obviously, $\mathcal{M}$ is a finitely generated R-submodule, and also a $\mathcal{P}$-submodule, since, by the definition of a cyclic code, $x_s \mathcal{M} = \mathcal{M}$ for $s \in \overline{1,k}$. Therefore, $\mathcal{M} = L_M(I)$, where $I = \mathrm{An}(\mathcal{M})$ (see 4.6), and (29.5) holds. The converse is easy. □

29.8. Example. Let $I \lhd \mathcal{P}_k$ be an ideal of maximal period $q^m - 1$ over $P = GF(q)$ (see 12.3), $Q = GF(q^m)$ be the field of a root of I over P, and $\alpha = (\alpha_1, \ldots, \alpha_k)$ be a root of I. Then $Q^* = \langle \alpha_1, \ldots, \alpha_k \rangle$ (see (12.3)). Let $\mathrm{ord}\, \alpha_s = N_s$, $s \in \overline{1,k}$. Then the code $\mathcal{K} = L_P^{(\mathbf{N})}(I)$ is a k-linear cyclic code, consisting of all $u(\Pi)$ such that u is a sequence of the form (12.4). If $\alpha_1, \ldots, \alpha_k$ are such that $N_1 \ldots N_k = q^m - 1$, or, equivalently, $Q^* = \langle \alpha_1 \rangle \dot{\times} \ldots \dot{\times} \langle \alpha_k \rangle$, then the unique nonzero cycle of the family $L_P(I)$ has the form $\mathcal{T}(u) = \{\mathbf{x}^{\mathbf{i}} u | \ \mathbf{i} \in \Pi\}$. In this case, the results of Section 26 imply that $\mathcal{K}$ is a *simplex code*, i.e., the distance between two arbitrary vectors of $\mathcal{K}$ is equal to

$$(q-1)q^{m-1} = N_1 \ldots N_k \cdot (1 - (q^{m-1} - 1)/(q^m - 1)).$$

This code is equivalent (see [39]) to the code from Example 29.4 (see also [128, 143, 157]).

29.9. Example. Let $I \lhd \mathcal{P}_k$ be an ideal of maximal period $T = (q^m - 1)q^{m(n-1)}$ over a Galois ring $R = GR(q^n, p^n)$ (see 19.19, 19.20) and $Q = GR(q^{mn}, p^n)$ be an extension of R. Suppose that $\alpha_1, \ldots, \alpha_k \in Q^*$ are elements such that $\alpha = (\alpha_1, \ldots, \alpha_k)$ is a root of the ideal I. Then (19.46) holds, and each k-LRS $u \in L_R(I)$ has the form (19.47), where $\xi \in Q$. Let $\operatorname{ord} \alpha_s = N_s$, $s \in \overline{1,k}$. Then $\mathcal{K} = L_R^{(\mathbf{N})}(I)$ is a k-linear cyclic code. If $\alpha_1, \ldots, \alpha_k$ are such that $Q^* = \langle \alpha_1 \rangle \dot{\times} \ldots \dot{\times} \langle \alpha_k \rangle$, i.e., $N_1 \ldots N_k = T$, then the vector with minimal weight in $L_R^{(\mathbf{N})}(I)$ is $u(\Pi)$, where $u \in L_R(I)$, $u(\mathbf{z}) = \operatorname{Tr}_P^Q(p^{n-1}\xi\alpha^{\mathbf{z}})$, $\xi \in Q^*$. This vector is, in fact, the $q^{m(n-1)}$-times repeated vector from Example 29.8. Hence,

$$d(\mathcal{K}) = Wt(u(\Pi)) = q^{m(n-1)}q^{m-1}(q-1) = N_1 \ldots N_k(1 - (q^{m-1}-1)/(q^m-1)).$$

30. Some Constructions of Nonlinear Cyclic Codes with the Help of Linear Recurrences over Galois Rings

A. Constructions of codes [25, 45, 47]. Let $R = GR(q^n, p^n)$ be a Galois ring. Recall (see Section 19.B) that each element $a \in R$ can be represented in the form

$$a = \gamma_0(a) + p\gamma_1(a) + \ldots + p^{n-1}\gamma_{n-1}(a), \qquad \gamma_t(a) \in \Gamma(R),$$

where $\Gamma(R)$ is the p-adic coordinate set of R.

Let $F(x) \in \mathcal{P} = R[x]$ be a reversible polynomial of degree m. The initial vector $u(\overline{0, m-1})$ of an LRS $u \in L_R(F)$ is uniquely determined by the vector

$$\gamma(u(\overline{0, m-1})) = (\gamma_0(u(0)), \ldots, \gamma_0(u(m-1)), \gamma_1(u(0)), \ldots, \gamma_{n-1}(u(m-1)))$$

of length mn over the field $\Gamma(R)$. Define the vector

$$\gamma_{n-1}(u(\overline{0, N-1})) = (\gamma_{n-1}(u(0)), \gamma_{n-1}(u(1)), \ldots, \gamma_{n-1}(u(N-1)))$$

of length $N = T(u)$ over $\Gamma(R)$. We say that this vector codes the information vector $\gamma(u(\overline{0, m-1}))$. We define the code $C^\gamma(F)$ as

$$C^\gamma(F) = \{\gamma_{n-1}(u(\overline{0, N-1}))|\ u \in L_R(F)\}.$$

In the case where $R = \mathbf{Z}_{p^n}$, an element $a \in R$ also has the p-ary representation (see Section 19.B)

$$a = \delta_0(a) + p\delta_1(a) + \ldots + p^{n-1}\delta_{n-1}(a), \qquad \delta_t(a) \in \overline{0, p-1},$$

and we can define $C^\delta(F)$ as the code, consisting of vectors

$$\delta_{n-1}(u(\overline{0, N-1})) = (\delta_{n-1}(u(0)), \delta_{n-1}(u(1)), \ldots, \delta_{n-1}(u(N-1))).$$

Note that we cannot even restore (in the general case) the information vector $\gamma(u(\overline{0, m-1}))$ by the code vector $\gamma_{n-1}(u(\overline{0, N-1}))$, since it is possible that $|C^\gamma(F)| < |L_R(F)| = q^{mn}$.

30.1. Theorem [25]. *If $F(x)$ is an MP-polynomial over R, then $C^\gamma(F)$ is a nonlinear cyclic code of length $N = p^{n-1}(q^m - 1)$, and $|C^\gamma(F)| = q^{mn}$. The information vector $\gamma(u(\overline{0, m-1}))$ can be uniquely restored by the code word $\gamma_{n-1}(u(\overline{0, N-1}))$ with the complexity $O(N)$. If $R = \mathbf{Z}_{p^n}$, then the same propositions are valid for the code $C^\delta(F)$. If $p^{n-1} < m(p-1)$, then $C^\delta(F)$ is equivalent to a subcode of the code*

$$\mathrm{RM}(p^{n-1}, p^m - 1)^{(p^{n-1})} = \mathrm{RM}(p^{n-1}, p^m - 1) \times \ldots \times \mathrm{RM}(p^{n-1}, p^m - 1),$$

where $\mathrm{RM}(p^{n-1}, p^m - 1)$ is the Reed–Muller code over $GF(p)$ of length $p^m - 1$ and of order p^{n-1} [4].

□ The desired results follow from the descriptions (19.42), (19.43) of the coordinate sequences of MP-recurrences over Galois rings. □

B. Codes based on recurrences over $GR(q^2, p^2)$. Let $F(x)$ be an MP-polynomial over $R = GR(q^2, p^2)$, $q = p^l$. In this case, we get a complete description of the structure of the vectors of $C^\gamma(F)$. Let ξ be a root of $F(x)$ in the Galois extension $Q = GR(q^{2m}, p^2)$ of R. Then $\xi_0 = \gamma_0(\xi)$ is a primitive element of the field $\Gamma(Q)$. Let $c = c_F = \gamma_1(\xi) \cdot \gamma_0(\xi)^{-1}$. For $\alpha, \beta \in \Gamma(Q)$, $k \in \overline{0, p-1}$ denote

$$\Psi_{\alpha,\beta,k}(x) = \Psi_1^{(l)}(\alpha x) \oplus \operatorname{tr}(\beta x) \oplus k \cdot \operatorname{tr}(c\alpha x),$$

where $\operatorname{tr}(x) = x \otimes x^q \otimes \ldots \otimes x^{q^{m-1}}$ is the trace mapping from $\Gamma(Q)$ into $\Gamma(R)$ and $\Psi_1^{(l)}(x)$ is defined in Section 19.C. For a function $f: \Gamma(Q) \to \Gamma(R)$ we denote $\vec{f}(x) = (f(e), f(\xi_0), \ldots, f(\xi_0^{q^m-2}))$.

30.2. Theorem [25]. *Let $F(x)$ be an MP-polynomial over R. Then the code $C^\gamma(F)$ of length $N = (q^m - 1)p$ is equivalent to the code C, consisting of all vectors of the form*

$$(\vec{\Psi}_{\alpha,\beta,0}(x), \vec{\Psi}_{\alpha,\beta,1}(x), \ldots, \vec{\Psi}_{\alpha,\beta,p-1}(x)),$$

where $\alpha, \beta \in \Gamma(Q)$. The code C is a subcode of the code $\mathrm{RM}(p, p^m - 1)^{(p)}$. The code distance of $C^\gamma(F)$ satisfies

$$\frac{q-1}{q}(N+p)\frac{p-1}{p} - p \le d(C^{(\gamma)}(F)) \le \frac{q-1}{q}(N+p) - p.$$

There exists an algorithm of complexity $O(N \cdot \log N)$, which corrects $\frac{1}{4}(p-1)(q^m - q^{m-1} - 1)$ mistakes in a code word.

□ The description of the code words of $C^\gamma(F)$ follows from the description (19.42) of the first coordinate sequence $\gamma_1(u)$ of the MP-recurrence $u \in L_R(F)$. In order to estimate $d(C^{(\gamma)}(F))$, we consider two distinct vectors $\gamma_1(u(\overline{0, N-1})), \gamma_1(u'(\overline{0, N-1})) \in C^\gamma(F)$, which correspond to two distinct recurrences $u, u' \in L_R(F)$. Then, by (24.5),

$$(x^\tau - \bar{e})(u_1 - u_1') = \overline{\Phi}^{(1)}(x)(u_0 - u_0'), \text{ where } \tau = q^m - 1.$$

If $u_0 \ne u_0'$, then the right part of the last equality is an MP-recurrence over $GF(q)$. Hence,

$$q^{m-1}(q-1)(p-1) + (q^{m-1}-1)p \ge d(\gamma_1(u(\overline{0, N-1})), \quad \gamma_1(u'(\overline{0, N-1}))) \ge q^{m-1}(q-1)(p-1).$$

If $u_0 = u_0'$, then it follows from (19.42) that $\overline{u}_1 - \overline{u}_1' \in L_{\overline{R}}(\overline{F})$, and $d(\gamma_1(u(\overline{0, N-1})), \gamma_1(u'(\overline{0, N-1}))) = p(q-1)q^{m-1}$.

In order to obtain the algorithm of decoding of $C^\gamma(F)$, it is necessary to double the well-known algorithm of decoding of linear cyclic codes over $GF(q^m)$ [39], which restores $\vec{\mathrm{tr}}(\alpha x)$ and $\vec{\mathrm{tr}}(\beta x)$ and makes it possible to restore α and β. This algorithm is a direct generalization of the algorithm of decoding of the Kerdoc codes [45]. □

C. Nonlinear cyclic codes based on recurrences over $GR(q^2, 2^2)$. In the case $R = GR(q^2, 2^2)$, $q = 2^l$, the theory of quadric quantics over a field of characteristic 2 [9, 37] makes it possible to determine the exact value of $d(C^\gamma(F))$ depending on some characteristics of the constant $c = \gamma_1(\xi) \cdot \gamma_0(\xi)^{-1}$ and also to determine $d(C^\gamma(F_*))$, where $F_*(x)$ is the distinquished polynomial corresponding to $F(x)$ (see Sect. 17.B), i.e., the monic polynomial over R of the degree m with the root $\xi_0 = \gamma_0(\xi)$, so that $\overline{F}_*(x) = \overline{F}(x)$, $T(F_*) = q^m - 1$.

We now formulate some results about quadrics over finite fields of characteristic 2 [9, 39]. Let $g(x)$ be a quadric over $L = GF(q^m)$, $q = 2^l$, with bilinear symmetric form $f(x, y) = g(x+y) + g(x) + g(y)$. There exists a basis $e_1, \ldots, e_m$ of the space L over $GF(q)$ such that for some $r \le m/2$

$$f(e_i, e_j) = \begin{cases} e, & \text{if } \{i, j\} = \{s, s+r\}\ s \le r; \\ 0 & \text{otherwise.} \end{cases}$$

This basis is called a *symplectic basis of f*, and $2r$ is called the *rank of f*: $\operatorname{rank} f = 2r$. Let

$$L^\perp = L_f^\perp = \{x \in L \mid f(x, y) = 0 \text{ for any } y \in L\}, \qquad \dim L^\perp = m_0,$$

and $h(x)$ be the restriction of $g(x)$ to $L^{\perp}$. Then $h: L^{\perp} \to GF(q)$ is a linear map, and $m_1 = \dim \operatorname{Ker} h \geq m_0 - 1$. In these notations, the *defect* $\operatorname{def} g$ and the *rank* $\operatorname{rank} g$ of $g(x)$ are defined by

$$\operatorname{def} g = m_0 - m_1, \qquad \operatorname{rank} g = \operatorname{rank} f + \operatorname{def} g.$$

30.3. Theorem [9, 37, 39]. *Let $g(x)$ be a quadric over $L = GF(q^m)$, $q = 2^l$, with bilinear symmetric form $f(x,y)$ of rank $2r$. Then there exists a symplectic basis $e_1, \ldots, e_m$ of L such that*

$$g(x) = \sum_{i=1}^{r} x_i x_{i+r} + x_{2r+1}^2 \text{ if } \operatorname{def} g = 1,$$

$$g(x) = \sum_{i=1}^{r} x_i x_{i+r} + \varepsilon(x_r^2 + x_{2r}^2) \text{ if } \operatorname{def} g = 0,$$

where $\varepsilon = \sum_{i=1}^{r} g(e_i) g(e_{i+r})$. The weight $Wt(g)$ of $g(x)$ satisfies

$$Wt(g) = (q-1)q^{m-1} \text{ if } \operatorname{def} g = 1,$$

$$Wt(g) = (q-1)(q^{m-1} - q^{m-1-r}) \text{ if } \operatorname{def} g = 0,\ \varepsilon = 0,$$

$$Wt(g) = (q-1)(q^{m-1} + q^{m-1-r}) \text{ if } \operatorname{def} g = 0,\ \varepsilon \neq 0, \square$$

30.4. Theorem [25]. *If $F(x)$ is an MP-polynomial of degree $m > 1$ over R, then the parameters of the nonlinear cyclic codes $C^{\gamma}(F(x))$ and $C^{\gamma}(F_*(x))$ are described by the following table.*

Length	Efficiency	Conditions on m, $c = c_F$		Code distance	No.
Code $C^{\gamma}(F_*(x))$					
$N = q^m - 1$	$(N+1)^2$	$m = 2\lambda + 1$		$\frac{q-1}{q}(N + 1 - \sqrt{q(N+1)}) - 1$	1
		$m = 2\lambda$		$\frac{q-1}{q}(N + 1 - q\sqrt{N+1}) - 1$	2
Code $C^{\gamma}(F(x))$					
$N = 2(q^m - 1)$	$(1/4)(N+2)^2$	$m = 2\lambda + 1$	$c \in \Gamma(R)$	$\frac{q-1}{q}(N + 2 - \sqrt{q(N+2)/2}) - 2$	3
			$c \notin \Gamma(R)$	$\frac{q-1}{q}(N + 2 - \sqrt{2q(N+2)}) - 2$	4
		$m = 2\lambda$	$c \in \Gamma(R)$ or $\operatorname{tr}(c) \neq 0$	$\frac{q-1}{q}(N + 2 - q\sqrt{(N+2)/2}) - 2$	5
			$c \notin \Gamma(R)$ and $\operatorname{tr}(c) \neq 0$	$\frac{q-1}{q}(N + 2 - q\sqrt{2(N+2)}) - 2$	6

$\square$ Consider the code $C^{\gamma}(F)$. For $p = 2$, by (19.33),

$$\Psi_1^{(l)}(x) = \varkappa(x^h), \text{ where } \varkappa(x) = \sum_{0 \leq k < t < m} x^{q^k + q^t}, \qquad h = 2^{l-1}.$$

By (19.42),

$$u_1(i) = \Psi_1^{(l)}(\alpha \xi_0^i) \oplus \operatorname{tr}(\beta \xi_0^i) \oplus i \cdot \operatorname{tr}(\alpha c \xi_0^i), \qquad i \geq 0,$$

where $\alpha, \beta \in \Gamma(Q)$. We split the code word $\gamma_1(u(\overline{0, N-1}))$ into two parts, consisting of the coordinates $u_1(i)$ for even and odd i respectively:

$$u_1(2i) = \Psi_1^{(l)}(\alpha\xi_0^{2i}) \oplus \mathrm{tr}\,(\beta\xi_0^{2i}), \qquad 0 \le i \le q^m - 2,$$

$$u_1(2i+1) = \Psi_1^{(l)}(\alpha\xi_0\xi_0^{2i}) \oplus \mathrm{tr}\,((\beta + c\alpha)\xi_0\xi_0^{2i}), \qquad 0 \le i \le q^m - 2,$$

or

$$u_1(2i) = \varkappa(\alpha^h\xi_0^{qi}) \oplus (\mathrm{tr}\,(\beta^h\xi_0^{qi}))^2,$$

$$u_1(2i+1) = \varkappa((\alpha\xi_0)^h\xi_0^{qi}) \oplus (\mathrm{tr}\,(((\beta + c\alpha)\xi_0)^h\xi_0^{qi})^2. \tag{30.1}$$

Since ξ_0^q is a primitive element of $\Gamma(S)$, (30.1) implies that $C^\gamma(F)$ is equivalent to the code C, consisting of all vectors of the form $\vec{\omega} = (\vec{\Psi}_0(x), \vec{\Psi}_1(x))$, where

$$\Psi_0(x) = \varkappa(\alpha x) \oplus (\mathrm{tr}\,(\beta x))^2,$$

$$\Psi_1(x) = \Psi_0(x) \oplus (\mathrm{tr}\,(\alpha c^h x))^2, \qquad \alpha, \beta \in \Gamma(Q).$$

Consider the distance between two arbitrary code words $\vec{\omega}$ and $\vec{\omega}' = (\vec{\Psi}'_0(x), \vec{\Psi}'_1(x))$ of C, where

$$\Psi'_0(x) = \varkappa(\alpha' x) \oplus (\mathrm{tr}\,(\beta' x))^2, \qquad \Psi'_1(x) = \Psi'_0(x) \oplus (\mathrm{tr}\,(\alpha' dx))^2, \qquad d = d_F = c_F^h.$$

This distance is equal to the sum $Wt(\Delta_0) + Wt(\Delta_1)$ of the weights of the functions

$$\Delta_0(x) = \Psi_0(x) \oplus \Psi'_0(x), \qquad \Delta_1(x) = \Psi_1(x) \oplus \Psi'_1(x).$$

If $\alpha' = \alpha$, then $\Delta_0(x)$ and $\Delta_1(x)$ are linear functions over $\Gamma(Q)$, and the sum of their weights is equal to $2(q-1)q^{m-1}$. If $\alpha' \ne \alpha$, then, without loss of generality, we may suppose that $\alpha' = e$, $\alpha \ne e$. Then $d(C^\gamma(F))$ is equal to the minimum of the sums $Wt(\Delta_0) + Wt(\Delta_1)$ of the weights of the functions

$$\Delta_0(x) = \varkappa(\alpha x) \oplus \varkappa(x) \oplus \mathrm{tr}\,((\beta + \beta')x)^2,$$

$$\Delta_1(x) = \Delta_0(x) \oplus \mathrm{tr}\,((\alpha + e)dx)^2$$

over all $\alpha, \beta, \beta' \in \Gamma(Q)$. Denote $\mu = (e+\alpha)^{-1}$, $\eta = (\beta + \beta')^2$, $x = \mu y$. Then

$$\Delta_0(y) = \varkappa(\mu y) \oplus \varkappa((e+\mu)y) \oplus \mathrm{tr}\,(\eta\mu y)^2,$$

$$\Delta_1(y) = \Delta_0(y) \oplus \mathrm{tr}\,(dy)^2.$$

If $L_a = \{y \in \Gamma(Q) \mid \mathrm{tr}\,(dy)^2 = a\}$, $a \in \Gamma(R)$, and $\Delta_0^{(a)}$, $\Delta_1^{(a)}$ are the restrictions of Δ_0, Δ_1 to L_a, then it can be immediately verified that

$$Wt(\Delta_0) + Wt(\Delta_1) = \sum_{a \in \Gamma(R)} (Wt(\Delta_0^{(a)}) + Wt(\Delta_1^{(a)})) =$$

$$\sum_{a \in \Gamma(R)} (Wt(\Delta_0) + Wt(\Delta_0 + a)) = q^m - q^{m-1} + \frac{q-2}{q-1} \cdot Wt(\Delta_0) + \frac{q}{q-1} \cdot Wt(\Delta_0^{(0)}). \tag{30.2}$$

To evaluate $Wt(\Delta_0)$ and $Wt(\Delta_0^{(0)})$, we use Theorem 30.3. Since $\varkappa(x)$ is a quadric over $\Gamma(Q)$ with bilinear symmetric form

$$\varkappa(x) \oplus \varkappa(y) \oplus \varkappa(x+y) = \mathrm{tr}\,(xy) \oplus \mathrm{tr}\,(x)\mathrm{tr}\,(y),$$

the space $L^\perp = L_{\Delta_0}^\perp$ for the quadric Δ_0 is defined by

$$\begin{aligned} &L^\perp = 0, && \text{if } m = 2\lambda,\ \mathrm{tr}\,(\mu) \ne e;\\ &L^\perp = \Gamma(R) \oplus \mu\Gamma(R), && \text{if } m = 2\lambda,\ \mathrm{tr}\,(\mu) = e;\\ &L^\perp = (e + \mu + \mathrm{tr}\,(\mu))\Gamma(R), && \text{if } m = 2\lambda + 1, \end{aligned}$$

and Theorem 30.3 yields

$$Wt(\Delta_0) \geq (q-1)(q^{m-1} - q^{\lambda}), \text{ where } \lambda = [m/2].$$

We now consider the quadric $\Delta_0^{(0)}$ (defined on L_0). An element $x \in L_0$ belongs to $L_0^{\perp} = L_{\Delta_0^{(0)}}^{\perp}$ if and only if $\mathrm{tr}\,(dx) = 0$ and the element $x \oplus \mu \mathrm{tr}\,(x) \oplus \mathrm{tr}\,((e+\mu)x)$ belongs to the subspace $d \cdot \Gamma(R)$, generated by d over $\Gamma(R)$. Therefore, $L_0^{\perp} \subseteq \Gamma(R) \oplus \mu \cdot \Gamma(R) \oplus d \cdot \Gamma(R)$, and $\dim L_0^{\perp} \leq 3$. If $m = 2\lambda$, then $dim L_0 = m-1$, $\dim L_0^{\perp} \in \{1,3\}$; if $m = 2\lambda + 1$, then $\dim L_0 = m-1$, $\dim L_0^{\perp} \in \{0,2\}$. By 30.3,

$$\begin{aligned}
&Wt(\Delta_0^{(0)}) \geq (q-1)(q^{m-2} - q^{\lambda-1}), && \text{if } m = 2\lambda, && \mathrm{tr}\,(d) \neq 0 \text{ or } d \in \Gamma(R);\\
&Wt(\Delta_0^{(0)}) \geq (q-1)(q^{m-2} - q^{\lambda}), && \text{if } m = 2\lambda, && \mathrm{tr}\,(d) = 0,\ d \notin \Gamma(R);\\
&Wt(\Delta_0^{(0)}) \geq (q-1)(q^{m-2} - q^{\lambda}), && \text{if } m = 2\lambda+1, && d \notin \Gamma(R);\\
&Wt(\Delta_0^{(0)}) \geq (q-1)(q^{m-2} - q^{\lambda-1}), && \text{if } m = 2\lambda+1, && d \in \Gamma(R);
\end{aligned}$$

Now (30.2) implies that the values defined in the table in our theorem are the lower bounds of $d(C^{\gamma}(F))$. The proof of the fact that $d(C^{\gamma}(F))$ is equal to these lower bounds consists in the step-by-step examination of four cases, enumerated in the table (depending on the properties of m and c). In each case we find a pair μ, η such that the weights $Wt(\Delta_0)$, $Wt(\Delta_0^{(0)})$ reach the minimum simultaneously.

The distance of the code $C^{\gamma}(F_*(x))$ is determined analogously. □

For $q = 2$ there exist extensions of the codes from the first and third rows of the table, which have parameters coinciding with the parameters of the best codes listed in [39]. Namely, they have the parameters of the Delsarte–Goethals linear cyclic code [39], and of the code, obtained from the Kerdoc code [39] by the elimination of two coordinates [45, 47]. See below **Added in Proof.**

31. Evaluation of Generator and Check Polynomials of Reed–Muller Codes

Let $f(x)$ be an MP-polynomial over $P = GF(p)$ of degree m, $1 \leq r < (p-1)m$, $R = \mathbf{Z}_{p^n}$, and $F_*(x)$, θ, $F_*^{\langle r \rangle}(x)$ be the notations introduced in Section 22.B. Then $\overline{F}_*(x)$ is an MP-polynomial over $\overline{R}$ of degree m with the root $\overline{\theta}$, and $\overline{F}_*^{\langle r \rangle}(x) = \prod\{x - \overline{\theta}^k \mid 1 \leq k \leq T,\ w(k) \leq r\}$. The last equality shows that $\overline{F}_*^{\langle r \rangle}(x)$ is the check polynomial of the shortened rth-order generalized Reed–Muller code of length $T = p^M - 1$, considered as a cyclic code over $\overline{R} = GF(p)$ [4, p. 362]. The generator polynomial of this code is equal to

$$(x - \overline{e})\overline{G}_*^{\langle (p-1)m-r-1 \rangle}(x), \text{ where } G_*(x) = F_*(0)^{-1} x^m F_*(1/x).$$

We can evaluate $\overline{F}_*^{\langle r \rangle}(x)$, using the following procedure. Divide the set $\{k \in \overline{1,T} \mid 1 \leq w(k) \leq r\}$ into the cyclotomic classes $\{k, kp, kp^2, \ldots\}$ modulo $T = p^M - 1$. For each class we find an irreducible polynomial over $\overline{R}$ with root $\overline{\theta}^k$ (and therefore with roots $\overline{\theta}^{kp}, \overline{\theta}^{kp^2}, \ldots$). Then $\overline{F}_*^{\langle r \rangle}(x)$ is the product of all of these polynomials.

We propose another method of evaluating $\overline{F}_*^{\langle r \rangle}(x)$. First, consider the case $p = 2$. Let $u \in L_P(f)$ be an LRS of maximal period over P and $n = r$. Define $\sigma : P \to R = \mathbf{Z}_{2^r}$ by $\sigma(0) = 0$, $\sigma(e_P) = e$. By Theorem 22.2, $F_*^{\langle r \rangle}(x)$ is the minimal polynomial of the LRS $v = \sigma(u)$ over R. To find $\overline{F}_*^{\langle r \rangle}(x)$, we solve the Hankel $(N \times N)$-system of linear equations over R (see (3.2)):

$$(c_0, \ldots, c_{N-1})\mathcal{G}_N(v) = v(\overline{N, 2N-1})$$

where, by 22.5, $N = \binom{m}{r} + \ldots + \binom{m}{2} + m$. For any solution $(c_0, \ldots, c_{N-1})$ of this system we have $\overline{F}_*^{\langle r \rangle}(x) = x^N - \overline{c}_{N-1}x^{N-1} - \ldots - \overline{c}_1 x - \overline{c}_0$.

If $p \geq 3$, we write r in the form $r = (p-1)t + l$, where $l \in \overline{1, p-1}$. Let $u \in L_P(f) \backslash 0$, $n = t+1$, and let the representation σ be defined by its polynomial $\Psi_\sigma(x) = p(x^{p-1} + \ldots + x^{l+1}) + x^l + \ldots + x$ (see 22.1). Then

$F_*^{(r)}(x)$ is the minimal polynomial of LRS $\sigma(u)$, and $\overline{F}_*^{(r)}(x)$ can be found as in the case $p = 2$. Methods of solving systems of linear equations over $\mathbf{Z}_{p^n}$ are described in [11, 12].

Added in Proof

Note, that in Section 30.C along with $C^\gamma(F)$ we can consider codes $C^\gamma(I)$ for reversible ideals $I \triangleleft R[x]$. If $T(I) = N$ then by definition

$$C^\gamma(I) = \{\gamma_1(u(\overline{0, N-1}))|\ u \in L_R(I)\}.$$

Under the condition of Theorem 30.4 let

$$I_* = (F_*(x)(x-e), 2F_*(x)), \qquad I = (F(x)(x-e), 2F(x)),$$

then

$$C^\gamma(I_*) = C^\gamma(F_*) \oplus \Gamma(R)(e, \ldots, e), \qquad C^\gamma(I) = C^\gamma(F) \oplus \Gamma(R)(e, \ldots, e).$$

The code $C^\gamma(I_*)$ has the same length and distance as $C^\gamma(F_*)$, but $|C^\gamma(I_*)| = q|C^\gamma(F_*)|$. It is nonlinear cyclic code with the parameters coincident to the parameters of the Delsart–Goethals linear cyclic code [39, 15.5 Corolarry 17].

The code $C^\gamma(I)$ has the same length and distance as $C^\gamma(F)$, and $|C^\gamma(I)| = q|C^\gamma(F)| = q/4(N+1)^2$. In the case $m = 2\lambda + 1$, $c_F \in \Gamma(R)$ this code has the largest code distance in comparison with others codes of Theorem 30.4; for $q = 2$ it is the distance of the code, obtained from the Kerdock code [39, 120] by the elimination of two coordinates, but the efficiency of $C^\gamma(I)$ is the half of the efficiency of the Kerdock code. Note, that Kerdock code has the optimal efficiency N^2 in the class of codes of the length N with the code distance $(N - \sqrt{N})/2$ [59]. This code may be constructed by the following way.

30.5. Theorem [25]. *If $F(x)$ is MP-polynomial of degree $m > 1$ over $\mathbf{Z}_4$, then $C^\gamma(F(x)(x - \xi e))$ is a nonlinear cyclic code having the length $N = 2(2^m - 1)$, the efficiency $(N+2)^2$ and the code distance, which is defined from the rows 3–6 of the Theorem 30.4 table for $q = 2$. If $m = 2\lambda + 1$, $c_F = e$, then this code is equivalent to the code, obtained from the Kerdock code by the elimination of two coordinates* [45, 47].

We remark, that as in [45, 47] in the paper Calderbank A. R., Hammons Jr. R., Kumak V., Sloane N. J. A., Sole R. *A Linear Construction for Certain Kerdock and Preparata Codes*, Bull. Am. Math. Soc., **29**, No. 2, 218–222 (1993), it is possible also to find a construction of the Kerdock code based on some linear code over $\mathbf{Z}_4$ (however in this article the Kerdock code is not in cyclic form).

The result of Theorem 30.5 concerning the Kerdock code can be obtained as the special case of the following general result.

Generalization of the Kerdock code for the case of the field of $q = 2^l$ elements. As before, let $R = CR(q^2, 2^2)$ $q = 2^l$, and let $R < Q = GR(q^{2m}, 2^2)$. First we construct a l–linear cyclic code $\mathcal{K}$ over R (see Section 29.B) of the volume $N_1 \times \ldots \times N_l$, where $N_1 = 2(q^m - 1)$, $N_2 = \ldots = N_l = 2$.

Let $a_1, \ldots, a_l$ be a basis of the field $\Gamma(R)$ over $GF(2)$. Then $\eta_1 = e + 2a_1, \ldots, \eta_l = e + 2a$ are elements of order 2 in the group R^*, and $e + 2R = <\eta_1> \dot{\times} \ldots \dot{\times} <\eta_l>$. Let ξ_0 be a primitive element of the field $\Gamma(R)$. Then $\xi = \xi_0\eta_1$ is a root of some MP-polynomial $F(x) \in R[x]$ of degree m.

The ideal $I = \{F(x_1)(x_1 - \eta_1),\ x_2 - \eta_2, \ldots, x_l - \eta_l) \triangleleft \mathcal{P}_l = R[x_1, \ldots, x_l]$ is reversible, and its group of periods $\mathfrak{P}(I)$ (see 6.21) is generated by the vectors $(N_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, N_l)$. The desired l–linear cyclic code is

$$\mathcal{K} = L_R^{\mathbf{N}}(I), \qquad \text{where} \qquad \mathbf{N} = (N_1, \ldots, N_l).$$

It consists of all polyhedrons $\mu(\Pi)$, where $\Pi = \Pi(\mathbf{N})$, $\mu \in L_R(I)$.

Now consider the following code over the field $\Gamma(R)$:

$$C^\gamma(I) = \{\gamma_1(\mu(\Pi))|\ \mu \in L_R(I)\}.$$

This is the code of the volume $N_1 \times \ldots \times N_l$, each its element can be identified with a vector over $\Gamma(R)$ of the length $N = N_1 \ldots N_l = (q^m - 1)q$. So, we can say that $C^\gamma(I)$ is a code of the length N.

30.6. Theorem (A.S.Kuzmin, A.A.Nechaev, 1993). *If $m = 2\lambda + 1 \geq 3$, then the code $C^\gamma(I)$ has the length $N = (q^m - 1)q$, the efficiency $(N+q)^2$ and the code distance*

$$d = \frac{q-1}{q}(N + q - \sqrt{N+q}) - q.$$

□ Since $I = I_1 \cap I_2$, where $I_1 = (F(x_1), x_2 - \eta_2, \ldots, x_l - \eta_l)$ and $I_2 = (x_1 - \eta_1,\ x_2 - \eta_2, \ldots, x_l - \eta_l)$ are comaximal ideals, $L_R(I) = L_R(I_1) \dot{+} L_R(I_2)$ is the family of all l-sequences of the form

$$\mu(z) = (\mathrm{Tr}_R^Q(u\xi^{z_1}) + c\eta_1^{z_1})\eta_2^{z_2} \ldots \eta_l^{z_l}, \quad u \in Q, \quad c \in R,$$

and $|L_R(I)| = |R|^{\deg F(x_1)(x-\eta_1)} = |R| = q^{2(m+1)}$. Any code word $\omega \in C^\gamma(I)$ is uniquely determined by the constants $u = u_0 + 2u_1$, $c = c_0 + 2c_1$, where $u_S \in \Gamma(Q)$, $c_S \in \Gamma(R)$, and the collection of coordinates of the vector ω is the collection of elements of the form

$$\omega(i_0, \ldots, i_l) = \gamma_l((\mathrm{Tr}_R^Q(u\xi_0^{i_0}) + c)\eta_1^{i_1} \ldots \eta_l^{i_l}),$$

$$0 \leq i_0 \leq q^m - 2, \quad 0 \leq i_1, \ldots, i_l \leq 1.$$

From here, using the notation and techniques of the proof of Theorem 30.4, we get

$$\omega(i_0, \ldots, i_l) = \gamma_1\left[(\mathrm{Tr}\,(u\xi_0^{i_0}) + c)(e + 2(i_1a_1 + \ldots + i_la_l))\right] = \gamma(\mathrm{Tr}\,(u\xi_0^{i_0}) + c) \oplus (i_1a_1 \oplus \ldots \oplus i_la_l)(\mathrm{tr}_{\Gamma(R)}^{\Gamma(Q)}(u\xi_0^{i_0}) \oplus c_0)$$

$$= \varkappa(u_0^h\xi_0^{hi_0}) \oplus \mathrm{tr}\,(u_0^hc_0^h\xi_0^{hi_0}) \oplus c_1 \oplus (i_1a_1 \oplus \ldots \oplus i_la_l)(\mathrm{tr}\,(u_0^h\xi_0^{hi_0}) \oplus c_0^h)^2.$$

Thus, for suitable constants $\alpha,\ \beta \in GF(q^m)$, $a, b \in GF(q)$ the set of coordinates of ω is the set of the values of the function

$$\Phi(x, y) = \varkappa(\alpha x) + \mathrm{tr}\,(\beta x)^2 + \mathrm{tr}\,(\alpha a x) + y(\mathrm{tr}\,(\alpha x) + a)^2 + b,$$

where x is the indeterminate on $GF(q^m)^*$, and y is on $GF(q)$. The code distance of $C^\gamma(I)$ is equal to the minimum of weights $Wt(\Delta(x, y))$ of the functions

$$\Delta(x, y) = \varkappa(\alpha x) + \varkappa(\alpha' x) + \mathrm{tr}\,(\bar\beta x)^2 + \mathrm{tr}\,((\alpha a + \alpha' a')x) + y(\mathrm{tr}\,((\alpha + a')x) + \alpha + a')^2 + \bar b$$

on $GF(q^m)^* \times GF(q)$ such that $(\alpha + \alpha', \bar\beta, a + a', \bar b) \neq (0, 0, 0, 0)$. This minimum is attained when $\alpha \neq \alpha'$. In that case we can assume that $\alpha' = e$. Then

$$\Delta(x, y) = \varphi(x) + y(\mathrm{tr}\,((\alpha + e)x) + \bar\alpha)^2,$$

where

$$\varphi(x) = \varkappa((\alpha + e)x) + \mathrm{tr}\,(\delta x)^2 + \mathrm{tr}\,(\alpha x)\mathrm{tr}\,(x) + \mathrm{tr}\,((\alpha a + a')x) + \bar b,$$

$$\alpha, \delta \in GR(q^m), \qquad a, a', \bar b \in GF(q), \qquad \bar a = a + a'.$$

Let

$$L_0 = \{x \in GF(q^m)^*|\ \mathrm{tr}\,((\alpha + e)x) = \bar a\}, \qquad L_1 = GF(q^m)^* \backslash L_0.$$

It is easy to see that if $\varphi_0(x) = \varphi|\,L_0$, then

$$Wt(\Delta(x, y)) = |L_1|(q - 1) + Wt(\varphi_0(x))q.$$

The definition of L_0 implies that

$$\varphi_0(x) = \varkappa((\alpha + e)x) + \mathrm{tr}\,(\hat{\delta}x)^2 + \hat{b}.$$

The change of variables $z = (\alpha + e)x + \bar{a}$ for m odd leads to $Wt(\varphi_0(x)) = Wt(\Delta_0^{(0)}(z))$, where the right part is the weight of the form $\Delta_0^{(0)}(z) = \varkappa(z) + \mathrm{tr}\,(\tilde{\delta}z)^z + \tilde{b}$ on the set $\tilde{L}_0 = \{(z \in GF(q^m) |\ \mathrm{tr}\,(z) = 0,\ z \neq \bar{a}\}$. It follows from the proof of Theorem 30.4 that

$$Wt(\Delta_0^{(0)}(z)) \geq (q-1)(q^{m-2} - q^{\lambda-1}) - \varepsilon, \quad \text{where} \quad \varepsilon = q^{m-1} - |\tilde{L}_0| \in \{0, 1\}.$$

Therefore, $Wt(\Delta(x, y)) \geq d$, where d is given in the formulation of the theorem. The attainability of this bound is proved by selection of the parameters in (1). □

This work was partially suppored by The Grands of Russian Foundation of Fundamental Research.

LITERATURE CITED

1. A. S. Ambrosimov, "On the distribution of frequencies of multigrams in linear recurring sequences over residue rings," *Uspekhi Mat. Nauk*, **48** (1993) (in press).
2. M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison Wesley (1969).
3. Yu. A. Bahturin, *Basic Structures of Modern Algebra* [in Russian], Nauka, Moscow (1990).
4. E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York (1968).
5. G. Birkhoff and T. C. Bartee, *Modern Applied Algebra*. McGraw-Hill, New York (1970).
6. Z. I. Borevich and I. R. Shafarevich, *Theory of Numbers, 3rd ed.* [in Russian], Nauka, Moscow (1985).
7. A. Gill, *Linear Sequential Circuits*, McGraw-Hill, New York (1966).
8. N. Jacobson, *The Theory of Rings*, Math. Surveys, No. 2 (1943).
9. J. Diedonne, *La Geometrie des Groupes Classiques. 3rd ed.*, Springer (1971).
10. J. Davenport, Y. Siret, and E. Tournier, *Calcul Formel*, Masson, Paris (1987).
11. V. P. Elizarov, "Systems of linear equations over commutative rings," *Uspekhi Mat. Nauk*, **48**, No. 2, 181–182 (1993).
12. V. P. Elizarov, "General solution of systems of linear homogeneous equations over a commutative ring," *Uspekhi Mat. Nauk*, **48** (1993) (in press).
13. O. Zariski and P. Samuel, *Commutative Algebra, I, II*, Princeton (1958, 1960).
14. F. Kasch, *Moduln und Ringe*, B. G. Teubner, Stuttgart (1977).
15. L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York (1974).
16. Ch. W. Curtes and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley, New York (1962).
17. A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups, I, II*, Amer. Math. Soc. (1964, 1967).
18. D. E. Knuth, *The Art of Computer Programming, Vol. 1. Fundamental Algorithms*, Addison-Wesley (1968).
19. N. M. Korobov, "Distribution of nonresidues and primitive roots in recurrent series," *Dokl. Akad. Nauk SSSR*, **88**, No. 4, 603–606 (1953).
20. N. M. Korobov, *Trigonometric Sums and Their Applications* [in Russian] Nauka, Moscow (1989).
21. A. S. Kuzmin, "Polynomials of maximal period over residue rings" In: *3rd International Conference in Algebra*, Krasnoyarsk (1993).
22. A. S. Kuzmin, "Distribution of elements on cycles of linear recurring sequences over residue rings," *Uspekhi Mat. Nauk*, **47**, No. 6, 213–214 (1993).
23. A. S. Kuzmin, "Lower bounds of ranks for coordinate sequences of linear recurring sequences over residue rings," *Uspekhi Mat. Nauk*, **48** (1993) (in press).

24. A. S. Kuzmin, "On periods of binary digits of linear recurring sequences over prime finite fields," *Uspekhi Mat. Nauk*, **48** (1993) (in press).

25. A. S. Kuzmin and A. A. Nechaev, "A construction of noise stable codes using linear recurrences over Galois rings," *Uspekhi Mat. Nauk*, **47**, No. 5, 183–184 (1992).

26. A. S. Kuzmin and A. A. Nechaev, "Linear recurring sequences over Galois rings," *Uspekhi Mat. Nauk*, **48**, No. 1, 167–168 (1993).

27. V. L. Kurakin, "Representations over the ring $\mathbf{Z}_{p^n}$ of linear recurring sequences of maximal period over the field GF(p)," *Diskr. Mat.*, **4**, No. 4, 96–116 (1992).

28. V. L. Kurakin, "Representations of linear recurring sequences and regular prime numbers," *Uspekhi Mat. Nauk*, **47**, No. 6, 215–216 (1992).

29. V. L. Kurakin, "Analytical structure of linear recurring sequences," *Uspekhi Mat. Nauk*, **48** (1993) (in press).

30. V. L. Kurakin, "Representations over a field of linear recurrences of maximal period over a residue ring," *Uspekhi Mat. Nauk*, **48** (1993) (in press).

31. V. L. Kurakin, "Convolution of linear recurring sequences," *Uspekhi Mat. Nauk*, **48**, No. 4 235–236 (1993).

32. V. L. Kurakin, "Structure of Hopf algebras of linear recurring sequences," *Uspekhi Mat. Nauk*, **48**, No. 5 117–178 (1993).

33. V. L. Kurakin, "The first coordinate sequence of a linear recurrence of maximal period over a Galois ring," *Diskr. Mat.* (in press).

34. V. L. Kurakin, "Representations of linear recurring sequences of maximal period over a finite field," *Diskr. Mat.* (in press).

35. D. Laksov, "Linear recurring sequences over finite fields," *Math. Scand.* **16**, 181–196 (1965).

36. V. N. Latyshev, *Combinatorial Ring Theory, Standard Bases*, [In Russian], MGU, Moscow (1988).

37. R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, London (1983).

38. E. S. Liapin, *Semigroups* [in Russian], Fizmatgiz, Moscow (1960).

39. F. J. McWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland (1977).

40. Yu. I. Manin, *Cubic Forms. Algebra, Geometry, Arithmetic* [in Russian] Nauka, Moscow (1972).

41. A. A. Markov, *Finite Difference Calculates* [in Russian], Odessa (1910), pp. 209–239.

42. A. A. Nechaev, "Finite principal ideal rings," *Mat. Sb.*, **91**, No. 3, 350–366 (1973).

43. A. A. Nechaev, "Criteria of completeness of system of functions over finite rings and quasi-Frobenius rings," *Sib. Mat. Zh.* **23**, No. 3, 175–187 (1982).

44. A. A. Nechaev, "Similarity of matrices over local commutative artinian rings," *Tr. Sem. Petrovskogo*, **9**, 81–101 (1983).

45. A. A. Nechaev, "Kerdoc code in a cyclic form," *Diskr. Math.*, **1**, No. 4, 123–139 (1989).

46. A. A. Nechaev, "Linear recurring sequences over commutative rings," *Diskr. Math.*, **3**, No. 4, 107–121 (1991).

47. A. A. Nechaev, "Trace function in Galois rings and noise stable codes," In: *Fifth All-Union Symp. of Theory of Rings, Algebras and Modules*, Novosibirsk (1982), p. 97.

48. A. A. Nechaev, "The cyclic types of linear substitutions over finite commutative rings," *Mat. Sb.*, **184**, No. 3, 21–56 (1993).

49. A. A. Nechaev, "Linear recurring sequences over quasi-Frobenius modules," *Uspekhi Mat. Nauk*, **48** (1993) (in press).

50. V. I. Nechaev, "Groups of nonsingular matrices over finite fields and recurring sequences," *Dokl. Akad. Nauk SSSR*, **152**, No. 2, 275–277 (1963).

51. V. I. Nechaev, "Linear recurring congruences with periodic coefficients," *Mat. Zametki*, **3**, No. 6, 625–632 (1968).

52. V. I. Nechaev, "Recurring sequences," *Uchen. Zap. Mosk. Ped. Inst.*, **375**, 103–123 (1971).

53. V. I. Nechaev, "Linear congruences on powers of a prime ideal and linear recurring sequences," *Uchen. Zap. Mosk. Ped. Inst.*, **375**, 124–132 (1971).

54. V. I. Nechaev, "Trigonometric sums for recurrent sequences of elements of a finite field," *Mat. Zametki*, **11**, No. 5, 597–607 (1972).

55. V. I. Nechaev, "Trigonometric sums for recurrent sequences," *Dokl. Akad. Nauk SSSR*, **206**, No. 4, 811–814 (1972).

56. V. I. Nechaev and A. M. Polosuev, "On distribution of non-residues and primitive roots in a sequence satisfying a finite difference equation with polynomial coefficients," *Vestnik MGU. Ser. 1, Mat., Mekh.*, No. 6, 75–84 (1964).

57. V. I. Nechaev and L. L. Stepanova, "Distribution of non-residues and primitive roots in recurring sequences over an algebraic number field," *Uspekhi Mat. Nauk*, **20**, No. 3, 197–203 (1965).

58. V. N. Sachkov, *Introduction to Combinatorical Methods of Discrete Mathematics* [in Russian], Nauka, Moscow (1982).

59. V. M. Sidelnikov, "On extremal polynomials used for estimating code cardinality," *Probl. Peredachi Inf.*, **16**, No. 3, 17–30 (1980).

60. V. M. Sidelnikov, "Bounds for number of symbols on a segment of a recurring sequence over a finite field," *Diskr. Math.*, **3**, No. 2, 87–95 (1991).

61. L. A. Skornjakov and A. V. Mikhalev, "Modules," In: *Algebra. Topologiya. Geometriya.* Vol. 14, *Itogi Nauki i Tekhn.*, All-Union Institute for Scientific and Technical Information (VINITI), Akad. Nauk SSSR, Moscow (1976), pp. 57–191.

62. I. M. Sobol, *Numerical Monte-Carlo Methods* [in Russian], Nauka, Moscow (1973).

63. D. A. Suprunenko. *Matrix Groups* [in Russian], Nauka, Moscow (1972).

64. A. I. Uzkow, "On Jordan–Hölder theorem," *Mat. Sb.*, **4**, No. 1, 29–43 (1938).

65. A. I. Uzkow, "Abstract foundation of Brandt's theory of ideals," *Mat. Sb.*, **6**, No. 2, 253–281 (1939).

66. A. I. Uzkov, "Zur Idealtheorie der kommutativen Ring. I," *Mat. Sb.*, **5**, No. 3, 513–520 (1939).

67. A. I. Uzkov, "An algebraic lemma and normalizing E. Noether theorem," *Mat. Sb.*, **22**, No. 2 349–350 (1948).

68. A. I. Uzkov, "On cyclic direct decomposability of modules over commutative rings," *Mat. Sb.*, **62**, No. 4, 469–475 (1963).

69. C. Faith, *Algebra II. Ring Theory*, Springer-Verlag (1976).

70. N. Zierler, "Linear recurring sequences," *SIAM J. Appl. Math.*, **7**, 31–48 (1959).

71. P. L. Chebyshev, *Theory of Probabilities. Lectures 1879–1880* [in Russian], Moscow–Leningrad (1936), pp. 139–147.

72. P. L. Chebyshev, *Congruence Theory. Complete Collection of Works* [in Russian], Vol. 1, Acad. Sci. USSR, Moscow–Leningrad (1944), pp. 10–172.

73. I. E. Sparlinsky, "Distribution of non-residues and primitive roots in recurring sequences," *Mat. Zametki*, **24**, No. 5, 605–615 (1978).

74. I. E. Shparlinski, "Distribution of fractional parts of recurring sequences," *Zh. Vychisl. Mat. Mat. Fiz.*, **21**, No. 6, 1588–1591 (1981).

75. I. E. Shparlinski, "On some properties of linear cyclic codes," *Probl. Peredachi Inf.*, **19**, No. 3, 106–110 (1983).

76. M. Antweiler and L. Bomer, "Complex sequences over GF(q) with a two-level autocorrelation function and a large linear span," *IEEE Trans. Inf. Theory*, **38**, No. 1, 120–130 (1992).

77. G. Azumaya, "A duality theory for injective modules (Theory of quasi-Frobenius modules)," *Am. J. Math.*, **81**, No. 1, 249–278 (1959).

78. B. Benzaghou and J.–P. Bezivin, "Proprietes algebriques de suites differentiellement sinies," *Bull. Soc. Mat. Fr.*, **120**, No. 3, 327–346 (1992).

79. D. Bollman, "Some periodicity properties of transformations on a vector space over residue class rings," *SIAM J. Appl. Math.*, **13**, No. 3, 902–912 (1965).

80. D. Bollman, "Some periodicity properties of modules over the ring of polynomials with coefficients in a residue class ring," *SIAM J. Appl. Math.*, **14**, No. 2, 237–241 (1966).

81. J. L. Brenner, "Linear recurrence relations," *Amer. Math. Monthly*, **61**, No. 3, 171–173 (1954).

82. A. Brousseau, "Recursion relations of products of linear recursion sequences," *Fibonacci Quart*, **14**, No. 2, 159–166 (1976).

83. L. Brynielsson, "On the linear complexity of combined shift register sequences," *Lect. Notes Comput. Sci.*, **219** (1985).

84. S. A. Burr, "On moduli for which the Fibonacci sequence contains a complete system of residues," *Fibonacci Quart*, **9**, 497–504 (1971).

85. D. Calabro and J. K. Wolf, "On the synthesis of two-dimensional arrays with disarable correlation properties," *Inf. Control*, **11**, 537–560 (1968).

86. R. D. Carmichael, "On sequences of integers defined by recurrence relations," *Quart. J. Pure Appl. Math.*, **48**, 343–372 (1920).

87. L. Cerlienco, G. Delogu, and F. Piras, "The search for quadratic divisors of a polynomial by the method of linear recurrent sequences," *Rend. Math. Appl.*, **1**, No. 4, 623–631 (1981).

88. L. Cerlienco, M. Mignotte, and F. Piras, "Linear recurrent sequences: algebraic and arithmetical properties," *Enseign. Math.*, **33**, No. 1–2, 67–108 (1987).

89. L. Cerlienco and F. Piras, "Resultant, l.c.m. and g.c.d. of two polynomials by the method of linear recurrent sequences," *Rend. Sem. Fac. Sci. Univ. Calgari.*, **50**, No. 3-4, 711–717 (1980).

90. L. Cerlienco and F. Piras, "*G-R*-sequences and incidence coalgebras of posets of full binomial type," *J. Math. Anal. Appl.*, **115**, No. 1, 46–56 (1986).

91. L. Cerlienco and F. Piras, "On the continuous dual of a polynomial bialgebra," *Commun. Algebra*, **19**, No. 10, 2707–2727 (1991).

92. A. H. Chan and H. A. Games, "On the linear span of binary sequences obtained from finite geometries," *Lect. Notes Comput. Sci.*, **263**, 405-417 (1987).

93. A. H. Chan and M. Goresky, "On the linear complexity of feedback register (extended abstract)," *Lect. Notes Comput. Sci.*, **434** (1990).

94. E. C. Dade, D. W. Robinson, O. Taussky, and M. Ward, "Divisors of recurrent sequences," *J. Reine Angew. Math.*, **214/215**, 180–183 (1964).

95. Z. D. Dai, T. Beth, and D. Gollmann, "Lower bounds for the linear complexity of sequences over residue rings," *Lect. Notes Comput. Sci.*, **473**, 189–195 (1991).

96. Z. D. Dai and Z. X. Wan, "A relationship between the Berlekamp–Massey and the Euclidean algorithms for linear feedback shift register synthesis," *Acta. Math. Sin. New Ser.*, **4**, No. 1, 55–63 (1988).

97. Z. D. Dai and K. C. Zeng, "Continued fractions and the Berlekamp–Massey algorithm," *Lect. Notes. Comput. Sci.*, **453**, 24–31 (1990).

98. D. J. De Carli, "A generalized Fibonacci sequence over an arbitrary ring," *Fibonaci Quart*, **8**, No. 2, 182–184 (1970).

99. D. J. De Carli, "Periodicity over the ring of matrices," *Fibonacci Quart*, **11**, No. 5, 466–468 (1973).

100. L. E. Dickson, *History of the Theory of Numbers.* Vol. 1, Carnegie Inst., Washington (1919).

101. L. L. Dornhoff and F. E. Hohn, *Applied Modern Algebra*, Macmillan, New York–London (1978).

102. H. J. A. Duparc, "Periodicity properties of recurring sequences. I, II," *Indagat. Math.*, **16**, No. 3, 331–342, **16**, No. 4, 473–485 (1954).

103. J. Eichenauer–Herrman, H. Grothe, and J. Lehn, "On the period length of pseudorandom vector-sequences generated by matrix generators," *Math. Comput.*, **2**, No. 185, 145–148 (1989).

104. H. T. Engstrom, "Periodicity in sequences defined by linear recurrence relations," *Proc. Natl. Acad. Sci. USA*, **16**, 663–665 (1930).

105. H. T. Engstrom, "On sequences defined by linear recurrence relations," *Trans. Am. Math. Soc.*, **33**, 210–218 (1931).

106. L. Euler, *Introduction to the Calculus of Infinitesimal Variables* (1748), *Leonardi Euleri opera omnia*, **8** (1922); **9** (1945).

107. H. J. Fell, "Linear complexity of transformed sequences," *Lect. Notes Comput. Sci.*, **514**, 205–214 (1991).

108. G. L. Feng and K. K. Tzeng, "A generalization of the Berlekamp–Massey algorithm for multisequence shift register synthesis with application to decoding cyclic codes," *IEEE Trans. Inf. Theory*, **37**, No. 5, 1274–1287 (1991).

109. S. D. Golic, "On the linear complexity of functions of periodic GF(q) sequences," *IEEE Trans. Inf. Theory*, **35**, No. 1, 69–75 (1989).

110. B. F. J. Green, J. E. K. Smith, and Klem Laura, "Empirical tests of an additive random number generator," *J. Assoc. Comput. Mach.*, **6**, 527–537 (1959).

111. H. Grothe, "Matrix generators for pseudo-random vector generation," *Statist. Hefte*, **28**, No. 3, 233–238 (1987).

112. F. G. Gustavson, "Analysis of the Berlekamp-Massey linear feedback shift register synthesis algorithm," *IBM J. Res. Dev.*, **20**, No. 3, 204–212 (1976).

113. M. Hall, "An isomorphism between linear recurring sequences and algebraic rings," *Trans. Am. Math. Soc.*, **44**, No. 2, 196–218 (1938).

114. P. Haukkanen, "On a convolution of linear recurring sequences over finite fields," *J. Algebra*, **149**, No. 1, 179–182 (1992).

115. K. Imamura and W. Yoshida, "A simple derivation of the Berlekamp–Massey algorithm and some applications," *IEEE Trans. Inf. Theory*, **33**, No. 1, 146–150 (1987).

116. T. Ikai, H. Kosako, and Y. Kojima, "Subsequences in linear recurring sequences," *Electron. Commun. Jpn.*, **53**, No. 12, 159–166 (1970).

117. C. J. A. Jansen and D. E. Boekee, "The shortest feedback shift register that can generate a given sequence," *Lect. Notes Comput. Sci.*, **435**, 90–99 (1990).

118. B. Jansson, *Random Number Generators*, Almqvist and Wiksell, Stockholm (1966).

119. S. M. Jennings, "Multiplexed sequences: some properties of the mimimum polynomial," *Lect. Notes Comput. Sci.*, **149** (1983).

120. A. M. Kerdock, "A class of low-rate non-linear codes," *Inform. Control.*, **20**, 182–187 (1972).

121. Klove Torleiv, "Periodicity of recurring sequences in rings," *Math. Scand.*, **32**, No. 2, 165–168 (1973).

122. L. Kronecker, *Vorlesungen uber Zahlentheorie*, Vol. 1, Teubner, Leipzig (1901).

123. A. S. Kuzmin and A. A. Nechaev, "Linear recurrent sequences over Galois rings," In: *Proc. 2nd Internat. Conf. Algebra*, Barnaul (1991).

124. J. L. Lagrange, "Recherches sur les suites recurrentes dont les termes varient de plusieurs manieres differentes, ou sur l'integration des equations lineaires aux differences finies et partielles; et sur l'usage de ces equations dans la theorie des hasards," In: *Nouv. Memoires Acad. Roy*, Berlin (1775), pp. 183–272; *Oeuvres*, **4**, Gauthier-Villars, Paris (1869), pp. 151–251.

125. R. R. Laxton and J. A. Anderson, "Linear recurrences and maximal length sequences," *Math. Gaz.*, **56**, 299–309 (1972).

126. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge Univ. Press (1986).

127. E. Lucas, "Theorie des fonctions numeriques simplement periodiques," *Am. J. Math.*, **1**, 184–240, 289–321 (1878).

128. F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proc. IEEE*, **64**, No. 11, 1715–1729 (1976).

129. M. Magidin and A. Gill, "Singular shift register over residue class ring," *Math. Syst. Theory*, **9**, No. 4, 345–358 (1976).

130. K. Mahler, *p-Adic Numbers and Their Functions*, 2nd ed., Cambridge Univ. Press, Cambridge (1981).

131. J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, **15**, No. 1, Part 1, 122–127 (1969).

132. B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York (1974).

133. R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer, Boston (1987).

134. K. Morita, "Duality for modules and its applications to the theory of rings with minimum condition," *Sci. Rep. Tokyo Kyoiku Daigaku*, **A6**, No. 15, May, 83–142 (1958).

135. M. Nagata, *Local Rings*, Int. Publ., New York (1962).

136. M. B. Nathanson, "Difference operators and periodic sequences over finite modules," *Acta Math. Acad. Sci. Hungary*, **28**, No. 3–4, 219–224 (1976).

137. A. A. Nechaev, "Linear recurring sequences and quasi-Frobenius modules," In: *International School in Algebra and Analysis*, Baikal (1992).

138. H. Niederreiter, "Some new exponential sums with applications to pseudorandom numbers," In: *Topics in Number Theory (Debrecen, 1974), Colloquia math. Soc. Janos Bolyai*, North-Holland, Amsterdam (1976), pp. 209–232.

139. H. Niederreiter, "On the cycle structure of linear recurring sequences," *Math. Scand.*, **38**, No. 1, 53–77 (1976).

140. H. Niederreiter and S. S. Shiue, "Equidistribution of linear recurring sequences in finite fields," *Acta Arithm.*, **38**, No. 2, 197–207 (1980).

141. H. Niederreiter, "Distribution properties of feedback shift register sequences," *Probl. Contr. Inform. Theory (Hungary)*, **15**, No. 1, 19–34 (1986).

142. H. Niederreiter, "A simple and general approach to the decimation of feedback shift register sequences," *Probl. Contr. Inform. Theory (Hungary)*, **17**, No. 5, 327–331 (1988).

143. T. Nomura and A. Fukuda, "Linear recurring planes and two-dimensional cyclic codes," *Electron. Commun. Jpn.*, **54**, No. 3, 23–30 (1971).

144. T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "A method of construction and some properties of planes having maximum area matrix," *Electron. Commun. Jpn.*, **54**, No. 5, 18–25 (1971).

145. T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "Some properties of the p-plane and its extension to three-dimensional space," *Electron. Commun. Jpn.*, **54**, No. 8, 27–34 (1971).

146. T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "A theory of two-dimensional linear recurring arrays," *IEEE Trans. Inf. Theory*, **18**, No. 6, 775–785 (1972).

147. B. Peterson and E. Y. Taft, "The Hopf algebra of linear recursive sequences," *Aequat. Math.*, **20**, 1–17 (1980).

148. R. Raghavendran, "A class of finite rings," *Compos. Math.*, **22**, No. 1, 49–57 (1970).

149. F. Rhodes, "Regular mappings of sequence space over finite fields," *Q. J. Math. Oxford, Ser. 2*, **37**, No. 146, 231–238 (1976).

150. D. W. Robinson, "A note on linear recurrent sequences modulo m," *Am. Math. Monthly*, **73**, No. 6, 619–621 (1966).

151. D. W. Robinson, "The rank and period of a linear recurrent sequence over a ring," *Fibonacci Quart.*, **14**, No. 3, 210–214 (1976).

152. R. A. Rueppel and O. J. Staffelbach, "Products of linear recurring sequences with maximum complexity," *IEEE Trans. Inf. Theory*, **33**, No. 1, 126–131 (1987).

153. S. Sakata, "Doubly linear recurring arrays and M-arrays," *Trans. Inst. Electron. Comm. Eng.*, **A60**, No. 10, 918–925 (1977).

154. S. Sakata, "General theory of doubly periodic arrays over an arbitrary finite field and its applications," *IEEE Trans. Inf. Theory*, **24**, 719–730 (1978).

155. S. Sakata, "On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals," *IEEE Trans. Inf. Theory*, **27**, No. 5, 556–565 (1981).

156. S. Sakata, "Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array," *J. Symbolic Comput.*, **34**, No. 3, 321–337 (1988).

157. S. Sakata, "Cycle representatives of quasi-irreducible two-dimensional cyclic codes," *IEEE Trans. Inf. Theory*, **34**, No. 4, 871–875 (1988).

158. S. Sakata, "Synthesis of two-dimensional linear feedback shift registers and Groebner bases," *Lect. Notes Comput. Sci.*, **356**, 394–407 (1989).

159. S. Sakata, "Extension of the Berlekamp–Massey algorithm to N dimensions," *Inform. Comput.*, **84**, No. 2, 207–239 (1990).

160. E. S. Selmer, *Linear Recurrence Relations over Finite Fields*, Univ. of Bergen (1966).

161. J. S. Shiue and T. L. Sheu, "On the periodicity of linear recurrence of second order in commutative rings," *Tamkang J. Math.*, **4**, 105–107 (1973).

162. N. J. A. Sloane and J. A. Reeds, "Shift register synthesis (modulo m)," *SIAM J.*, **14**, No. 3, 505–513 (1985).

163. M. Sweedler, *Hopf Algebras*, Benjamin, New York (1969).

164. I. Vajda and T. Nemetz, "Substitution of characters in q-ary m-sequences," *Lect. Notes Comput. Sci.*, **508**, 96–105 (1991).

165. A. Vince, "Period of a linear recurrence," *Acta Arithm.*, **39**, No. 4, 303–311 (1981).

166. M. Ward, "The arithmetical theory of linear recurring series," *Trans. Am. Math. Soc.*, **35**, No. 3, 600–628 (1933).

167. M. Ward, "Arithmetical properties of sequences in rings," *Ann. Math.*, **39**, 210–219 (1938).

168. W. A. Webb and C. T. Long, "Distribution modulo p of the general linear second-order recurrence," *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.*, **58**, No. 2, 92–100 (1975).

169. R. Wisbauer, *Grundlagen der Modul und Ringtheorie*, Verl. Reinhard Fischer, Munich (1988).

170. R. B. Yale, "Error correcting codes and linear recurring sequences," *Report 34-37, M. I. T. Lincoln Laboratory*, Lexington, Massachusetts (1958).

171. L. A. Zadeh and E. Polak, *System Theory*, McGraw-Hill, New York (1969).

172. K. C. Zeng and M. Q. Huang, "Solving equations in sequences," *Lect. Notes Comput. Sci.*, **453**, 327–332 (1990).

173. N. Zierler, "Linear recurring sequences and error-correcting codes," In: *Error Correcting Codes*, Wiley, New York (1968), pp. 47–59.

174. N. Zierler and W. H. Mills, "Products of linear recurring sequences," *J. Algebra*, **27**, No. 1, 147–157 (1973).