OCCURRENCE OF ZERO IN A LINEAR RECURSIVE SEQUENCE

N. K. Vereshchagin

Introduction. A sequence of algebraic numbers $\{u_n\}$ $(n = 0, 1, \ldots)$ is called a linear recursive sequence (LRS) of order m if for all $n \geqslant m$ we have a relation

$$u_n = a_1 u_{n-1} + \ldots + a_m u_{n-m}, \tag{1}$$

where $a_1, \ldots, a_m$ are fixed algebraic numbers (that do not depend on n). An algebraic number α can be defined by its fundamental polynomial $p_\alpha(x)$ and a circular neighborhood W, with a rational center and a radius which is a rational Gaussian number, that contains α but no other zeros of $p_\alpha(x)$. The pair $\langle p_\alpha(x), W\rangle$ will be called a definition of α. By a definition of a LRS $\{u_n\}$ we mean a procession composed of definitions of the numbers $a_1, \ldots, a_m$, $u_0, \ldots, u_{m-1}$. The polynomial $x^m - a_1 x^{m-1} - \ldots - a_m$ will be called the characteristic polynomial of the LRS. If R is a subring of A (the field of algebraic numbers) such that $a_1, \ldots, a_m$ lie in R and $\forall n\, (u_n \in R)$, then we will call $\{u_n\}$ an R-LRS.

We will consider problems connected with the set of zeros of a LRS, i.e., the set $\{n| u_n = 0\}$. The structure of this set was described by Mahler [1], using a p-adic method of Skolem [2].

Definition. A set of natural numbers is called semilinear if it is the union of a finite set D and a finite number of arithmetic progressions; it is easy to see that the differences of these progressions can be assumed to be the same. Thus a set is semilinear if it can be represented in the form $D \cup (b_1 + l\mathbf{N}) \cup \ldots \cup (b_\rho + l\mathbf{N})$; the procession $\langle D, l, b_1, \ldots, b_\rho\rangle$ is called a semilinear definition of the considered set.

THEOREM A (Mahler [1]). The set of zeros of any LRS is semilinear.

We can extract from Mahler's proof a method for finding the numbers l and $b_1, \ldots, b_\rho$, occurring in the definition of the set of zeros, but the proof contains no effective method for finding the set D, i.e., the set of zeros can actually be found to within a finite number of elements. The problem of making Mahler's theorem effective is still open:

Problem I: Construct an algorithm for finding a semilinear definition of the set of zeros of a LRS from a definition of this sequence.

Another open (and, at first glance, more special) problem is the "problem of the emptiness of the set of zeros": Construct an algorithm for determining from a definition of a LRS whether its set of zeros is empty (this problem is open even for Z-LRS). The emptiness problem for Z-LRS was said in [3] to have important significance for the theory of formal languages. Actually, it is not difficult to prove that Problem I and the emptiness problem are equivalent (the reducibility of the emptiness problem to Problem I is obvious).

It is known that the following properties of the set of zeros are decidable for Z-LRS (i.e., there exists an algorithm for determining from any definition of a Z-LRS whether the set of zeros possess the corresponding property):

1) the property of being finite (Berstel and Mignotte [4]);*

2) the property of having a finite complement [3, Sec. II.12];

3) the property of being equal to all of N [3, Sec. II.12].

The proofs in [3 and 4] can easily be generalized to any LRS, hence properties 1)-3) are decidable for all LRS; the decidability of these properties also follows from the fact that in Mahler's proof the numbers $l, b_1, \ldots, b_\rho$ can be effectively determined.

*Moreover, there exists an algorithm that yields an upper bound for the number of zeros of a given LRS, if this number is finite [5].

M. V. Lomonosov Moscow State University. Translated from Matematicheskie Zametki, Vol. 38, No. 2, pp. 177-189, August, 1985. Original article submitted January 20, 1984.

0001-4346/85/3812-0609$09.50

The problem of the emptiness of the set of zeros for Z-LRS admits an equivalent formulation in terms of integral matrices: Construct an algorithm for determining whether some positive power of a given integral matrix has a zero in the upper right corner. The generalization of this problem to the case of several matrices is undecidable [3, Sec. II.12].

In the present paper Problem I is solved for any LRS of order $\leqslant 3$ and for $(A \cap R)$-LRS of order $\leqslant 4$ (Theorems 3 and 4). In particular, this provides a solution of the emptiness problem for Z-LRS of order $\leqslant 4$. The result on the decidability of Problem I for Z-LRS of order $\leqslant 3$ was announced in [5] and for any LRS of order $\leqslant 3$ in [6].

1. The value of a LRS $\{u_n\}$ at a point n is a quasipolynomial in n (see, e.g., [3, Sec. II.9]). A quasipolynomial is a function of the form $g(n)=\sum_{i=1}^{k} P_i(n)\alpha_i^n$, where the $P_i(x)$ are polynomials with algebraic coefficients and $\alpha_1, \ldots, \alpha_k$ are distinct algebraic numbers. We will call the quantity $\sum_{i=1}^{k}(\deg P_i+1)$ the degree of the quasipolynomial. The numbers $\alpha_1, \ldots, \alpha_k$ and the coefficients of the polynomials $P_1(x), \ldots, P_k(x)$ will be called the coefficients of g(n). A definition of a quasipolynomial is a process consisting of definitions of its coefficients.

<u>THEOREM 1.</u> From the definition of a LRS $\{u_n\}$ of order m we can find a definition of a quasipolynomial g(n) of degree $\leqslant m$, such that

$$u_n = g(n) = \sum_{i=1}^{k} P_i(n)\alpha_i^n, \tag{2}$$

where $\alpha_1, \ldots, \alpha_k$ are some of the zeros of the characteristic polynomial of $\{u_n\}$.

<u>Proof.</u> That a quasipolynomial with the required properties exists is well known (see, e.g., [3, p. 56]). We will prove only that the transition is effective. For this purpose we use known algorithms working with definitions of algebraic numbers:

a) From definitions of algebraic numbers α and β we can find definitions of $\alpha\pm\beta$, $\alpha\cdot\beta$, α/β and recognize whether $\alpha=\beta$ (see [7]).

b) From a definition of a polynomial with algebraic coefficients we can find definitions of all its zeros [8].*

We will find definitions of all zeros of the characteristic polynomials of the LRS $\{u_n\}$. Suppose these zeros are $\alpha_1, \ldots, \alpha_s$. We will assume that $P_1(x), \ldots, P_s(x)$ are polynomials of degree $(m-1)$ with unknown coefficients: $P_i(x)=y_{i0}+y_{i1}x+\ldots+y_{i(m-1)}x^{m-1}$. We calculate the first sm values of $\{u_n\}$ and, equating the values of the quasipolynomial $\sum_{i=1}^{s} P_i(n)\alpha_i^n$ to the values u_n, obtain a system of sm linear equations in the y_{ij}:

$$u_n = \sum_{i=1}^{s}\sum_{j=0}^{m-1} y_{ij}n^j\alpha_i^n \qquad (n=0, 1, \ldots, sm-1). \tag{3}$$

Its determinant is not zero [9, p. 152]. Using algorithms a) and b) and relation (1), we find definitions of $u_0, \ldots, u_{sm-1}$. We now have definitions of all coefficients of system (3). We can now find a definition of its determinant and of the determinants obtained by replacing the l-th column by a column of free coefficients. Then by Cramer's rule we can find definitions of the solutions of the system; these definitions constitute a definition of the quasipolynomial g(n).

Theorem 1 enables us to reduce the problem of finding a definition of the set of zeros to that of finding the natural zeros of the quasipolynomial we are using. (The reverse reduction is also valid, i.e., from the quasipolynomial g(n) of degree m we can find a definition of the LRM $\{g(n)\}$, and its order is at most m.)

2. It is simpler to investigate quasipolynomials $\sum_{i=1}^{s} P_i(n)\alpha_i^n$, for which there are no roots of 1 among the quotients α_i/α_j with i < j. Such quasipolynomials (and the LRS connected with them by means of (2)) are called nonsingular. Lemma 1 shows how nonsingular

*In [8] this fact was proved for polynomials with integral coefficients. If we have $P(x)\in A[x]$, then, using a standard construction [9, Sec. 3.2], we can find an integral polynomial Q(x) equal to zero at all zeros of P(x), find definitions of all zeros of Q(x), and, using calculations with sufficient precision, discard the superfluous roots.

quasipolynomials can be used to investigate the general case. Before stating it we mention a simple result (see, e.g., [10]) used in the proof.

THEOREM B. From a definition of a number α we can discover whether it is a root of 1 and, if it is, we can find the smallest $d > 0$ such that $\alpha^d = 1$ (this d is called the order of α).

LEMMA 1. From a definition of a quasipolynomial g(n) we can find an l such that each of the quasipolynomials $g_1(n), \ldots, g_l(n)$, defined by $g_j(n) = g(j-1+ln)$, is nonsingular or zero.

Proof. Let us take as l the least common multiple of all orders of the roots of 1 occurring in the set $\{\alpha_i/\alpha_j \mid i, j \leqslant k\}$. Let $\beta_1, \ldots, \beta_{k'}$ be the distinct elements of the set $\{\alpha_1^l, \ldots, \alpha_k^l\}$. For each j the quasipolynomial $g_j(n) = \sum_{i=1}^{k} P_i(j-1+ln)\alpha_i^{j-1+ln} = \sum_{i=1}^{k'} Q_i(n)\beta_i^n$ is nonsingular or zero, since $(\alpha_i^l/\alpha_m^l)^t = 1$ implies, by definition of l, that $\alpha_i^l = \alpha_m^l$.

Method. We will denote by $c, c_1, \ldots$ certain positive quantities that can be effectively calculated from the degrees and heights of the coefficients of g(n) and from l. We will denote by K the field obtained by adjoining to Q the coefficients of the quasipolynomial g(n).

1) By Lemma 1, we can find quasipolynomials $g_1(n), \ldots, g_l(n)$, each of which is nonsingular or zero, whose degrees do not exceed the degree m of the quasipolynomial g(n). We then find a definition of the set N_j of zeros of each quasipolynomial $g_j(n)$. If we know these, then it is easy to form a definition of the set of zeros of g(n), since

$$\{n \mid g(n) = 0\} = N_1 \cup (1 + lN_2) \cup \ldots \cup (l - 1 + lN_l).$$

2) If $g_j(n)$ is zero, then its set of zeros is equal to all of N.

If $g_j(n)$ is nonsingular, then we will prove that it has a finite number of zeros and we will find c such that $g_j(n) = 0 \Rightarrow n \leqslant c$. Since the heights of the coefficients $g_1(n), \ldots g_l(n)$ can be effectively expressed in terms of a definition of g(n) and l, we will prove only the effective dependence of c on the coefficients of $g_1(n), \ldots, g_l(n)$. (Indeed, it follows from Theorem A that any nonsingular quasipolynomial has a finite number of zeros, but we do not need this fact.) To find a definition of the set of zeros of $g_j(n)$ it suffices to calculate $g_j(0), \ldots, g_j(c)$.

How do we find the required c? Suppose $g_j(n) = \sum_{i=1}^{k} P_i(n)\alpha_i^n$ and $|\alpha_1| = \ldots = |\alpha_v| > |\alpha_{v+1}| \geqslant \ldots$. For a quasipolynomial of degree $\leqslant 3$ we will prove that we can find c_1, c_2, c_3, such that for $n \geqslant c_3$ we have $|P_1(n)\alpha_1^n + \ldots + P_v(n)\alpha_v^n| \geqslant c_1 |\alpha_1|^n n^{-c_2}$ (in this case, obviously, $v \leqslant 3$). If $g_j(n)$ has a principal term, i.e., the degrees of $P_2(x), \ldots, P_v(x)$ are less than the degree of $P_1(x)$, then the existence of c_1, c_2, c_3 is obvious (and $c_2 = 0$). If this is not so, then $g_j(n)$ has the form $a_1\alpha_1^n + a_2\alpha_2^n + a_3\alpha_3^n$, and we obtain for the modulus of this sum the lower bound $c_1 |\alpha_1|^n n^{-c_2}$ for $n \geqslant c_3$ (this estimate is given in Lemmas 3 and 4).

In the case of a fourth-degree quasipolynomial we will use various valuations of the field K. Recall that all inequivalent valuations on an algebraic number field are either Archimedean, i.e., valuations of the form

$$\varphi(x) = |\sigma(x)|, \tag{4}$$

where σ is an isomorphism of K, or p-adic, i.e.,

$$\varphi(x) = p^{-v_\mathfrak{p}(x)/e_\mathfrak{p}}, \tag{5}$$

where $\mathfrak{p}$ is a prime ideal of Z_K, containing the prime number p, $v_\mathfrak{p}$ is its exponent, and $e_\mathfrak{p} = v_\mathfrak{p}(p)$ is its ramification index (see [11]).

Suppose φ is a valuation on K and $\varphi(\alpha_1) = \ldots = \varphi(\alpha_v) > \varphi(\alpha_{v+1}) \geqslant \ldots$. Let G(n) denote the sum of the leading terms, i.e., $G(n) = \sum_{i=1}^{v} P_i(n)\alpha_i^n$, and let h(n) denote the rest, i.e., $h(n) = g_j(n) - G(n)$. We will prove that there exists either an Archimedean valuation φ, for which $v \leqslant 3$, or a p-adic valuation φ with p at most c_4 for which $v \leqslant 2$, and we will find c_5, c_6, c_7, such that

$$\varphi(G(n)) \geqslant \varphi(\alpha_1)^n e^{-c_6(\ln n)^2} \quad \text{for} \quad n \geqslant c_7. \tag{6}$$

The quantities c_5, c_6, c_7 depend only on the definition of the quasipolynomial g(n) and l, not on the valuation φ. We will not find φ; we know only that it exists.

3) If we know there exists the valuation φ on K and we have c_5, c_6, c_7 such that (6) holds, then we can find c_8 and c_9 such that $\varphi(h(n)) \leqslant c_8\varphi(\alpha_{v+1})^n n^{c_9}$. This is easy to do, since for all valuations φ we have $\varphi(\alpha) < H(\alpha) + 1$ (where H(α) is the height of α).* We can then find $c_{10} > 0$, such that $\varphi(\alpha_1/\alpha_{v+1}) \geqslant 1 + c_{10}$. This can be done because if φ is Archimedean, $\varphi(x) = |\sigma(x)|$, then $\varphi(\alpha_1/\alpha_{v+1}) = |\alpha_1^{(s)}/\alpha_{v+1}^{(t)}|$, where $\alpha_1^{(s)}$, $\alpha_{v+1}^{(t)}$ are certain conjugates of α_1 and α_{v+1}. The degree and height of the number $|\alpha_1^{(s)}/\alpha_{v+1}^{(t)}|$ can be effectively bounded above in terms of the degrees and heights of α_1 and α_{v+1}, hence Liouville's theorem [10, p. 29] yields an effective lower bound for $||\alpha_1^{(s)}/\alpha_{v+1}^{(t)}| - 1|$. If φ is p-adic, then $\varphi(\alpha_1/\alpha_{v+1}) \geqslant p^{1/e_\mathfrak{p}} \geqslant 2^{1/d}$, where d is the degree of K.

Now the equality $g_j(n) = 0$ implies $c_5(1+c_{10})^n e^{-c_6(\ln n)^2} \leqslant c_8 n^{c_9}$, from which we obtain an upper bound of those n for which $g_j(n) = 0$.

Effective computability is understood in Lemmas 2, 3, 4 and Theorem 2 to mean that the quantities being computed depend effectively on the heights and degrees of the numbers in the input. The algorithms working with definitions of algebraic numbers are used only in Lemma 1 to determine which of $g_1(n), \ldots, g_l(n)$ are zero and to calculate $g_j(0), \ldots, g_j(c)$.

The method has been described. We will complete the proofs of all theorems by obtaining effective lower bounds of the indicated form for the sum of the leading terms. In obtaining these lower bounds we will use:

a) a consequence of the estimates of Fel'dman [9] for a linear form in the logarithms of algebraic numbers:

<u>THEOREM C.</u> For algebraic numbers α_1, α_2 we can find numbers c_1, c_2, such that $|\alpha_1^n - \alpha_2| > c_1 n^{-c_2}$, if the left-hand side is nonzero.

b) a result of van der Poorten [12] generalizing the estimates of a linear form in logarithms to p-adic valuations:

<u>THEOREM D.</u> For algebraic numbers α_1, α_2 and a prime number p we can find constants c_1, c_2, such that for any p-adic valuation φ on $\mathbf{Q}(\alpha_1, \alpha_2)$ we have $\varphi(\alpha_1^n - \alpha_2) > c_2 e^{-c_1(\ln n)^2}$, if the left-hand side is nonzero.

3. In this section we will obtain the promised lower bounds.

<u>LEMMA 2.</u> Suppose K is an algebraic number field, $\alpha \in K$, and α is not a root of unity. Then there exist c_3 and c_4, depending effectively on the degree and height of α, such that for some metric φ on K we have $\varphi(\alpha) > 1 + c_3$, and, if φ is p-adic, $p \leqslant c_4$.

<u>Proof.</u> Assume $\alpha \in \mathbf{Z}_A$. Then, by Kronecker's theorem, there exists a conjugate $\alpha^{(i)}$ of α such that $|\alpha^{(i)}| > 1 + c_3$, where c_3 depends effectively on the degree of α (see [13, p. 32]). Let σ be an isomorphism of K sending α into $\alpha^{(i)}$; then we can define φ by means of (4).

Suppose $\alpha \notin \mathbf{Z}_A$. Then, as is well known [11], for some prime ideal $\mathfrak{p}$ of $\mathbf{Z}_{\mathbf{Q}(\alpha)}$ we have $v_\mathfrak{p}(\alpha) < 0$. If we define φ by means of (5), then $\varphi(\alpha) \geqslant p^{1/e_\mathfrak{p}} \geqslant 2^{1/d}$, where d is the degree of K. The extension of φ to K satisfies the condition of the lemma. We will now find c_4. Let a be the leading coefficient of $p_\alpha(x)$; then $a\alpha \in \mathbf{Z}_A$, hence $v_\mathfrak{p}(a\alpha) > 0$, and so $v_p(a) = e_\mathfrak{p} v_\mathfrak{p}(a) > 0$, i.e., p divides a. Thus, c_4 can be taken to be $|a|$.

As a consequence of Lemma 2 we obtain an upper bound of those n for which $\alpha^n = \beta$ (if α is not a root of 1). Such a bound was obtained in [10] for the case where β is given as a polynomial in α. An analysis of the proof shows that it is actually based on Lemma 2: if $\varphi(\alpha) > 1$, then $\varphi(\alpha^n)$ tends to infinity, whereas $\varphi(\beta)$ is constant.

<u>COROLLARY.</u> For given algebraic numbers α and β we can find a c_3 such that $\alpha^n = \beta \Rightarrow n \leqslant c_3$, provided that α is not a root of 1.

<u>Proof.</u> Suppose $K = \mathbf{Q}(\alpha, \beta)$ and φ is the valuation in Lemma 2. Then $\alpha^n = \beta$ implies $n = \ln\varphi(\beta)/\ln\varphi(\alpha)$. Since $\varphi(\beta)$ can be estimated from above in terms of the height of β and

---

*For Archimedean valuations, this follows from the inequality $|\alpha^{(i)}| < H(\alpha) + 1$ [9, p. 17]; if φ is p-adic and a is the leading coefficient of $P_\alpha(x)$, then $\varphi(\alpha) \leqslant p^{v_\mathfrak{p}(a)/e_\mathfrak{p}} \leqslant |a|$.

Lemma 2 provides a lower bound for $\varphi(\alpha)$, we can calculate the required c_3

LEMMA 3. For given algebraic numbers $a_1 \neq 0$, $a_2 \neq 0$, α_1, α_2 such that α_1/α_2 is not a root of 1 and for $c \in \mathbf{N}$ we can find numbers c_5, c_6, c_7, c_8, c_9, such that for $n \geqslant c_5$ we have $|a_1\alpha_1^n + a_2\alpha_2^n| \geqslant c_6 |\alpha_1|^n n^{-c_7}$, if $|\alpha_1| \geqslant |\alpha_2|$, and $\varphi(a_1\alpha_1^n + a_2\alpha_2^n) \geqslant c_8 \varphi(\alpha_1)^n e^{-c_9(\ln n)^2}$ for any p-adic valuation φ with $p \leqslant c$, if $\varphi(\alpha_1) \geqslant \varphi(\alpha_2)$.

Proof. We will assume that $\alpha_2 \neq 0$, since the assertion is obvious otherwise. Applying the corollary to the numbers α_1/α_2 and a_2/a_1, we can find a c_4 such that for $n \geqslant c_4$ we have $a_1\alpha_1^n + a_2\alpha_2^n \neq 0$. Our assertion now follows from Theorem C or Theorem D. The restriction $p \leqslant c$ is necessary because in Theorem D the numbers c_1, c_2 depend on p.

Lemma 4 is a generalization of Lemma 3 for the norm $|\cdot|$ to the case of three summands. (Lemma 4 was proved by Mignotte [14] for a sum of the form $a_1\alpha_1^n + a_2\alpha_2^n + \bar{a}_2\bar{\alpha}_2^n$ with $|\alpha_1| = |\alpha_2|$ and $a_1 \in \mathbf{R}$, $\alpha_1 \in \mathbf{R}$, under the condition that the sum is nonzero.)

LEMMA 4. For given algebraic numbers $a_1, a_2, a_3, \alpha_1, \alpha_2, \alpha_3$ such that $|\alpha_1| = |\alpha_2| = |\alpha_3|$ and α_i/α_j is not a root of 1 for i < j we can find c_9, c_{10}, c_{11}, such that for $n \geqslant c_9$ we have

$$|a_1\alpha_1^n + a_2\alpha_2^n + a_3\alpha_3^n| \geqslant c_{10} |\alpha_1|^n n^{-c_{11}}. \tag{7}$$

Proof. The letters $A, A_1, \ldots, \delta, \delta_1$ will denote quantities that can be calculated from the degrees and heights of a_1, a_2, a_3. The proof is based on the following geometric idea. Let ε denote the left-hand side of inequality (7). Then $(\alpha_1/\alpha_3)^n$ and $(\alpha_2/\alpha_3)^n$ satisfy the system of equations

$$a_1x_1 + a_2x_2 + (a_3 - \varepsilon) = 0, \quad |x_1| = 1, \quad |x_2| = 1. \tag{8}$$

The geometric interpretation of this system is as follows: the sum of the vectors a_1x_1, a_2x_2, $a_3 - \varepsilon$ of lengths $|a_1|$, $|a_2|$, $|a_3 - \varepsilon|$ is zero, i.e., these vectors form a triangle. Knowing the lengths of the sides of the triangle, we can find the sides themselves, i.e., we can find all solutions of system (8). We will prove that if $\varepsilon = 0$, any solution θ_1, θ_2 of system (8) consists of algebraic numbers, and we will then use the corollary to obtain an upper bound of those n for which $(\alpha_1/\alpha_3)^n = \theta_1$. We will take c_9 to be this upper bound. We will also prove that for any solution d_1, d_2 of system (8) there exists a solution θ_1, θ_2 of this system with ε equal to 0 such that d_1 differs from θ_1 by a quantity of order $|\varepsilon|^{1/2}$, i.e., we can find A and $\delta > 0$, not depending on ε, d_1, θ_1, such that

$$|d_1 - \theta_1| < A|\varepsilon|^{1/2} \text{ if } |\varepsilon| < \delta. \tag{9}$$

In particular, this will hold for d_1 equal to $(\alpha_1/\alpha_3)^n$. If $n \geqslant c_9$, then $(\alpha_1/\alpha_3)^n - \theta_1 \neq 0$. Consequently, by Theorem C, $|(\alpha_1/\alpha_3)^n - \theta_1| > c_1 n^{-c_2}$, and this inequality, together with (9), implies $|\varepsilon| > \min\{\delta, A^{-2}c_1^2 n^{-2c_2}\}$.

Thus, it remains for us to solve system (8) and find c_9, A, δ. To solve (8) we denote $a_3 - \varepsilon$ by $\tilde{a}_3$ and introduce new real variables v_1, v_2, w_1, w_2, connected with x_1, x_2 by the equalities $v_j + iw_j = a_jx_j/\tilde{a}_3$. The new variables satisfy the system $v_1 + v_2 + 1 = 0$, $w_1 = -w_2$, $v_j^2 + w_j^2 = b_j^2$, where $b_j = |a_j|/|\tilde{a}_3|$. This system can easily be reduced to quadratic equations and solved. We at once obtain the values of x_1, x_2:

$$\begin{cases} x_1 = x_1(\varepsilon) = \dfrac{\tilde{a}_3(|a_2|^2 - |a_1|^2 - |\tilde{a}_3|^2 \pm i\sqrt{D(\varepsilon)})}{2a_1|\tilde{a}_3|^2}, \\ x_2 = x_2(\varepsilon) = \dfrac{\tilde{a}_3(|a_1|^2 - |a_2|^2 - |\tilde{a}_3|^2 \mp i\sqrt{D(\varepsilon)})}{2a_2|\tilde{a}_3|^2}, \\ D(\varepsilon) = ((|a_1| + |a_2|)^2 - |\tilde{a}_3|^2)(|\tilde{a}_3|^2 - (|a_1| - |a_2|)^2), \end{cases}$$

and a solution exists if and only if $D(\varepsilon) \geqslant 0$. We can show that $D(\varepsilon) \geqslant 0$ means that each of $|a_1|$, $|a_2|$, $|\tilde{a}_3|$ is at most the sum of the other two, which corresponds to the geometric interpretation of the system.

If $\varepsilon = 0$, then x_1 and x_2 can be expressed with the aid of the signs $\pm, \cdot, /, \sqrt{}$ in terms of a_1, a_2, a_3 and their moduli, from which it follows that x_1, x_2 are algebraic numbers with heights and degrees bounded by some polynomial in the heights and degrees of a_1, a_2, a_3. By the corollary, knowing α_1/α_3 and an upper bound of the height of x_1 we can find a c_9 such that $(\alpha_1/\alpha_3)^n = x_1 \Rightarrow n \leqslant c_9$.

Let us estimate $|x_1(\varepsilon) - x_1(0)|$, where $x_1(\varepsilon)$ and $x_1(0)$ are obtained by choosing the same sign in front of the square root. We may assume without loss of generality that $|a_1| \leqslant |a_2| \leqslant |a_3|$. Suppose $\varepsilon < |a_3|/4$; consider two cases: $D(0) \geqslant 0$, $D(0) < 0$.

1) $D(0) \geq 0$. Split the difference $x_1(\varepsilon) - x_1(0)$ into two differences:

$$\left| \frac{(a_3-\varepsilon)(|a_2|^2-|a_1|^2-|a_3-\varepsilon|^2)}{2a_1|a_3-\varepsilon|^2} - \frac{a_3(|a_2|^2-|a_1|^2-|a_3|^2)}{2a_1|a_3|^2} \right| \leqslant \frac{A_1|\varepsilon|}{|a_1|},$$

$$\left| \frac{(a_3-\varepsilon)\sqrt{D(\varepsilon)}}{2a_1|a_3-\varepsilon|^2} - \frac{a_3\sqrt{D(0)}}{2a_1|a_3|^2} \right| \leqslant \frac{A_2|\varepsilon|}{|a_1|} + \left| \frac{\sqrt{D(\varepsilon)}-\sqrt{D(0)}}{a_1a_3} \right|.$$

If D(0) = 0, the second summand is bounded by $A_3|\varepsilon|^{1/2}$; if D(0) > 0, the second summand is bounded by $A_4|\varepsilon|$. A detailed calculation shows that we can take $A_1 = 14$, $A_2 = 10$, $A_3 = 6\sqrt{|a_3|}$, $A_4 = 30|a_3|^3/\sqrt{D(0)}$.

2) D(0) < 0, i.e., $|a_1| + |a_2| < |a_3|$. In this case we can find a $\delta_1 > 0$, such that for $|\varepsilon| < \delta_1$ we have $D(\varepsilon) < 0$, hence Eq. (8) has no solutions. (We can calculate that $\delta_1 = \frac{|D(0)|}{15|a_3|^3}$.)

Put $A = \frac{A_1+A_2}{|a_1|} + \max\left\{\frac{A_3}{|a_1|}, A_4\right\}$, $\delta = \min\left\{1, \delta_1, \frac{|a_3|}{4}\right\}$. Then for $|\varepsilon| < \delta$, if $x_1(\varepsilon), x_2(\varepsilon)$ are solutions of system (8), it follows that $x_1(0), x_2(0)$ are defined and $|x_1(\varepsilon) - x_1(0)| \leqslant A|\varepsilon|^{1/2}$.

We can obviously estimate A from above and δ from below, knowing only the heights and degrees of a_1, a_2, a_3. The lemma is proved.

4. Main Results. THEOREM 2. From the degrees and heights of the coefficients of a nonsingular quasipolynomial g(n) of degree $\leqslant 3$ we can find a c such that g(n) = 0 implies $n \leqslant c$.

Proof. If g(n) has principal term $a_1 n^j \alpha_1^n$, then, using the fact that $|a_1| > \frac{1}{1+H(a_1)}$, we can find c_8, c_9 such that for $n \geqslant c_8$ we have $|P_1(n)\alpha_1^n| \geqslant c_9 n^j |\alpha_1|^n$. If there is no principal term, then g(n) has the form $a_1\alpha_1^n + a_2\alpha_2^n + a_3\alpha_3^n$, where $|\alpha_1| = |a_2| \geqslant |\alpha_3|$. If $|\alpha_1| = |\alpha_2| > |\alpha_3|$, then, using the estimate of Lemma 3, we can find c_4, c_5, c_6, such that for $n \geqslant c_4$ we have $|a_1\alpha_1^n + a_2\alpha_2^n| \geqslant c_5|\alpha_1|^n n^{-c_6}$.

If $|\alpha_1| = |\alpha_2| = |\alpha_3|$, then the number c_9 in Lemma 4 provides a bound for those n for which g(n) = 0.

THEOREM 3. Problem I has a solution for LRS of order $\leqslant 3$, i.e., there exists an algorithm for finding a semilinear definition of the set of zeros of any LRS of order $\leqslant 3$ from a definition of the sequence.

Proof. The assertion of the theorem follows from Theorem 2, Lemma 1, and Theorem 1.

THEOREM 4. There exists an algorithm for finding a definition of the set of zeros of any $(\mathbf{A} \cap \mathbf{R})$-LRS (and therefore any $\mathbf{Z}$-LRS) of order $\leqslant 4$ from a definition of the sequence.

Proof. The symbols $c_{10}, c_{11}, \ldots$ will denote positive quantities depending effectively on the definition of the LRS.

Suppose $\{u_n\}$ satisfies (2), where g(n) is a quasipolynomial of degree $\leqslant 4$. By Lemma 1, we can find the nonsingular or zero quasipolynomials $g_1(n), \ldots, g_l(n)$. We will find a definition of the set of zeros of each $g_j(n)$. Let $g_j(n) = \sum_{i=1}^{k'} Q_i(n)\beta_i^n$ be any nonzero quasipolynomial among $g_1(n), \ldots, g_l(n)$.

We consider two cases.

1) $k' \leqslant 3$. If $g_j(n)$ has a principal term, we argue as in the proof of Theorem 2. Of the quasipolynomials of degree $\leqslant 4$ (with $k' \leqslant 3$) those that do not have principal terms have one of two forms:

$$g_j(n) = b_1\beta_1^n + b_2\beta_2^n + (b_3 n + b_4)\beta_3^n,$$
$$g_j(n) = (b_1 n + b_2)\beta_1^n + (b_3 n + b_4)\beta_2^n, \ |\beta_1| = |\beta_2| > |\beta_3|.$$

The first case was analyzed in the proof of Theorem 1.

In the second case, according to Lemma 2, we can find $c_4 \in \mathbf{N}$, such that for some valuation φ on K we have $\varphi(\beta_1) > \varphi(\beta_2)$, and, if φ is p-adic, $p \leqslant c_4$. By Liouville's theorem or its generalization to p-adic valuations [15], $\varphi(b_1 n + b_2) \geqslant c_{10} n^{-c_{11}}$ for $n \geqslant c_{12}$, where c_{10}, c_{11},

c_{12} can be calculated knowing c_4 and definitions of b_1, b_2. Thus, we have $\varphi((b_1 n + b_2)\beta_1^n) \geqslant c_{10}\varphi(\beta_1)^n n^{-c_{11}}$ for $n \geqslant c_{12}$.

2) $k' = 4$, $g_j(n) = b_1\beta_1^n + \ldots + b_4\beta_4^n$. By definition of $g_j(n)$, we have in this case $\beta_i = \alpha_i$, $l = 1$. If for at least one Archimedean valuation $\varphi(x) = |\sigma(x)|$ at most three of the numbers $\alpha_1, \ldots, \alpha_4$ have maximal norm, say $\varphi(\alpha_1) = \ldots = \varphi(\alpha_v) > \varphi(\alpha_{v+1}) \geqslant \ldots$, then we apply Lemma 3 or 4 to the numbers $\sigma b_1, \ldots, \sigma b_v, \sigma\alpha_1, \ldots, \sigma\alpha_v$. The heights and degrees of these numbers agree with the heights and degrees of the b_i, α_i, hence the quantities given by the lemmas depend effectively on the degrees and heights of the coefficients of g(n). Thus, by Lemmas 3 and 4, for $n \geqslant c_7$ we have $\varphi(b_1\alpha_1^n + \ldots + b_v\alpha_v^n) \geqslant c_8\varphi(\alpha_1)^n n^{-c_9}$.

Assume that for all Archimedean valuations φ we have $\varphi(\alpha_1) = \ldots = \varphi(\alpha_4)$, in particular, $|\alpha_1| = |\alpha_2| = |\alpha_3| = |\alpha_4|$. By Lemma 2, there exists a p-adic valuation φ, such that $p \leqslant c_4$ and $\varphi(\alpha_1) > \varphi(\alpha_2)$. We will prove that at most two of the numbers $\alpha_1, \ldots, \alpha_4$ have maximal norm.

Since $\{u_n\}$ is an $(\mathbf{A} \cap \mathbf{R})$-LRS, the characteristic polynomial of $\{u_n\}$ has real coefficients. It follows from Theorem 1 that the characteristic polynomial is equal to $(x - \alpha_1)\cdot\ldots\cdot(x - \alpha_4)$, hence $\alpha_1, \ldots, \alpha_4$ are real or consist of two pairs of complex conjugates. However $\alpha_1, \ldots, \alpha_4$ cannot all be real, since $|\alpha_i| = |\alpha_m|$ and, in view of nonsingularity, $\alpha_i \neq \pm\alpha_m$. We will therefore assume that $\alpha_2 = \bar{\alpha}_1$, $\alpha_4 = \bar{\alpha}_3$. From $\alpha_1\alpha_2 = \alpha_3\alpha_4 = |\alpha_1|^2$, follows $\varphi(\alpha_1)\varphi(\alpha_2) = \varphi(\alpha_3)\varphi(\alpha_4)$, in view of which the equality $\varphi(\alpha_1) = \varphi(\alpha_3) = \varphi(\alpha_4)$ is impossible.

We now apply Lemma 2 to the sum of the two monomials largest in norm and obtain a lower bound in the valuation φ of the form $c_5\varphi(\alpha_1)^n e^{-c_6(\ln n)^2}$ for $n \geqslant c_7$. The theorem is proved.

The author would like to thank A. L. Semenov and A. A. Muchnik for their interest in this research.

Addendum (January 10, 1985). After this paper was submitted for publication there appeared the article [16], in which similar results were obtained, namely Theorem 3 and Theorem 4 were proved for nonsingular LRS.

LITERATURE CITED

1. K. Mahler, "Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen," Konink. Akad. Wettensch. Amsterdam, 38, No. 1, 50-60 (1935).
2. T. Skolem, "Ein Verfahren zur Behandlung gewisser exponentialer und Diophantischer Gleichungen," in: C.R. VIII Congr. Math., Stockholm (1934), pp. 163-168.
3. A. Salomaa and M. Soittola, Automata-Theoretic Aspects of Formal Power Series, Springer-Verlag, Berlin (1978).
4. J. Berstel and M. Mignotte, "Deux problèmes décidables des suites récurrentes linéaires," Bull. Soc. Math. France, 104, 175-184 (1976).
5. N. K. Vereshchagin, "On an algorithmic problem for linear recursive sequences," in: Abstracts of Reports of the Sixth All-Union Conference on Mathematical Logic, Tbilisi, Izd. Tbilis. Gos. Univ. (1982).
6. N. K. Vereshchagin, "Zeros of linear recursive sequences," Dokl. Akad. Nauk SSSR, 278, No. 5, 1036-1039 (1984).
7. K. Stolarsky, Algebraic Numbers and Diophantine Approximations, Academic Press, New York (1974).
8. J. R. Pinkert, "An exact method for finding the roots of a complex polynomial," ACM Trans. Math. Software, 2, No. 4, 351-363 (1976).
9. N. I. Fel'dman, Approximations of Algebraic Numbers [in Russian], Moscow State Univ. (1981).
10. R. Kannan and R. J. Lipton, "The orbit problem is decidable," in: Proc. 12th Annual ACM Symp. Theor. Comp. (1980), pp. 252-261.
11. Z. I. Borevich and I. R. Shafarevich, Number Theory [in Russian], Nauka, Moscow (1972).
12. A. J. van der Poorten, "Linear forms in logarithms in the p-adic case," in: Transcendence Theory: Advances and Applications, London (1977), pp. 29-57.
13. V. G. Sprindzhuk, Classical Diophantine Equations in Two Unknowns [in Russian], Nauka, Moscow (1982).
14. M. Mignotte, "A note on linear recursive sequences," J. Austral. Math. Soc., 20, (Ser. A), 242-244 (1975).
15. K. Mahler, "Über transzendente P-adische Zahlen," Compos. Math., 2, 259-275 (1935).
16. M. Mignotte, T. N. Shorey, and R. Tijdeman, "The distance between terms of an algebraic linear recursive sequence," J. Reine Angew. Math., 349, No. 4, 63-76 (1984).