Journal of Mathematical Sciences, Vol. 89, No. 2, 1998

DIOPHANTINE REPRESENTATIONS OF LINEAR RECURRENCES. I

M. A. Vsemirnov

UDC 511.216

Direct constructions of Diophantine representations of linear recurrent sequences are discussed. These constructions generalize already known results for second-order recurrences. Some connections of this problem with the theory of units in rings of algebraic integers are shown. It is proved that the required representations exist only for second-, third-, and fourth-order sequences. In the two last-mentioned cases certain additional restrictions on their coefficients must be imposed. Bibliography: 14 titles.

The construction of a Diophantine representation of the set $\{ \langle n, u \rangle : u = F_{2n} \}$, where F_n denotes the Fibonacci sequence

$$F_{n+1} = F_n + F_{n-1},$$
$$F_0 = 0, \quad F_1 = 1,$$

became the crucial step in the negative solution of Hilbert's tenth problem (see [9, 12]).

We recall that the set $\mathfrak{M}$ consisting of n-tuples of nonnegative integers is called Diophantine if there exists a polynomial $P(y_1, \dots, y_n, x_1, \dots, x_m)$ with integer coefficients such that

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \Leftrightarrow \exists x_1 \dots x_m [P(a_1, \dots, a_n, x_1, \dots, x_m) = 0]. \tag{1}$$

(All variables $x_1, \dots, x_m$ range over the nonnegative integers.) The equivalence (1) is called a Diophantine representation of $\mathfrak{M}$.

One may replace F_n by second-order linear recurrences whose values are exactly all nonnegative solutions of Pell's equation

$$x^2 - (A^2 - 1)y^2 = 1, \tag{2}$$

and obtain representations similar to that in [9]. For example, see [3, 8, 14].

This allows us to prove in a simple way that exponentiation is Diophantine, i.e., the set of triples $\{ \langle a, b, c \rangle : a = b^c \}$ is Diophantine. The reader may find a detailed exposition of this technique in [3, 4, 8, 12, 13].

Up to now, all known ways of proving the fact that exponentiation is Diophantine are based on Diophantine representations of second-order recurrences. But this is insufficient for some applications. Thus, we have need for a larger collection of sequences of exponential growth that allow for direct constructions of their Diophantine representations.

One might expect that some results of [3, 8, 12, Chap. 2, 14] are extended to higher order linear recurrent sequences. As the first step in this direction we must find a Diophantine equation such that its solutions are exactly all elements of a given sequence. (Note that we consider all integer solutions, and not just positive.) This problem was stated in [12, open question 2.3]. More precisely, open question 2.3 is concerned with certain equations obtained from matrix relations.

This article is the first one in the series of papers that contain a complete solution of the problem under consideration.

Remark. A Diophantine representation of the $2k + 2$-ary relation "v is the nth element of the linear recurrence with coefficients $b_0, \dots, b_{k-1}$ and initial values $a_0, \dots, a_{k-1}$" ($a_i, b_i \in \mathbb{Z}$) was constructed in [10]. But the technique of positional coding, which was used in this case, is also based on the Diophantine representation of the exponential function. Therefore, this result is inapplicable to our purposes.

Translated from *Zapiski Nauchnykh Seminarov POMI*, Vol. 227, 1995, pp. 52–60. Original article submitted March 3, 1995.

1072-3374/98/8902-1113$20.00 ©1998 Plenum Publishing Corporation

Now, we give a formal statement of our problem. Let a sequence a_n be defined by the recurrent relation

$$a_{n+k} = b_{k-1}a_{n+k-1} + \cdots + b_0 a_n \tag{3}$$

with integer coefficients b_i and $b_0 = \pm 1$ and by the initial conditions

$$a_0 = 1, \quad a_{-1} = a_{-2} = \cdots = a_{-k+1} = 0. \tag{4}$$

In particular, a_n is an integer for any positive value of n.

We assume that the polynomial

$$f(\lambda) = \lambda^k - b_{k-1}\lambda^{k-1} - \cdots - b_1\lambda - b_0 \tag{5}$$

is irreducible over $\mathbf{Q}$. This case is most interesting for applications.

We extend our sequence to all negative values of the index n by the relation

$$a_n = (a_{n+k} - b_{k-1}a_{n+k-1} - \cdots - b_1 a_{n+1})/b_0 \tag{6}$$

that may be easily deduced from (3). Since $b_0 = \pm 1$, the sequence a_n is an integer-valued sequence.

We observe that the restriction on the coefficient b_0 is necessary for the method described below. This restriction also occurs in all known Diophantine representations of second-order recurrences.

As the following lemma shows, the assumption (4) is not necessary but all of the remaining cases can be reduced to this one.

Lemma 1. *Let α_n be an integer-valued sequence that satisfies the recurrent relation*

$$\alpha_{n+k} = b_{k-1}\alpha_{n+k-1} + \cdots + b_0\alpha_n. \tag{7}$$

Then there exist uniquely determined integers $l_0, l_1, \ldots, l_{k-1}$ such that

$$\alpha_n = a_n l_0 + a_{n-1} l_1 + \cdots + a_{n+k-1} l_{k-1} \tag{8}$$

for all n.

Proof. It is sufficient to find the l_i that satisfy (8) for $n = 0, 1, \ldots, k-1$. Then, by relations (3), (7), (6) and the analog of (6) for α_n, relation (8) holds for all n. Taking the initial conditions (4) into account we get the following system of linear equations (in matrix form):

$$\begin{pmatrix} 1 & 0 & \ldots & 0 \\ * & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & \ldots & * & 1 \end{pmatrix} \begin{pmatrix} l_0 \\ l_1 \\ \vdots \\ l_{k-1} \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{k-1} \end{pmatrix}.$$

As one may see, this system is uniquely solvable for any set $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ and, if all of α_i are integers, then the l_i are also integers. The proof is complete.

Consider the square $k \times k$ matrices (below E denotes the identity matrix)

$$B = \begin{pmatrix} 0 & 0 & \ldots & 0 & b_0 \\ 1 & 0 & \ldots & 0 & b_1 \\ 0 & 1 & \ldots & 0 & b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & b_{k-1} \end{pmatrix}, \tag{9}$$

$$A(x_0,x_1,\dots,x_{k-1}) = \sum_{l=0}^{k-1} x_l\big(B^l - \sum_{j=1}^{l} b_{k-j}B^{l-j}\big) =$$
$$= x_0E + x_1(B - b_{k-1}E) + \dots + x_{k-1}(B^{k-1} - b_{k-1}B^{k-2} - \dots - b_1E), \tag{10}$$

$$A(n) = A(a_n, a_{n-1}, \dots, a_{n-k+1}). \tag{11}$$

We note that the characteristic polynomial of the matrix B is the polynomial $f(\lambda)$ defined by (5). Thus,

$$B^k - b_{k-1}B^{k-1} - \dots - b_1B - b_0E = 0. \tag{12}$$

An easy computation based on the definitions (10), (11) and relations (3), (12) shows that

$$A(n)B = A(n+1).$$

In addition, $A(0) = E$ by (4), (10) and (11). Therefore,

$$A(n) = B^n \tag{13}$$

and the latter relation holds for any integer n.

We define a homogeneous polynomial of kth degree in k variables:

$$F_B(x_0,x_1,\dots,x_{k-1}) = \det A(x_0,x_1,\dots,x_{k-1}). \tag{14}$$

We write the subscript B to show that the coefficients of this polynomial depend on the entries of the matrix B, i.e., on b_i, $i = 0,1,\dots,k-1$.

Relations (11) and (13) imply that $F_B(a_n,a_{n-1},\dots,a_{n-k+1}) = \det B^n = (\pm b_0)^n = \pm 1$. Analogously, $F_B(-a_n,-a_{n-1},\dots,-a_{n-k+1}) = \pm 1$.

The main problem. Under what restrictions on the coefficients b_i does the relation

$$F_B(x_0,x_1,\dots,x_{k-1}) = \pm 1 \tag{15}$$

with integer numbers x_0, x_1, ... , x_{k-1} imply that either $x_0 = a_n$, $x_1 = a_{n-1}$, ... , $x_{k-1} = a_{n-k+1}$ or $x_0 = -a_n$, $x_1 = -a_{n-1}$, ... , $x_{k-1} = -a_{n-k+1}$ for some n? In this case we say that (15) is a characteristic condition for the sequence under consideration.

Remark. We may examine another construction that is a more natural generalization of the method for the second-order recurrences presented in [12, Chap. 2]. But it leads to the same polynomial F_B. Let

$$\widetilde{A}(n) = \begin{pmatrix} a_{n-k+1} & a_{n-k+2} & \dots & a_n \\ a_{n-k+2} & a_{n-k+3} & \dots & a_{n+1} \\ \dots & \dots & \dots & \dots \\ a_n & a_{n+1} & \dots & a_{n+k-1} \end{pmatrix}. \tag{16}$$

Taking recurrent relations (3) into account, we may regard $\det \widetilde{A}(n)$ as a polynomial in the variables a_n, a_{n-1}, ... , a_{n-k+1}. After a formal substitution of x_0, x_1, ... , x_{k-1} for a_n, a_{n-1}, ... , a_{n-k+1}, we obtain a homogeneous polynomial

$$\widetilde{F}_B(x_0,x_1,\dots,x_{k-1}),$$

which will be examined along with F_B. It is easy to check that

$$\widetilde{A}(n)B = \widetilde{A}(n+1).$$

Together with (13), this implies that $\widetilde{A}(n+1) = \widetilde{A}(0)B^n = \widetilde{A}(0)A(n)$. But by (4) and (16), the matrix $\widetilde{A}(0)$ has the following form:

$$\begin{pmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 1 & * \\ \dots & \dots & \dots & \dots \\ 1 & * & \dots & * \end{pmatrix}.$$

Thus, $\det A(n)$ and $\det \widetilde{A}(n)$ have the same (up to sign) expressions in terms of a_n, a_{n-1}, ... , a_{n-k+1}. Therefore,

$$\widetilde{F}_B(x_0, x_1, \dots, x_{k-1}) = \pm F_B(x_0, x_1, \dots, x_{k-1}).$$

Two different matrix constructions lead to the same equation (15). It will be more convenient to deal with the matrices $A(n)$. For another definition of the polynomial F_B that is very sophisticated, see [6].

Below we show a relationship between our main problem and some properties of the invertible elements (units) in orders of algebraic numbers.

Let λ be a root of the polynomial f that is defined by (5). Since we assume that f is irreducible over $\mathbf{Q}$, the extension of $\mathbf{Q}$ generated by λ is of degree k, $[\mathbf{Q}(\lambda) : \mathbf{Q}] = k$. One may regard $\mathbf{Q}(\lambda)$ as a vector space over the field $\mathbf{Q}$. For any number $\mu \in \mathbf{Q}(\lambda)$, let $\hat{\mu}$ be a linear transformation of this vector space that acts as follows: $\hat{\mu}(\xi) = \mu\xi$. We define (for example, see [2, §47, §23]) a ring monomorphism

$$T : \mathbf{Q}(\lambda) \to \mathrm{M}_n(\mathbf{Q})$$

mapping any number $\mu \in \mathbf{Q}(\lambda)$ to the matrix of the transformation $\hat{\mu}$ in the basis $\langle 1, \lambda, \dots, \lambda^{k-1} \rangle$, i.e., the jth column of the matrix $T(\mu)$ contains the coefficients of the decomposition of $\mu\lambda^{j-1}$ with respect to this basis:

$$\mu\lambda^{j-1} = \sum_{i=0}^{k-1} T(\mu)_{ij}\lambda^i.$$

In particular, $T(\lambda) = B$. Thus, by (10), (11) and (13), we have

$$\begin{aligned} T(a_n + a_{n-1}(\lambda - b_{k-1}) + \dots + a_{n-k+1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1)) \\ = A(n) = B^n = T(\lambda^n). \end{aligned} \tag{17}$$

Since T is a monomorphism, as a consequence we deduce that

$$\lambda^n = a_n + a_{n-1}(\lambda - b_{k-1}) + \dots + a_{n-k+1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1). \tag{18}$$

This formula generalizes the representations of λ^n already known in the following cases: λ is a root of a cubic irreducible polynomial with negative discriminant [6, Theorem 3], or λ is a root of polynomial $\lambda^{2k} - \lambda^k - 1$ [7].

If $\mu \in \mathbf{Z}[\lambda]$, then $T(\mu) \in \mathrm{M}_n(\mathbf{Z})$. The converse is also true.

Lemma 2. *Let $\mu \in \mathbf{Q}(\lambda)$. If $T(\mu) \in \mathrm{M}_n(\mathbf{Z})$, then $\mu \in \mathbf{Z}[\lambda]$.*

Proof. Write μ in the form $\mu = t_0 + t_1\lambda + \dots + t_{k-1}\lambda^{k-1}$ with rational coefficients t_i. Then

$$T(\mu) = t_0E + t_1B + \dots + t_{k-1}B^{k-1}.$$

Since $T(\mu) \in \mathrm{M}_n(\mathbf{Z})$ and

$$B^j = \begin{pmatrix} \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 1 & * & \dots & * \end{pmatrix}$$

(there are $k - j - 1$ zeros in the last row, and the unity is located at the $(k - j)$th place), we successively conclude that t_{k-1}, t_{k-2}, ... , t_0 are integers. The proof is complete.

By $(\mathbf{Z}[\lambda])^*$ we denote, as usual, the multiplicative group of all invertible elements in the order $\mathbf{Z}[\lambda]$.

Corollary. *For any $\mu \in \mathbf{Z}[\lambda] \setminus \{0\}$ we have $\mu \in (\mathbf{Z}[\lambda])^*$ if and only if* $\det T(\mu) = \pm 1$.

Proof. Since $T(\mu)T(\mu^{-1}) = T(\mu\mu^{-1}) = E$, we have, by Lemma 2, that μ is invertible in $\mathbf{Z}[\lambda]$ if and only if $T(\mu)$ is invertible in $\mathrm{M}_n(\mathbf{Z})$, i.e., $\det T(\mu) = \pm 1$. The proof is complete.

The following theorem yields a necessary condition for (15) to be characteristic.

Theorem 1. *Let a_n be the sequence defined by the recurrent relation* (3) *and by the initial condition* (4). *Let the polynomial f that is defined by* (5) *be irreducible over $\mathbf{Q}$. In order that relation* (15) *be characteristic for the sequence a_n it is necessary that one of the following conditions hold:*

(1) $k = 2$;
(2) $k = 3$ *and the polynomial f has exactly one real root;*
(3) $k = 4$ *and the polynomial f has no real roots.*

Proof. It is clear that

$$\langle 1, \lambda - b_{k-1}, \dots, \lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_2\lambda - b_1 \rangle$$

is a basis of the order $\mathbf{Z}[\lambda]$. By our definition of the polynomial F_B (see (14)) and by the corollary to Lemma 2, relation (15) holds for some integers x_0, x_1, ... , x_{k-1} if and only if the number μ,

$$\mu = x_0 + x_1(\lambda - b_{k-1}) + \dots + x_{k-1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1),$$

is invertible in $\mathbf{Z}[\lambda]$. Note that $T(\mu) = A(x_0, x_1, \dots, x_{k-1})$. In accordance with the representation (18), the solutions

$$\langle a_n, a_{n-1}, \dots, a_{n-k+1} \rangle, \qquad \langle -a_n, -a_{n-1}, \dots, -a_{n-k+1} \rangle.$$

correspond to the numbers λ^n and $-\lambda^n$, respectively. Therefore, (15) is a characteristic condition if and only if

$$(\mathbf{Z}[\lambda])^* = \{ \pm\lambda^n : n \in \mathbf{Z} \}. \tag{19}$$

Let $U(\lambda)$ be the multiplicative group of all roots of unity in $\mathbf{Z}[\lambda]$. By the Dirichlet theorem (see [1, Chap. II, §4, Theorem 5]), $G = (\mathbf{Z}[\lambda])^*/U(\lambda)$ is a free Abelian group. Moreover, if (19) holds, then the free rank of G does not exceed 1. But, by the Dirichlet theorem, this is possible only in the three cases listed above. The proof is complete.

Remark 1. If $k = 2$ and the equation $f(\lambda) = 0$ has no real roots (i.e., $\mathbf{Q}(\lambda)$ is an imaginary quadratic extension of $\mathbf{Q}$), then the group $(\mathbf{Z}[\lambda])^*$ is finite. In this case the second-order recurrence under consideration is periodic. Since the set of its values is finite, the Diophantine representation of this sequence can be easily constructed.

Remark 2. The problem on the existence of single-fold (or at least finite-fold) Diophantine representations was a reason that stimulated the statement of open question 2.3 in [12]. (For definitions, see [5, 12, Chap. 7].) Since single-fold exponential Diophantine representations are known to exist (see [11, 12]), this reduces the given problem to its partial case where we ask for single-fold (finite-fold) Diophantine representations for the exponential function. One might obtain such representations if it would be possible to find direct single-fold (finite-fold) Diophantine representations for linear recurrences of a special type. Unfortunately, for all such sequences the corresponding extensions of the field $\mathbf{Q}$ have at least two fundamental units, and by Theorem 1 the answer to open question 2.3 in [12] is negative in these cases.

In conclusion, we present without proof a complete solution of our main problem for third-order recurrences.

Theorem 2. *Let a_n be the sequence defined by* (3) *and* (4) *with* $k = 3$. *Relation* (15) *is characteristic if and only if the following two conditions are fulfilled:*

(1) $b_1^2b_2^2 + 4b_1^3 - 4b_0b_2^3 - 27b_0^2 - 18b_0b_1b_2 < 0$.

(2) *The triple* $\langle b_0, b_1, b_2 \rangle$ *is not contained on the list*

$$\begin{array}{rrrr}
\langle 1,3,2\rangle, & \langle 1,-2,-3\rangle, & \langle -1,3,-2\rangle, & \langle -1,-2,3\rangle, \\
\langle 1,5,6\rangle, & \langle 1,-6,-5\rangle, & \langle -1,5,-6\rangle, & \langle -1,-6,5\rangle, \\
\langle 1,-4,5\rangle, & \langle 1,-5,4\rangle, & \langle -1,-4,-5\rangle, & \langle -1,-5,-4\rangle, \\
\langle 1,-2,3\rangle, & \langle 1,-3,2\rangle, & \langle -1,-2,-3\rangle, & \langle -1,-3,-2\rangle, \\
\langle 1,-3,4\rangle, & \langle 1,-4,3\rangle, & \langle -1,-3,-4\rangle, & \langle -1,-4,-3\rangle, \\
\langle 1,-5,7\rangle, & \langle 1,-7,5\rangle, & \langle -1,-5,-7\rangle, & \langle -1,-7,-5\rangle, \\
\langle 1,7,12\rangle, & \langle 1,-12,-7\rangle, & \langle -1,7,-12\rangle, & \langle -1,-12,7\rangle, \\
\langle 1,2t,t^2\rangle, & \langle 1,-t^2,-2t\rangle, & \langle -1,2t,-t^2\rangle, & \langle -1,-t^2,2t\rangle,
\end{array}$$

where $t = -1$ *or* $t \geq 1$.

We observe that condition (1) in Theorem 2 means that the polynomial f has negative discriminant, i.e., f has exactly one real root (compare with condition 2 in Theorem 1). Thus, Theorem 1 yields a necessary (but not sufficient) condition for (15) to be characteristic. However, we may indicate all exceptional cases.

The proof of Theorem 2 and a complete solution of the main problem for the fourth-order recurrences will be presented in further publications.

Research described in this publication was made possible in part by Grant No. R43000 from the International Science Foundation.

Translated by M. A. Vsemirnov.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory* [in Russian], Nauka, Moscow (1972).
2. B. L. van der Waerden, *Algebra*, Springer-Verlag (1971).
3. M. Davis "An explicit diophantine definition of the exponential function," *Commun. Pure Appl. Math.*, **24**, No. 2, 137–145 (1971).
4. M. Davis, "Hilbert's tenth problem is unsolvable," *Am. Math. Monthly*, **80**, No. 3, 233–269 (1973).
5. M. Davis, Yu. V. Matiyasevich, and J. Robinson, "Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution," *Proc. Symp. Pure Math.*, **28**, 323–378 (1976).
6. P. Kiss, "On some properties of linear recurrences," *Publicationes Mathematicae (Debrecen, Hungary)*, **30**, 273–281 (1983).
7. C. Kliorys, "Fibonacci number identities from algebraic units," *Fibonacci Quart.*, **19**, 149–153 (1981).
8. N. K. Kosovskiĭ, "Diophantine representation of the sequence of solutions of the Pell equation," *Zap. Nauchn. Semin. LOMI*, **20**, 49–59 (1971).
9. Yu. V. Matiyasevich, "Enumerable sets are Diophantine," *Dokl. Akad. Nauk SSSR*, **191**, No. 2, 278–282 (1970).
10. Yu. V. Matiyasevich, "Diophantine representations of enumerable predicates," *Isv. Akad. Nauk SSSR. Ser. Mat.*, **35**, No. 1, 3–30 (1971).
11. Yu. V. Matiyasevich, "Existence of noneffectivizable estimates in the theory of exponential Diophantine equations," *Zap. Nauchn. Semin. LOMI*, **40**, 77–93 (1974).
12. Yu. V. Matiyasevich, *Hilbert's Tenth Problem* [in Russian], Nauka, Moscow (1993).
13. Yu. V. Matiyasevich and J. Robinson, "Reduction of an arbitrary diophantine equation to one in 13 unknowns," *Acta Arithm.*, **27**, 521–553 (1975).
14. G. V. Chudnovskii, "Diophantine predicates," *Usp. Mat. Nauk*, **25**, No. 4, 185–186 (1970).