Annales Univ. Sci. Budapest., Sect. Comp. 20 (2001) 195-206

GENERALIZED BINARY NUMBER SYSTEMS

A. Kovács (Budapest, Hungary)

Abstract. The object of this note is to analyse canonical radix expansions in algebraic number fields, especially using 0 and 1 as digits. We shall prove that infinitely many such binary number systems exist and we enumerate all of them up to degree 8, where degree means the degree of the defining polynomial. In general, we prove that there are infinitely many canonical number systems in each dimension even if the number of digits is "small".

1. Introduction

A *lattice* in $\mathbb{R}^k$ is the set of all integer combinations of k linearly independent vectors. Let Λ be a lattice. This can be viewed as a set of points in a Euclidean space, a $\mathbb{Z}$-module or as a finitely generated free Abelian group. Let $M : \Lambda \to \Lambda$ be a group endomorphism such that $\det(M) \neq 0$ and let D be a finite subset of Λ containing 0.

Definition. The triple (Λ, M, D) is called a *number system* (or having the unique representation property) if every element n of Λ has a unique finite representation of the form $n = \sum_{i=0}^{l} M^i a_i$, where $a_i \in D$ and l is a non-negative integer. The endomorphism M is called the *base* or *radix*, D is the *digit set*.

Clearly, both Λ and $M\Lambda$ are Abelian groups under addition. The order of the factor group $\Lambda/M\Lambda$ is $t = |\det M|$. Let A_j $(j = 1, \ldots, t)$ denote the cosets of this group. If two elements are in the same residue class A_j, then we say that they are congruent modulo M. Necessary conditions for the number system property are as follows: D must be a full residue system modulo M, all eigenvalues of M have modulus greater than one and $\det(I - M) \neq \pm 1$ (see e.g. [8]).

Let Λ be spanned by k linearly independent vectors. The following question arises naturally. For an arbitrary $M : \Lambda \to \Lambda$ satisfying the previously

The research was supported by OTKA-T031877 and Ericsson-ELTE CN Laboratory.

mentioned necessary conditions is there any digit set D for which (Λ, M, D) has the unique representation property? In many cases the answer is positive. If $\|M^{-1}\|_2 \leq 1/(1+\sqrt{k})$ then there always exists a digit set D for which (Λ, M, D) is a number system [8]. Here $\|\cdot\|_2$ means the operator norm induced by the Euclidean vector norm of $\mathbb{R}^k$.

It is well-known that a basis transformation in Λ does not change the number system property, hence, number expansions can be examined without loss of generality on the cubic lattice $\mathbb{Z}^k$. Furthermore, it was proved in [7] that for an arbitrary $z \in \Lambda$ the path $z, \Phi(z), \Phi^2(z), \ldots$ is ultimately periodic, where

$$\Phi : \Lambda \to \Lambda, \quad \Phi(z) = M^{-1}(z-d), \quad d \in D, \; z \equiv d \bmod M.$$

Via these periods a classification can be made for the points of Λ and the radix system (Λ, M, D) is a number system iff the only period is $0 \to 0$. We denote the set of periodic points by $\mathcal{P}$. If $\pi \in \mathcal{P}$ then the length of period of π is the smallest positive integer l for which $\pi = \Phi^l(\pi)$. Moreover, in [8] a CLASSIFICATION ALGORITHM was presented and it was noted that the time and space complexity of the algorithm depends strongly on the chosen basis of the lattice determined by the radix M.

Let $\Lambda = \mathbb{Z}^k$. Now, we examine special kinds of digit sets. A set of vectors $D_M^{(j)} \subset \mathbb{Z}^k$ is called *j-canonical* with respect to the matrix M $(1 \leq j \leq k)$ if all the elements have the form νe_j, where e_j denotes the j-th unit vector, $\nu = 0, \ldots, t-1$. If the set $D_M^{(j)}$ forms a complete residue system modulo M then we call it a *j-canonical digit set* and denote it by $D^{(j)}$. If there exists a j for which $(\mathbb{Z}^k, M, D^{(j)})$ is a number system then it is called *j-canonical number system*. If M is Jordan-diagonizable, i.e. it is similar to the companion matrix of a monic univariate polynomial, then 1-canonical digit sets are called simply canonical. Unfortunately, j-canonical complete residue systems do not always exist, necessary and sufficient conditions for that were given in [7]. Furthermore, 1-canonical digit sets are called simply canonical.

2. CNS-polynomials

2.1. Construction

The following construction provides an expansive M and a canonical digit set modulo M. Consider the polynomial

$$(1) \qquad f(x) = c_k x^k + c_{k-1}x^{k-1} + \ldots + c_0 = (x-\theta_1)\ldots(x-\theta_k), \; c_k = 1$$

over $\mathbb{Z}[x]$. Let us denote the quotient ring $\mathbb{Z}[x]/(f)$ by Λ_f. Let $\beta = x + (f)$ denote the image of x in Λ_f. Then Λ_f has the structure of a free Abelian group with basis $\{1, \beta, \beta^2, \ldots, \beta^{k-1}\}$. Hence, Λ_f is a lattice, addition and multiplication of lattice points is just addition and multiplication in the ring $\mathbb{Z}[x]/(f)$. To be more precise consider the polynomial $f(x)$ in (1) and assume that $|\theta_i| > 1$ $(i = 1, \ldots, k)$. where θ_i denotes the roots of $f(x)$ over $\mathbb{C}$. Observe that Λ_f is the set of elements of form $u_0 + u_1\beta + \ldots + u_{k-1}\beta^{k-1}$ $(u_j \in \mathbb{Z})$. Then Λ_f is a ring. For the addition it is isomorphic with the additive group $\mathbb{Z}^k$. Clearly, $I_\beta = \{\beta\sigma : \sigma \in \Lambda_f\}$ is an ideal in Λ_f, the number of residue classes in the factor ring Λ_f/I_β is $t = |\theta_1 \ldots \theta_k|$. Choosing an element from each residue class the digit set can be defined as $D_\beta = \{a_0 = 0, a_1, \ldots, a_{t-1}\} \subseteq \Lambda_f$. Let $\alpha \in \Lambda_f$. Then there exists a unique $a \in D_\beta$ and a unique $\alpha_1 \in \Lambda_f$ for which $\alpha = a + \beta\alpha_1$. The function $\Phi : \Lambda_f \to \Lambda_f$ is defined as $\Phi(\alpha) = \alpha_1$. Observe that the map $\alpha \to \beta\alpha$ can be formulated as a linear transformation, which has a simple form in the basis $\{1, \beta, \beta^2, \ldots, \beta^{k-1}\}$, namely the Frobenius matrix

$$M_f = \begin{pmatrix} 0 & 0 & & 0 & -c_0 \\ 1 & 0 & & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & 0 & & 1 & -c_{k-1} \end{pmatrix}. \tag{2}$$

Hence, all the problems regarding number expansions can be formulated in $\mathbb{Z}^k$ instead of making it in Λ_f. The digit set has $|(-1)^k c_0|$ elements. Since $M_f^*[k, 1] = (-1)^{k+1}$, therefore by [7, Theorem 8] the canonical digit set always exists. Here M^* means the adjoint of M, i.e. the elements are the adjoints of the appropriate sub-determinants. In the special case, when $f(x)$ is irreducible over $\mathbb{Z}[x]$ then $\Lambda_f = \mathbb{Z}[x]/(f)$ is isomorphic with $\mathbb{Z}[\theta]$, where θ is any root of $f(x)$ in an appropriate extension field of the rationals. Hence, we may replace β to θ in the above reasoning. The next lemma provides a sufficient condition for $\mathbb{Z}[x]/(f)$ being isomorphic with $\mathbb{Z}[\theta]$.

Lemma 1. *Consider the polynomial $f(x)$ in (1) and assume that $|\theta_i| > 1$ $(1 \leq i \leq k)$. If $f(0) = c_0$ is prime then $f(x)$ is irreducible.*

Proof. Suppose indirectly that $f(x) = u(x)v(x)$, $u, v \in \mathbb{Z}[x]$, $\deg(u) \geq 1, \deg(v) \geq 1$ and both u and v are monic. Since $c_0 = f(0) = u(0)v(0)$ is prime, therefore either $u(0)$ is ± 1 or $v(0)$ is ± 1. Assume that $u(0)$ is ± 1. Since the constant term of $u(x)$ is the product of some roots of f in module, this is impossible.

Consider the canonical radix system (Λ_f, M_f, D). Computing the Smith normal form of M_f by $UM_fV = G$ it is easy to see that

$$U = \begin{pmatrix} 0 & 1 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 1 \\ -\mathrm{sgn}(c_0) & 0 & 0 \end{pmatrix}$$

and $G = \mathrm{diag}(1, \ldots, 1, |c_0|)$. Hence, by [7, Theorem 4] the function Φ can be given as

$$\begin{aligned} &\Phi(\underline{x}) = \Phi([x_1, \ldots, x_k]^T) = \\ &= \left[-\frac{c_1}{c_0}x^* + x_2, -\frac{c_2}{c_0}x^* + x_3, \ldots, -\frac{c_{k-1}}{c_0}x^* + x_k, -\frac{x^*}{c_0}\right]^T, \end{aligned} \tag{3}$$

where $x^* = x_1 - d$, $0 \le d < |c_0|$ and $c_0 \mid x^*$. Using the notation $y = \lfloor x_1/c_0 \rfloor$ in (3) the function Φ can also be written as

$$\Phi(\underline{x}) = [-c_1 y + x_2, -c_2 y + x_3, \ldots, -c_{k-1}y + x_k, -y]^T. \tag{4}$$

If the system (Λ_f, M_f, D) is a canonical number system then we call the polynomial $f(x)$ as a *cns-polynomial*, or we say that the polynomial $f(x)$ has the *cns-property*. In this case for every $\underline{x} \in \mathbb{Z}^k$ there is a $j \in \mathbb{N}_0$ for which $\Phi^j(\underline{x}) = 0$.

2.2. Necessary conditions for the cns-property

Now we give some necessary conditions for constructing canonical number systems via cns-polynomials. These conditions are quite obvious, most of them were used in different research papers by W.Gilbert, I.Kátai and A.Pethő. We prove it for the sake of completeness.

Lemma 2. *If (Λ_f, M_f, D) is a canonical number system defined by the cns-polynomial (1), then*

(a) $c_0 \ge 2$;

(b) if $-1 \le r \in \mathbb{R}$ *then* $f(r) > 0$, *if* $-1 \le z \in \mathbb{Z}$ *then* $f(z) \ge 1$;

(c) $f(1) \ge c_0$;

(d) if k is even then $f(-c_0) \ge 1$, *if k is odd then* $f(-c_0) \le -1$;

(e) $\sum_{i=0}^{\lfloor k/2 \rfloor} c_{2i} \ge \lfloor (c_0 + 1)/2 \rfloor$.

Proof. (a) It is obvious that every real root of $f(x)$ (if exist) must be less then -1. Hence, $c_0 = (-1)^k\theta_1 \dots \theta_k > 1$. Concerning (b) the previous idea can also be applied. (c) It is known that the only periodic element in the number system (Λ_f, M_f, D) is the null vector. Now we analyse how can we avoid the loops $\Phi(\underline{x}) = \underline{x}$ different from $0 \to 0$. Suppose that there is a loop. Using (4) the following system of equations can be set up: $\{x_1 = x_2 - c_1 y, x_2 = x_3 - c_2 y, \dots, x_{k-1} = x_k - c_{k-1} y, x_k = -y\}$. From these equations it is easy to deduce that $x_k(1 + c_{k-1} + \dots + c_0) = d \in D$. If $x_k = 0$ then $\underline{x} = 0$ which is a known case. If $x_k \neq 0$ then applying (a) the number of loops is $\lfloor (c_0 - 1)/f(1) \rfloor$. Hence, if $c_0 \leq f(1)$ then there does not exist any loop. Concerning (d) if $\theta_i \in \mathbb{C} \setminus \mathbb{R}$ for all $0 \leq i \leq k$, then the assertion is obvious. On the other hand observe that there does not exist any real θ_i for which $\theta_i \leq -c_0$, otherwise there would be a θ_j for which $|\theta_j| < 1$. Hence $-c_0 < \theta_i < -1$ for all real roots of $f(x)$. It means that if k is even then $f(-c_0) \geq 1$, if k is odd then $f(-c_0) \leq -1$. (e) is immediately follows from (a) and (b) by $z = -1$.

Let $c_0 \geq 2$ and k be fixed. Since all roots of the polynomial $f(x)$ has moduli greater then one - we also say that the polynomial satisfies the root-condition -, therefore the number of cns-polynomials is finite. Next, we provide upper bounds for the absolute value of the coefficients $c_i, 1 \leq i \leq k-1$ in (1).

Lemma 3. *Let $f(x)$ be the cns-polynomial defined by (1) and let $2 \leq k \leq 9$. Then the coefficients of $f(x)$ can be bounded as*

$$|c_j| \leq s(1 - c_0) + c_0 \binom{k}{j} - 1,$$

$$|c_{k-j}| \leq s(c_0 - 1)(1 - \lfloor k/j \rfloor) + c_0 \binom{k}{j} - 1,$$

$$\text{where} \quad s = \left\lfloor \binom{k}{j} / \lfloor k/j \rfloor \right\rfloor, \quad 1 \leq j \leq \lfloor k/2 \rfloor.$$

Proof. We use the relationship between roots and coefficients of polynomials and the inequalities

$$\alpha + \beta < 1 + \alpha\beta \quad \text{and} \quad \frac{1}{\alpha} + \frac{1}{\beta} < 1 + \frac{1}{\alpha\beta}, \tag{5}$$

where $\alpha, \beta > 1$. For brevity let $z_i = |\theta_i|$. To have a better view into the formulas let us consider the special case $k = 7, j = 2$. Then

$$\sum_{1 \leq i_1 < i_2 \leq 7} z_{i_1} z_{i_2} <$$

$$< z_1z_2\ z_4z_5\ z_6z_7 + z_1z_3\ z_2z_5\ z_4z_7 + z_1z_4\ z_2z_6\ z_3z_7 + z_1z_5\ z_2z_4\ z_3z_6 +$$

$$+z_1z_6\ z_2z_3\ z_5z_7 + z_1z_7\ z_3z_4\ z_5z_6 + z_2z_7\ z_3z_5\ z_4z_6 + 2 \cdot 7 < 7c_0 + 14.$$

In the given range $2 \leq k \leq 9$ such a sort is always possible. Hence,

$$|c_{k-j}| = \sum_{1 \leq i_1 < \ldots < i_j \leq k} z_{i_1} \ldots z_{i_j} < sc_0 + s(\lfloor k/j \rfloor - 1) \quad \text{and}$$

$$|c_j| = c_0 \sum_{1 \leq i_1 < \ldots < i_j \leq k} \frac{1}{z_{i_1}} \ldots \frac{1}{z_{i_j}} < c_0 \left(\frac{s}{c_0} + s(\lfloor k/j \rfloor - 1) \right),$$

from which the lemma follows.

Remarks. (1) These estimates are good enough for searching canonical number systems algorithmically.

(2) By using these formulas we got the following estimations ($c_k = 1$):

$k = 2$, $|c_1| \leq c_0$;

$k = 3$, $|c_1| \leq 2c_0, |c_2| \leq c_0 + 1$;

$k = 4$, $|c_1| \leq 3c_0, |c_2| \leq 3c_0 + 2, |c_3| \leq c_0 + 2$;

$k = 5$, $|c_1| \leq 4c_0, |c_2| \leq 5c_0 + 4, |c_3| \leq 5c_0 + 4, |c_4| \leq c_0 + 3$;

$k = 6$, $|c_1| \leq 5c_0, |c_2| \leq 10c_0 + 4, |c_3| \leq 10c_0 + 9, |c_4| \leq 5c_0 + 9,$
$|c_5| \leq c_0 + 4$;

$k = 7$, $|c_1| \leq 6c_0, |c_2| \leq 14c_0 + 6, |c_3| \leq 18c_0 + 16, |c_4| \leq 18c_0 + 16,$
$|c_5| \leq 7c_0 + 13, |c_6| \leq c_0 + 5$;

$k = 8$, $|c_1| \leq 7c_0, |c_2| \leq 21c_0 + 6, |c_3| \leq 28c_0 + 27, |c_4| \leq 35c_0 + 34,$
$|c_5| \leq 28c_0 + 27, |c_6| \leq 7c_0 + 20, |c_7| \leq c_0 + 6$;

$k = 9$, $|c_1| \leq 8c_0, |c_2| \leq 27c_0 + 8, |c_3| \leq 56c_0 + 27, |c_4| \leq 63c_0 + 62,$
$|c_5| \leq 63c_0 + 62, |c_6| \leq 28c_0 + 55, |c_7| \leq 9c_0 + 26, |c_8| \leq c_0 + 7.$

2.3. Some results

The systematic research of canonical number systems in algebraic number fields was initiated by I.Kátai and J.Szabó [6]. I.Kátai published many papers with different co-authors in this area. W.Gilbert, B.Kovács and A.Pethő have also dealt with these systems. The concept of canonical number systems generated by arbitrary square-free polynomials was introduced by A.Pethő [11].

Further we mention some important results. It was observed that a wide class of polynomials can serve for constructing canonical number systems. B.Kovács [9] proved that if $f(x) \in \mathbb{Z}[x]$ is irreducible, its zeroes have moduli greater than one and if $c_k \leq c_{k-1} \leq \ldots \leq c_0$, $c_0 \geq 2$, then $f(x)$ is a cns-polynomial. His proof can be applied for reducible polynomials as well. Moreover, if c_0 is "big enough" then S.Akiyama and A.Pethő [1] gave a method determining the cns-property of arbitrary polynomials. They also proved that if $c_2, \ldots, c_{k-1}, \sum_{i=1}^{k} c_i \geq 0$ and $c_0 > 2 \sum_{i=1}^{k} |c_i|$ then $f(x)$ is a cns-polynomial and the last inequality can be replaced by $c_0 \geq 2 \sum_{i=1}^{k} |c_i|$ when all $c_i \neq 0$.

Recently, H.Brunotte [2] provided an algorithm, which attempts to prove the cns-property for a given irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$ satisfying the root-condition. His algorithm works for arbitrary monic polynomials in $\mathbb{Z}[x]$ as well. His method differs essentially from the method of S.Akiyama and A.Pethő. Instead of using power basis he chose a different one. In H.Brunotte's basis the function $\overline{\Phi} : \mathbb{Z}^k \to \mathbb{Z}^k$ has the form

$$\overline{\Phi}([x_1, \ldots, x_k]^T) = \left[-\mathrm{sgn}(c_0) \left\lfloor \frac{\sum_{j=1}^{k-1} c_j x_j + x_k}{|c_0|} \right\rfloor, x_1, \ldots, x_{k-1} \right]^T$$

His algorithm based on the following theorem. Suppose that the set $E \subseteq \mathbb{Z}^k$ has the recursive definition (i) $[0, \ldots, 0]^T, [-1, 0, \ldots, 0]^T, [0, \ldots, 0, -1]^T \in E$, (ii) for every $[x_1, \ldots, x_k]^T \in E$ and $d \in D = \{0, 1, \ldots, |c_0| - 1\}$ the element $\overline{\Phi}([x_1, \ldots, x_{k-1}, x_k + d]^T)$ belongs to E. If for every $e \in E$ there exists a $j_e \in \mathbb{N}_0$ such that $\overline{\Phi}^{j_e}(e) = 0$ then the polynomial $f(x)$ has the cns-property.

Let us see some examples. Let $k = 2$. Then by Lemma 2 and Lemma 3 we get that $-1 \leq c_1 \leq c_0$. It is easy to see that in these cases the roots of $f(x)$ are outside the complex unit disc. Using the previous algorithm of H.Brunotte it is also not hard to see that $E \subseteq \{[x_1, x_2]^T, x_1, x_2 \in \{-1, 0, 1\}\}$ and applying the function $\overline{\Phi}$ we have that the cns-property always holds. In fact, we got a kind of generalization of the result of I.Kátai, B.Kovács [4,5] and of W.Gilbert [3].

If $k = 3$ then we are only able to write a set of inequalities between the coefficients of $f(x)$ (see also [1,2]). Nevertheless, the following assertion holds.

Assertion. *The following polynomials are cns-polynomials in* $\mathbb{Z}[x]$*:*
(i) $x^k + c_1 x + c_0$ *for every* $k \geq 3$ *iff* $-1 \leq c_1 \leq c_0 - 2$, $c_0 \geq 2$,

(ii) $x^k + px^{k-1} + px^{k-2} + \ldots + px + p$ *for all* $2 \leq p \in \mathbb{N}$,
(iii) $x^k + x^{k-1} + x^{k-2} + \ldots + x + p$ *for all* $2 \leq p \in \mathbb{N}$,
(iv) $x^k + px^{k-1} + p^2x^{k-2} + \ldots + p^{k-1}x + p^k$ *for all* $2 \leq p \in \mathbb{N}$.

Proof. The case (i) was proved in [2]. In order to check that the roots of the polynomials (ii) and (iii) are outside the complex unit disc one can use the method of Lehmer-Schur [10]. The proof is easy, we leave it to the reader. It is also obvious that the moduli of the roots of polynomial (iv) are equal and greater than one. Since the coefficients of the polynomials (ii)-(iv) are positive and monotonically increasing, the theorem of B.Kovács can be applied. The proof is finished.

Remarks. (1) We proved that there are infinitely many cns-polynomials (therefore canonical number systems) in each dimension k even if the constant term of the polynomial is "small".

(2) The polynomials (iv) and (i) for $c_1 = 0$ show that for every $e > 1$ there is a base M such that (Λ, M, D) is a canonical number system and the moduli of each eigenvalues of M are smaller than or equal to e. This shows that the second necessary condition mentioned in the first section for satisfying the unique representation property is sharp.

2.4. Searching for cns-polynomials

Now we provide an algorithm for searching canonical number systems by computer. To decide whether the polynomial $f(x)$ has a root inside the complex unit disc the method of Lehmer-Schur can be used. To analyse the possible roots in the unit circle we have the following well-known lemma.

Lemma 4. *Let* $Q(x) = q_0 + q_1x + \ldots + q_kx^k \in \mathbb{Z}[x], Q(\gamma_i) = 0, |\gamma_i| \geq 1$. *Then* $|\gamma_i| > 1$ *if and only if* $\gcd(Q(x), x^kQ(1/x))$ *is a constant polynomial.*

Algorithm: CNS-Sieve. Searching candidates for cns-polynomials. The inputs are the constant term c_0 and the degree k of the monic polynomial $f(x) \in \mathbb{Z}[x]$.

1. Let S be the finite set of polynomials determined by Lemma 3;
2. **if** $S \neq \emptyset$ **then** p :=get-a-new-candidate(S); $S := S \setminus \{p\}$;
   else goto step 5;
3. **if** Lemma 2 (e), (b) with $z = -1$, (c) and (d) hold for the polynomial p **then goto** step 4; **else goto** step 2;
4. Apply Lehmer-Schur and Lemma 4 for the polynomial p;
   if all roots of p have moduli greater than one **then print**(p);
   goto step 2;
5. STOP;

The algorithm terminates since S is a finite set. Observe that the CNS-SIEVE algorithm contains computationally easy-to-check methods. Moreover, if Lemma 2 fails for the polynomial p then possibly more than one polynomials can be deleted from the set S, depending on which part of Lemma 2 does not hold. Clearly, the CNS-SIEVE algorithm can also be applied for $k > 9$ but in this case bounds for the coefficients of $f(x)$ must be determined.

2.5. CNS-polynomials with constant term $c_0 = 2$

Now we turn our attention to generalized binary number expansions, i.e. $c_0 = 2$. The case $k = 1$ is well-known, and the case $k = 2$ was analyzed in Section 2.3. Let $k \geq 3$. Suppose that the polynomial $f(x)$ is obtained by the CNS-SIEVE ALGORITHM for some k. Then, a periodic element $0 \neq \pi \in \mathcal{P}$ would be a test proving that $f(x)$ is not a cns-polynomial. If one does not find such a π by searching a small finite portion of the space systematically or randomly then one can use the CLASSIFICATION ALGORITHM [8] or H.Brunotte's algorithm [2] to prove that $f(x)$ is really a cns-polynomial. If $f(x)$ is not a cns-polynomial then these algorithms serve also the test.

The author implemented the CNS-SIEVE ALGORITHM in C language. The following table shows the results up to degree 8.

Degree (k)	Output of CNS-SIEVE ALGORITHM (number of polynomials)	Number of cns-polynomials
3	5	4
4	22	12
5	18	7
6	73	25
7	62	12
8	215	20

Table 1.

Further, we enumerate the computed cns-polynomials. $k = 3$, $2 - x + x^3, 2 + x^3, 2 + x + x^2 + x^3, 2 + 2x + 2x^2 + x^3$.

$k = 4$, $2 - x + x^4, 2 + x^4, 2 - x^2 + x^4, 2 + x^2 + x^4, 2 + 2x^2 + x^4, 2 + x + x^3 + x^4, 2 + x + x^2 + x^3 + x^4, 2 + 2x + x^2 + x^3 + x^4, 2 + x + 2x^2 + x^3 + x^4, 2 + 2x + 2x^2 + x^3 + x^4, 2 + 2x + 2x^2 + 2x^3 + x^4, 2 + 3x + 3x^2 + 2x^3 + x^4$.

$k = 5$, $2 - x + x^5, 2 + x^5, 2 - x + x^2 + x^5, 2 + x^2 + x^3 + x^5, 2 + x + x^4 + x^5, 2 + x + x^2 + x^3 + x^4 + x^5, 2 + 2x + 2x^2 + 2x^3 + 2x^4 + x^5$.

$k = 6$, $2-x+x^6, 2-x^2+x^6, 2-x^3+x^6, 2+x^6, 2+x^3+x^6, 2+2x^3+x^6, 2+x^2-x^3+x^4+x^6, 2+x^2+x^4+x^6, 2+x^2+x^3+x^4+x^6, 2+2x^2+2x^4+x^6, 2+x-x^2-x^3+x^5+x^6, 2+x-x^3+x^5+x^6, 2+x+x^5+x^6, 2+x+x^2+x^3+x^4+x^5+x^6, 2+2x+x^2+x^3+x^4+x^5+x^6, 2+2x+2x^2+x^3+x^4+x^5+x^6, 2+x+x^2+2x^3+x^4+x^5+x^6, 2+2x+2x^2+2x^3+x^4+x^5+x^6, 2+x+2x^2+x^3+2x^4+x^5+x^6, 2+2x+2x^2+2x^3+2x^4+x^5+x^6, 2+2x+3x^2+2x^3+2x^4+x^5+x^6, 2+2x+2x^2+2x^3+2x^4+2x^5+x^6, 2+3x+3x^2+3x^3+3x^4+2x^5+x^6, 2+3x+4x^2+4x^3+3x^4+2x^5+x^6, 2+x+x^2+x^4+x^5+x^6$.

$k = 7$, $2 - x + x^7, 2 - 2x + 2x^2 - x^3 + x^5 - x^6 + x^7, 2 - x + x^2 + x^4 + x^7, 2 + x^3 + x^4 + x^7, 2 + x^2 + x^5 + x^7, 2 + x + x^6 + x^7, 2 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7, 2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6 + x^7, 2 + 2x + 2x^2 + 2x^3 + 2x^4 + x^5 + x^6 + x^7, 2 + 2x + 2x^2 + 2x^3 + 2x^4 + 2x^5 + 2x^6 + x^7, 2 + 3x + 4x^2 + 4x^3 + 4x^4 + 3x^5 + 2x^6 + x^7$.

$k = 8$, $2-x+x^8, 2-x^2+x^8, 2-x^4+x^8, 2+x^8, 2+x^4+x^8, 2+2x^4+x^8, 2+x^3+x^5+x^8, 2+x^2+x^6+x^8, 2+x^2+x^4+x^6+x^8, 2+2x^2+x^4+x^6+x^8, 2+x^2+2x^4+x^6+x^8, 2+2x^2+2x^4+x^6+x^8, 2+2x^2+x^3+x^4+x^5+x^6+x^8, 2+2x^2+2x^4+2x^6+x^8, 2+3x^2+3x^4+2x^6+x^8, 2+x+x^7+x^8, 2+x+x^2+x^4+x^6+x^7+x^8, 2+x+x^2+x^3+x^5+x^6+x^7+x^8, 2+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8, 2+2x+x^2+x^3+x^4+x^5+x^6+x^7+x^8, 2+2x+2x^2+2x^3+x^4+x^5+x^6+x^7+x^8, 2+2x+2x^2+2x^3+2x^4+x^5+x^6+x^7+x^8, 2+2x+2x^2+2x^3+2x^4+2x^5+2x^6+x^7+x^8, 2+2x+2x^2+2x^3+2x^4+2x^5+2x^6+2x^7+x^8, 2+x+x^2+x^3+2x^4+x^5+x^6+x^7+x^8, 2+x+2x^2+x^3+2x^4+x^5+2x^6+x^7+x^8, 2+x+3x^2+2x^3+3x^4+2x^5+2x^6+x^7+x^8, 2+2x+3x^2+3x^3+3x^4+2x^5+2x^6+x^7+x^8, 2+3x+3x^2+3x^3+3x^4+3x^5+3x^6+2x^7+x^8, 2+3x+4x^2+5x^3+5x^4+4x^5+3x^6+2x^7+x^8, 2+4x+5x^2+5x^3+5x^4+4x^5+3x^6+2x^7+x^8$.

The output of the CNS-SIEVE ALGORITHM shows that the estimates in Lemma 2 and Lemma 3 may be complemented and improved. It is also clear that the time complexity of the algorithm is exponential in k. Moreover, in higher dimensions proving that a given polynomial obtained by the CNS-SIEVE ALGORITHM is really a cns-polynomial is hard. The following conjecture would help, but the author was unable to prove this.

Conjecture. *Suppose that the lattice Λ is generated with the power basis and the polynomial $f(x)$ is obtained by the CNS-SIEVE ALGORITHM. If there does not exist any periodic element π for which $\|\pi\|_\infty = 1$ then $f(x)$ is a cns-polynomial.*

Obviously, if such a π exists then the polynomial is not a cns-polynomial. We used this idea to test the output of the CNS-SIEVE ALGORITHM.

Remarks. (1) The case $k = 3$ in Table 1 was known to A. Járai (unpublished).

(2) Suppose that the polynomial $f(x)$ is obtained by the CNS-SIEVE ALGORITHM and it is not a cns-polynomial. Then, the CLASSIFICATION ALGORITHM provides more than one periods. The following questions are quite interesting: how many such periods exist and what are the length of them? The general characterization seems to be hard. The following table shows some computational results.

the polynomial $f(x)$	$\pi \in \mathcal{P}$ $\|\pi\|_\infty = 1$	the length of period of π
$2+x+x^2+x^4$	$[-1,1,0,0]^T$	11
$2+x+2x^2+2x^3+x^4+x^5$	$[-1,-1,-1,0,0]^T$	21
$2+x+x^3+x^4+x^5+x^6$	$[-1,-1,-1,0,0,0]^T$	33
$2+x+2x^3+2x^4+x^6+x^7$	$[-1,-1,1,-1,0,1,0]^T$	47
$2+2x+x^2+x^6+2x^7+x^8$	$[-1,-1,0,0,0,0,0,0]^T$	64

Table 2.

(3) In order to decide the cns-property of a given polynomial the algorithm of H.Brunotte is preferable. The author is grateful to J.Sziliczi who programmed this algorithm in C++ in a very fine way. This shows among others that for the cns-polynomial $2+x+2x^2+x^3+2x^4+x^5+2x^6+x^7+x^8$ the algorithm uses 344 iteration steps, the number of integer vectors in the set E is 143123, while for the cns-polynomial $2+3x+3x^2+3x^3+3x^4+3x^5+3x^6+2x^7+x^8$ the algorithm uses 253 iteration steps and number of integer vectors in the set E is 241719.

References

[1] **Akiyama S. and Pethő A.,** *On canonical number systems*, preprint, 1999, 1-12.

[2] **Brunotte H.,** *On trinomial bases of radix representation of algebraic integers*, preprint, 2000, 1-9.

[3] **Gilbert W.J.,** Radix representation of quadratic fields, *J.Math. Anal. Appl.*, **83** (1991), 264-274.

[4] **Kátai I. and Kovács B.,** Kanonische Zahlensysteme bei reelen quadratischen algebraischen Zahlen, *Acta Sci. Math.*, **42** (1980), 99-107.

[5] **Kátai I. and Kovács B.,** Canonical number systems in imaginary quadratic fields, *Acta Math. Hung.*, **37** (1981), 159-164.

[6] **Kátai I. and Szabó J.,** Canonical number systems for complex integers, *Acta Sci. Math.*, **37** (1975), 255-260.

[7] **Kovács A.,** On computation of attractors for invertible expanding linear operators in $\mathbb{Z}^k$, *Proc. Numbers, Functions, Equations'98, Noszvaj, Hungary, Leaflets in Mathematics,* Janus Pannonius Univ., Pécs, 1998, 108-109, *Publ. Math. Debrecen,* **56** (1-2) (2000), 97-120.

[8] **Kovács A.,** On number expansion in lattices, *Proc. 5th Int. Conf. on Applied Informatics, Eger, Hungary, 2001.* (submitted)

[9] **Kovács B.,** Canonical number systems in algebraic number fields, *Acta Math. Acad. Sci. Hung.*, **37** (4) (1981), 405-407.

[10] **Lehmer D.H.,** A machine method for solving polynomial equations, *J. ACM,* **2** (1961), 151-162.

[11] **Pethő A.,** On a polynomial transformation and its application to the construction of a public key cryptosystem, *Proc. Computational Number Theory,* Walter de Gruyter Publ. Co., 1991, 31-44.

(Received March 22, 2001)

A. Kovács
Department of Computer Algebra
Eötvös Loránd University
H-1518 Budapest, P.O.B. 32.
attila@compalg.inf.elte.hu