Publ. Math. Debrecen
87/1-2 (2015), 111–131
DOI: 10.5486/PMD.2015.7063

Divisiblity of certain standard multinomials by CNS factors of small degree

By HORST BRUNOTTE (Düsseldorf)

Abstract. In this article we study reducibility questions of integer polynomials whose constant terms exceed 1 and whose other coefficients are 0 or 1. Specifically, it is shown that infinitely many CNS polynomials of this type are divisible by linear or quadratic CNS polynomials.

1. Introduction

Some decades ago the systematic study of canonical number systems (CNS) as generalizations of our ordinary decimal number system has been initiated by the Hungarian school (see [24], [22], [23], [26]). Detailed background information on historical developments and relations to other areas such as shift radix systems, finite automata or fractal tilings can be found in the works by Kátai [21], Barat *et al.* [5], Berthé [6] and by Kirschenhofer and Thuswaldner [25].

The general notion of canonical number systems and the concept of CNS polynomials[1] were introduced by Pethő [31]. Let us briefly recall the definition and basic properties of CNS polynomials. The monic polynomial $f \in \mathbb{Z}[X]$ with non-vanishing constant term is called a CNS polynomial if for every $A \in \mathbb{Z}[X]$ there exists a polynomial $B \in \{0, \dots, |f(0)| - 1\}[X]$ such that $A \equiv B \pmod{f}$. Among other things, it is known (see [30] and [3, Section 1]) that the roots of CNS polynomials lie outside the closed unit disk and are non-positive. The structure of CNS polynomials of degree at most two is well-known: A monic linear integer

Mathematics Subject Classification: 11R09, 12Y05, 11C08, 12E10, 11A63.
Key words and phrases: trinomial, multinomial, factorization, canonical number system, reducibility.

[1] CNS polynomials are named complete base polynomials in [12].

polynomial is a CNS polynomial if and only if its constant term is at least 2 ([16], [1, Remark 4.5]), and $X^2 + bX + c \in \mathbb{Z}[X]$ is a CNS polynomial if and only if $-1 \leq b \leq c$ and $c \geq 2$ ([22], [23], [15], [10], [37], [4]). Furthermore, the CNS property of a given polynomial can algorithmically be decided [36], [7], [12], however, the characterization of CNS polynomials of degree larger than 2 has remained an open problem.

In view of this situation various aspects of product decomposition of CNS polynomials have found some interest in recent years (e.g., see Akiyama *et al.* [2], Pethő [32], Kane [20], Chen [12] and van de Woestijne [39]). Our motivation here is to treat a class of easily accessible, but interesting polynomials in which we study multiples of given CNS polynomials and factorizations of CNS polynomials.

Recall that a standard r-nomial is a univariate polynomial of the form

$$\sum_{i=1}^{r} a_i X^{n_i} \quad (n_r > \cdots > n_2 > n_1 = 0 \text{ and } a_r = 1)$$

where the coefficients belong to a field of characteristic zero; this notion was coined and discussed by Győry and Schinzel [17]. Reducibility and factorization questions of standard multinomials have found a broad interest for a long time, in particular, r-nomials of the form

$$p_{r,n,a} := \sum_{i=2}^{r} X^{n_i} + a \in \mathbb{Z}[X] \quad (n \in N_r,\ a \in \mathbb{Z}),$$

where we use the set

$$N_r := \left\{(n_r, \ldots, n_2) \in \mathbb{N}^{r-1} : n_r > \cdots > n_2 > 0\right\}$$

and denote by $\mathbb{N}$ the set of nonnegative rational integers. Properties of polynomials of this type have extensively been investigated: For instance, the trinomials $p_{3,n,\pm 1}$ by Selmer [33], Ljunggren [27], Tverberg [38] and $p_{3,n,\pm 4}$ by Jonassen [19], the quadrinomials $p_{4,n,\pm 1}$ by Ljunggren [27] and Mills [28] and $p_{4,n,a}$ by Bremner and Ulas [9], and the Newman polynomials $p_{r,n,1}$ by Odlyzko and Poonen [29], Borwein and Mossinghoff [8], Dubickas [13], Dubickas and Jankauskas [14] and van de Woestijne [40].

In this article we exhibit infinitely many irreducible CNS polynomials in the set

$$\mathcal{P}_r := \{p_{r,n,a} \in \mathbb{Z}[X] : n \in N_r,\ a \in \mathbb{Z}\}$$

and study the divisibility of CNS multinomials in $\mathcal{P}_r$ by linear or quadratic CNS polynomials. It turns out that for a given $r \geq 3$ every linear CNS polynomial divides infinitely many CNS multinomials in $\mathcal{P}_r$, and that irreducible quadratic CNS polynomials q with non-vanishing linear term divide infinitely many CNS trinomials in $\mathcal{P}_3$ provided that the quotient of the roots of q is a root of unity. Further, we characterize irreducible quadratic CNS polynomials with non-vanishing linear term which divide infinitely many CNS polynomials $p_{r,n,a}$ such that the exponents $n_r, \dots, n_2$ do not have a non-trivial common factor. We comment on the CNS property of the quotient of these CNS multinomials and their linear (quadratic, respectively) CNS divisors and include several numerical examples. Our method is based on ideas of the work of Bremner and Ulas cited above.

2. Linear divisors of CNS polynomials in the set $\mathcal{P}_r$

This section is devoted to the study of linear CNS divisors of CNS polynomials in $\mathcal{P}_r$. For the sake of completeness we explicitly present infinitely many (irreducible) CNS polynomials among the polynomials of fixed degree in $\mathcal{P}_r$. Then we construct infinitely many CNS polynomials in $\mathcal{P}_r$ which are divisible by a given linear CNS polynomial. To prepare these results we first recall two fundamental statements on CNS polynomials which shall frequently be applied in the sequel; for convenience we denote the set of CNS polynomials by $\mathcal{C}$.

Theorem 2.1. *Let $p \in \mathbb{Z}[X]$ be monic.*

(i) *If all coefficients of p are nonnegative, $p(0) > 1$ and $p(1) < 2p(0)$ then $p \in \mathcal{C}$.*

(ii) *If $p \in \mathcal{C}$ then $p(0) \leq p(1)$.*

Proof. (i) [4, Theorem 3.2] or [20, Theorem 11].

(ii) [3, Lemma 2]. □

An immediate application of the first part of this theorem allows us to present infinitely many irreducible CNS polynomials in $\mathcal{P}_r$.

Proposition 2.2. *Let $r \geq 2$, $n \in N_r$ and $a \in \mathbb{Z}$ such that $a \geq r$. Then $p_{r,n,a}$ is a CNS polynomial. Moreover, if a is prime then $p_{r,n,a}$ is irreducible.*

Proof. Setting $p := p_{r,n,a}$ and observing

$$2p(0) = 2a > r - 1 + a = p(1)$$

our first assertion is a direct consequence of Theorem 2.1 (i).

Now, let us assume that a is prime and that there exist monic polynomials $g, h \in \mathbb{Z}[X]$ such that $p = gh$ and $\deg(g)$, $\deg(h) < \deg(p)$. W.l.o.g. we may suppose $g(0) = \pm a$, hence $h(0) = \pm 1$. Therefore not all roots of h are larger than 1 in modulus, i.e., there exists a root ζ of h such that $|\zeta| \leq 1$. But then we find $p(\zeta) = 0$, i.e., p admits a root inside the closed unit disk which is impossible (see Section 1). □

From now on we turn our interest to reducible CNS polynomials $p \in \mathcal{P}_r$ which admit prescribed linear or quadratic factors g, and we describe some properties of the quotient p/g. To this end we recall the definition

$$\gamma(f) = \inf \{\deg(g) : g \in \mathbb{Z}[X],\ gf \in \mathcal{C}\}$$

for monic polynomials $f \in \mathbb{Z}[X]$; obviously, $\gamma(f) = 0$ means $f \in \mathcal{C}$. This quantity may be regarded as a measure of the distance of f to $\mathcal{C}$; for more details the reader is referred to [11, Section 3]. The following simple lower bound for $\gamma(f)$ turns out to be useful for our purposes here.

Lemma 2.3. *Let $k \in \{1, 2\}$ and $f \in \mathbb{Z}[X]$ be a monic polynomial such that*

$$f(0) > \left(2 - \frac{1}{k}\right) f(1).$$

Then we have $\gamma(f) \geq k$.

Proof. If $f(1) \leq 0$ then f has a real nonnegative root. Hence, by what we have seen in Section 1 f cannot be a factor of a CNS polynomial, thus $\gamma(f) = \infty$, and our assertion is trivially true.

Therefore we now assume $f(1) > 0$ and $\gamma(f) < k$. First we observe that $\gamma(f) > 0$: Indeed, suppose $\gamma(f) = 0$. Then f is a CNS polynomial, and Theorem 2.1 (ii) and our prerequisites yield

$$f(1) \geq f(0) > \left(2 - \frac{1}{k}\right) f(1),$$

hence $1 > 2 - (1/k)$ which is absurd.

Thus $\gamma(f) \geq 1$ and the case $k = 1$ is done. Now we assume $k = 2$ and $\gamma(f) < 2$, thus $\gamma(f) = 1$. Then there exists an integer $c \geq 2$ such that $(X + c) \cdot f \in \mathcal{C}$. We infer

$$(1 + c)f(1) \geq cf(0)$$

from Theorem 2.1 (ii), hence

$$f(1) \geq \frac{c}{c+1} \cdot f(0) > \frac{3c}{2(c+1)} f(1).$$

But then we have contradiction $2 > c$. □

Remark 2.4. We remark in passing that Lemma 2.3 does not hold for $k = 3$: For

$f := X^{13} - X^{12} + 2X^{10} - 4X^9 + 4X^8 - 8X^6 + 16X^5 - 16X^4 + 32X^2 - 64X + 64$

we have

$$(X^2 + 2X + 2) \cdot f = X^{15} + X^{14} + 128 \in \mathcal{C}$$

by Theorem 2.1 (i), hence $\gamma(f) \leq 2$, but

$$f(0) = 2^6 > \frac{2(2^6+1)}{3} = \frac{5}{3} \cdot \frac{2+2^7}{5} = \left(2 - \frac{1}{3}\right) f(1).$$

Lemma 2.3 allows the following simple determination of γ-values which will frequently be applied in the sequel.

Corollary 2.5. *Let $f \in \mathbb{Z}[X]$.*

(i) *If $f(0) > f(1)$ and $(X + c) \cdot f \in \mathcal{C}$ for some $c \in \mathbb{N}$ then we have $\gamma(f) = 1$.*

(ii) *If $f(0) > (3/2)f(1)$ and $(X^2 + bX + c) \cdot f \in \mathcal{C}$ for some $b, c \in \mathbb{Z}$ then we have $\gamma(f) = 2$.*

Proof. (i) The second condition and the definition of $\gamma(f)$ yield $\gamma(f) \leq 1$, and by Lemma 2.3 we know $\gamma(f) \geq 1$. Thus we conclude $\gamma(f) = 1$.

(ii) Analogously as the proof of (i). □

We reformulate a remark of [9, Introduction] as the first statement of Theorem 2.6 below where we give a criterion for the divisibility of a element in $\mathcal{P}_r$ by a monic linear polynomial. In the second part we present our main statement on the divisibility of certain CNS multinomials by linear CNS polynomials.

Theorem 2.6. *Let $r \geq 2$, $n \in N_r$ and $a, c \in \mathbb{Z}$.*

(i) *$X + c$ divides $p_{r,n,a}$ if and only if*

$$a = \sum_{i=2}^{r} (-1)^{n_i - 1} c^{n_i}. \qquad (1)$$

(ii) *Let $c \geq 2$, n_r be odd and a be given by (1). Then $p_{r,n,a}$ is a CNS polynomial and we have $\gamma(p_{r,n,a}/(X + c)) \leq 1$. Moreover, if $a > (r-1)c$ then we have $\gamma(p_{r,n,a}/(X + c)) = 1$.*

Proof. Set $p := p_{r,n,a}$.

(i) This is clear by

$$p(-c) = 0 \iff p_{r,n,a}(-c) = 0 \iff a = -\sum_{i=2}^{r} (-1)^{n_i} c^{n_i} = \sum_{i=2}^{r} (-1)^{n_i - 1} c^{n_i}.$$

(ii) The proof is accomplished in three steps. First, we show

$$a \geq r. \tag{2}$$

Indeed, this is trivial for $r = 2$, and for $r > 2$ we set $n_r = 2m + 1$ and show

$$\sum_{i=2}^{r-1} (-1)^{n_i - 1} c^{n_i} \geq -\sum_{i=1}^{m} c^{2i}$$

by induction on r. Then we deduce

$$\begin{aligned} a &= c^{2m+1} + \sum_{i=2}^{r-1} (-1)^{n_i-1} c^{n_i} \geq c^{2m+1} - \sum_{i=1}^{m} c^{2i} \geq c^{2m+1} - (c^{2m} + c^{2m-1} - 2) \\ &= c^{2m-1}(c^2 - c - 1) + 2 \geq c^{2m-1} + 2 \geq 2m + 2 \geq r. \end{aligned}$$

Second, we infer from Proposition 2.2 and (2) that p is indeed a CNS polynomial. For the quotient $g := p/(X + c)$ we thus have $\gamma(g) \leq 1$ since

$$(X + c) \cdot g = p \in \mathcal{C}.$$

Third, in view of what we have just seen the assumption $a > (r - 1)c$ and Lemma 2.3 imply $\gamma(g) = 1$ since we have

$$g(0) = \frac{a}{c} > \frac{r - 1 + a}{1 + c} = g(1) \qquad \square.$$

The following examples illustrate the situation described in Theorem 2.6 (ii). We tacitly use the characterization of linear and quadratic CNS polynomials cited in Section 1.

Example 2.7. (i) Let $m \geq 3$ be odd, $c \geq 2$ and g be the quotient of the two CNS polynomials $X^m + c^m$ and $X + c$ (for the CNS property of the first polynomial see [10, Theorem 1]). Since $c^m > c$ we have $\gamma(g) = 1$.

(ii) For

$$g := \frac{p_{3,(3,2),4}}{X + 2} = \frac{X^3 + X^2 + 4}{X + 2} = X^2 - X + 2$$

we have $\gamma(g) = 0$.

Remark 2.8. If $c \neq 0$ then (1) is equivalent to

$$\frac{a}{c^{n_2}} = \sum_{i=2}^{r} (-1)^{n_i - 1} c^{n_i - n_2},$$

and this equation can be regarded as the representation of the positive integer $a/(c^{n_2})$ in base c with digit set $\{-1, 0, 1\}$.

According to Jankauskas [18] we say that a polynomial f is primitive if it is not of the form $g(X^k)$ for some $k > 1$. Note that the primitivity of a polynomial is equivalent to the fact that the greatest common divisor of the exponents of X whose coefficients do not vanish equals 1.

Theorem 2.9. *If $r \geq 3$ then every linear CNS polynomial ℓ divides infinitely many primitive CNS polynomials $p \in \mathcal{P}_r$ such that $\gamma(p/\ell) = 1$.*

Proof. Let $\ell := X + c$ be a CNS polynomial, hence $c \geq 2$ (see Section 1). Pick $k \geq \max\{2,\ r-2\}$, let n_r be the odd element of the set $\{k+r-1,\ k+r\}$, and define $n_i := k+i-1$ $(1 < i < r)$ and a by (1). Then we observe

$$\begin{aligned} a \geq c^{k+r-1} - \sum_{i=2}^{r-1} c^{k+i-1} &= c^{k+1}\left(c^{r-2} - \sum_{j=0}^{r-3} c^j\right) \\ &\geq c^{r-1}\left(c^{r-2} - \frac{c^{r-2}-1}{c-1}\right) \geq c^{r-1}. \end{aligned} \tag{3}$$

We convince ourselves that $a > (r-1)c$: By our choice of k this is clear for $r = 3$, and then we proceed by induction exploiting (3).

In particular, we have shown $a \geq c$, hence $p := p_{r,n,a}$ is a CNS polynomial by Proposition 2.2. We infer from Theorem 2.6 that ℓ divides p and $\gamma(p/\ell) = 1$. □

Remark 2.10. Note that we must have $r > 2$ in Theorem 2.9 since a binomial in $\mathcal{P}_2$ which is divisible by the linear polynomial ℓ is either not primitive or equals ℓ.

3. Quadratic divisors of CNS polynomials in the set $\mathcal{P}_r$

In this section we study CNS polynomials $p \in \mathcal{P}_r$ with given quadratic factor q, and analogously as in Section 2 we treat the quotient p/q. We start with an elementary criterion for the divisibility of a polynomial in $\mathcal{P}_r$ by q (Theorem 3.1) and we consider the case $r = 3$ in more detail (Proposition 3.7). Then we concentrate on CNS divisors q. Again trinomials deserve special attention (Proposition 3.9), and we conclude by our main results on non-primitive or reducible q (Theorem 3.13) and primitive irreducible q (Theorem 3.13).

A straightforward extension of [9, Corollary 3.2] yields a criterion for the divisibility of an element of $\mathcal{P}_r$ by a monic quadratic polynomial.

Theorem 3.1. *Let $r \geq 3$, $n \in N_r$, $a, b, c \in \mathbb{Z}$ and $q = X^2 + bX + c$. Define* *a sequence of integers* $(a_k)_{k\in\mathbb{N}}$ *by*

$$a_0 = 0, \quad a_1 = 1, \quad a_k = -ba_{k-1} - ca_{k-2} \quad (k \geq 2).$$

Then q *divides* $p_{r,n,a}$ *if and only if*

$$\sum_{k=2}^{r} a_{n_k} = 0 \quad \text{and} \quad a = c\sum_{k=2}^{r} a_{n_k-1}. \tag{4}$$

In this case, we have

$$\frac{p_{r,n,a}}{q} = \sum_{k=2}^{r} g_{n_k}$$

where the sequence of integer polynomials $(g_k)_{k\in\mathbb{N}}$ *is defined by*

$$g_0 = g_1 = 0, \quad X^k = qg_k + a_kX - ca_{k-1} \quad (k \geq 2). \tag{5}$$

Proof. Set

$$b_0 = 1, \quad b_k = -ca_{k-1} \quad (k \geq 1)$$

and let us first assume that q divides $p_{r,n,a}$. In view of

$$\sum_{k=2}^{r} X^{n_k} + a \equiv 0 \pmod q$$

we infer

$$\left(\sum_{k=2}^{r} a_{n_k}\right)X + \left(\sum_{k=2}^{r} b_{n_k}\right) + a \equiv 0 \pmod q$$

from Lemma 3.3. Therefore, we have

$$\sum_{k=2}^{r} a_{n_k} = 0 \quad \text{and} \quad a = -\sum_{k=2}^{r} b_{n_k} = c\sum_{k=2}^{r} a_{n_k-1}. \tag{6}$$

Now we suppose that (4) holds. By definition of the sequences (a_k) and (b_k) there are polynomials $g_k \in \mathbb{Z}[X]$ which satisfy (5). Summing up and using (6) we obtain

$$\begin{aligned}\sum_{k=2}^{r} X^{n_k} + a &= q\sum_{k=2}^{r} g_{n_k} + \left(\sum_{k=2}^{r} a_{n_k}\right)X + \sum_{k=2}^{r} b_{n_k} + a\\ &= q\sum_{k=2}^{r} g_{n_k} - a + a = q\sum_{k=2}^{r} g_{n_k}.\end{aligned}$$

□

Remark 3.2. Using the same method as in the proof of Theorem 3.1 we can easily convince ourselves that a monic quadratic integer polynomial with non-vanishing constant term cannot divide any standard binomial with non-vanishing constant term.

To prepare our main results we now study the divisibility of multinomials by certain quadratic integer polynomials. Our investigation is based on results by Bremner and Ulas [9] which we briefly recall. Fix $b, c \in \mathbb{Z}$ and define integers $A_k(b,c)$ and $B_k(b,c)$ by

$$X^k \equiv A_k(b,c)\,X + B_k(b,c) \pmod{X^2 + bX + c} \quad (k \in \mathbb{N}).$$

Lemma 3.3 ([9, Lemma 3.1, Remark 6.3])**.** *We have*

$$A_0(b,c) = 0, \quad A_1(b,c) = B_0(b,c) = 1,$$

and for $k \geq 1$ the following equations hold:

(i) $A_{k+1}(b,c) = -bA_k(b,c) - cA_{k-1}(b,c)$,

(ii) $B_k(b,c) = -cA_{k-1}(b,c)$,

(iii) $A_k(bt, ct^2) = t^{k-1}A_k(b,c)$ $(t \in \mathbb{Z})$.

Lemma 3.4. *For $n \in \mathbb{N}$ we have:*

(i) $A_{3n}(1,1) = 0$, $A_{3n+1}(1,1) = 1$, $A_{3n+2}(1,1) = -1$,

(ii) $A_{n+1}(2,1) = (-1)^n(n+1)$,

(iii) $A_{4n}(2,2) = 0$, $A_{4n+1}(2,2) = (-1)^n 2^{2n}$, $A_{4n+2}(2,2) = -A_{4n+3}(2,2) = (-1)^{n+1}2^{2n+1}$,

(iv) $A_{6n}(3,3) = 0$, $A_{6n+1}(3,3) = (-1)^n 3^{3n}$, $A_{6n+2}(3,3) = (-1)^{n+1}3^{3n+1}$, $A_{6n+3}(3,3) = 2(-1)^n 3^{3n+1}$, $A_{6n+4}(3,3) = (-1)^{n+1}3^{3n+2}$, $A_{6n+5}(3,3) = (-1)^n 3^{3n+2}$,

(v) $A_{2n}(0,c) = 0$, $A_{2n+1}(0,c) = (-c)^n$ $(c \in \mathbb{Z})$.

Proof. (i), (ii), (v) Using induction these facts can easily be checked by Lemma 3.3.

(iii), (iv) See [9, Lemma 6.1]. □

The following elementary fact concerns the sequences introduced above and is a basic tool in our subsequent considerations.

Lemma 3.5. *Let $r > 1$, $n_r > \cdots > n_1 > 0$, and $b \in \{2,3\}$. For $n \in \mathbb{N}$ we set*

$$a_b(n) := e_b(n)\, b^{\lfloor n/2 \rfloor}$$

if $2b$ does not divide n, and $a_b(n) = 0$, otherwise; here we use the notation

$$e_2(n) := \begin{cases} (-1)^{\lfloor n/4 \rfloor} & (n \equiv 1,3 \pmod 4), \\ (-1)^{\lfloor n/4 \rfloor + 1} & (n \equiv 2 \pmod 4), \end{cases}$$

and

$$e_3(n) := \begin{cases} (-1)^{\lfloor n/6 \rfloor} & (n \equiv 1,5 \pmod 6), \\ (-1)^{\lfloor n/6 \rfloor + 1} & (n \equiv 2,4 \pmod 6), \\ 2 \cdot (-1)^{\lfloor n/6 \rfloor} & (n \equiv 3 \pmod 6). \end{cases}$$

Let $t \in \mathbb{Z} \setminus \{0\}$ and

$$\sum_{i=1}^{r} t^{n_i - 1} a_b(n_i) = 0. \tag{7}$$

If $2b$ does not divide n_i for some $i \in \{1, \dots, r\}$, then we have $t \in \{-1, 1\}$.

Proof. In (7) we may omit all zero summands, i.e., we may assume that $2b$ does not divide n_i for all $i \in \{1, \dots, r\}$ with a possibly smaller r. Clearly, we still have a sum with at least two summands.

For simplicity we write

$$s_i := \lfloor n_i/2 \rfloor \quad (i = 1, \dots, r).$$

Observe that we have

$$s_1 \le s_2 \le \cdots \le s_r \quad \text{and} \quad |e_1| = \cdots = |e_r| = 1.$$

From

$$a_b(n_1) = -\sum_{i=2}^{r} t^{n_i - n_1}\, a_b(n_i)$$

we infer

$$\begin{aligned} b^{s_1} &= |t|^{n_2 - n_1} \cdot \left| \sum_{i=2}^{r} t^{n_i - n_2}\, e_b(n_i)\, b^{s_i} \right| \\ &= |t|^{n_2 - n_1} \cdot b^{s_2} \cdot \left| e_b(n_2) + \sum_{i=3}^{r} t^{n_i - n_2}\, e_b(n_i)\, b^{s_i - s_2} \right| \end{aligned}$$

which yields

$$1 = |t|^{n_2 - n_1} \cdot b^{s_2 - s_1} \cdot \left| e_b(n_2) + \sum_{i=3}^{r} t^{n_i - n_2}\, e_b(n_i)\, b^{s_i - s_2} \right|$$

and finally $|t| = 1$. □

The next lemma is easy to check and certainly well-known, however, the author was unable to find a suitable reference.

Lemma 3.6. *Assume that $q = X^2 + bX + c \in \mathbb{Z}[X]$ is irreducible and $b \neq 0$. If the quotient of the roots of q is a root of unity then there exist $n \in \{1, 2, 3\}$ and $t \in \mathbb{Z} \setminus \{0\}$ such that $b = nt$ and $c = nt^2$.*

For the particular quadratic polynomials described in Lemma 3.6 we determine all trinomial multiples in $\mathcal{P}_3$.

Proposition 3.7. *Let $a, t \in \mathbb{Z}$ and $n, k, d \in \mathbb{N}$ such that $t \neq 0$ and $d > k > 0$. Set $q = X^2 + ntX + nt^2$ and $p = X^d + X^k + a \in \mathcal{P}_3$.*

(i) *Let $n = 1$. Then q divides p if and only if one of the following three conditions is satisfied:*

(a) $k \equiv d \equiv 0 \pmod 3$ *and* $a = -t^k(t^{d-k} + 1)$,

(b) $k \equiv 1 \pmod 3$, $d \not\equiv 0 \pmod 3$, $t = \pm 1$ *and either*

$$d \equiv 1 \pmod 3, \quad t = -1 \quad \text{and} \quad a = 0$$

or

$$d \equiv 2 \pmod 3, \quad \text{and} \quad a = t^k,$$

(c) $k \equiv 2 \pmod 3$, $d \not\equiv 0 \pmod 3$, $t = \pm 1$ *and either*

$$d \equiv 1 \pmod 3, \quad d \not\equiv k \pmod 2, \quad t = 1 \quad \text{and} \quad a = 1$$

or

$$d \equiv 1 \pmod 3, \quad d \equiv k \pmod 2 \quad \text{and} \quad a = t^k,$$

or

$$d \equiv 2 \pmod 3, \quad \text{and} \quad a = 0.$$

(ii) *Let $n = 2$. Then q divides p if and only if one of the following two conditions is satisfied:*

(a) $k \equiv d \equiv 0 \pmod 4$ *and*

$$a = (-1)^{(k/4)-1}\, 2^{k/2}\, t^k \left((-1)^{(d-k)/4}\, 2^{(d-k)/2}\, t^{d-k} + 1\right),$$

(b) $k \equiv 2 \pmod 4$, $d = k + 1$, $t = 1$ *and*

$$a = (-1)^{(k+2)/4}\, 2^{k/2}.$$

(iii) *Let $n = 3$. Then q divides p if and only if one of the following two conditions is satisfied:*

(a) $k \equiv d \equiv 0 \pmod 6$ *and*

$$a = (-1)^{(k/6)-1}\, 3^{k/2}\, t^k\, \big((-1)^{(d-k)/6}\, 3^{(d-k)/2}\, t^{d-k} + 1\big),$$

(b) $k \equiv 4 \pmod 6$, $d = k+1$, $t = 1$ *and*

$$a = (-1)^{(k+2)/6}\, 3^{k/2}.$$

Proof. We proceed similarly as in the proof of Lemma 3.5. Using the notation introduced above we sloppily set

$$a_m := A_m(n,n) \quad (m \in \mathbb{N}) \tag{8}$$

and infer from Theorem 3.1 and Lemma 3.3

$$\begin{aligned} q \,|\, p \iff & A_d(nt,nt^2)+A_k(nt,nt^2)=0 \text{ and } a = nt^2(A_{d-1}(nt,nt^2) + A_{k-1}(nt,nt^2)) \\ \iff & t^{d-1}a_d + t^{k-1}a_k = 0 \text{ and } a = nt^2(t^{d-2}a_{d-1} + t^{k-2}a_{k-1}) \\ \iff & t^{d-k}a_d = -a_k \text{ and } a = nt^k(t^{d-k}a_{d-1} + a_{k-1}). \end{aligned}$$

The proof is completed by exploiting this last condition for $n = 1,2,3$; here we only treat the case $n = 3$ and leave the first two (easier) cases to the reader.

Set

$$k = 6\ell + r,\ d = 6m + s \quad (r,s \in \{0,1,\dots,5\}\,,\ 0 \le \ell \le m)$$

and distinguish six cases.

Case 1 $r = 0$

Exploiting Lemma 3.4 we successively deduce $a_k = 0$, $a_d = 0$, $s = 0$ and $0 < \ell < m$, hence

$$\begin{aligned} a = 3t^k(t^{d-k}a_{6(m-1)+5} + a_{6(k-1)+5}) = 3t^k\big(t^{d-k}(-1)^{m-1}3^{3(m-1)+2} \\ + (-1)^{\ell-1}\, 3^{3(\ell-1)+2}\big) = (-1)^{\ell-1}3^{3\ell}t^k\big((-1)^{m-\ell}3^{3(m-\ell)}t^{d-k} + 1\big). \end{aligned}$$

Case 2 $r = 1$

Similarly as above we find

$$|t|^{d-k}\,|a_d| = 3^{3\ell},$$

hence $s \neq 0, 3$. If $s = 1$ we have $m > \ell$ and again by Lemma 3.4

$$|t|^{d-k}\, 3^{3(m-\ell)} = 1,$$

which is impossible, and if $s \in \{2,4,5\}$ we analogously obtain

$$|t|^{6(m-\ell)+s-1}\, 3^{3(m-\ell)+\delta} = 1$$

with some $\delta > 0$ which is impossible, too.

Case 3 $r = 2$

We have

$$|t|^{d-k}\, |a_d| = 3^{3\ell+1},$$

hence $s \neq 0, 3$. If $s \in \{1,2\}$ then we have $m > \ell$ and again by Lemma 3.4

$$|t|^{d-k}\, 3^{3(m-\ell)-\delta} = 1$$

with some $\delta \in \{0,1\}$ which is absurd. Analogously, the assumption $s \in \{4,5\}$ implies the impossible equation

$$|t|^{d-k}\, 3^{3(m-\ell)+1} = 1.$$

Case 4 $r = 3$

We have

$$|t|^{d-k}\, |a_d| = 2 \cdot 3^{3\ell+1},$$

hence $s \neq 0$. If $s = 3$ we have $m > \ell$ and

$$|t|^{d-k}\, 3^{3(m-\ell)} = 1$$

which is impossible, and if $s \neq 3$ we are successively led to

$$|t| = 2, \quad d-k = 1, \quad s = 4, \quad m = \ell, \quad 3^{2-1} = 1,$$

which is absurd.

Case 5 $r = 4$

We have

$$t^{d-k} a_d = (-1)^{\ell} 3^{3\ell+2},$$

hence $s \neq 0, 3$. If $s \in \{1,2,4\}$ then we have $m > \ell$ which leads to contradictions similarly as above. Now let $s = 5$. Then we deduce

$$(-1)^{\ell+m}\, t^{d-k}\, 3^{3(m-\ell)} = 1,$$

further $m = \ell$, $d - k = 1$, $t = 1$, and then

$$a = 3(a_{6m+4} + a_{6m+3}) = (-1)^{\ell+1} 3^{3\ell+2}.$$

Case 6 $\qquad r = 5$

We have $m > \ell$ and

$$|t|^{d-k} |a_d| = 3^{3\ell+2},$$

hence $s \neq 0, 3$, and the remaining subcases $s \in \{1, 2, 4, 5\}$ are excluded as above. The proof is completed. □

Remark 3.8. Using Proposition 3.7 we can easily construct infinitely many non-primitive CNS trinomials which are multiples of the CNS polynomial $X^2 + ntX + nt^2$ for $n \in \{1, 2, 3\}$ and $t \geq 2$.

We are now in a position to determine all trinomials in $\mathcal{P}_3$ which are multiples of those particular quadratic CNS polynomials which will play a key role in our further considerations.

Proposition 3.9. *Let $n \in \{2, 3\}$, $t \in \mathbb{Z}$ and $a, k, d \in \mathbb{N}_{>0}$ such that $t \neq 0$ and $d > k$. If $q := X^2 + ntX + nt^2$ divides $p := X^d + X^k + a$ then the following statements hold:*

(i) *We have $t \geq 1$, $p \in \mathcal{C}$ and $\gamma(p/q) \in \{1, 2\}$. If $t \in \{1, 2\}$ then $\gamma(p/q) = 2$.*

(ii) *Let $n = 2$. If $k \equiv 2 \pmod 4$ then there exists $u \geq 0$ such that*

$$d = 8u + 7, \quad k = 8u + 6, \quad a = 2^{4u+3},$$

and if $k \equiv 0 \pmod 4$ then there exist $u \geq 0, v > 0$ such that $d = 8(u+v)+4$ and

$$k = 8u + 4, \quad a = 2^{4u+2}\, t^{8u+4}\big(2^{4v} t^{8v} + 1\big)$$

or

$$k = 8v, \quad a = 2^{4v} t^{8v}\big(2^{4u+2} t^{8u+4} - 1\big).$$

(ii) *Let $n = 3$. If $k \equiv 4 \pmod 6$ then there exists $u \geq 0$ such that*

$$d = 12u + 11, \quad k = 12u + 10, \quad a = 3^{6u+5},$$

and if $k \equiv 0 \pmod 6$ then there exist $u \geq 0, v > 0$ such that $d = 12(u+v)+6$ and

$$k = 12u + 6, \qquad a = 3^{6u+3}\, t^{12u+6}\, \big(3^{6v}\, t^{12v} + 1\big)$$

or

$$k = 12v, \qquad a = 3^{6v}\, t^{12v}\, \big(3^{6u+3}\, t^{12u+6} - 1\big).$$

Proof. Exploiting $a > 0$ we infer from Lemma 3.7 that $t \geq 1$ and that p has the form indicated above; further, we verify $a \geq 3$. Consequently, $p \in \mathcal{C}$ by Proposition 2.2, thus for the quotient $g := p/q$ we have $\gamma(g) \leq 2$ by definition. We check $g(0) > g(1)$, hence $\gamma(g) \geq 1$ by Corollary 2.5, and therefore $\gamma(g) \in \{1, 2\}$. For $t = 1, 2$ an easy computation reveals $g(0) > (3/2)g(1)$, and then Corollary 2.5 yields $\gamma(g) = 2$ in these cases. □

Let us include some numerical examples.

Example 3.10. (i) For

$$\begin{aligned} g :=\ & X^{29} - X^{28} + 2X^{26} - 2^2X^{25} + 2^2X^{24} - 2^3X^{22} + 2^4X^{21} - 2^4X^{20} \\ & + 2^5X^{18} - 2^6X^{17} + 2^6X^{16} - 2^7X^{14} + 2^8X^{13} - 2^8X^{12} + 2^9X^{10} \\ & - 2^{10}X^9 + 2^{10}X^8 - 2^{11}X^6 + 2^{12}X^5 - 2^{13}X^4 + 2^{13}X^2 - 2^{14}X + 2^{14} \end{aligned}$$

we have

$$(X^2 + 2X + 2) \cdot g = X^{31} + X^{30} + 2^{15}$$

and $\gamma(g) = 2$ by Proposition 3.9.

(ii) The quotient of $X^{12} + X^8 + 2^4 \cdot 3^8 \cdot 17 \cdot 19$ and $X^2 + 6X + 18$ is the polynomial

$$\begin{aligned} g :=\ & X^{10} - 2 \cdot 3X^9 + 2 \cdot 3^2X^8 - 17 \cdot 19X^6 + 2 \cdot 3 \cdot 17 \cdot 19X^5 - 2 \cdot 3^2 \cdot 17 \cdot 19X^4 \\ & + 2^2 \cdot 3^4 \cdot 17 \cdot 19X^2 - 2^3 \cdot 3^5 \cdot 17 \cdot 19X + 2^3 \cdot 3^6 \cdot 17 \cdot 19. \end{aligned}$$

Proposition 3.9 yields $\gamma(g) \geq 1$, then we have $\gamma(g) \geq 2$ by Lemma 3.11 below, and we conclude $\gamma(g) = 2$ by Proposition 3.9.

Lemma 3.11. *Let $f = \sum_{i=1}^{r} a_iX^i \in \mathbb{Z}[X] \setminus \mathcal{C}$ be a monic polynomial of degree $d \geq 2$ such that for all $c \geq 2$ the following two conditions hold:*

(i) $|c + a_{d-1}| + \sum_{i=1}^{d-1} |ca_i + a_{i-1}| < ca_0$

(ii) $a_{d-1} + c < -1$ *or* $(a_{d-1} + 1)c + a_{d-1} + a_{d-2} < -1.$

Then we have $\gamma(f) \geq 2$.

Proof. We immediately infer from [4, Theorem 5.2] that for every $c \geq 2$ we have $(X + c) \cdot f \notin \mathcal{C}$. □

Now we present our main results on quadratic CNS divisors of CNS polynomials in $\mathcal{P}_r$. Let us start with non-primitive and reducible quadratic divisors.

Theorem 3.12. *Let $r \geq 3$ and q be a quadratic CNS polynomial.*

(i) *If q is non-primitive then q divides infinitely many CNS polynomials in $\mathcal{P}_r$.*

(i) *If q is reducible then q divides at most finitely many CNS polynomials in $\mathcal{P}_r$.*

Proof. (i) Write $q(X) = \ell(X^2)$ with a linear CNS polynomial ℓ and apply Theorem 2.9 and [10, Theorem 1].

(ii) Clearly, we can write $q = (X + s)(X + t)$ with $s, t \geq 2$. Assume that q divides infinitely many $p_{r,n,a} \in \mathcal{P}_r$, thus the sequence $(A_k(b, c))_{k\in\mathbb{N}}$ described in Lemma 3.3 has infinitely many zeros. It is well-known that then the quotient of the roots of q is a root of unity (e.g., see [34, Corollary C.1]), hence $s = t$ and $q = X^2 + 2tX + t^2$. From Theorem 3.1 we deduce

$$\sum_{k=2}^{r} A_{n_k}(2t, t^2) = 0,$$

and Lemmas 3.3 and 3.4 yield

$$0 = \sum_{k=2}^{r} t^{n_k-1} A_{n_k}(2, 1) = \sum_{k=2}^{r} (-t)^{n_k-1}\, n_k = (-t)^{n_2-1} \sum_{k=2}^{r} (-t)^{n_k-n_2} n_k,$$

hence

$$\sum_{k=2}^{r} (-t)^{n_k-n_2} n_k = 0$$

and then

$$n_2 = -\sum_{k=3}^{r} (-t)^{n_k-n_2} n_k.$$

However, we can check

$$n_2 = \left| \sum_{k=3}^{r} (-t)^{n_k-n_2} n_k \right| \geq t^{n_r-n_2} n_r - \sum_{k=3}^{r-1} t^{n_k-n_2} n_k \geq n_3$$

which contradictions our prerequisites. □

In view of Theorem 3.12 we now restrict our attention to primitive irreducible quadratic CNS polynomials as divisors of elements of $\mathcal{P}_r$. It turns out that a decisive role is played by the two polynomials in the set

$$Q := \left\{X^2 + 2X + 2, X^2 + 3X + 3\right\}.$$

Theorem 3.13. *Let $r \geq 3$ and q be an irreducible primitive quadratic CNS polynomial. The following statements are equivalent:*

(i) *q divides infinitely many primitive multinomials in $\mathcal{P}_r$.*

(ii) *q divides infinitely many primitive CNS polynomials $p \in \mathcal{P}_r$ with $\gamma(p/q) = 2$.*

(iii) *q belongs to Q.*

Proof. By what we have seen in Section 1 we can write $q = X^2 + bX + c$ with $c \geq 2$, $b \neq 0$ and $-1 \leq b \leq c$.

(i) $\Longrightarrow$ (iii) Since q divides infinitely many $p \in \mathcal{P}_r$ the sequence $(A_k(b,c))_{k\in\mathbb{N}}$ described in Lemma 3.3 has infinitely many zeros. It is well-known that then the quotient of the roots of q is a root of unity (e.g., see [34, Corollary C.1]). Therefore we infer from Lemma 3.6 that there exist $n \in \{1,2,3\}$ and $t \in \mathbb{Z} \setminus \{0\}$ such that $b = nt$ and $c = nt^2$, and then Theorem 3.1 yields

$$\sum_{k=2}^{r} A_{n_k}(b,c) = 0.$$

Note that by the primitivity of p we have $n_k \not\equiv 0 \pmod{2n}$ for at least one k. We infer $|t| = 1$ from Lemma 3.5, thus $t = 1$. Then clearly $n \neq 1$, and we are done.

(iii) $\Longrightarrow$ (ii) For the polynomials $X^2 + nX + n$ with $n \in \{2,3\}$ we exhibit infinite sequences of primitive CNS multiples in $\mathcal{P}_r$.

Let $r = 3$ and s be a nonnegative integer. If $n = 2$ then by Propositions 3.9 and 2.2 the polynomial $X^{8s+7} + X^{8s+6} + 2^{4s+3}$ is a CNS multiple of q. Similarly, for $n = 3$ the polynomial $X^{12s+11} + X^{12s+10} + 3^{6s+5}$ satisfies our requirements.

Now, let $r > 3$ and $s \geq r - 2$ be an odd integer. Again we apply the sloppy notation (8). First, let $n = 2$ and set

$$n_{r-k} = 4(s-k+2) \quad (k = 3, \dots, r-2),$$
$$n_{r-2} = 4s, \quad n_{r-1} = 4s+2, \quad n_r = 4s+3$$

and

$$a = 2 \cdot \sum_{k=2}^{r} a_{n_k - 1}.$$

Then $p := p_{r,(n_r,\dots,n_2),a}$ is primitive, and from Theorem 3.1 we know that q divides p, since using Lemma 3.4 we find

$$\begin{aligned}\sum_{k=2}^{r} a_{n_k} &= a_{4s+3} + a_{4s+2} + a_{4s} + \sum_{j=3}^{r-2} a_{n_{r-j}} \\ &= (-1)^{s+2}2^{2s+1} + (-1)^{s+1}2^{2s+1} + \sum_{j=3}^{r-2} a_{4(s-j+2)} = 0.\end{aligned}$$

Furthermore, we check

$$a = \frac{2^{2(s-r+4)}}{5} \cdot \left(2^{2r-7} \cdot 7 + (-1)^r\right)$$

and verify

$$2a \geq 3r - 2. \tag{9}$$

This immediately implies $a \geq r$, and thus $p \in \mathcal{C}$ by Proposition 2.2. For the quotient $g := p/q$ inequality (9) implies

$$g(0) = \frac{a}{2} > \frac{3}{2} \cdot \frac{r-1+a}{5} = \frac{3}{2} \cdot g(1),$$

hence $\gamma(g) = 2$ by Corollary 2.5.

Second, let $n = 3$. Now, we define

$$n_k = 6(k-1) \quad (k = 2, \ldots, r-3),$$
$$n_{r-2} = 6(s-1), \quad n_{r-1} = 6s + 4, \quad n_r = 6s + 5$$

and

$$a = 3 \cdot \sum_{k=2}^{r} a_{n_k - 1}.$$

Analogously as before, we check that

$$\sum_{k=2}^{r} a_{n_k} = 0$$

and

$$a = \frac{27}{28}\left(7 \cdot 8 \cdot 121 \cdot 3^{3(s-2)} + (-1)^{r-1} \cdot 3^{3(r-4)} + 1\right)$$

and verify

$$14a > 9(a + r - 1).$$

Then we deduce that $p_{r,(n_r,\ldots,n_2),a}$ indeed satisfies our requirements.

(ii) $\Longrightarrow$ (i) Trivial. □

We conclude with several numerical examples which illustrate the growth of the constant terms of the multinomials constructed in the proof of Theorem 3.13.

Example 3.14. For $r = 4, \ldots, 7$ some primitive CNS multiples $p \in \mathcal{P}_r$ of $q \in \mathcal{Q}$ are listed; in each case we have $\gamma(g) = 2$ for the quotient polynomial $g := p/q$.

(i) The quadrinomial

$$X^{11} + X^{10}X^{6} + 2 \cdot 3^{3} \cdot 5$$

can be written as the product

$$(X^{2} + 3X + 3)(X^{9} - 2X^{8} + 3X^{7} - 3X^{6} + 2 \cdot 5X^{4} \\ - 2 \cdot 3 \cdot 5X^{3} + 2^{2} \cdot 3 \cdot 5X^{2} - 2 \cdot 3^{2} \cdot 5X + 2 \cdot 3^{2} \cdot 5).$$

(ii) The quintinomial

$$X^{23} + X^{22} + X^{20} + X^{16} + 2^{8} \cdot 11$$

is a multiple of $X^2 + 2X + 2$ with the quotient

$$X^{21} - X^{20} + 3X^{18} - 6X^{17} + 6X^{16} - 11X^{14} + 2 \cdot 11X^{13} - 2 \cdot 11X^{12} \\ + 2^{2} \cdot 11X^{10} - 2^{3} \cdot 11X^{9} + 2^{3} \cdot 11X^{8} - 2^{4} \cdot 11X^{6} + 2^{5} \cdot 11X^{5} - 2^{5} \cdot 11X^{4} \\ + 2^{6} \cdot 11X^{2} - 2^{7} \cdot 11X + 2^{7} \cdot 11.$$

(iii) The sextinomial

$$X^{35} + X^{34} + X^{24} + X^{12} + X^{6} + 2^{2} \cdot 3^{3} \cdot 5 \cdot 238163$$

is the product of $X^2 + 3X + 3$ and

$$X^{33} - 2X^{32} + 3X^{31} - 3X^{30} + 3^{2}X^{28} - 3^{3}X^{27} + 2 \cdot 3^{3}X^{26} - 3^{4}X^{25} + 3^{4}X^{24} \\ - 2 \cdot 11^{2}X^{22} + 2 \cdot 3 \cdot 11^{2}X^{21} - 2^{2} \cdot 3 \cdot 11^{2}X^{20} + 2 \cdot 3^{2} \cdot 11^{2}X^{19} - 2 \cdot 3^{2} \cdot 11^{2}X^{18} \\ + 2 \cdot 3^{3} \cdot 11^{2}X^{16} - 2 \cdot 3^{4} \cdot 11^{2}X^{15} + 2^{2} \cdot 3^{4} \cdot 11^{2}X^{14} - 2 \cdot 3^{5} \cdot 11^{2}X^{13} \\ + 2 \cdot 3^{5} \cdot 11^{2}X^{12} - 176417X^{10} + 3 \cdot 176417X^{9} - 2 \cdot 3 \cdot 176417X^{8} + 3^{2} \cdot 176417X^{7} \\ - 3^{2} \cdot 176417X^{6} + 2^{2} \cdot 5 \cdot 238163X^{4} - 2^{2} \cdot 3 \cdot 5 \cdot 238163X^{3} + 2^{3} \cdot 3 \cdot 5 \cdot 238163X^{2} \\ - 2^{2} \cdot 3^{2} \cdot 5 \cdot 238163X + 2^{2} \cdot 3^{2} \cdot 5 \cdot 238163.$$

(iv) The septinomial

$$X^{23} + X^{22} + X^{20} + X^{16} + X^{12} + X^{8} + 2^{4} \cdot 179$$

is a multiple of $X^2 + 2X + 2$ with the quotient

$$X^{21} - X^{20} + 3X^18 - 2 \cdot 3X^{17} + 2 \cdot 3X^{16} - 11X^{14} + 2 \cdot 11X^{13} - 2 \cdot 11X^{12} \\ + 3^{2} \cdot 5X^{10} - 2 \cdot 3^{2} \cdot 5X^{9} + 2 \cdot 3^{2} \cdot 5X^{8} - 179X^{6} + 2 \cdot 179X^{5} - 2 \cdot 179X^{4} \\ + 2^{2} \cdot 179X^{2} - 2^{3} \cdot 179X + 2^{3} \cdot 179.$$

Acknowledgement. The author is much indebted to the anonymous referee whose critical comments and insightful suggestions helped to improve a former version of this paper. The computations were done with sage [35].

References

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. M. Thuswaldner, Generalized radix representations and dynamical systems I, *Acta Math. Hungar.* **108** (2005), 207–238.

[2] S. Akiyama, H. Brunotte and A. Pethő, Cubic CNS polynomials, notes on a conjecture of W. J. Gilbert, *J. Math. Anal. Appl.* **281** (2003), 402–415.

[3] S. Akiyama and A. Pethő, On canonical number systems, *Theoret. Comput. Sci.* **270** (2002), 921–933.

[4] S. Akiyama and H. Rao, New criteria for canonical number systems, *Acta Arith.* **111** (2004), 5–25.

[5] G. Barat, V. Berthé, P. Liardet and J. Thuswaldner, Dynamical directions in numeration, *Ann. Inst. Fourier (Grenoble)* **56** (2006), 1987–2092, Numération, pavages, substitutions.

[6] V. Berthé, Numeration and discrete dynamical systems, *Computing* **94** (2012), 369–387.

[7] T. Borbély, Általánosított számrendszerek, *Master Thesis, University of Debrecen*, 2003.

[8] P. Borwein and M. J. Mossinghoff, Newman polynomials with prescribed vanishing and integer sets with distinct subset sums, *Math. Comp.* **72** (2003), 787–800.

[9] A. Bremner and M. Ulas, Some observations concerning reducibility of quadrinomials, arXiv:1310.5346v1, 2013.

[10] H. Brunotte, Characterization of CNS trinomials, *Acta Sci. Math. (Szeged)* **68** (2002), 673–679.

[11] H. Brunotte, On expanding real polynomials with a given factor, *Publ. Math. Debrecen* **83** (2013), 161–178.

[12] A. Chen, On the reducible quintic complete base polynomials, *J. Number Theory* **129** (2009), 220–230.

[13] A. Dubickas, The divisors of Newman polynomials, *Fiz. Mat. Fak. Moksl. Semin. Darb.* **6** (2003), 25–28.

[14] A. Dubickas and J. Jankauskas, On Newman polynomials which divide no Littlewood polynomial, *Math. Comp.* **78** (2009), 327–344.

[15] W. J. Gilbert, Radix representations of quadratic fields, *J. Math. Anal. Appl.* **83** (1981), 264–274.

[16] V. Grünwald, Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale), *Giornale di Matematiche di Battaglini* **23** (1885), 203–221, 367.

[17] K. Győry and A. Schinzel, On a conjecture of Posner and Rumsey, *J. Number Theory* **47** (1994), 63–78.

[18] J. Jankauskas, On the reducibility of certain quadrinomials, *Glas. Mat. Ser. III* **45** (2010), 31–41.

[19] A. T. Jonassen, On the irreduciblity of the trinomials $x^m \pm x^n \pm 4$, *Math. Scand.* **21** (1967), 177–189, (1969).

[20] D. M. Kane, Generalized base representations, *J. Number Theory* **120** (2006), 92–100.

[21] I. Kátai, Generalized number systems in Euclidean spaces, *Math. Comput. Modelling* **38** (2003), 883–892, Hungarian applied mathematics and computer applications.

[22] I. Kátai and B. Kovács, Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen, *Acta Sci. Math. (Szeged)* **42** (1980), 99–107.

[23] I. Kátai and B. Kovács, Canonical number systems in imaginary quadratic fields, *Acta Math. Acad. Sci. Hungar.* **37** (1981), 159–164.

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

[25] P. Kirschenhofer and J. M. Thuswaldner, Shift radix systems – a survey, *RIMS Kôkyûroku Bessatsu* **B46** (2014), 1–59.

[26] B. Kovács, Canonical number systems in algebraic number fields, *Acta Math. Acad. Sci. Hungar.* **37** (1981), 405–407.

[27] W. Ljunggren, On the irreducibility of certain trinomials and quadrinomials, *Math. Scand.* **8** (1960), 65–70.

[28] W. H. Mills, The factorization of certain quadrinomials, *Math. Scand.* **57** (1985), 44–50.

[29] A. M. Odlyzko and B. Poonen, Zeros of polynomials with $0,1$ coefficients, *Enseign. Math.* **39** (1993), 317–348.

[30] A. Pethő, On a polynomial transformation and its application to the construction of a public key cryptosystem, in: Computational Number Theory (Debrecen, 1989), (A. Pethő M.E. Pohst, H.C. Williams, H. Zimmer, eds.), *de Gruyter, Berlin*, 1991, 31–43.

[31] A. Pethő, Connections between power integral bases and radix representations in algebraic number fields, in: Proceedings of the 2003 Nagoya Conference "Yokoi–Chowla Conjecture and Related Problems", (S. Katayama, C. Levesque, and T. Nakahara, eds.), *Saga, Saga Univ.*, 2004, 115–125.

[32] A. Pethő, Notes on CNS polynomials and integral interpolation, in: More Sets, Graphs and Numbers. A Salute to Vera Sós and András Hajnal, vol. 15 of Bolyai Soc. Math. Stud., (E. Győri, Gy.O.H. Katona, L. Lovász, eds.), *Springer, Berlin*, 2006, 301–315.

[33] E. S. Selmer, On the irreducibility of certain trinomials, *Math. Scand.* **4** (1956), 287–302.

[34] T. N. Shorey and R. Tijdeman, Exponential Diophantine Equations, vol. 87 of Cambridge Tracts in Mathematics, *Cambridge University Press, Cambridge*, 1986.

[35] W. A. Stein *et al.*, Sage Mathematics Software (Version 5.3), *The Sage Development Team*, 2012, http://www.sagemath.org.

[36] A. Tátrai, Parallel implementations of Brunotte's algorithm, *J. Parallel Distrib. Comput.* **71** (2011), 565–572.

[37] J. M. Thuswaldner, Elementary properties of canonical number systems in quadratic fields, in Applications of Fibonacci numbers, Vol. 7 (Graz, 1996), *Kluwer Acad. Publ., Dordrecht*, 1998, 405–414.

[38] H. Tverberg, On the irreducibility of the trinomials $x^n \pm x^m \pm 1$, *Math. Scand.* **8** (1960), 121–126.

[39] C. E. Van de Woestijne, Number systems and the Chinese remainder theorem, Preprint, available at arXiv:1106.4219v1, 2011.

[40] C. E. Van de Woestijne, Factors of disconnected graphs and polynomials with nonnegative integer coefficients, *Ars Math. Contemp. 5* (2012), 307–323.

HORST BRUNOTTE
HAUS-ENDT-STRASSE 88
D-40593 DÜSSELDORF
GERMANY

E-mail: brunoth@web.de

(Received May 14, 2014; revised March 17, 2015)