Canad. Math. Bull. Vol. **56** (3), 2013 pp. 510–519
http://dx.doi.org/10.4153/CMB-2011-179-0

Linear Forms in Monic Integer Polynomials

Artūras Dubickas

Abstract. We prove a necessary and sufficient condition on the list of nonzero integers $u_1, \dots, u_k$, $k \geqslant 2$, under which a monic polynomial $f \in \mathbb{Z}[x]$ is expressible by a linear form $u_1 f_1 + \cdots + u_k f_k$ in monic polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$. This condition is independent of f. We also show that if this condition holds, then the monic polynomials $f_1, \dots, f_k$ can be chosen to be irreducible in $\mathbb{Z}[x]$.

1 Representations by a Linear Form

In 1965, Hayes [4] proved that every polynomial in $\mathbb{Z}[x]$ of degree $d \geqslant 1$ is expressible as the sum of two irreducible polynomials in $\mathbb{Z}[x]$, each of degree d. This result was later rediscovered by Rattan and Stewart in [8], and its various generalizations and specializations (for monic polynomials, for polynomials in the ring $R[x]$, where R is not necessarily $\mathbb{Z}$, for matrices, etc.) have been given in [1,3,5,7,11–13]. In particular, for a monic polynomial f in the ring $\mathbb{Z}[x]$, there is an asymptotical formula for the number of representations of f by the sum of several irreducible monic polynomials, each of height at most T (see [2,6,9]).

To give a more complete treatment of the subject, we shall investigate the representations of a monic polynomial $f \in \mathbb{Z}[x]$ of degree $d \geqslant 2$ by a linear form

$$f(x) = u_1 f_1(x) + u_2 f_2(x) + \cdots + u_k f_k(x) \tag{1.1}$$

in monic irreducible polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$, $k \geqslant 2$, each of height at most T, where u_i, $i = 1, \dots, k$, are some fixed nonzero integers. The cases $k = 2$, $u_1 = u_2 = 1$, and $k \geqslant 2$, $u_1 = \cdots = u_k = 1$, have been considered in [2,6,9]. It is shown that then there are asymptotically $c_{k,d} T^{(k-1)(d-1)}$ of such representations as $T \to \infty$, where $d = \deg f \geqslant 2$ and $c_{k,d} > 0$ is a constant independent of T.

Obviously, for some collections $u_1, \dots, u_k$, there are no representations (1.1) in monic polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$. For instance, if there is an integer $s > 1$ that divides all the numbers $u_1, \dots, u_k$ then the right hand side of (1.1) is a polynomial whose coefficients are all divisible by s, so no monic polynomial f can be represented by (1.1). The same is true if, for instance, $k = 2$, $u_1 = 5$, $u_2 = -2$. Then no polynomial of the form $5f_1 - 2f_2$ is a monic polynomial provided that f_1, f_2 are monic, because the leading coefficient of $5f_1 - 2f_2$ is in the set $\{-2, 3, 5\}$.

However, if, for instance, $k = 3$, $u_1 = 5$, $u_2 = -2$, $u_3 = -3$, then one can prove that every monic polynomial $f \in \mathbb{Z}[x]$ of degree at least 1 can be represented by the linear form (1.1). Selecting, *e.g.*, $f(x) = x^3 - x - 3$, we see that

$$x^3 - x - 3 = 5 \cdot (x^m + 2x^3 - 2x + 2) - 2 \cdot (x^m + 2) - 3 \cdot (x^m + 3x^3 - 3x + 3)$$

Received by the editors January 4, 2011.
Published electronically September 15, 2011.
AMS subject classification: **11R09**, 11C08, 11B83.
Keywords: irreducible polynomial, height, linear form in polynomials, Eisenstein's criterion.

https://doi.org/10.4153/CMB-2011-179-0 Published online by Cambridge University Press

for every $m \geqslant 4$. Moreover, the polynomials x^m+2x^3-2x+2, x^m+2 and x^m+3x^3-3x+3, where $m \geqslant 4$, are irreducible by Eisenstein's criterion. Thus, for the polynomial $f(x) = x^3 - x - 3$, there are infinitely many of representations $f = 5f_1 - 2f_2 - 3f_3$ in monic integer polynomials f_1, f_2, f_3 of height at most 3.

In this note we shall investigate the following natural questions:

- Given a monic polynomial $f \in \mathbb{Z}[x]$ of degree $d \geqslant 1$ and an integer $k \geqslant 2$, find all collections $u_1, \dots, u_k \in \mathbb{Z}^*$ such that f can be represented by the linear form (1.1) in monic integer polynomials $f_1, \dots, f_k$.
- In the case when such a representation is possible, determine whether there is a positive integer T_0 such that for $T = T_0$ (and so for each $T \geqslant T_0$) there are infinitely many of such representations in monic integer irreducible polynomials of height at most T.

The answers to those questions are nontrivial, and we need some definitions before stating them. In particular, we remark that the answers given in Theorem 1.1 do not depend on the choice of f.

For every finite collection of nonzero integers $u_{j_1}, \dots, u_{j_s}$ with $J = \{j_1, \dots, j_s\} \subseteq \{1, \dots, k\}$, we denote the greatest common divisor of its elements by

$$\gcd(u_j \ : \ j \in J) = \gcd(u_{j_1}, \dots, u_{j_s}).$$

Recall that it is the largest positive integer dividing each of the numbers $u_{j_1}, \dots, u_{j_s}$. In case $J = \{j\}$, $j \in \{1, \dots, k\}$, we have $\gcd(u_j) = |u_j|$.

We say that the list of nonzero integers $u_1, \dots, u_k$, $k \geqslant 2$, *satisfies condition* (C_0) if there are some nonempty sets of indices $J_0, \dots, J_\ell$, $\ell \geqslant 1$, $J_s \neq J_t$ (except perhaps for $J_{\ell-1} = J_\ell$),

$$\varnothing \subset J_0 \subset J_1 \subset \cdots \subset J_{\ell-1} \subseteq J_\ell \subseteq \{1, 2, \dots, k\},$$

such that

$$\sum_{j \in J_0} u_j = 0, \tag{1.2}$$

$$\gcd(u_j \ : \ j \in J_t) \ \Big| \sum_{j \in J_{t+1} \setminus J_t} u_j \tag{1.3}$$

for every $t = 0, \dots, \ell - 2$ (if $\ell \geqslant 2$), and

$$\gcd(u_j \ : \ j \in J_{\ell-1}) \ \Big| \ \Big(-1 + \sum_{j \in J_\ell \setminus J_{\ell-1}} u_j\Big). \tag{1.4}$$

(Throughout, the sum over the empty set is assumed to be zero.) In particular, for $\ell = 1$, we have only two sets of indices J_0 and J_1 satisfying $\varnothing \subset J_0 \subseteq J_1 \subseteq \{1, \dots, k\}$ and there are no conditions (1.3), but only (1.2) and (1.4), *i.e.,*

$$\sum_{j \in J_0} u_j = 0 \quad \text{and} \quad \gcd(u_j \ : \ j \in J_0) \ \Big| \ \Big(-1 + \sum_{j \in J_1 \setminus J_0} u_j\Big). \tag{1.5}$$

https://doi.org/10.4153/CMB-2011-179-0 Published online by Cambridge University Press

It may happen that no set $J_0 \neq \varnothing$ for which (1.2) holds exists, for instance, when all of the u_i are positive integers. In this case (when there is no set $J_0 \neq \varnothing$ for which (1.2) holds), we say that the list of nonzero integers $u_1, \dots, u_k$ *satisfies condition* (C_1) if there is a nonempty set $J_1 \subseteq \{1, \dots, k\}$ for which

$$\sum_{j \in J_1} u_j = 1. \tag{1.6}$$

The above set $u_1 = 5$, $u_2 = -2$, $u_3 = -3$ satisfies (1.5) with $J_0 = J_1 = \{1, 2, 3\}$, because $5 - 2 - 3 = 0$ and $\gcd(5, -2, -3) = 1$, so it satisfies condition (C_0). The set

$$u_1 = 10, \quad u_2 = -10, \quad u_3 = -20, \quad u_4 = -19$$

satisfies condition (C_0) with $J_0 = \{1, 2\}$ ($u_1 + u_2 = 10 - 10 = 0$, so (1.2) holds), $J_1 = \{1, 2, 3\}$ ($\gcd(10, -10) = 10$ divides $u_3 = -20$, so (1.3) holds), and $J_2 = \{1, 2, 3, 4\}$ ($\gcd(10, -10, -20) = 10$ divides $u_4 - 1 = -20$, so (1.4) holds). The set

$$u_1 = 10, \quad u_2 = -10, \quad u_3 = 3, \quad u_4 = 2 \tag{1.7}$$

does not satisfy condition (C_0). Indeed, if the set (1.7) satisfies (C_0), then J_0 must be $\{1, 2\}$, and it is impossible to choose J_1 for which (1.3) or (1.4) holds, because $J_1 \neq J_0$ and the number $\gcd(10, -10) = 10$ does not divide any of the numbers in the list $u_3, u_4, u_3 + u_4, u_3 - 1, u_4 - 1, u_3 + u_4 - 1$. The set (1.7) does not satisfy condition (C_1) either, by the definition of (C_1). Similarly, the set $6, -6, 12, -36, 7$ satisfies condition (C_0), but the set $6, -6, 12, -36, 5$ does not satisfy condition (C_0).

The aim of this paper is to prove the following theorem:

Theorem 1.1 *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree $d \geqslant 1$, and let $k \geqslant 2$, $u_1, \dots, u_k$ be nonzero integers.*

(a) *Then f can be represented by the linear form (1.1) in some monic polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$ if and only if the list of integers $u_1, \dots, u_k$ satisfies one of the conditions (C_0) or (C_1).*

(b) *Moreover, for fixed $T \in \mathbb{N}$, there are only finitely many such representations in monic polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$ of height at most T if and only if the list $u_1, \dots, u_k$ satisfies condition (C_1).*

(c) *Finally, if the list of integers $u_1, \dots, u_k$ satisfies condition (C_0), then there is a positive integer T_0 such that for each $T \geqslant T_0$ there are infinitely many representations (1.1) in monic irreducible polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$ of height at most T.*

It is well known that if $a_1, \dots, a_s$ are some fixed nonzero integers, then $a \in \mathbb{Z}$ is expressible in the form $a_1\mathbb{Z} + \cdots + a_s\mathbb{Z}$ if and only if $\gcd(a_1, \dots, a_s) | a$. Therefore, we can write condition (1.3) in the equivalent form

$$\sum_{j \in J_t} u_j z_{j,t} + \sum_{j \in J_{t+1} \setminus J_t} u_j = 0, \tag{1.8}$$

https://doi.org/10.4153/CMB-2011-179-0 Published online by Cambridge University Press

where $t = 0, \dots, \ell - 2$ (if $\ell \geqslant 2$) and $z_{j,t} \in \mathbb{Z}$. Analogously, condition (1.4) can be written in the equivalent form

$$\sum_{j \in J_{\ell-1}} u_j z_{j,\ell-1} + \sum_{j \in J_\ell \setminus J_{\ell-1}} u_j = 1 \tag{1.9}$$

for some integers $z_{j,\ell-1}$.

Note that if the collection of nonzero integers $u_1, \dots, u_k$ satisfies condition (C_0) (resp. (C_1)), then (1.9) (resp. (1.6)) implies

$$\gcd(u_1, \dots, u_k) = 1. \tag{1.10}$$

The example (1.7) shows that the converse of this statement is false.

2 Proof of Part (c) and Sufficiency of Part (a)

For the proof of the theorem we need the following elementary lemma.

Lemma 2.1 *Let $b_1, \dots, b_m$ be nonzero integers $b \in \mathbb{Z}$, $t \in \mathbb{N}$, $m \geqslant 2$, and $t \leqslant m$. Suppose that $p_1, \dots, p_t$ are any distinct prime numbers greater than $\max(|b_1|, \dots, |b_m|)$. If*

$$b_1 y_1 + b_2 y_2 + \cdots + b_m y_m = b \tag{2.1}$$

is solvable in integers $y_1, \dots, y_m$, then one can choose $y_1, \dots, y_t$ so that each y_i ($i = 1, \dots, t$) is divisible by p_i but not by p_i^2.

Proof of the lemma Set $g := \gcd(b_1, \dots, b_m)$. As we remarked above, the linear equation (2.1) is solvable in integers if and only if $g | b$. Assume that $p_1, \dots, p_t > \max(|b_1|, \dots, |b_m|)$ and select $y_i = p_i^2 z_i + p_i$, $z_i \in \mathbb{Z}$, for $i = 1, \dots, t$. Then y_i is a multiple of p_i but not a multiple of p_i^2. It remains to show that the linear equation

$$b_1 p_1^2 z_1 + \cdots + b_t p_t^2 z_t + b_{t+1} y_{t+1} + \cdots + b_m y_m = b - b_1 p_1 - \cdots - b_t p_t \tag{2.2}$$

is solvable in integers $z_1, \dots, z_t, y_{t+1}, \dots, y_m$. This is indeed the case, because, by the choice of p_i, we have

$$\gcd(b_1 p_1^2, b_2 p_2^2, \dots, b_t p_t^2, b_{t+1}, \dots, b_m) = g.$$

Furthermore, g divides b and $b_1, \dots, b_m$, so g also divides the right-hand side of (2.2). ■

Now, we will prove part (c) of the theorem. Assume that the list $u_1, \dots, u_k$ satisfies condition (C_0). Without restriction of generality (by changing the indices of the integers in the list $u_1, \dots, u_k$ if necessary) we may assume that there exist the indices i_t, $t = 0, \dots, \ell$, satisfying $2 \leqslant i_0 < i_1 < \cdots < i_{\ell-1} \leqslant i_\ell \leqslant k$ such that

$$J_0 = \{1, \dots, i_0\}, \quad J_1 = \{1, \dots, i_1\}, \quad \dots, \quad J_\ell = \{1, \dots, i_\ell\}.$$

https://doi.org/10.4153/CMB-2011-179-0 Published online by Cambridge University Press

Set also $J_{\ell+1} := \{1,\dots,k\}$ and $J_{-1} := \varnothing$. Clearly, $J_{\ell+1} = J_\ell$ when $i_\ell = k$. Fix some integers

$$N_{\ell+1} := d-1 < N_\ell := d < N_{\ell-1} < \cdots < N_0.$$

For each index $i \in \{1,\dots,k\}$ that belongs to the set $J_t \setminus J_{t-1}$, where $t = 0,1,\dots,\ell+1$, we will construct a monic polynomial $f_i \in \mathbb{Z}[x]$ whose degree will be equal to N_t.

Observe that in the case $i_\ell < k$, we can take any $k - i_\ell$ irreducible monic polynomials $f_{i_\ell+1},\dots,f_k \in \mathbb{Z}[x]$ (say, of degree $N_{\ell+1} = d-1$ each), and apply the argument to the polynomial $f - \sum_{i=i_\ell+1}^{k} u_i f_i$ instead of f and i_ℓ ($i_\ell \geqslant i_0 \geqslant 2$) instead of k. So assume from now on that $i_\ell = k$. Then $J_\ell = J_{\ell+1} = \{1,\dots,k\}$, and all the polynomials $f_1,\dots,f_k$ will be of degree at least d. Note that the set $J_\ell \setminus J_{\ell-1}$ can be empty, so it may happen that there are no polynomials of degree $N_\ell = d$.

We shall construct the polynomials $f_1, \dots, f_k$ in the form of a matrix $\mathcal{M}$ with $N_0 + 1$ columns and k rows, where the i-th row of the matrix $\mathcal{M}$ is composed from the coefficients of $f_i(x) := \sum_{j=0}^{N_0} m(j,i)x^j$, written as

$$\big(m(N_0,i), m(N_0-1,i),\dots,m(0,i)\big).$$

To prove the irreducibility of the monic polynomials $f_1,\dots,f_k \in \mathbb{Z}[x]$, we fix k distinct prime numbers $p_1,\dots,p_k$ greater than $\max(|u_1|,\dots,|u_k|)$. It will be shown that the polynomial f_i, $i = 1,\dots,k$, is irreducible by Eisenstein's criterion with respect to the prime number p_i.

Let

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0.$$

Clearly, (1.1) holds if the coefficients $m(j,i)$ are chosen so that

$$\sum_{i=1}^{k} u_i m(j,i) = \begin{cases} 0 & \text{for } j > d,\\ 1 & \text{for } j = d,\\ a_j & \text{for } 0 \leqslant j < d. \end{cases} \tag{2.3}$$

To ensure that the first i_0 polynomials are monic, we must take

$$m(N_0,1) = \cdots = m(N_0,i_0) = 1.$$

The first column of $\mathcal{M}$ is completed by zeros $m(N_0,i_0+1) = \cdots = m(N_0,k) = 0$, because $\deg f_i < N_0$ for $i > i_0$. In view of (1.2) this gives $\sum_{i=1}^{k} u_i m(N_0,i) = \sum_{i=1}^{i_0} u_i = \sum_{j\in J_0} u_j = 0$, which corresponds to the first line in (2.3).

We also select the coefficients for x^j, where $N_1 + 1 \leqslant j < N_0$, to be zeros, namely,

$$m(j,1) = \cdots = m(j,k) = 0 \quad \text{for} \quad N_1 + 1 \leqslant j < N_0.$$

This gives $\sum_{i=1}^{k} u_i m(j,i) = 0$ for $N_1+1 \leqslant j < N_0$, which checks the next $N_0 - N_1 - 1$ lines in (2.3).

https://doi.org/10.4153/CMB-2011-179-0 Published online by Cambridge University Press

By Lemma 2.1, we may select the integers $z_{j,t}$, $t = 0, \dots, \ell - 1$ that appear in (1.8) and (1.9) so that, for each $j \in J_t$, the number $z_{j,t}$ is divisible by p_j, *i.e.*,

$$p_j | z_{j,t} \quad \text{for} \quad j \in J_t, \;\; t = 0, \dots, \ell - 1.$$

In order to use (1.8) for $t = 0$ (this step applies only if $\ell \geqslant 2$), we select

$$m(N_1, i) = z_{i,0} \quad \text{for} \quad 1 \leqslant i \leqslant i_0,$$
$$m(N_1, i_0 + 1) = \cdots = m(N_1, i_1) = 1,$$

and $m(N_1, i) = 0$ for $i > i_1$. Then by (1.8),

$$\sum_{i=1}^{k} u_i m(N_1, i) = \sum_{i=1}^{i_0} u_i z_{i,0} + \sum_{i=i_0+1}^{i_1} u_i = 0.$$

In the same way, for each $j = N_{t+1}$, where $0 \leqslant t \leqslant \ell - 1$, we take

$$m(N_{t+1}, i) = z_{i,t} \quad \text{for} \quad 1 \leqslant i \leqslant i_t, \tag{2.4}$$

$$m(N_{t+1}, i_t + 1) = \cdots = m(N_{t+1}, i_{t+1}) = 1, \tag{2.5}$$

and $m(N_{t+1}, i) = 0$ for $i > i_{t+1}$. For $N_{t+1} + 1 \leqslant j < N_t$, $t = 0, \dots, \ell - 1$, we take the coefficients for x^j to be zeros, *i.e.*,

$$m(j, 1) = \cdots = m(j, k) = 0 \quad \text{for} \quad N_{t+1} + 1 \leqslant j < N_t. \tag{2.6}$$

Now, by (2.4)–(2.6), in view of (1.8) (resp. (1.9)), as above we obtain

$$\sum_{i=1}^{k} u_i m(j, i) = 0$$

for each j greater than d (resp.

$$\sum_{i=1}^{k} u_i m(d, i) = \sum_{i=1}^{k} u_i m(N_\ell, i) = \sum_{i=1}^{i_{\ell-1}} u_i z_{i,\ell-1} + \sum_{i=i_{\ell-1}+1}^{i_\ell} u_i = 1$$

for $j = N_\ell = d$). This verifies the first $N_0 - d + 1$ lines in (2.3). It remains to choose $m(j, i)$ for $j \leqslant d - 1$ and to check the last d lines of (2.3).

In case $d \geqslant 2$, using Lemma 2.1, for every j in the range $1 \leqslant j \leqslant d - 1$, we can select some $m(j, i) \in \mathbb{Z}$ divisible by p_i, $i = 1, \dots, k$ such that

$$\sum_{i=1}^{k} u_i m(j, i) = a_j,$$

https://doi.org/10.4153/CMB-2011-179-0 Published online by Cambridge University Press

because, by (1.10), $\gcd(u_1,\dots,u_k) = 1$. (For $d = 1$ we just do not use this step.) This checks that all of the equalities in (2.3) hold except perhaps for the last equality. As for the last equality, we will use the full statement of Lemma 2.1; namely, we take $m(0,i) \in \mathbb{Z}$ divisible by p_i, not divisible by p_i^2, such that

$$\sum_{i=1}^{k} u_i m(0,i) = a_0.$$

This completes the construction of the matrix $\mathcal{M}$ with the property (2.3).

In this way, for $i = 1,\dots,k$, we obtain k monic polynomials

$$f_i(x) = \sum_{j=0}^{N_0} m(j,i)x^j,$$

$i = 1,\dots,k$, of degrees $N_0, N_1,\dots,N_{\ell-1}$ and possibly $N_\ell = d$ (when $J_{\ell-1} \neq J_\ell$) satisfying (1.1). Moreover, by Eisenstein's criterion with respect to the prime number p_i, the polynomial f_i, $i = 1,\dots,k$ is irreducible in $\mathbb{Z}[x]$.

Set $T_0 := \max_{0\leqslant j\leqslant N_0,\ 1\leqslant i\leqslant k} |m(j,i)|$. Since N_0 can be arbitrarily large and its selection does not change the number T_0, we obtain infinitely many collections of monic irreducible polynomials $f_1,\dots,f_k \in \mathbb{Z}[x]$, each of height at most T_0, for which (1.1) holds. This completes the proof of Theorem 1.1(c).

In order to complete the proof of sufficiency in part (a), assume that condition (C_1) holds. Without restriction of generality we may assume that the set J_1 satisfying (1.6) is $J_1 = \{1,\dots,s\}$, where $1 \leqslant s \leqslant k$. Suppose first that $s \geqslant 2$. Fix any monic irreducible polynomials $f_{s+1},\dots,f_k \in \mathbb{Z}[x]$ of degrees at most $d-1$. We claim that the polynomial

$$f(x) - u_{s+1}f_{s+1}(x) - \cdots - u_k f_k(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

can be written in the form $\sum_{i=1}^{s} u_i f_i(x)$ with monic irreducible polynomials $f_1,\dots,f_s \in \mathbb{Z}[x]$. To do this we take

$$f_i(x) = x^d + m(d-1,i)x^{d-1} + \cdots + m(0,i) \in \mathbb{Z}[x], \quad i = 1,\dots,s,$$

where

$$\sum_{i=1}^{s} u_i m(j,i) = a_j \tag{2.7}$$

for $j = 0,\dots,d-1$. As above, using (1.6), we see that the leading coefficient of the polynomial $u_1 f_1 + \cdots + u_s f_s$ is equal to $\sum_{i=1}^{s} u_i = 1$. This yields $\gcd(u_1,\dots,u_s) = 1$. Now, using this condition and Lemma 2.1, for every $i = 1,\dots,s$, we may choose $m(j,i)$ in (2.7) divisible by p_i for $j = 1,\dots,d-1$ and also $m(0,i)$ divisible by p_i and not by p_i^2. Consequently, the polynomials $f_1,\dots,f_s$ are irreducible.

https://doi.org/10.4153/CMB-2011-179-0 Published online by Cambridge University Press

Assume next that $s = 1$. Then $u_1 = 1$. Take $f_3(x) = \cdots = f_k(x) = 1$ and $f_2(x) = x + t$, where $t \in \mathbb{N}$ will be chosen later. Then (1.1) holds for the polynomial

$$f_1(x) := f(x) - u_2 x - \sum_{j=3}^{k} u_j - u_2 t.$$

By Hilbert's irreducibility theorem (see, *e.g.*, [10, p. 298]), there are infinitely many $t \in \mathbb{N}$ for which the polynomial f_1 is irreducible in $\mathbb{Z}[x]$, *i.e.*, no polynomials $g_1, g_2 \in \mathbb{Z}[x]$ of degrees strictly less than $\deg f_1$ exist for which $f_1 = g_1 g_2$. Taking one of those t we obtain the required representation (1.1) and so complete the proof in case $s = 1$.

This proves that if condition (C_0) or (C_1) holds, then every monic polynomial $f \in \mathbb{Z}[x]$ of degree $d \geqslant 1$ can be represented by the linear form (1.1) in some monic irreducible polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$.

3 Proof of Necessity of Part (a) and of Part (b)

Assume that we have some representation (1.1) in monic polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$. There are two cases: first, when in (1.1) at least one f_i has degree greater than d and, second, when there is no representation as in the first case but there is a representation when all the polynomials f_i are of degree at most d. We claim that in the first (resp. second) case the list of integers $u_1, \dots, u_k$ satisfies condition (C_0) (resp. (C_1)).

In the first case we must have a subset of indices $J_0 \subseteq \{1, \dots, k\}$ for which (1.2) holds, namely, $\sum_{j \in J_0} u_j = 0$. This set consists of indices of polynomials f_i of the largest degree, say, $N_0 > d$. Suppose we also have the degrees $N_1 > \cdots > N_{\ell-1}$ $(\ell \geqslant 1)$ greater than d in the list of degrees $\deg f_1, \dots, \deg f_k$. More precisely, let

$$I_j := \{1 \leqslant i \leqslant k \, : \, \deg f_i = N_j\}$$

for $j = 0, \dots, \ell - 1$, so that $J_0 = I_0$. Put $J_j := \bigcup_{l=0}^{j} I_l$ for $j = 0, \dots, \ell - 1$.

Consider the coefficient for x^{N_1} in the left-hand side of (1.1) if $\ell \geqslant 2$. Since $\deg f < N_{\ell-1}$, it must be zero. Assuming that the coefficients of f_j, $j \in J_0$, for x^{N_1} are $z_{j,0}$ we obtain $\sum_{j \in J_0} u_j z_{j,0} + \sum_{j \in J_1 \setminus J_0} u_j = 0$, *i.e.*, the first equality in (1.8). Similarly, for every $t = 1, \dots, \ell - 2$, assuming that the coefficients of f_j, $j \in J_t$, for $x^{N_{t+1}}$ are $z_{j,t}$, we obtain $\sum_{j \in J_t} u_j z_{j,t} + \sum_{j \in J_{t+1} \setminus J_t} u_j = 0$, *i.e.*, the equality in (1.8) corresponding to t.

Assume now that the coefficients for x^d in f_j, where $j \in J_{\ell-1}$, are $z_{j,\ell-1}$. The coefficient of the left hand side of (1.1) for x^d is equal to 1, hence the coefficient of the right hand side of (1.1) for x^d must be 1 too. It follows that there exists a set J_ℓ such that $J_{\ell-1} \subseteq J_\ell \subseteq \{1, \dots, k\}$ for which

$$\sum_{j \in J_{\ell-1}} u_j z_{j,\ell-1} + \sum_{j \in J_\ell \setminus J_{\ell-1}} u_j = 1,$$

i.e., (1.9) holds. This proves that the list $u_1, \dots, u_k$ satisfies condition (C_0).

In the second case, when there is no representation (1.1) as in the first case, but there is a representation (1.1) with $\deg f_i \leqslant d$ for $i = 1, \dots, k$ there must be a set $J_1 \subseteq \{1, \dots, k\}$ for which (1.6) holds. In order to prove that the list $u_1, \dots, u_k$ satisfies condition (C_1) it remains to show that no nonempty set $J_0 \subseteq \{1, \dots, k\}$ exists for which (1.2) holds. For a contradiction, assume that there is such a set J_0. Then $\sum_{j\in J_0} u_j = 0$ and $\sum_{j\in J_1} u_j = 1$. This implies that the conditions (1.2) and (1.9) are satisfied for $\ell = 1$ and the first two sets J_0 and $J_0 \cup J_1$, with $z_{j,0} = 1$ for $j \in J_0$. Indeed, then $(J_0 \cup J_1) \setminus J_0 = J_1$, so that

$$\sum_{j\in J_0} u_j z_{j,0} + \sum_{j\in J_1} u_j = \sum_{j\in J_0} u_j + \sum_{j\in J_1} u_j = 0 + 1 = 1.$$

Therefore, the list $u_1, \dots, u_k$ satisfies condition (C_0). Hence, by sufficiency of part (a), we have infinitely many representations (1.1) in monic polynomials of bounded height, where some degrees of $f_1, \dots, f_k$ are greater than d, a contradiction. This completes the proof of necessity of (a).

Finally, let us prove part (b) Assume that the list of integers $u_1, \dots, u_k$ satisfies condition (C_1). The results of Section 2 imply that there exist monic (even irreducible) polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$ for which (1.1) holds. In order to prove that there are only finitely many representations (1.1) in polynomials $f_1, \dots, f_k$ of height at most T we shall use the fact that there is no nonempty set of indices $J_0 \subseteq \{1, \dots, k\}$ for which (1.2) holds (by the definition of (C_1)). In particular, this implies that the degree of each f_i does not exceed d. Obviously, there are only finitely many polynomials of bounded degree and height, so there are only finitely many collections of monic polynomials $f_1, \dots, f_k$ satisfying $\deg f_i \leqslant d$, $H(f_i) \leqslant T$, $i = 1, \dots, k$ and (1.1). (In fact, by the same method as in [2], one can show that for each monic f of degree $d \geqslant 2$ there are asymptotically $cT^{(d-1)(k-1)}$ of such representations as $T \to \infty$, with some positive constant $c = c(u_1, \dots, u_k, d)$ independent of T.)

On the other hand, assume that there are only finitely many representations (1.1) in monic polynomials $f_1, \dots, f_k \in \mathbb{Z}[x]$ of height at most T. If there is at least one set of indices J_0 for which (1.2) holds, then, by the necessity of part (a), the list of integers $u_1, \dots, u_k$ satisfies condition (C_0). However, then there are infinitely many of such representations by part (c), a contradiction. So there is no such set of indices J_0. Thus, by part (a), if there is at least one such representation, then the list $u_1, \dots, u_k$ must satisfy condition (C_1). This completes the proof of Theorem 1.1(b).

References

[1] C. Betts, *Additive and subtractive irreducible monic decompositions in* $\mathbb{Z}[x]$. C. R. Math. Acad. Sci. Soc. R. Can. **20**(1998), no. 3, 86–90.

[2] A. Dubickas, *Polynomials expressible by sums of monic integer irreducible polynomials* Bull. Math. Soc. Sci. Math. Roumanie **54(102)**(2011), no. 1, 65–81.

[3] G. W. Effinger and D. R. Hayes, *A complete solution to the polynomial* 3*-primes problem.* Bull. Amer. Math. Soc. (N.S.) **24**(1991), no. 2, 363–369. http://dx.doi.org/10.1090/S0273-0979-1991-16035-0

[4] D. R. Hayes, *A Goldbach theorem for polynomials with integer coefficients.* Amer. Math. Monthly, **72**(1965), 45–46. http://dx.doi.org/10.2307/2312999

[5] ———, *The expression of a polynomial as a sum of three irreducibles.* Acta Arith. **11**(1966), 461–488.

[6] M. Kozek, *An asymptotic formula for Goldbach's conjecture with monic polynomials.* Amer. Math. Monthly **117**(2010), no. 4, 365–369. http://dx.doi.org/10.4169/000298910X480856

https://doi.org/10.4153/CMB-2011-179-0 Published online by Cambridge University Press

[7] P. Pollack, *On polynomial rings with a Goldbach property.* Amer. Math. Monthly, **118**(2011), no. 1, 71–77.

[8] A. Rattan and C. Stewart, *Goldbach's conjecture for* $\mathbb{Z}[x]$. C. R. Math. Acad. Sci. Soc. R. Can. **20**(1998), no. 3, 83–85.

[9] F. Saidak, *On Goldbach's conjecture for integer polynomials.* Amer. Math. Monthly **113**(2006), no. 6, 541–545. http://dx.doi.org/10.2307/27641978

[10] A. Schinzel, *Polynomials with special regard to irreducibility.* Encyclopedia of Mathematics and its Applications, 77, Cambridge University Press, Cambridge, 2000.

[11] L. N. Vaserstein, *Noncommutative number theory.* In: Algebraic K-theory and algebraic number theory (Honolulu, Haway, 1987), Contemp. Math., 83, American Mathematical Society, Providence, RI, 1989, pp. 445–449.

[12] J. Wang, *Goldbach's problem in the ring* $M_n(\mathbf{Z})$, Amer. Math. Monthly **99**(1992), no. 9, 856–857. http://dx.doi.org/10.2307/2324122

[13] S. Wang, *The Goldbach* 3*-primes property for polynomial rings over certain infinite fields.* Chinese Sci. Bull. **43**(1998), no. 15, 1256–1260. http://dx.doi.org/10.1007/BF02884136

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania

and

Institute of Mathematics and Informatics, Vilnius University, Akademijos 4, Vilnius LT-08663, Lithuania
e-mail: arturas.dubickas@mif.vu.lt

https://doi.org/10.4153/CMB-2011-179-0 Published online by Cambridge University Press