On a problem of Sárközy and Sós for multivariate linear forms

Juanjo Rué [a,1,2] and Christoph Spiegel [a,1,3]

[a] *Universitat Politècnica de Catalunya, Dept. of Mathematics, Barcelona, Spain, and Barcelona Graduate School of Mathematics, Barcelona, Spain*

Abstract

We prove that for pairwise co-prime numbers $k_1, \ldots, k_d \geq 2$ there does not exist any infinite set of positive integers $\mathcal{A}$ such that the representation function $r_{\mathcal{A}}(n) = \#\{(a_1, \ldots, a_d) \in \mathcal{A}^d : k_1 a_1 + \ldots + k_d a_d = n\}$ becomes constant for n large enough. This result is a particular case of our main theorem, which poses a further step towards answering a question of Sárközy and Sós and widely extends a previous result of Cilleruelo and Rué for bivariate linear forms (Bull. of the London Math. Society 2009).

Keywords: Additive combinatorics, representation functions, additive basis

[1] Supported by the Spanish Ministerio de Economía y Competitividad projects MTM2014−54745-P, MTM2017−82166-P and the María de Maetzu research grant MDM−2014−0445 (BGSMath). C. S. is also suppported by an FPI grant under the project projects MTM2014−54745−P.

[2] Email:`juan.jose.rue@upc.edu`

[3] Email:`christoph.spiegel@upc.edu`

1 Introduction

Let $\mathcal{A} \subseteq \mathbb{N}_0$ be an infinite set of positive integers and $k_1, \ldots, k_d \in \mathbb{N}$. We are interested in studying the behaviour of the representation function

$$r_{\mathcal{A}}(n) = r_{\mathcal{A}}(n; k_1, \ldots, k_d) = \#\{(a_1, \ldots, a_d) \in \mathcal{A}^d : k_1 a_1 + \ldots + k_d a_d = n\}.$$

More specifically, Sárközy and Sós [5, Problem 7.1.] asked for which values of $k_1, \ldots, k_d$ one can find an infinite set $\mathcal{A}$ such that the function $r_{\mathcal{A}}(n; k_1, \ldots, k_d)$ becomes constant for n large enough. For the base case, it is clear that $r_{\mathcal{A}}(n; 1, 1)$ is odd whenever $n = 2a$ for some $a \in \mathcal{A}$ and even otherwise, so that the representation function cannot become constant. For $k \geq 2$, Moser [3] constructed a set $\mathcal{A}$ such that $r_{\mathcal{A}}(n; 1, k) = 1$ for all $n \in \mathbb{N}_0$. The study of bivariate linear forms was completely settled by Cilleruelo and the first author [1] by showing that the only cases in which $r_{\mathcal{A}}(n; k_1, k_2)$ may become constant are those considered by Moser.

The multivariate case is less well studied. If $\gcd(k_1, \ldots, k_d) > 1$, then one trivially observes that $r_{\mathcal{A}}(n; k_1, \ldots, k_d)$ cannot become constant. The only non-trivial case studied so far was the following: for $m > 1$ dividing d, Rué [4] showed that if in the d-tuple of coefficients $(k_1, \ldots, k_d)$ each element is repeated m times, then there cannot exists an infinite set $\mathcal{A}$ such that $r_{\mathcal{A}}(n; k_1, \ldots, k_d)$ becomes constant for n large enough.

Here we provide a step beyond this result and show that whenever the set of coefficients is pairwise co-prime, then there does not exists any infinite set $\mathcal{A}$ for which $r(n; k_1, \ldots, k_d)$ is constant for n large enough. This is a particular case of our main theorem, which covers a wide extension of this situation:

Theorem 1.1 *Let $k_1, \ldots, k_d \geq 2$ be given for which there exist pairwise co-prime integers $q_1, \ldots, q_m \geq 2$ and $b(i,j) \in \{0, 1\}$, such that for each i there exists at least one j such that $b_{i,j} = 1$. Let $k_i = q_1^{b(i,1)} \cdots q_m^{b(i,m)}$ for all $1 \leq i \leq d$. Then, for every infinite set $\mathcal{A} \subseteq \mathbb{N}_0$ $r_{\mathcal{A}}(n; k_1, \ldots, k_d)$ is not a constant function for n large enough.*

Our method starts with some ideas introduced in [1] dealing with generating functions and cyclotomic polyomials. The main new idea in this paper is to use an inductive argument in order to be able to show that a certain multivariate recurrence relation is not possible to be satisfied unless some initial condition is trivial.

2 Tools

The language in which we will approach this problem goes back to [2]. Let $f_{\mathcal{A}}(z) = \sum_{a\in\mathcal{A}} z^a$ denote the *generating function* associated with $\mathcal{A}$ and observe that $f_{\mathcal{A}}$ defines an analytic function in the complex disc $|z| < 1$. By a simple argument over the generating functions, it is easy to verify that the existence of a set $\mathcal{A}$ for which $r_{\mathcal{A}}(n; k_1, \ldots, k_d)$ becomes constant would imply that

$$f_{\mathcal{A}}(z^{k_1}) \cdots f_{\mathcal{A}}(z^{k_d}) = \frac{P(z)}{1-z}$$

for some polynomial P with positive integer coefficients satisfying $P(1) \neq 0$. To simplify notation, we will generally consider the d-th power of this equations, that is for $F(z) = f_{\mathcal{A}}^d(z)$ we have

$$F(z^{k_1}) \cdots F(z^{k_d}) = \frac{P^d(z)}{(1-z)^d}. \tag{1}$$

Observe that $F(z)$ also defines an analytic function in the complex disk $|z| < 1$.

Let us define the *cyclotomic polynomial of order* n as

$$\Phi_n(z) = \prod_{\xi\in\phi_n} (z - \xi) \in \mathbb{Z}[z]$$

where $\phi_n = \{\xi \in \mathbb{C} : \xi^k = 1,\ k \equiv 0 \bmod n\}$ denotes the set of primitive roots of order $n \in \mathbb{N}$. Note that $\Phi_n(z) \in \mathbb{Z}[z]$, that is it has integer coefficients. Cyclotomic polynomials have the property of being irreducible over $\mathbb{Z}[z]$ and therefore it follows that for any polynomial $P(z) \in \mathbb{Z}[z]$ and $n \in \mathbb{N}$ there exists a unique integer $s_n \in \mathbb{N}_0$ such that

$$P_n(z) := P(z)\, \Phi_n^{-s_n}(z) \tag{2}$$

is a polynomial in $\mathbb{Z}[z]$ satisfying $P_n(\xi) \neq 0$ for all $\xi \in \phi_n$.

This factoring out of the roots is not guaranteed to hold for arbitrary functions F, that is it is possible that for a given $n \in \mathbb{N}$ there does not exist any $r_n \in \mathbb{R}$ satisfying

$$\lim_{z\to\xi} F(z)\, \Phi_n^{-r_n}(z) \notin \{0, \pm\infty\}$$

for all $\xi \in \phi_n$. One can easily verify however, that if such a number does exist, it is uniquely defined. Now let $q_1, \ldots, q_m$ be fixed co-prime integers. Given some $\mathbf{j} = (j_1, \ldots, j_m) \in \mathbb{N}_0^m$ we will use the following short-hand notation

$$\Phi_{\mathbf{j}}(z) := \Phi_{q_1^{j_1}\cdots q_m^{j_m}}(z),\ \phi_{\mathbf{j}}(z) := \phi_{q_1^{j_1}\cdots q_m^{j_m}}(z),\ s_{\mathbf{j}} := s_{q_1^{j_1}\cdots q_m^{j_m}} \text{ and } r_{\mathbf{j}} := r_{q_1^{j_1}\cdots q_m^{j_m}}.$$

3 Proof Outline

The main strategy of the proof is to show that for a hypothetical function $F(z) = f_{\mathcal{A}}^d(z)$ satisfying Equation (1) the exponents $r_{\mathbf{j}}$ would have to exist for all $\mathbf{j} \in \mathbb{N}_0^m$ – at least with respect to some appropriate limit – and fulfil certain relations between them. The goal will be to find a contradiction in these relations, negating the possibility of such a function and therefore such a set $\mathcal{A}$ existing in the first place.

We establish the existence and relations of the values $r_{\mathbf{j}}$ for any $k_1, \ldots, k_d \in \mathbb{N}$ and later derive a contradiction from these relations in the specific case stated in Theorem 1.1. For any $a, b \in \mathbb{N}_0$, $\mathbf{j} = (j_1, \ldots, j_m) \in \mathbb{N}_0^m$ and $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{N}_0^m$, we will use the notation

$$a \ominus b = \max\{a - b, 0\} \quad \text{and} \quad \mathbf{j} \ominus \mathbf{b} = (j_1 \ominus b_1, \ldots, j_m \ominus b_m).$$

Furthermore, whenever we write some limit $\lim_{z\to\xi} F(z)$, where ξ is a unit root, we are referring to $\lim_{z\to 1} F(z\,\xi)$ where $0 \le z < 1$ as F will always be analytic in the disc $|z| < 1$.

Proposition 3.1 *Let $k_1, \ldots, k_d \in \mathbb{N}$ and $q_1, \ldots, q_m \ge 2$ pairwise co-prime integers for which there exist $b(i,j) \in \mathbb{N}_0$ such that $k_i = q_1^{b(i,1)} \cdots q_m^{b(i,m)}$ for all $1 \le i \le d$. Furthermore, let $P \in \mathbb{Z}[z]$ be a polynomial satisfying $P(1) \ne 0$ and $F : \mathbb{C} \to \mathbb{C}$ a function analytic in the disc $|z| < 1$ such that*

$$F(z^{k_1}) \cdots F(z^{k_d}) = \frac{P^d(z)}{(1-z)^d}. \tag{3}$$

Then for all $\boldsymbol{j} \in \mathbb{N}_0^m$ there exist integers $r_{\boldsymbol{j}} \in \mathbb{N}_0$ such that

$$\lim_{z\to\xi} F(z)\, \Phi_{\boldsymbol{j}}^{-r_{\boldsymbol{j}}}(z) \notin \{0, \pm\infty\} \tag{4}$$

for any $\xi \in \phi_{\boldsymbol{j}}$. Writing $\boldsymbol{b}_i = (b(i,1), \ldots, b(i,m))$ for $1 \le i \le m$, these exponents satisfy the relations

$$r_{\mathbf{0}} = -1 \quad \text{and} \quad r_{\boldsymbol{j}\ominus\boldsymbol{b}_1} + \ldots + r_{\boldsymbol{j}\ominus\boldsymbol{b}_d} = d s_{\boldsymbol{j}} \quad \text{for all } \boldsymbol{j} \in \mathbb{N}_0^m \setminus \{\mathbf{0}\} \tag{5}$$

and we have $r_{\boldsymbol{i}} \equiv -1 \bmod d$ for all $\boldsymbol{i} \in \mathbb{N}_0^m$.

We will now use this proposition to prove Theorem 1.1 by contradiction. We start by introducing some necessary notation and definitions. We write $\mathbf{c}_i = (c(i,1), \ldots, c(i,m))$ and for any $1 \le \ell \le m$ we use the notation

$$S_\ell = \{1 \le i \le d : c(i,\ell) = 0\} \quad \text{and} \quad S'_\ell = \{1, \ldots, d\} \setminus S_\ell.$$

Definition 3.2 For $m \geq 1$, we define an *m-structure* to be any set of values $\{v_{\mathbf{j}} \in \mathbb{Q}\}_{\mathbf{j} \in \mathbb{N}_0^m}$ for which there exist $\mathbf{c}_1, \ldots, \mathbf{c}_d \in \mathbb{N}_0^m$ and $\{u_{\mathbf{j}} \in \mathbb{Z}\}_{\mathbf{j} \in \mathbb{N}_0^m \setminus \{\mathbf{0}\}}$ so that the values satisfy the relation

$$v_{\mathbf{j} \ominus \mathbf{c}_1} + \ldots + v_{\mathbf{j} \ominus \mathbf{c}_d} = u_{\mathbf{j}} \quad \text{for all } \mathbf{j} \in \mathbb{N}_0^m \setminus \{\mathbf{0}\}.$$

Additionally, we define the following:

(i) We say that an m-structure is *regular* if we have that the corresponding vectors $\mathbf{c}_1, \ldots, \mathbf{c}_d \in \{0,1\}^m \setminus \{\mathbf{0}\}$ for all $1 \leq i \leq d$ as well as $S_\ell \neq \emptyset$ for all $1 \leq \ell \leq m$.

(ii) We say that an m-structure is *homogeneous outside* $\boldsymbol{t} = (t_1, \ldots, t_m) \in \mathbb{N}_0^m$ if the corresponding vectors $\{u_{\mathbf{j}} \in \mathbb{Z}\}_{\mathbf{j} \in \mathbb{N}_0^m \setminus \{\mathbf{0}\}}$ satisfy $u_{\mathbf{j}} = 0$ for all $\mathbf{j} \in \mathbb{N}_0^m \setminus [0, t_1] \times \ldots \times [0, t_m]$.

By finding an appropriate substructure that reduces the value of m, one can now inductively prove the following statement.

Lemma 3.3 *A regular m-structure that is homogeneous outside $\boldsymbol{t} = (t_1, \ldots, t_m) \in \mathbb{N}_0^m$ satisfies $v_{\boldsymbol{i}} = 0$ for all $\boldsymbol{i} \in \mathbb{N}_0^m \setminus [0, t_1] \times \ldots \times [0, t_m]$.*

Using this result, we can proof our main statement.

Proof. [Proof of Theorem 1.1] We write $F(z) = f_{\mathcal{A}}(z)^d$. Recall that the existence of a set $\mathcal{A}$ for which $r_{\mathcal{A}}(n; k_1, \ldots, k_d)$ is a constant function for n large enough would imply the existence of some polynomial $P(z) \in \mathbb{Z}[z]$ satisfying $P(1) \neq 0$ such that

$$F(z^{k_1}) \cdots F(z^{k_d}) = \frac{P^d(z)}{(1-z)^d}.$$

Using Proposition 3.1 we see that if a such a function $F(z)$ were to exist, then the values $\{r_{\mathbf{i}}\}_{\mathbf{i} \in \mathbb{N}_0^m}$ together with $\mathbf{b}_1, \ldots, \mathbf{b}_m$ and $\{s_{\mathbf{j}}\}_{\mathbf{j} \in \mathbb{N}_0^m \setminus \{\mathbf{0}\}}$ would define an m-structure. By the requirements of the theorem we have $\mathbf{b}_i \in \{0,1\}^m$ and since $k_1, \ldots, k_d \geq 2$ we have $\mathbf{b}_i \neq \mathbf{0}$. We may also assume that $S_\ell \neq \emptyset$ for all $1 \leq \ell \leq d$ as otherwise there exists some ℓ' such that $q_{\ell'} \mid k_i$ for all $1 \leq i \leq d$, in which case the representation function clearly cannot become constant, so that this m-structure would be regular. It would also be homogeneous outside some appropriate $\mathbf{t} \in \mathbb{N}_0^m$ as $P(z)$ is a polynomial and hence $s_{\mathbf{j}} \neq 0$ only for finitely many $\mathbf{j} \in \mathbb{N}_0^m$. Finally, since $r_{\mathbf{i}} \equiv -1 \bmod d$ for all $\mathbf{i} \in \mathbb{N}_0^m$, this would contradict the statement of Lemma 3.3, proving Theorem 1.1. $\square$

4 Concluding Remarks

We have shown that under very general conditions for the coefficients $k_1, \ldots, k_d$ the representation function $r_{\mathcal{A}}(n; k_1, \ldots, k_d)$ cannot be constant for n sufficiently large. However, there are cases that our method does not cover. This includes those cases where at least one of the k_i is equal to 1. The first case that we are not able to study is the representation function $r_{\mathcal{A}}(n; 1, 1, 2)$.

On the other side, let us point out that Moser's construction [3] can be trivially generalized to the case where $k_i = k^{i-1}$ for some integer value $k \geq 2$. In view of our results and this construction, we state the following conjecture:

Conjecture 4.1 *There exists some infinite set of positive integers $\mathcal{A}$ such that $r_{\mathcal{A}}(n; k_1, \ldots, k_d)$ is constant for n large enough if and only if, up to permutation of the indices, $(k_1, \ldots, k_d) = (1, k, k^2, \ldots, k^{d-1})$, for some $k \geq 2$.*

References

[1] J. Cilleruelo and J. Rué. On a question of Sárközy and Sós for bilinear forms. *Bulletin of the London Mathematical Society*, 41(2):274–280, 2009.

[2] G. Dirac. Note on a problem in additive number theory. *Journal of the London Mathematical Society*, 1(4):312–313, 1951.

[3] L. Moser. An application of generating series. *Mathematics Magazine*, 35(1):37–38, 1962.

[4] J. Rué. On polynomial representation functions for multilinear forms. *European Journal of Combinatorics*, 34(8):1429–1435, 2011.

[5] A. Sárközy and V. Sós. On additive representation functions. In *The mathematics of Paul Erdős I*, pages 129–150. Springer, 1997.