JOURNAL OF COMBINATORIAL THEORY, Series A 31, 21–32 (1981)

Homogeneous Collinear Sets in Partitions of $\mathbb{Z}^n$

R. L. GRAHAM

Bell Laboratories, Murray Hill, New Jersey 07974

WEN-CHING WINNIE LI*

Pennsylvania State University, University Park, Pennsylvania 16802

AND

J. L. PAUL

University of Cincinnati, Cincinnati, Ohio 45221

Communicated by the Managing Editors

Received October 14, 1980

INTRODUCTION

For fixed positive integers n and r, let χ be a mapping of the integer points $\mathbb{Z}^n = \{(z_1,..., z_n): z_k \text{ an integer}\}$ into $\{1,..., r\}$. Denote by $L(\chi)$ the maximum number of consecutive collinear points of $\mathbb{Z}^n$ contained in any $\chi^{-1}(i)$, $1 \leqslant i \leqslant r$. Such points can always be put into the form

$$z_i = c_i + td_i, \qquad 1 \leqslant t \leqslant L(\chi),$$

where g.c.d. $\{d_1,..., d_n\} = 1$. Finally, define $\rho_r(n)$ by

$$\rho_r(n) = \inf_{\chi} L(\chi),$$

where χ ranges over all mappings of $\mathbb{Z}^n$ into $\{1, 2,..., r\}$.

A fundamental result of Hales and Jewett [4] shows that for any r,

$$\lim_{n\to\infty} \rho_r(n) = \infty. \qquad (1)$$

However, the best known lower bound grows so slowly that it is not even primitive recursive.

* Work performed while at Bell Laboratories.

0097-3165/81/040021-12$02.00/0

In the other direction, it has been shown by one of the authors in [5] that

$$\rho_2(n) \leqslant 2n-1. \tag{2}$$

In this note, we will strengthen (2) considerably and provide an improved upper bound on $\rho_r(n)$ for arbitrary r. The proof will depend on several striking properties of the binomial coefficients modulo a prime.

The Functions g_a

Let p be a prime and let q be a positive power of p. Suppose a sequence of functions $g_a\colon \mathbb{Z} \to \mathbb{Z}_p$, $a = 0, 1, 2, \ldots$, satisfies the following three properties:

(i) $g_a(x) = 0$ if $0 \leqslant x < a$,
$= 1$ if $x = a$,

(ii) $g_a(x)$ has period q^{t+1}, where $q^t \leqslant a < q^{t+1}$, and $g_0(x)$ has period 1,

(iii) $g_a(x+1)$ is a linear combination (over $\mathbb{Z}_p$) of $g_i(x)$, $0 \leqslant i \leqslant a$.

THEOREM 1. *A sequence g_a, $a = 0, 1, 2, \ldots$, satisfies* (i)–(iii) *if and only if*

$$g_a(x) \equiv \frac{x(x-1)\cdots(x-a+1)}{a!}$$

$$\overset{\text{def}}{\equiv} \binom{x}{a} \pmod{p}, \qquad a \geqslant 0. \tag{3}$$

Proof. We will prove by induction on a the existence and uniqueness of the g_a. It will follow from the proof that the binomial coefficients $\binom{x}{a}$ $(\operatorname{mod} p)$ satisfy (i)–(iii).

When $a = 0$, conditions (i) and (ii) imply that $g_0(x) = 1$ for all x. Condition (iii) is thus automatically satisfied. Note that in this case $g_0(x) \equiv \binom{x}{0} \equiv 1 \pmod{p}$ for all x.

Suppose now we have shown that the g_i, $0 \leqslant i < a$, exist and are uniquely determined by (i)–(iii). We examine g_a. Condition (iii) asserts

$$g_a(x+1) = \sum_{i=0}^{a} \alpha_i g_i(x), \qquad \alpha_i \in \mathbb{Z}_p,$$

(with all arithmetic in $\mathbb{Z}_p$). Evaluating the above expression at $x = 0, 1, \ldots, a$, and applying (i) to the g_i, $0 \leqslant i \leqslant a$, we obtain

$$\alpha_a = g_a(a+1) - g_{a-1}(a), \qquad \alpha_{a-1} = 1$$

and

$$\alpha_{a-2} = \cdots = \alpha_0 = 0.$$

Thus,

$$g_a(x) = \alpha_a g_a(x-1) + g_{a-1}(x-1).$$

Applying this formula repeatedly to $x \geqslant a$ yields

$$\begin{aligned} g_a(x) &= \alpha_a g_a(x-1) + g_{a-1}(x-1) \\ &= \alpha_a(\alpha_a g_a(x-2) + g_{a-1}(x-2)) + g_{a-1}(x-1) \\ &= \cdots \\ &= \alpha_a^{x-a} g_a(a) + \alpha_a^{x-a-1} g_{a-1}(a) + \alpha_a^{x-a-2} g_{a-1}(a+1) \\ &\quad + \cdots + \alpha_a g_{a-1}(x-2) + g_{a-1}(x-1). \end{aligned} \tag{4}$$

Combining this with condition (ii) gives

$$\begin{aligned} g_a(x) &= g_a(x+q^{t+1}) \\ &= \alpha_a^{x-a+q^{t+1}} g_a(a) + \alpha_a^{x-a-1+q^{t+1}} g_{a-1}(a) + \cdots \\ &\quad + \alpha_a^{q^{t+1}} g_{a-1}(x-1) + \alpha_a^{q^{t+1}-1} g_{a-1}(x) \\ &\quad + \alpha_a^{q^{t+1}-2} g_{a-1}(x+1) + \cdots \\ &\quad + \alpha_a g_{a-1}(x+q^{t+1}-2) + g_{a-1}(x+q^{t+1}-1) \\ &= \alpha_a^{q^{t+1}} g_a(x) + \sum_{0 \leqslant j < a} \beta_j g_j(x), \qquad \text{where} \quad \beta_j \in \mathbb{Z}_p. \end{aligned}$$

Here the last summation follows from (iii) satisfied by g_{a-1}. Evaluating the above expression at $x = 0, 1, \ldots, a$, gives

$$\alpha_a^{q^{t+1}} = 1 \tag{5}$$

and

$$\beta_0 = \beta_1 = \cdots = \beta_{a-1} = 0.$$

This shows that $\alpha_a = \alpha_a^{q^{t+1}}$ is the identity element in $\mathbb{Z}_p$. Therefore, for $x \geqslant a$, we can rewrite (4) as

$$g_a(x) = g_{a-1}(a-1) + g_{a-1}(a) + \cdots + g_{a-1}(x-1).$$

The existence and uniqueness of g_a now follows from that of g_{a-1}. Also, the induction hypothesis $g_{a-1}(x) \equiv \binom{x}{a-1} \pmod p$ implies

$$\begin{aligned} g_a(x) &\equiv \binom{a-1}{a-1} + \binom{a}{a-1} + \cdots + \binom{x-1}{a-1} \\ &\equiv \binom{x}{a} \pmod p. \end{aligned}$$

This proves the theorem. ∎

If g_a took values in some finite field extension of $\mathbb{Z}_p$, (5) would still imply that α_a is the identity element of the field and (4) would imply that g_a actually takes values in the prime field $\mathbb{Z}_p$ because g_0 does. If g_a took values in the ring $\mathbb{Z}/m\mathbb{Z}$, then for given $g_0, \ldots, g_{a-1}$, the number of g_a's satisfying (i)–(iii) is equal to the number of α_a's satisfying (5), namely, the number of units in $\mathbb{Z}/m\mathbb{Z}$ whose orders divide g.c.d. $(q^{t+1}, \phi(m))$.

Note that the functions g_a are independent of q. In fact the function g_a has period p^{t+1}, where $p^t \leqslant a < p^{t+1}$. Since

$$g_a(x+1) = g_a(x) + g_{a-1}(x),$$

then as an immediate consequence we have

FACT 1. *For any integer c,*

$$g_a(x+c) = g_a(x) + \sum_{0 \leqslant i < a} \gamma_i g_i(x)$$

for some elements $\gamma_0, \ldots, \gamma_{a-1}$ in $\mathbb{Z}_p$ depending on c.

A similar formula holds for $g_a(dx)$:

PROPOSITION. *Suppose $a > 0$ and d is any integer. Then*

$$g_a(dx) = d^a g_a(x) + \sum_{0 \leqslant i < a} \alpha_i g_i(x)$$

for some $\alpha_i \in \mathbb{Z}_p$ depending on d.

Proof. Consider the $\mathbb{Z}$-valued functions

$$f_i(x) = \binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!}, \qquad i \geqslant 0,$$

on $\mathbb{Z}$. Clearly, $f_i(x)$ is a polynomial of degree i and $f_0(x), \ldots, f_{a-1}(x)$ span all polynomials over $\mathbb{Q}$ of degree less than a. The polynomial $f_a(dx) - d^a f_a(x)$ is a polynomial of degree less than a with rational coefficients, and hence there are rational numbers $\alpha_0, \ldots, \alpha_{a-1}$ such that

$$f_a(dx) = d^a f_a(x) + \sum_{0 \leqslant i < a} \alpha_i f_i(x). \tag{6}$$

Moreover, we can determine these α_i using the fact that $f_i(x) = 0$ if $0 \leqslant x < i$ and $f_i(i) = 1$ as follows:

$$\alpha_0 = f_a(d \cdot 0) = 0,$$

$$\alpha_i = f_a(di) - \sum_{0 \leqslant j < i} \alpha_j f_j(i) \qquad \text{for } 0 < i < a.$$

This in particular shows that each a_i is in fact an integer. The desired formula for $g_a(dx)$ is (6) modulo p. ∎

There is more to be said about $g_a(dx)$ for the case that p divides d. Write $x = \sum_{i \geqslant 0} x_i p^i$ and $a = \sum_{i \geqslant 0} a_i p^i$ in their base p expansions, where $0 \leqslant x_i, a_i < p$. Lucas' theorem (see [3]) asserts that

$$g_a(x) \equiv \binom{x}{a} \equiv \prod_{i \geqslant 0} \binom{x_i}{a_i} \pmod{p}. \tag{7}$$

The above product is finite since $a_i = 0$ for almost all i. One sees immediately that $g_a(x) = 0$ if p divides x and p does not divide a. Further, if p divides both x and a, then $x_0 = a_0 = 0$ and

$$g_a(x) \equiv \prod_{i \geqslant 1} \binom{x_i}{a_i} \equiv g_{a/p}(x/p) \pmod{p}$$

since $x/p = \sum_{i \geqslant 1} x_i p^{i-1}$ and $a/p = \sum_{i \geqslant 1} a_i p^{i-1}$. This proves

FACT 2.

$$\begin{aligned} g_a(p\,dx) &= 0 && \text{if } p \text{ does not divide } a, \\ &= g_{a/p}(dx) && \text{if } p \text{ divides } a. \end{aligned}$$

PRODUCTS OF THE FUNCTIONS g_a

As observed before, the function $f_a(x) = \binom{x}{a}$, $a \geqslant 0$, is a polynomial of degree a. Thus the product

$$f_a(x) f_b(x) \cdots f_c(x) = \sum_{0 \leqslant i \leqslant a+b+\cdots+c} A_i x^i$$

is a polynomial of degree $a + b + \cdots + c$ with the leading coefficient $1/a!b! \cdots c!$. Since

$$\begin{aligned} \sum_{x \in \mathbb{Z}_p} x^i &= 0 && \text{if } p-1 \text{ does not divide } i \text{ or } i = 0, \\ &= -1 && \text{if } p-1 \text{ divides } i \text{ and } i \neq 0, \end{aligned}$$

we see that, modulo p,

$$\begin{aligned} &\sum_{0 \leqslant x < p} f_a(x) f_b(x) \cdots f_c(x) \\ &\equiv 0 && \text{if } 0 \leqslant a+b+\cdots+c < p-1, \\ &\equiv \frac{-1}{a!b! \cdots c!} && \text{if } a+b+\cdots+c = p-1. \end{aligned}$$

This analysis combined with (7) gives

LEMMA 1. *Suppose* $0 \leqslant a, b, \ldots, c < p^{t+1}$. *Then* $\sum_{0 \leqslant x < p^{t+1}} g_a(x) g_b(x) \cdots g_c(x)$ *is* 0 *if there is an* i, $0 \leqslant i \leqslant t$, *such that* $a_i + b_i + \cdots + c_i < p-1$; *it is equal to* $\prod_{0 \leqslant i \leqslant t} (-1)(a_i! b_i! \cdots c_i!)^{-1}$ *if for all* i, $0 \leqslant i \leqslant t$, $a_i + b_i + \cdots + c_i = p-1$.

Here (as later) $a_i, b_i, \ldots, c_i$ are the ith coefficients of the base p expansions of $a, b, \ldots, c$, respectively. The following two corollaries are immediate consequences.

COROLLARY 1. *If* $a, b, \ldots, c \geqslant 0$ *and* $a + b + \cdots + c < p^{t+1} - 1$ *then* $\sum_{0 \leqslant x < p^{t+1}} g_a(x) g_b(x) \cdots g_c(x) = 0$.

COROLLARY 2. *If* $a, b, \ldots, c \geqslant 0$ *and* $a + b + \cdots + c = p^{t+1} - 1$ *then* $\sum_{0 \leqslant x < p^{t+1}} g_a(x) g_b(x) \cdots g_c(x)$ *is nonzero if and only if* $a_i + b_i + \cdots + c_i = p-1$ *for all* i, $0 \leqslant i \leqslant t$.

Let us consider the integral valued functions $f_a(x) = \binom{x}{a}$. As discussed above, the product $f_a(x) f_b(x) \cdots f_c(x)$ is a polynomial of degree $r = a + b + \cdots + c$ and hence is a linear combination of $f_i(x)$ with $0 \leqslant i \leqslant r$:

$$f_a(x) f_b(x) \cdots f_c(x) = \alpha(a, b, \ldots, c) f_r(x) + \sum_{0 \leqslant i < r} \alpha_i f_i(x), \tag{8}$$

where

$$\alpha(a, b, \ldots, c) = \frac{(a + b + \cdots + c)!}{a!\, b! \cdots c!}$$

(by comparing the leading coefficients of both sides) and α_i, $0 \leqslant i < r$, are rational numbers. Arguing as in the proof of the Proposition, we know that the α's in (8) are integers. Thus (8) remains valid if f is replaced by g. This proves the first assertion of the following result.

LEMMA 3. *Suppose* $a, b, \ldots, c \geqslant 0$. *Let* $r = a + b + \cdots + c$. *Then*

$$g_a(x) g_b(x) \cdots g_c(x) = \sum_{0 \leqslant i \leqslant r} \alpha_i g_i(x), \qquad \alpha_i \in \mathbb{Z}_p,$$

with

$$\alpha_r = \alpha(a, b, \ldots, c) \equiv \frac{(a + b + \cdots + c)!}{a! b! \cdots c!} \pmod{p}.$$

Moreover, α_r *is nonzero if and only if* $a_i + b_i + \cdots + c_i \leqslant p-1$ *for all* $i \geqslant 0$.

Proof. To prove the second assertion, let $r^* = p^{t+1} - 1 - r$, where $p^t \leqslant r < p^{t+1}$. Consider

$$\sum_{0 \leqslant x < p^{t+1}} g_{r^*}(x)\, g_a(x)\, g_b(x) \cdots g_c(x)$$

$$= \sum_{0 \leqslant i \leqslant r} \alpha_i \sum_x g_{r^*}(x)\, g_i(x)$$

$$= \alpha_r \sum_x g_{r^*}(x)\, g_r(x)$$

by Corollary 1 (since $r^* + i < p^{t+1} - 1$ if $i < r$). Lemma 1 implies that $\sum_{0 \leqslant x < p^{t+1}} g_{r^*}(x)\, g_r(x)$ is nonzero. Thus $\alpha_r \neq 0$ if and only if $\sum_{0 \leqslant x < p^{t+1}} g_{r^*}(x)\, g_a(x)\, g_b(x) \cdots g_c(x) \neq 0$, which happens, by Corollary 2, if and only if $r_i + a_i + b_i + \cdots + c_i = p - 1$ for $0 \leqslant i \leqslant t$, or equivalently, $a_i + b_i + \cdots + c_i \leqslant p - 1$ for all $i \geqslant 0$. ▮

LEMMA 4. *If $g(x) = \sum_{0 \leqslant i \leqslant r} \alpha_i g_i(x)$ with $r > 0$ and $\alpha_r \neq 0$, then there are at most r consecutive integers at which g takes the same value.*

Proof. Suppose not. Then there are at least $r + 1$ consecutive integers at which g takes the same value, say β. Replacing α_0 by $\alpha_0 - \beta$, we may assume that $\beta = 0$. Let $r^* = p^{t+1} - 1 - r$, where $p^t \leqslant r < p^{t+1}$. There is an integer c such that $\tilde{g}(x) = g(x + c)$ vanishes for $r^* \leqslant x \leqslant r^* + r$. We know from Fact 1 that

$$\tilde{g}(x) = \alpha_r g_r(x) + \sum_{0 \leqslant i < r} \beta_i g_i(x), \qquad \beta_i \in \mathbb{Z}_p.$$

Now consider the sum

$$\sum_{0 \leqslant x < p^{t+1}} g_{r^*}(x)\, \tilde{g}(x).$$

It is equal to zero since $g_{r^*}(x) = 0$ for $0 \leqslant x < r^*$ and $\tilde{g}(x) = 0$ for $r^* \leqslant x \leqslant r^* + r = p^{t+1} - 1$. On the other hand, Corollaries 1 and 2 imply that

$$\sum_{0 \leqslant x < p^{t+1}} g_{r^*}(x) \tilde{g}(x)$$

$$= \alpha_r \sum_x g_{r^*}(x)\, g_r(x) + \sum_{0 \leqslant i < r} \beta_i \sum_x g_{r^*}(x)\, g_i(x)$$

$$= \alpha_r \sum_x g_{r^*}(x)\, g_r(x) \neq 0.$$

This is impossible. Hence there can be at most r consecutive integers at which $g(x)$ takes the same value. ▮

PARTITIONING $\mathbb{Z}^n$

We have now developed sufficient machinery to be able to partition $\mathbb{Z}^n$ so that there are no long "homogeneous" (i.e., belonging to one class of the partition) consecutive collinear sets. Let n and r denote fixed integers exceeding 1.

THEOREM 2.

$$\rho_r(n) \leqslant \frac{2n}{\log n} \frac{r \log r}{(r-1)^2} (1 + o(1)), \tag{9}$$

where the $o(1)$ term depends on r but not on n.

Proof. The technique will be a variation of that used in [5]. For ease of notation we introduce a new variable M. At the last step we will describe how M and n are related. Let p denote the greatest prime not exceeding r. For each m, $M < m \leqslant Mp$, write $m = \sum_{i \geqslant 0} m_i p^i$ in its base p expansion and define $w = w(m) = \sum_i m_i$.

To begin with, we need a homogeneous polynomial $f_m(x_1,..., x_w)$ of degree w over $\mathbb{Z}_p$ which vanishes only at $(0,..., 0)$. The following construction (suggested by A. M. Odlyzko; also see [1]) supplies such a polynomial. Choose an element α_m from an algebraic closure of $\mathbb{Z}_p$ such that the field $\mathbb{Z}_p(\alpha_m)$ has degree w over $\mathbb{Z}_p$. Then the *norm* of $x_1 + x_2\alpha_m + \cdots + x_w\alpha_m^{w-1}$ with $x_1,..., x_w$ in $\mathbb{Z}_p$ is a homogeneous polynomial in $x_1,..., x_w$ of degree w with coefficients in $\mathbb{Z}_p$. Denote this polynomial by

$$f_m(x_1,..., x_w) = \sum \gamma(a_1,..., a_w)\, x_1^{a_1} \cdots x_w^{a_w},$$

where the sum is taken over all compositions of $w = a_1 + \cdots + a_w$, $a_i \geqslant 0$. Since $1, \alpha_m,..., \alpha_m^{w-1}$ are linearly independent over $\mathbb{Z}_p, f_m$ is zero if and only if $x_1 = \cdots = x_w = 0$ in $\mathbb{Z}_p$, which is what was required.

Next, to each composition $w = a_1 + \cdots + a_w$, we associate a composition of $m = b_1 + \cdots + b_w$ such that:

(i) The sum of the ith coefficients in the base p expansions of the b_k's is m_i;

(ii) $w(b_j) = a_j$ (where as previously mentioned, $w(x)$ denotes the sum of the base p coefficients of x).

There are usually many such compositions of m. We fix some particular choice.

Note that for any integer d, $d^{b_i} \equiv d^{a_i} \pmod{p}$ since $d^p \equiv d \pmod{p}$.

Finally, define the function

$$h_m(x_1, \ldots, x_w) = \sum \gamma(a_1, \ldots, a_w)\, \alpha(b_1, \ldots, b_w)^{-1} g_{b_1}(x_1) \cdots g_{b_w}(x_w),$$

where the sum is taken over all compositions of $w = a_1 + \cdots + a_w$ and the $\alpha(b_1, \ldots, b_w)$ come from Lemma 3, i.e.,

$$\alpha(b_1, \ldots, b_w) \equiv \frac{m!}{b_1! \cdots b_w!} \pmod{p}.$$

Observe that by our construction, the criterion that $\alpha(b_1, \ldots, b_w)$ is invertible in $\mathbb{Z}_p$ given in Lemma 3 is satisfied.

The following result shows that on each collinear set (= line) of lattice points in $\mathbb{Z}^w$, h_m is a linear combination of g_i with $0 \leqslant i \leqslant m$. Moreover, the coefficient of g_m will be explicitly given in terms of f_m and the direction numbers of the line.

LEMMA 5. *For integers c_i, d_i, $1 \leqslant i \leqslant w$, the function*

$$\tilde{h}_m(x) = h_m(c_1 + d_1 x, \ldots, c_w + d_w x)$$

is equal to

$$f_m(d_1, \ldots, d_w)\, g_m(x) + \sum_{0 \leqslant i < m} \alpha_i g_i(x)$$

for some $\alpha_0, \ldots, \alpha_{w-1}$ in $\mathbb{Z}_p$ depending on the c_i and d_i. Furthermore, if p divides g.c.d. $(d_1, \ldots, d_w)$ *then*

$$\tilde{h}_m = \sum_{0 \leqslant i \leqslant m/p} \alpha_i g_i.$$

Proof. It follows from Fact 1 and the Proposition that

$$g_a(c + dx) = d^a g_a(x) + \sum_{0 \leqslant i < a} \beta_i(a)\, g_i(x)$$

with $\beta_i(a)$ depending on c, d and a. Thus

$$\begin{aligned} &g_{b_1}(c_1+d_1x)\cdots g_{b_w}(c_w+d_wx)\\ &\quad=\Big(d_1^{b_1}g_{b_1}(x)+\sum_{0\leqslant i<b_1}\beta_i(b_1)\,g_i(x)\Big)\\ &\qquad\cdots\Big(d_w^{b_w}g_{b_w}(x)+\sum_{0\leqslant i<b_w}\beta_i(b_w)\,g_{b_w}(x)\Big)\\ &\quad=d_1^{b_1}\cdots d_w^{b_w}g_{b_1}(x)\cdots g_{b_w}(x)+\text{linear combinations of}\\ &\qquad g_a(x)\,g_b(x)\cdots g_c(x)\quad\text{with}\quad a+b+\cdots c<m\\ &\quad=d_1^{a_1}\cdots d_w^{a_w}\alpha(b_1,\dots,b_w)\,g_m(x)+\sum_{0\leqslant i<m}\beta_i\,g_i(x) \end{aligned}$$

by Lemma 3, where $\beta_i\in\mathbb{Z}_p$. Substituting this into $\bar{h}_m$ yields

$$\begin{aligned} \bar{h}_m(x)&=h_m(c_1+d_1x,\dots,c_w+d_wx)\\ &=\sum\gamma(a_1,\dots,a_w)\,\alpha(b_1,\dots,b_w)^{-1}\\ &\quad\times g_{b_1}(c_1+d_1x)\cdots g_{b_w}(c_w+d_wx)\\ &=\sum\gamma(a_1,\dots,a_w)\,d_1^{a_1}\cdots d_w^{a_w}g_m(x)+\sum_{0\leqslant i<m}\alpha_i\,g_i(x)\\ &=f_m(d_1,\dots,d_w)\,g_m(x)+\sum_{0\leqslant i<m}\alpha_i\,g_i(x) \end{aligned}$$

for some $\alpha_0,\dots,\alpha_{m-1}$ in $\mathbb{Z}_p$. This proves the first assertion.

If p divides g.c.d. $(d_1,\dots,d_w)$ then by Facts 1 and 2 and the Proposition,

$$g_{b_i}(c_i+d_ix)=\sum_{0<j\leqslant(b_i)/p}\beta_j(b_i)\,g_j(x)$$

and hence, $g_{b_1}(c_1+d_1x)\cdots g_{b_k}(c_k+d_kx)$ is a linear combination of products $g_a(x)\,g_b(x)\cdots g_c(x)$ with

$$a+b+\cdots+c\leqslant\frac{b_1}{p}+\frac{b_2}{p}+\cdots+\frac{b_w}{p}=\frac{m}{p}.$$

Thus, by Lemma 3, it is in fact a linear combination of $g_i(x)$ with $0\leqslant i\leqslant m/p$. Consequently, the same is true for $\bar{h}_m(x)$. This proves Lemma 5. ∎

To complete the proof of Theorem 2, we combine the h_m, $M<m\leqslant Mp$, as

follows. For $n=\sum_{M<m\leqslant Mp} w(m)$, define a partition of $\mathbb{Z}^n$ into p classes by the mapping

$$\begin{aligned}\chi(x_{M+1,1},\ldots,x_{M+1,w(M+1)},\ldots,x_{Mp,1},\ldots,x_{Mp,w((Mp))})\\ =\sum_{M<m\leqslant Mp} h_m(x_{m,1},\ldots,x_{m,w(m)}) \pmod p\end{aligned}$$

(i.e., the classes of the partition are $\chi^{-1}(i)$, $i\in\mathbb{Z}_p$).

Let us estimate the length of the longest homogeneous set of consecutive collinear points. Any such set can be parametrized by $x_{m,j}=c_{m,j}+d_{m,j}x$ with $c_{m,j}$, $d_{m,j}$ in $\mathbb{Z}$ and g.c.d.$_{m,j}$ $(d_{m,j})=1$. We claim that there are at most Mp consecutive lattice points on which χ takes the same value. This will imply $L(\chi)\leqslant Mp$ and hence,

$$\rho_r(n)\leqslant Mp. \tag{10}$$

To prove the claim, consider the function $\tilde{\chi}(x)$ of the single variable x given by

$$\tilde{\chi}(x)=\sum_{M<m\leqslant Mp} h_m(c_{m,1}+d_{m,1}x,\ldots,c_{m,w(m)}+d_{m,w(m)}x). \tag{11}$$

Let a denote the largest $m>M$ such that not all $d_{m,1},\ldots,d_{m,w(m)}$ are divisible by p. Since g.c.d.$_{m,j}$ $(d_{m,j})=1$ then such an $a\leqslant Mp$ exists. Thus, by Lemma 5, for $a<m\leqslant Mp$, $h_m(c_{m,1}+d_{m,1}x,\ldots,c_{m,w(m)}+d_{m,w(m)}x)$ is a linear combination of g_i with $0\leqslant i\leqslant m/p\leqslant M<a$. For $M<m<a$, $h_m(c_{m,1}+d_{m,1}x,\ldots,c_{m,w(m)}+d_{m,w(m)}x)$ is a linear combination of g_i with $0\leqslant i<a$. Finally,

$$\begin{aligned}h_a(c_{a,1}+d_{a,1}x,\ldots,c_{a,w(a)}+d_{a,w(a)}x)\\ =f_a(d_{a,1},\ldots,d_{a,w(a)})\,g_a(x)+\sum_{0\leqslant i<a}\alpha_i g_i(x), \qquad \alpha_i\in\mathbb{Z}_p.\end{aligned}$$

Substituting these into (11) yields

$$\tilde{\chi}(x)=f_a(d_{a,1},\ldots,d_{a,w(a)})\,g_a(x)+\sum_{0\leqslant i<a}\beta_i g_i(x).$$

It follows from the choice of a and properties of f_a that the coefficient of g_a is nonzero. The desired result now follows at once from Lemma 4.

The last step in the proof is to eliminate M and p from the estimate in (10). It is well known (see [2]) that

$$\sum_{k=1}^{m} w(k)=(1+o(1))\frac{(p-1)}{2}\frac{m\log m}{\log p}$$

as $m \to \infty$. Thus,

$$n = (1 + o(1)) \frac{(p-1)^2}{2 \log p} M \log M. \tag{12}$$

Inverting (12) and using the fact that the ratio of consecutive primes tends to 1, we obtain (9). This completes the proof of Theorem 2. ∎

Concluding Remarks

We should note that the construction in Theorem 2 shows that (9) actually applies to collinear sets $x_i = c_i + d_i x$, $x = 0, 1, 2, \ldots$, for which g.c.d. $(d_1, \ldots, d_n) \not\equiv 0 \pmod p$ (i.e., it is not necessary that the g.c.d. be 1).

We have no idea what the truth concerning $\rho_r(n)$ is. The gap between the known upper and lower bounds is still enormous. It seems very likely that $\rho_r(n) = o(n^\varepsilon)$ for every $\varepsilon > 0$, for example, but new ideas will be required to prove this.

References

1. Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.
2. L. E. Bush, An asymptotic formula for the average sum of the digits of integers, *Amer. Math. Monthly* **47** (1940), 154–156.
3. L. E. Dickson, "History of the Theory of Numbers," Vol. 1, p, 271, Chelsea, New York, 1952.
4. A. W. Hales and R. I. Jewett, Regularity and positional games, *Trans. Amer. Math. Soc.* **106** (1963), 222–229.
5. J. L. Paul, Partitioning the lattice points in $\mathbb{R}^n$, *J. Combin. Theory Ser. A* **26** (1979), 238–248.