TWO COMBINATORIAL THEOREMS ON ARITHMETIC PROGRESSIONS

By Wolfgang M. Schmidt

1. **Introduction.** According to a well-known theorem of van der Waerden [6] there exists an $m(k, l)$ defined for integers $k \geq 2$, $l \geq 3$, such that if we split the integers between 1 and m into k classes, at least one class contains an arithmetic progression of l distinct elements. We shall prove

Theorem 1. *For some absolute constant* $c > 0$,

$$m(k, l) \geq k^{l - c(l \log l)^{\frac{1}{2}}}. \tag{1}$$

For large l this is an improvement of the estimate

$$m(k, l) \geq [2(l-1)k^{l-1}]^{\frac{1}{2}} \tag{2a}$$

given by Erdös and Rado [2] and of the estimate

$$m(k, l) \geq lk^{C \log k} \tag{2b}$$

of Moser [4].

Throughout, $P, Q, \cdots$ will denote arithmetic progressions of l distinct integers between 1 and m. Consider real numbers α between 0 and 1 written in scale $k : \alpha = 0, \alpha_1\alpha_2 \cdots$. Write $N(\alpha; k, l, m)$ for the number of progressions $P = \{p_1, \cdots, p_l\}$ such that

$$\alpha_{p_1} = \alpha_{p_2} = \cdots = \alpha_{p_l}.$$

Theorem 2. *Keep* $k, l, \epsilon > 0$ *fixed. Then for almost every* α,

$$N(\alpha; k, l, m) = m^2 \frac{k^{1-l}}{2(l-1)} + O(m \log^{\frac{3}{2}+\epsilon} m). \tag{3}$$

2. **The idea of the proof of Theorem 1.** There is a 1-1 correspondence between divisions of $1, \cdots, m$ into classes $C_1, \cdots, C_k$ and functions $f(x)$ defined on $1, \cdots, m$ whose values are integers between 1 and k. We write

$$f(\sigma) = j$$

for a set σ of integers between 1 and m if $f(x) = j$ for every $x \in \sigma$. Put

$$P \mid f$$

if $f(P)$ is defined, i.e., if $f(p_1) = \cdots = f(p_l)$ for the elements $p_1, \cdots, p_l$ of P. In this terminology Theorem 1 means that for $m < k^{l - c(l \log l)^{\frac{1}{2}}}$ there exists some f such that $P \mid f$ for no P.

Received May 19, 1961.

Let u be a fixed integer in the range $1 \leq u < l/2$. We set

$$f[P] = j$$

if there is a subset σ of P of at least $l - u$ elements having $f(\sigma) = j$. For integers j in $1 \leq j \leq k$ define $j+$ by

$$j + = \begin{cases} j + 1, & \text{if } j < k \\ 1, & \text{if } j = k. \end{cases}$$

We say *f is of type F_j* $(j = 1, \cdots, k)$ if there exists a Q and $P_1, \cdots, P_r$, $l \geq r \geq u + 1$, having $P_i \neq P_t$ for $i \neq t$, with the following properties.

$$f[P_i] = j \qquad (1 \leq i \leq r), \tag{4a}$$

and the elements $q_1, \cdots, q_l$ of Q can be ordered in such a way that

$$q_i \in P_i \qquad (1 \leq i \leq r) \tag{4b}$$

$$f(q_i) = j+ \qquad (r + 1 \leq i \leq l). \tag{4c}$$

It may happen that $r = l$, and in this case the last condition is to be omitted. f is said to be of type F if it is of at least one of the types $F_1, \cdots, F_k$.

Lemma 1. *If there exists an f not of type F, then there exists a function g such that $P \mid g$ for no P.*

Proof. Write U for the set of $P - s$ where $f[P]$ is defined. With each $P \in U$ associate some $x = x(P) \in P$ having $f(x) = f[P]$. Define the function g by

$$g(x) = \begin{cases} f(x) + & \text{if } x = x(P) \text{ for at least one } P \in U, \\ f(x) & \text{otherwise.} \end{cases}$$

We claim that $Q \mid g$ for no Q.

Otherwise, if $Q \mid g$, assume $g(Q) = 1$. $f[Q] = 1$ would imply $f(x(Q)) = 1$, $g(x(Q)) = 1 + = 2$, a contradiction. But if $f[Q]$ is not 1, then there are at least $u + 1$ integers $x \in Q$ with $f(x) \neq 1$. Write $x_1, \cdots, x_r (r \geq u + 1)$ for the elements of Q having $f(x) \neq 1$, $y_{r+1}, \ldots, y_l$ for the elements of Q having $f(y) = 1$, if such integers exist. Now each x_i belongs to some P_i with $f[P_i] = f(x_i)$. $1 = g(x_i) = f(x_i) +$ implies $f[P_i] = f(x_i) = k$. Therefore f would be of type F_k, a contradiction.

To prove Theorem 1 it will be sufficient to show the existence of a function f not of type F. We shall derive bounds for the number of functions of type F and shall show in §5 that if u is the integral part of $(l/\log l)^{\frac{1}{2}}$ and if (1) holds, then the number of such functions is smaller than k^m, the total number of functions f.

3. **Auxiliary lemmas on arithmetic progressions.** Besides progressions $P, Q, \cdots$ of l elements we have to study arithmetic progressions R of an arbitrary

number $z = z(R) \geq 2$ of elements which are integers between 1 and m. Progressions R with $z(R) = 2$ are pairs of integers. Generally, $z(\sigma)$ will denote the number of elements of any set σ of integers. Write $d(R)$ for the common difference $r_2 - r_1 = r_3 - r_2 = \cdots$ of the elements $r_1 < r_2 < \cdots < r_z$ of R. The letter T will be reserved for progressions T having

$$l \leq z(T) < 2l. \tag{5}$$

$R_1 \cap R_2$ is again an arithmetic progression unless $z(R_1 \cap R_2) \leq 1$.

LEMMA 2. *Let* R_1, R_2 *be progressions and put* $z_i = z(R_i)$, $d_i = d(R_i)$, $d_i = e_i d (i = 1, 2)$ *where* $d =$ g.c.d. (d_1, d_2). *Then*

$$z(R_1 \cap R_2) \leq \min\left(\frac{z_1 - 1}{e_2} + 1, \frac{z_2 - 1}{e_1} + 1\right). \tag{6}$$

Proof. We may assume $z(R_1 \cap R_2) \geq 2$. Then $R_1 \cap R_2$ is a progression having $d(R_1 \cap R_2) = e_1 e_2 d = e_2\, d(R_1)$. Hence

$$z(R_1 \cap R_2) \leq \frac{z_1 - 1}{e_2} + 1.$$

LEMMA 3. *Let* R_1, R_2, R_3 *be arithmetic progressions having* $z_i = z(R_i) \geq l (i = 1, 2, 3)$ *and different* d_1, d_2, d_3 *where* $d_i = d(R_i) (i = 1, 2, 3)$. *Then*

$$z(R_1 \cup R_2 \cup R_3) \geq 2l - 5. \tag{7}$$

Proof. We may assume $z_1 = z_2 = z_3 = l$. Let i, j, t be a permutation of the integers 1, 2, 3. We define $d_{ij} = d_{ji}$, e_{ij}, e_{ji}, e_t by

$$d_{ij} = d_{ji} = \text{g.c.d.} \quad (d_i, d_j),$$

$$d_i = e_{ij}\, d_{ij}, \qquad d_j = e_{ji}\, d_{ij},$$

$$e_t = \max(e_{ij}, e_{ji}).$$

Lemma 2 implies $z(R_i \cap R_j) \leq (l - 1)/e_t + 1$. This gives

$$z(R_1 \cup R_2 \cup R_3) \geq 3l - l\left(\frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3}\right) - 3.$$

Hence the lemma is true if

$$\frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3} \leq 1. \tag{8}$$

We may assume that (8) does not hold and that at least one of e_1, e_2, e_3, let's say e_3, equals 2. Then either $e_1 \geq 3$, $e_2 \geq 3$ or we may assume $e_1 = 2$. But $e_3 = e_1 = 2$ implies $e_2 = 4$. Hence we have

$$e_3 = 2 \quad \text{and} \quad \begin{cases} \text{either} \quad e_1 \geq 3, \quad e_2 \geq 3 \\ \\ \text{or} \quad e_1 = 2, \quad e_2 = 4. \end{cases} \tag{9}$$

We have either $e_{12} = 2$ or $e_{21} = 2$, therefore either $d_1 = 2d_2$ or $d_2 = 2d_1$. In the first case of (9) we may assume $d_2 = 2d_1$ because we may change the roles of R_1, R_2. In the second case we have $d_1 = 2d_2 = 4d_3$ or $d_3 = 2d_2 = 4d_1$ and again we may assume $d_2 = 2d_1$.

If R is a progression write $R^1(R^2)$ for the set of $x \in R$ such that $x < r(x > r)$ for every $r \in R_1$. Write R^0 for the set of $x \in R$ such that $r \leq x \leq r'$ for suitable elements r, r' of R_1. Then R is the disjoint union of R^0, R^1, R^2 and R^i is an arithmetic progression with $d(R^i) = d(R)$ unless $z(R^i) \leq 1 (i = 0, 1, 2)$.

We may assume

$$r = z(R_1 \cap R_2) \geq 2, \qquad s = z(R_1 \cap R_3) \geq 2,$$

because otherwise $R_1 \cup R_2$ or $R_1 \cup R_3$ would have at least $2l - 1$ elements. We observe

$$r \leq l/2 + 1, \qquad s \leq l/e_2 + 1. \tag{10}$$

$d_2 = 2d_1$ implies $R_2^0 = R_1 \cap R_2$. This gives

$$z(R_2^1) + z(R_2^2) = l - r. \tag{11}$$

Now $d(R_1 \cap R_3) = e_{13}\, d(R_3) = e_{13}\, d(R_3^0)$. Hence

$$z(R_3^0) \geq e_{13} z(R_1 \cap R_3) - 1 = e_{13} s - 1 \geq 2s - 1$$

unless $e_{13} = 1$, $d_1 \mid d_3$. Thus

$$z(R_3^1) + z(R_3^2) \leq l - 2s + 1 \tag{12}$$

unless $d_1 | d_3$.

We distinguish two cases.

a) $e_1 = e_{32}$. Then $R_2^i \cap R_3$ consists of at most $z(R_2^i)/e_{32} + 1$ elements, therefore $(R_2^1 \cup R_2^2) \cap R_3$ of at most $(l-r)/e_1 + 2$ elements. Now $z(R_1 \cup R_2) = 2l - r$ and the number of integers of R_3 belonging to neither R_1 nor R_2 is at least $l - s - (l - r)/e_1 - 2$. Thus

$$\begin{aligned} z(R_1 \cup R_2 \cup R_3) &\geq 3l - r - s - (l - r)/e_1 - 2 \\ &\geq 3l - l/e_1 - l/e_2 - (l/2 + 1)(1 - 1/e_1) - 3 \\ &\geq 3l - 4 - l(1/2 + 1/2e_1 + 1/e_2) \\ &\geq 2l - 4. \end{aligned}$$

b) $e_1 = e_{23}$. This means $d_2 > d_3$. We observe $d_1 \nmid d_3$ because otherwise $d_2 > d_3 \geq 2d_1$, which is impossible. $R_3^i \cap R_2$ has at most $z(R_3^i)/e_{23} + 1$; therefore $(R_3^1 \cup R_3^2) \cap R_2$ at most $(l - 2s)/e_1 + 3$ elements. We obtain the lower bound

$$\begin{aligned} 3l - r - s - (l - 2s)/e_1 - 3 &\geq 2l + l/2 - l/e_1 - l/e_2(1 - 2/e_1) - 5 \\ &= 2l - 5 + l/2(1 - 2/e_1)(1 - 2/e_2) \\ &\geq 2l - 5. \end{aligned}$$

A *structure* S will mean either a progression T having $z(T) > l$ or the union of two progressions T_1, T_2 which have at least two common elements and satisfy $d(T_1) \neq d(T_2)$. A *superstructure* is the union of three progressions T_1, T_2, T_3 such that $z(T_1 \cap T_2) \geq 2$, $z((T_1 \cup T_2) \cap T_3) \geq 2$ and either $d(T_1)$, $d(T_2)$, $d(T_3)$ are all different or T_1, T_3 have no common element.

$c_1, c_2, \cdots$ will denote positive constants.

LEMMA 4.

i) *The number of progressions P does not exceed m^2. The number of T's is at most $m^2 l$.*

ii) *The number of P containing a fixed integer x does not exceed ml.*

iii) *The number of progressions T or structures S containing fixed integers $x \neq y$ is at most l^{c_1}.*

iv) *The number of superstructures is bounded by $m^2 l^{c_2}$.*

Proof.

i) $P = \{p_1 < \cdots < p_l\}$ is determined by p_1, p_l which gives the bound m^2. The number of T with given $z = z(T)$ is again at most m^2. Summing over z from l to $2l - 1$ we obtain the desired bound.

ii) If $P = \{p_1 < \cdots < p_l\}$ and $x \varepsilon P$, then $x = p_i$ for some i. P is determined by i and p_{i+}. This gives at most ml possibilities.

iii) For given $z = z(T)$, $T = \{t_1 < \cdots < t_z\}$ is determined by i and j where $x = t_i$, $y = t_j$. This gives less than z^2 choices. Summing over z from l to $2l - 1$ we obtain the bound $4l^3$.

For structures S consisting of a single T we obtain the same estimate. Now let S be $T_1 \cup T_2$. For given $z_i = z(T_i)(i = 1, 2)$, if

$$T_1 = \{t_1 < \cdots < t_{z_1}\}, \qquad T_2 = \{s_1 < \cdots < s_{z_2}\},$$

write

$$t_{z_1+1} = s_1, \cdots, t_{z_1+z_2} = s_{z_2}.$$

Now for $x \varepsilon S$, $y \varepsilon S$ there exist $i_1, i_2, i_3, i_4, j_1, j_2$ such that

$$t_{i_1} = s_{j_1}, \qquad t_{i_2} = s_{j_2}, \qquad t_{i_3} = x, \qquad t_{i_4} = y.$$

Since S is determined by $i_1, \cdots, i_4, j_1, j_2$ and since each of $i_1, \cdots i_4, j_1, j_2$ is between 1 and $4l$, we obtain the bound $(4l)^6$. Summing over z_1, z_2 and adding $4l^3$ we obtain the bound l^{c_1}.

iv) The proof of iv) is similar and can be left to the reader.

Put

$$P \wedge Q \tag{13}$$

if $d(P) = d(Q)$ and if P, Q have at least one common element. Now if U is a set of progressions P, set $\bar{U}$ for the set of progressions R such that R is the union of progressions $P_1, \cdots, P_t$ of U where $P_1 \wedge P_2, \cdots, P_{t-1} \wedge P_t$. We say *$R$ is built of $P_1, \cdots, P_t$*. Write U^* for the set of maximal progressions in $\bar{U}$, that is, the set of $R \varepsilon \bar{U}$ where $R' \varepsilon \bar{U}$, $R' \supseteq R$, $d(R') = d(R)$ implies $R' = R$. For example, let l be 4 and let U consist of $P_1 = \{1, 3, 5, 7\}$, $P_2 = \{7, 9, 11, 13\}$, $P_3 = \{11, 13, 15, 17\}$. Then $\bar{U}$ consists of P_1, P_2, P_3, $P_1 \cup P_2$, $P_2 \cup P_3$, $P_1 \cup P_2 \cup P_3$ while U^* consists of $P_1 \cup P_2 \cup P_3$ only.

LEMMA 5. *Suppose $S = T_1 \cup T_2$ is a structure where T_1 and T_2 are built of $P_1, \cdots, P_{h_1}$ and $P_1', \cdots, P_{h_2}'$ respectively.* Then

$$z(S) \geq l + h_1 + h_2 - 2. \tag{14}$$

Proof. Clearly, $z_i = z(T_i) \geq l + h_i - 1 (i = 1, 2)$. Lemma 2 yields

$$z(T_1 \cap T_2) \leq (z_2 - 1)/2 + 1 = (z_2 + 1)/2.$$

Thus

$$\begin{aligned} z(T_1 \cup T_2) &\geq z_1 + (z_2 - 1)/2 \\ &\geq l + h_1 + (l + h_2)/2 - 2 \\ &\geq l + h_1 + h_2 - 2. \end{aligned}$$

We used $h_2 \leq l$, an inequality which follows from $z(T) < 2l$.

4. **Bounds for the number of certain functions.** Denote the set of P having $f[P] = j$ by $U_j = U_j(f) (j = 1, \cdots, k)$. *$f$ is of type G_j* if there is an R in $\bar{U}_j$ having $z(R) \geq 2l$. f is said to be *of type H_j* if there is a superstructure $T_1 \cup T_2 \cup T_3$ whose progressions T_1, T_2, T_3 belong to $\bar{U}_j (j = 1, \cdots, k)$.

Write $e_k(\alpha)$ for k^α.

LEMMA 6. *The number $| G_j |$ of f of type $G_j (j = 1, \cdots, k)$ is less than*

$$m^2 e_k(m - 2l + c_3 u \log l). \tag{15}$$

Proof. Assume $j = 1$. Suppose R is in $\bar{U}_1$, $z(R) \geq 2l$ and R is built of $P_1, \cdots, P_t$, $P_i \varepsilon U_1$. We may assume $P_1, \cdots, P_t$ are ordered in such a way that their smallest elements $p^{(1)}, \cdots, p^{(t)}$ satisfy $p^{(1)} < p^{(2)} < \cdots < p^{(t)}$. There is a smallest $p^{(i)}$ such that $p^{(1)} + (l - 1) d < p^{(i)}$, where $d = d(R)$. Then $p^{(1)} + (l - 1) d < p^{(i)} \leq p^{(1)} + (2l - 1) d$ and $R' = P_1 \cup \cdots \cup P_i$ is an $R' \varepsilon \bar{U}$ having $2l \leq z(R') \leq 3l - 1$. Hence we may assume

$$2l \leq z(R) \leq 3l - 1. \tag{16}$$

There are at most m^2 progressions P_1. Because of (16), there are not more than l possibilities for P_t once P_1 is given. On P_1, P_t there are $(l - u)$-tuples σ_1, σ_t of integers such that $f(\sigma_1) = f(\sigma_t) = 1$. There are $C_{l-u}^l \leq l^u$ choices for σ_1 and for σ_t. There are $m - 2l + 2u$ integers in $1 \leq x \leq m$ outside σ_1, σ_t, and this implies that there exist exactly $e_k(m - 2l - 2u)$ functions f having $f(\sigma_1 \cup \sigma_t) = 1$. Altogether, we obtain

$$| G_1 | \leq m^2 l l^{2u} e_k(m - 2l + 2u) \leq m^2 e_k(m - 2l + c_3 u \log l).$$

LEMMA 7. *The number* $| H_j |$ *of* f *of type* $H_j (j = 1, \cdots, k)$ *satisfies*

$$| H_j | \leq m^2 e_k(m - 2l + c_4 u \log l). \tag{17}$$

Proof. We assume $j = 1$. Lemma 4 implies that the number of superstructures $T_1 \cup T_2 \cup T_3$ is at most $m^2 l^{c_3}$.

Now any $T \varepsilon \bar{U}_j$ is built of $P_1, \cdots, P_t$ of U_j where we may assume the smallest elements $p^{(i)}$ of P_i satisfy $P^{(1)} < \cdots < p^{(t)}$. Either $t = 1$ and $T = P_1$ or $t > 1$, $T = P_1 \cup P_t$, because $p^{(t)} \leq p^{(1)} + (l - 1)\, d$, since $z(T) < 2l$ for every T. Hence there exists a $2u$-tuple τ in T such that $f(x) = 1$ for x not in τ.

There exist such sets τ_1, τ_2, τ_3 in T_1, T_2, T_3. For each τ_i we have at most $(2l)^{2u}$ choices in T_i. Now if σ is the set of integers in the superstructure which are not in τ_1, τ_2, τ_3, then $f(\sigma) = 1$ and $z(\sigma) \geq 2l - 5 - 6u$ according to Lemma 3 and the definition of superstructures. There are altogether at most $m^2 l^{c_3} (2l)^{6u}$ ways to choose σ, and the number of f having $f(\sigma) = 1$ does not exceed $e_k(m - 2l + 6u + 5)$. This proves the lemma.

Now let f be of type F_1 but not of type G_1 or H_1. There will be progressions $Q, P_1, \cdots, P_r$ associated with f satisfying (4a), (4b) and (4c). There could be several sets of progressions $Q, P_1, \cdots$ with these properties; we pick just one such set. Write V for the set of progressions $P_1, \cdots, P_r$. Since f is not of type G_1, $z(R) < 2l$ for every $R \varepsilon V^*$. Denote the elements of V^* by $T_1, \cdots, T_t$. Write W for the set of structures S which either

a) are of type $S = T_i \cup T_j$, or

b) of type $S = T_i$, $z(T_i) > l$, and there exists no $T_j \neq T_i$ such that $T_i \cup T_j$ is a structure. Write X for the set of P in V which are not part of any structure of W. Denote the elements of W by $S_1, \cdots, S_s$, the elements of X by $Q_1, \cdots, Q_q$.

LEMMA 8.

i) *If* $T \varepsilon \bar{V}$ *and if* $S \varepsilon W$ *and either* $S = T_i$, $T \not\subseteq T_i$, *or* $S = T_i \cup T_j$, $T \not\subseteq T_i$, $T \not\subseteq T_j$, *then* $z(S \cap T) \leq 1$.

ii) *Each* $P \varepsilon V$ *is either part of exactly one* S_j *or* $P = Q_j$ *for one* Q_j.

iii) $Q_i \neq Q_j$ *implies* $z(Q_i \cap Q_j) \leq 1$. $S_i \neq S_j$ *implies* $z(S_i \cap S_j) \leq 2$.

Proof.

i) Assume $z(S \cap T) \geq 2$. If $S = T_i$, then $d(T) = d(T_i)$ would imply that $T \cup T_i \varepsilon \bar{V}$ and T_i would not be maximal, while $d(T) \neq d(T_i)$ would imply that $T \cup T_i$ were a structure, and T_i would not be in W, because of the condition in b). If $S = T_i \cup T_j$, then our argument is similar. $T_i \cup T_j \cup T$ cannot be a superstructure because f is not of type H_1. Hence $d(T_i)$, $d(T_j)$, $d(T)$ must not all be different, and if $d(T_i) = d(T)$, let's say, then $z(T_i \cap T) \geq 1$. But $d(T_i) = d(T)$ together with $T_i \cap T \neq 0$ implies that $T_i \cup T$ is in $\bar{V}$ and that T_i is not maximal in $\bar{V}$, which gives a contradiction.

ii) Suppose P is a part of S_i as well as of S_j. There is a unique $T \varepsilon V^*$ having $P \subseteq T$, $d(P) = d(T)$. The only conceivable way for $T \subseteq S_i$, $T \subseteq S_j$ would be that $S_i = T \cup T_i$, $S_j = T \cup T_j$. Then T_j would have at least 2 integers in common with S_i, a contradiction to i).

iii) $z(Q_i \cap Q_j) \geq 2$ would imply that $Q_i \cup Q_j$ is a structure if $d(Q_i) \neq d(Q_j)$; it would imply $Q_i \cup Q_j \varepsilon \bar{V}$ if $d(Q_i) = d(Q_j)$. And $z(S_i \cap S_j) \geq 3$ implies $z(T \cap S_j) \geq 2$ for some T of S_i, which contradicts i) again.

We call f of type $F_1^{(i)} (i = 1, 2, 3)$ if f is of type F_1 and not of type G_1 or H_1 and if

$F_1^{(1)}$: q, the number of elements of X, is at least u.

$F_1^{(2)}$: $q < u$ and $s = 1$, where s is the number of elements of W.

$F_1^{(3)}$: $s \geq 2$.

Similarly we define $F_j^{(i)}$ for $j = 2, \cdots, k$. Naturally, f can be of several types for several systems $Q, P_1, \cdots, P_r$

LEMMA 9. *We have*

$$|F_1^{(1)}| \leq m^{u+2} e_k(m - lu + c_5 u^2 \log l), \tag{18i}$$

$$\left.\begin{array}{l} |F_1^{(2)}| \quad \text{(18ii)} \\ |F_1^{(3)}| \quad \text{(18iii)} \end{array}\right\} \leq m^2 e_k(m - 2l + c_6 u \log l)$$

for the numbers $|F_1^{(i)}|$ *of functions of type* $F_1^{(i)}$.

Proof.

i) Take u of the progressions of X, let's say $Q_1, \cdots, Q_u$. According to (4b), there exist different elements $q_1, \cdots, q_u$ of Q belonging to $Q_1, \cdots, Q_u$, respectively. There are less than m^2 ways to choose Q, at most l^u ways to choose $q_1, \cdots, q_u$ and for given q_i there are not more than ml ways to find a Q_i having $q_i \varepsilon Q_i$. Altogether, there are at most $m^{u+2} l^{2u}$ ways to pick $Q, Q_1, \cdots, Q_u$.

On each $Q_i (i = 1, \cdots, u)$ there is an $(l - u)$-tuple σ_i where $f(\sigma_i) = 1$. There are fewer than l^u ways of picking σ_i, fewer than l^{u^2} ways to pick $\sigma_1, \cdots, \sigma_u$. By Lemma 8iii) there are not more than $\binom{u}{2} \leq u^2$ integers belonging to at least two of the sets $\sigma_1, \cdots, \sigma_u$. Hence there exist at most $e_k(m - lu + u^2)$ functions f having $f(\sigma_1) = \cdots = f(\sigma_u) = 1$. We obtain

$$|F_1^{(1)}| \leq m^{u+2} l^{u^2+2u} e_k(m - lu + u^2) \leq m^{u+2} e_k(m - lu + c_5 u^2 \log l).$$

ii) Let S be the only structure of W. According to Lemma 5 we have $z(S) \geq l + h - 2$ if S is built of progressions $P_1, \cdots, P_h$ of V. According to (4b) there are elements $x_1, \cdots, x_h$ belonging to $P_1 \cap Q, \cdots, P_h \cap Q$, respectively.

The argument at the beginning of the proof of Lemma 7 shows that any $T \varepsilon \bar{V}$ is the union of at most 2 progressions $P \varepsilon V$, therefore S is union of at most 4 progressions $P \varepsilon V$, and there is a subset σ of S of max $(z(S) - 4u, 0)$ elements such that $f(\sigma) = 1$.

Now if X consists of $Q_1, \cdots, Q_q$, there are integers $y_1, \cdots, y_q$, let's say, belonging to $Q_1 \cap Q, \cdots, Q_q \cap Q$. Let ρ be the set of elements of Q which are neither $x_1, \cdots, x_h$ nor $y_1, \cdots, y_q$. Every $z \in \rho$ has $f(z) = 1 + =2$ according to (4c). This implies $z(\sigma \cap \rho) = 0$, therefore $z(S \cap \rho) \leq 4u$. Let τ be the set of elements of ρ which do not belong to S. Then $f(\tau) = 2$ and $z(\tau) \geq l - h - 5u$. The advantage of τ over ρ is that τ is determined by Q, S and $y_1, \cdots, y_q$, and we do not need to know $x_1, \cdots, x_h$.

As can be shown by the methods used to prove Lemma 4, there are at most $m^2 l^{c_7}$ ways to pick a Q and an S having $z(Q \cap S) \geq 2$. h can be between 1 and l. There are at most $(4l)^{4u}$ ways to choose the set σ in S and then at most l^u ways to choose τ, since τ is determined by Q, S and $y_1, \cdots, y_q$. The number of functions f having $f(\sigma) = 1$ and $f(\tau) = 2$ equals

$$e_k(m - z(\sigma) - z(\tau)) \leq e_k(m - l - h + 2 + 4u - l + h + 5u) = e_k(m - 2l + 9u + 2).$$

Hence

$$| F_1^{(2)} | \leq m^2 l^{c_7 + 1 + 4u + u} e_k(m - 2l + 9u + 2) \leq m^2 e_k(m - 2l + c_6 u \log l).$$

iii) Let S_1, S_2 be structures of W. There are at most $m^2 l^{c_8}$ ways to pick Q and structures S_1, S_2 such that $z(Q \cap S_i) \geq 2 (i = 1, 2)$. On $S_i (i = 1, 2)$ there is a set σ_i of at least $z(S_i) - 4u$ elements where $f(x) = 1$. σ_i can be chosen in at most $(4l)^{4u}$ ways. Lemma 8iii) implies $z(\sigma_1 \cap \sigma_2) \leq 2$, therefore $z(\sigma_1 \cup \sigma_2) \geq z(S_1) + z(S_2) - 8u - 2 \geq 2l - 8u - 2$. The number of f having $f(\sigma_1 \cup \sigma_2) = 1$ is not larger than $e_k(m - 2l + 8u + 2)$. Combining our estimates we obtain the desired result.

5. **Proof of Theorem 1.** Using Lemma 9 we find

$$2A = 2 \sum_{i=1}^{k} (| G_i | + | H_i | + | F_i^{(2)} | + | F_i^{(3)} |) \leq m^2 e_k(m - 2l + c_9 u \log l),$$

$$2B = 2 \sum_{i=1}^{k} | F_i^{(1)} | \leq m^{u+2} e_k(m - lu + c_{10} u^2 \log l)$$
$$\leq k^m \left\{ m e_k\left(-l \frac{u}{u+2} + c_{10} u \log l \right) \right\}^{u+2}$$
$$\leq k^m \{ m e_k(-l + 2l/u + c_{10} u \log l) \}^{u+2}.$$

Choosing u to be the integral part of $(l/\log l)^{\frac{1}{2}}$ and assuming $m < e_k[l - c(l \log l)^{\frac{1}{2}}]$ for a large enough constant c, we easily find $A < k^m$, $B < k^m$. Since the number of functions f of type F is at most $(A + B)/2$, the Theorem follows.

6. **Proof of the metrical theorem.** The integers k and l will be considered fixed in this section. Many of the expressions defined will depend on k and l although this will not always be clear from the notation. For instance, we write $M(m)$ for the number of progressions of l different terms all of which are integers in $1 \leq x \leq m$.

LEMMA 10.

$$M(m) = \frac{m^2}{2(l-1)} + O(m). \tag{19}$$

Proof. For any integer d in $1 \leq d \leq (m-1)/(l-1)$ the number of progressions P between 1 and m with $d(P) = d$ equals $m - (l-1)\,d$. We obtain

$$M(m) = \sum_{d=1}^{r} (m - (l-1)\,d)$$

where r is the integral part of $(m-1)/(l-1)$. (The sum is empty if $r = 0$.) This gives

$$M = \tfrac{1}{2}r(2m - (r+1)(l-1)) = \frac{m^2}{2(l-1)} + O(m).$$

Instead of $N(\alpha; k, l, m)$ we shall write simply $N(\alpha; m)$. Put $M(0) = 0$, $N(\alpha; 0) = 0$, $L(\alpha; m) = N(\alpha, m) - k^{1-l}M(m)$ and

$$\begin{aligned} M(m_1, m_2) &= M(m_2) - M(m_1) \\ N(\alpha; m_1, m_2) &= N(\alpha; m_2) - N(\alpha; m_1) \qquad (0 \leq m_1 < m_2). \\ L(\alpha; m_1, m_2) &= L(\alpha; m_2) - L(\alpha; m_1) \end{aligned} \tag{20}$$

LEMMA 11.

$$\int_0^1 L^2(\alpha; m_1, m_2)\, d\alpha = O(M(m_1, m_2)). \tag{21}$$

Proof. The measure of the set of α's where $\alpha_{p_1} = \cdots = \alpha_{p_l}$ for a fixed progression $p_1, \cdots, p_l$ is k^{1-l}. This gives

$$\int_0^1 N(\alpha; m_1, m_2)\, d\alpha = k^{1-l}M(m_1, m_2).$$

Next,

$$\int_0^1 N^2(\alpha; m_1, m_2)\, d\alpha = \sum_{\substack{P,\, m_1 < p_l \leq m_2 \\ Q,\, m_1 < q_l \leq m_2}} \mu(P, Q)$$

where the sum is over progressions P, Q whose largest element is in $m_1 < x \leq m_2$ and where $\mu(P, Q)$ is the measure of the set of α's having $\alpha_{p_1} = \cdots = \alpha_{p_l}$ and $\alpha_{q_1} = \cdots = \alpha_{q_l}$. Note that $\mu(P, Q) = k^{2(1-l)}$ unless $z(P \cap Q) \geq 2$. On the other hand, the number of pairs P, Q of the desired type having $z(P \cap Q) \geq 2$ is $O(M(m_1, m_2))$ and we trivially have $\mu(P, Q) \leq 1$ for such pairs. Hence

$$\int_0^1 N^2(\alpha; m_1, m_2)\, d\alpha = k^{2(1-l)}M^2(m_1, m_2) + O(M(m_1, m_2)),$$

and (21) follows.

Theorem 2 is now a result of Lemma 10 and the following result in probability theory, which in the terminology of Halmos [3] can be stated as follows.

LEMMA 12. *Let* $L(\alpha; m)$, $m = 0, 1, 2, \cdots$ *be a sequence of real-valued measur-*

able functions on a probability space (X, S, μ). *Let* $M(m)$, $m = 0, 1, \cdots$ *be a sequence of constants satisfying* $M(m + 1) \geq M(m)$,

$$M(2m) = O(M(m)) \tag{22}$$

and

$$M(m) > m^{c_0} \quad \text{for large } m, \quad \text{where} \quad c_0 > 0 \quad \text{is a constant.} \tag{23}$$

Define $M(m_1, m_2)$ *and* $L(\alpha; m_1, m_2)$ *by* (20) *and assume that*

$$\int L^2(\alpha; m_1, m_2)\, d\mu(\alpha) = O(M(m_1, m_2)). \tag{24}$$

Let $\epsilon > 0$. *Then*

$$L(\alpha; m) = O(M^{\frac{1}{2}}(m) \log^{\frac{3}{2}+\epsilon} M(m)) \tag{25}$$

almost everywhere.

Remarks. This lemma was the underlying idea of proofs in [1] and [5], although further complications there may have obscured this. Using ideas of [5], particularly Lemma 1, one could remove the conditions (22) and (23). In our application (22) and (23) are satisfied.

Proof. Write L_s for the set of intervals $(u, v]$ of the type $0 \leq u = t2^r < v = (t + 1)2^r < 2^s$ for non-negative integers r, t. Using (24) we obtain

$$\sum_{(u,v] \varepsilon L_s} \int L^2(\alpha; u, v)\, d\mu(\alpha) = O(sM(2^s))$$

since the intervals of L_s with given r cover $0 \leq x < 2^s$ at most once and therefore give a contribution not exceeding $O(M(2^s))$. Define S_s, $s = 1, 2, \cdots$ to be the subset of X where

$$\sum_{(u,v] \varepsilon L_s} L^2(\alpha; u, v) < s^{2+\epsilon} M(2^s). \tag{26}$$

The measure of S_s is $1 - O(s^{-1-\epsilon})$. Let S_0 be the set of elements α which are in S_s whenever $s > s_0(\alpha)$. S_0 has measure 1 because $\sum s^{-1-\epsilon}$ is convergent.

Let α be an element of S_0. Assume $m \geq 2^{s_0(\alpha)}$. Choose s so that $2^{s-1} \leq m < 2^s$. The interval $(0, m]$ is the union of at most s intervals of L_s, therefore

$$L(\alpha; m) = \sum L(\alpha; u, v) \tag{27}$$

where the sum is over at most s intervals $(u, v]$ of L_s. Using (26), (27) and Cauchy's inequality we obtain

$$L^2(\alpha; m) \leq s^{3+\epsilon} M(2^s).$$

This, together with (22) and (23) gives

$$\begin{aligned} L(\alpha; m) &= O(s^{\frac{3}{2}+\epsilon} M^{\frac{1}{2}}(2^s)) \\ &= O(M^{\frac{1}{2}}(2^s) \log^{\frac{3}{2}+\epsilon} M(2^s)) \\ &= O(M^{\frac{1}{2}}(m) \log^{\frac{3}{2}+\epsilon} M(m)). \end{aligned}$$

References

1. J. W. S. Cassels, *Some metrical theorems in Diophantine approximation*. III, Proceedings of the Cambridge Philosophical Society, vol. 46(1950), pp. 219–225.
2. P. Erdös and R. Radó, *Combinatorial theorems on classifications of subsets of a given set*, Proceedings of the London Mathematical Society (3), vol. 2(1952), pp. 417–439.
3. P. R. Halmos, *Measure Theory*, New York, 1950.
4. L. Moser, *On a theorem of van der Waerden*, Canadian Mathematical Bulletin, vol. 3(1960), pp. 23–25.
5. W. M. Schmidt, *A metrical theorem in Diophantine approximation*, Canadian Journal of Mathematics, vol. 12(1960), pp. 619–631.
6. B. L. van der Waerden, *Beweis einer Baudet'schen Vermutung*, Nieuw Archief voor Wiskunde, vol. 15(1925–28), pp. 212–216.

University of Colorado