Quantitative Forms of a Theorem of Hilbert

T. C. BROWN

Simon Fraser University, Burnaby, British Columbia, Canada V5A1S6

P. ERDÖS

Hungarian Academy of Sciences, Budapest, Hungary

AND

F. R. K. CHUNG AND R. L. GRAHAM

Bell Laboratories, Murray Hill, New Jersey

Communicated by the Managing Editors

Received April 20, 1983

INTRODUCTION

In an influential paper published in 1892, Hilbert proved the following result, which in some sense could be considered the first theorem in Ramsey theory. For positive integers m, a, and a_k, $1 \leqslant k \leqslant m$, define an *m-cube* $Q_m = Q_m(a, a_1, ..., a_m)$ to be the set

$$\left\{ a + \sum_{k=1}^{m} \varepsilon_k a_k : \varepsilon_k = 0 \text{ or } 1,\ 1 \leqslant k \leqslant m \right\}.$$

LEMMA (Hilbert [7]). *For any positive integers m and r there exists a least integer $h(m, r)$ such that if the set $\{1, 2, ..., h(m, r)\}$ is arbitrarily partitioned into r classes C_k, $1 \leqslant k \leqslant r$, some C_i must contain an m-cube.*

Hilbert needed this lemma in connection with certain results on the irreducibility of rational functions and, as far as is known, never pursued the combinatorial directions to which it pointed. Others did, however, beginning with Schur, who in 1916 showed that for any r, there is an $s(r)$ so that in any partition of $\{1, 2, ..., s(r)\}$ into r classes, some class contains a *projective* 2-cube, i.e., $Q_2^*(a_1, a_2) = Q_2(a, a_1, a_2) - \{0\}$ with $a = 0$. (This combinatorial result actually arose in Schur's investigations [11] of a modular version of Fermat's conjecture.) This was later extended by Rado

[9] (who was Schur's student) who (implicitly) proved that any partition of a sufficiently long interval of integers into r classes must have at least one class which contains a projective m-cube. This was also proved independently later by Folkman (see [3]) and Sanders [10]. Finally, in 1974, Hindman [8] proved the much stronger result that in any partition of all the positive integers into finitely many classes, some class must contain an *infinite* projective cube, i.e., for positive integers $a_1, a_2, \ldots$, a set

$$\left\{ \sum_{k=1}^{\infty} \varepsilon_k a_k : \varepsilon_k = 0 \text{ or } 1 \text{ with } 0 < \sum_{k=1}^{\infty} \varepsilon_k < \infty \right\}.$$

In this note we investigate the function $h(m, r)$ and several related ones. In particular we derive rather sharp bounds on them for the (first interesting) case $m = 2$. We should point out here that in contrast to the rapidly growing functions associated with projective m-cubes (e.g., $s(r)$ is known [1, 2, 11] to satisfy $c \cdot 315^{r/5} < s(r) \leqslant [er!]$, for a suitable $c > 0$), for any fixed m, $h(m, r)$ is bounded by a polynomial in r.

2-cubes

To begin with, an easy calculation shows that a set $A \subseteq \mathbb{Z}^+$ (the positive integers) contains no 2-cube if and only if

$$a, b, c, d \in A,\ a + b = c + d \Rightarrow \{a, b\} = \{c, d\}, \tag{1}$$

i.e., all the pair sums $x + y$, $x, y \in A$, are distinct. Such sets A (often called B_2-sets) have been extensively studied in the literature (e.g., see [6]). In particular, it is known [6] that if $A \subseteq [n] := \{1, 2, \ldots, n\}$ satisfies (1) then

$$|A| \leqslant (1 + o(1)) \sqrt{n}. \tag{2}$$

Thus, if we partition $[n]$ into B_2-sets, say,

$$[n] = \bigcup_{k=1}^{t} A_k \tag{3}$$

then by (2) we must have

$$t \geqslant \frac{n}{\max_k |A_k|} \geqslant (1 + o(1)) \sqrt{n}. \tag{4}$$

This implies

$$h(2, r) \leqslant (1 + o(1))\, r^2. \tag{5}$$

Our next goal is to establish the reverse inequality in (5). It is well known (see [12]) that for any prime p there exists a simple difference set

$D = \{d_0, d_1, ..., d_p\} \pmod{p^2+p+1}$. That is, any nonzero $t \in \mathbb{Z}_{p^2+p+1}$ has a *unique* representation as $t \equiv d_i - d_j \pmod{p^2+p+1}$ and consequently, all $d_i - d_j$, $i \neq j$, are distinct. Define

$$D_j := D - d_j = \{d_i - d_j : 0 \leqslant i \leqslant p\} \pmod{p^2+p+1},$$

where we have translated all the elements of D_j so that they lie between 0 and p^2+p. We claim that D_j satisfies (1). For if not then for some i_1, i_2, i_3, i_4 with $\{i_1, i_2\} \neq \{i_3, i_4\}$,

$$(d_{i_1} - d_j) + (d_{i_2} - d_j) \equiv (d_{i_3} - d_j) + (d_{i_4} - d_j) \pmod{p^2+p+1},$$

i.e.,

$$d_{i_1} - d_{i_3} \equiv d_{i_4} - d_{i_2} \pmod{p^2+p+1}$$

which by the definition of a simple difference set implies $i_1 = i_4$, $i_3 = i_2$. However, this implies $\{i_1, i_2\} = \{i_3, i_4\}$ which is a contradiction. Furthermore, observe that since any $t \in \mathbb{Z}_{p^2+p+1}$ can be written as $t \equiv d_i - d_j \pmod{p^2+p+1}$ then the D_j, $0 \leqslant j \leqslant p$, *cover* $[p^2+p]$. Thus, $[p^2+p]$ can be partitioned into $p+1$ B_2-sets and so,

$$h(2, p+1) \geqslant p^2+p+1. \tag{6}$$

Since the ratio between consecutive primes tends to 1 we then have

$$h(2, r) \geqslant (1+o(1))\, r^2. \tag{7}$$

Combining (5) and (7) we finally obtain:

THEOREM 1.

$$h(2, r) = (1+o(1))\, r^2. \tag{8}$$

We should point out that this result is closely related to the value of the Ramsey number for 4-cycles (see [4]).

Deleted 2-cubes

It is natural to expect that if the conditions on the forbidden subsets are relaxed then the number of classes in a valid partition must increase. As an example of this, we now consider what could be called *deleted* 2-cubes. By this we just mean sets of the form $\{a+x, a+y, a+x+y\}$ for some $a \geqslant 0$ and $x, y \geqslant 1$, i.e., an ordinary 2-cube with the point corresponding to $\varepsilon_1 = \varepsilon_2 = 0$ deleted. It turns out it makes a rather substantial difference whether we allow $x = y$ or not. Define $\bar{h}(2, r)$ to be the least integer $\bar{h}$ such that in any partition of $[\bar{h}]$ into r classes, some class contains a set $\bar{Q}(a, x, y) = \{a+x, a+y, a+x+y\}$ for some $a \geqslant 0$ and $1 \leqslant x \leqslant y$.

Similarly define $h^*(2, r)$ in the same way except that now we require $1 \leqslant x < y$.

THEOREM 2.

(i) $\bar{h}(2, r) = 2r$;

(ii) $h^*(2, r) \geqslant (1 + o(1)) \frac{11}{3} r$;

(iii) $h^*(2, r) \leqslant (1 + o(1)) \frac{26}{7} r$.

Proof. The proof of (i) is straightforward. For any partition of $[2r]$ into r classes, some class C must contain integers u and v satisfying $r \leqslant u < v \leqslant 2r$. Since $a := 2u - v \geqslant 0$ then the set $\bar{Q}(a, v-u, v-u)$ belongs to C, and so, $\bar{h}(2, r) \leqslant 2r$. On the other hand, the partition $[2r-1] = \bigcup_{k=1}^{r-1} \{k, k+r\} \cup \{r\}$ shows that $\bar{h}(2, r) > 2r - 1$.

Proof of (ii). It is easy to check that a set $A \subseteq \mathbb{Z}^+$ contains no set of the form $\{a+x, a+y, a+x+y\}$ with $a \geqslant 0$, and $1 \leqslant x < y$ if and only if

$$u, v, w \in A \text{ with } u < v < w \Rightarrow u + v < w. \tag{9}$$

We want to show that it is always possible to partition $[11n]$ into $3n + o(n)$ such sets. To do this, we describe a specific construction. Define $A(k)$, $B(k)$, and $C(k)$, $1 \leqslant k < n$, by

$$A(k) = \{2n - 2k, 2n + k, 4n - k + 1, 7n - k + 1, 11n - 2k + 3\}$$

$$B(k) = \{2n - 2k - 1, 7n + k, 9n - k\}$$

$$C(k) = \{5n - k, 6n - k, 11n - 2k + 2\}.$$

It is easy to check that for $1 \leqslant k < n$, each of $A(k)$, $B(k)$, and $C(k)$ satisfies (9) and furthermore, with the exception of a bounded number of elements, their union covers $[11n]$. Thus

$$h^*(2, 3n) \geqslant 11n + o(1)$$

and consequently (ii) holds.

Proof of (iii). Suppose we have a partition of $[\frac{11}{39}n, \ldots, n]$ into classes, each of which satisfies (9). We will show that there must be at least $\frac{7}{26}n + o(n)$ classes, which in turn, will establish (iii). We distinguish three types of classes in the partition, depending on the number of elements in the class. We have

$$A_i = \{a_1^{(i)} < a_2^{(i)} < a_3^{(i)} < a_4^{(i)}\}, \qquad 1 \leqslant i \leqslant an,$$

$$B_i = \{b_1^{(i)} < b_2^{(i)} < b_3^{(i)}\}, \qquad 1 \leqslant i \leqslant bn,$$

$$C_i = \{c_1^{(i)} < c_2^{(i)}\}, \qquad 1 \leqslant i \leqslant cn.$$

Note that since all elements are greater than $n/5$ and each class satisfies (9) then no class can have 5 or more elements. Also, any two sets each with a single element can be combined without loss of generality to form a C_i. By hypothesis,

$$\begin{aligned} a_1^{(i)} + a_2^{(i)} &< a_3^{(i)} \\ a_2^{(i)} + a_3^{(i)} &< a_4^{(i)} \\ b_1^{(i)} + b_2^{(i)} &< b_3^{(i)}. \end{aligned} \tag{10}$$

Summing these inequalities we obtain

$$\sum_{i=1}^{an} (a_1^{(i)} + 2a_2^{(i)}) + \sum_{j=1}^{bn} (b_1^{(j)} + b_2^{(j)}) < \sum_{i=1}^{an} a_4^{(i)} + \sum_{j=1}^{bn} b_3^{(j)}. \tag{11}$$

Also, by counting the total number of elements we have

$$4a + 3b + 2c \leqslant \tfrac{28}{39}. \tag{12}$$

We want to *minimize* the number of classes $w = (a + b + c)\, n$.

To begin with, it is not difficult to see that the least value the LHS of (11) can assume is obtained by taking the $a_2^{(i)}$ as small as possible (because of the coefficient 2). Basically, this means that $[\frac{11}{39}n, \ldots, n]$ is partitioned as

$$(a_1^{(1)} a_2^{(1)} a_1^{(2)} a_2^{(2)} a_1^{(3)} a_2^{(3)} \cdots b_1^{(1)} b_2^{(1)} b_1^{(2)} b_2^{(2)} \cdots].$$

Thus

$$\begin{aligned} &\sum_{i=1}^{an} (a_1^{(i)} + 2a_2^{(i)}) + \sum_{j=1}^{bn} (b_1^{(j)} + b_2^{(j)}) \\ &\quad \geqslant \sum_{k=1}^{(2a+2b)n} (\tfrac{11}{39}n + k) + \sum_{k=1}^{an} (\tfrac{11}{39}n + 2k) \\ &\quad = n^2((3a + 2b) \cdot \tfrac{11}{39} + 2(a + b)^2 + a^2) + o(n^2). \end{aligned} \tag{13}$$

On the other hand, the RHS of (11) is bounded above by

$$\begin{aligned} \sum_{i=1}^{an} a_4^{(i)} + \sum_{j=1}^{bn} b_3^{(j)} &\leqslant \sum_{k=1}^{(a+b)n} (n - k + 1) \\ &= n^2(a + b - \tfrac{1}{2}(a + b)^2) + o(n^2). \end{aligned} \tag{14}$$

Combining (11), (13), and (14) we obtain

$$\tfrac{11}{39}(3a + 2b) + 2(a + b)^2 + a^2 \leqslant a + b - \tfrac{1}{2}(a + b)^2 + o(1)$$

which simplifies to

$$\tfrac{7}{2}a^2 + 5ab + \tfrac{5}{2}b^2 \leqslant \tfrac{6}{39}a + \tfrac{17}{39}b. \tag{15}$$

It is now straightforward to solve this quadratic programming problem (subject, of course, to the conditions that $a, b, c \geqslant 0$). The result is that the minimum value of $a+b+c$ is $\frac{7}{26}$, which is attained when $a = \frac{1}{39}$, $b = \frac{5}{39}$, $c = \frac{3}{26}$. This proves (iii).

With more complicated arguments, it is possible to increase the bound $\frac{7}{26}n$ somewhat, but at present we are unable to close the gap between the lower bound and the upper bound of $\frac{3}{11}n$ (which may well be the "truth").

Larger values of m

Relatively little is known for $h(m, r)$ with $m > 2$. An easy induction argument (used in [7]) shows that

$$h(m, r) \leqslant (r+1)^{F_{2m}},$$

where F_k denotes the kth Fibonacci number, i.e., $F_0 = 0, F_1 = 1$, and $F_{k+2} = F_{k+1} + F_k$. Thus

$$h(m, r) < r^{c^m}$$

for a suitable c.

In fact, a stronger "density" result actually holds here. In [13] (see also [5]), Szemerédi shows that if $A \subseteq [M]$ has

$$|A| > M/r$$

and

$$M > (3r)^{c^m}$$

then A contains an m-cube.

We do not at present have anything interesting to state concerning lower bounds for $h(m, r)$ (although bounds of the form r^{cm} are easy to obtain).

For projective m-cubes, Taylor [14] has recently shown that if the set $[N]$ is partitioned into r classes then some class contains a projective m-cube provided

$$N \geqslant \sqrt[2r(m-1)]{2^{r^{3^r}}} \qquad \text{for} \quad m, r \geqslant 2.$$

While this bound may appear large, it was actually a tremendous improvement over previous bounds (being primitive recursive, for example).

REFERENCES

1. F. R. K. CHUNG AND C. M. GRINSTEAD, A survey of bounds for classical Ramsey numbers, *Journal of Graph Theory* **7** (1983), 25–37.
2. H. FREDERICKSON, Schur numbers and the Ramsey numbers $N(3, 3,..., 3; 2)$, *J. Combin. Theory Ser. A* **27** (1979), 376–377.
3. R. L. GRAHAM AND B. L. ROTHSCHILD, A survey of finite Ramsey theorems, *in* "Proc. 2nd Louisiana Conf. on Combinatorics, Graph Theory and Computing, Louisiana State Univ., 1971," pp. 21–40.
4. R. L. GRAHAM, "Rudiments of Ramsey Theory," Amer. Math. Soc., Providence, R.I., 1981.
5. R. L. GRAHAM, B. L. ROTHSCHILD, AND J. H. SPENCER, "Ramsey Theory," Wiley, New York, 1980.
6. H. HALBERSTAM AND K. E. ROTH, "Sequences I," Oxford Univ. Press, Oxford, 1966.
7. D. HILBERT, Über die irreducibilität ganzer rationaler Functionen mit ganzzahligen Koeffizienten, *J. Reine Angew. Math.* **110** (1982), 104–129.
8. N. HINDMAN, Finite sums from sequences within cells of a partition of N, *J. Combin. Theory Ser. A* **17** (1974), 1–11.
9. R. RADO, Studien zur Kombinatorik, *Math. Z.* **36** (1933), 424–480.
10. J. SANDERS, "A Generalization of Schur's Theorem," dissertation, Yale University, 1969.
11. I. SCHUR, Uber die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$, *Jahresber. Deutsch. Math.-Verein* **25** (1916), 114–116.
12. T. STORER, Cyclotomy and difference sets, Lectures in Adv. Math. No. 2, Markham, Chicago, 1967.
13. E. SZEMERÉDI, On sets of integers containing no k term arithmetic progression, *Acta Arith.* **27** (1975), 199–245.
14. A. D. TAYLOR, Bounds for the disjoint unions theorem, *J. Combin. Theory Ser. A* **30** (1981), 339–344.