COMBINATORICA 1(2) (1981) 203—208

SURESUMS

Joel SPENCER

SUNY at Stony Brook
Stony Brook, L. I., New York
11733 U.S.A.

Received 20 May 1979

A *suresum* is a pair (A, n), $A\subset\{1, \ldots, n-1\}$, so that whenever A is 2-colored some monochromatic set sums to n. A "finite basis" for the suresum (A, n) with $|A|\leqq c$ is proven to exist. For c fixed, it is shown that no suresum (A, n) exist if n is a sufficiently large prime. Generalizations to r-colorations, $r>2$, are discussed.

Introduction

It is not too difficult to show that if the first twelve positive integers are two-colored some monochromatic set sums to thirteen. A *suresum* is defined to be a pair (A, n), n integral, $A\subset\{1, \ldots, n-1\}$ so that whenever A is 2-colored, there exists a monochromatic set with sum n. Paul Erdős observed that if $n=13m$, there exists a suresum (A, n) with $|A|=12$: $A=\{m, 2m, \ldots, 12m\}$. He then asked if there existed an absolute constant c such that for all sufficiently large n, there existed suresum (A, n) with $|A|\leqq c$. This question we answer in the negative.

Set $f(n)$ equal the minimal $|A|$ for suresum (A, n). We show

$$\frac{c\ln n}{\ln\ln n}\leqq f(n) \quad \textit{for infinitely many } n,$$

$$f(n)\leqq c\ln n \quad \textit{for all sufficiently large } n.$$

More generally, for $r\geqq 2$, an *r-suresum* is a pair (A, n), n integral, $A\subset\{1, \ldots, n-1\}$ so that whenever A is r-colored, there exists a monochromatic set with sum n. Let $f_r(n)$ equal the minimal $|A|$ for r-suresum (A, n). For $r\geqq 3$, fixed, we show

$$f_r(n)\leqq e^{c_r\sqrt{\ln n}}.$$

As a corollary, $(\{1, \ldots, n-1\}, n)$ is an r-suresum for n sufficiently large. To restate in Ramseyian language: For all r, there exists n_0 so that if $n>n_0$ and $\{1, \ldots, n-1\}$ is r-colored, some monochromatic set sums to n.

AMS subject classification (1980): 05 C 15

1. Suresum of fixed cardinality

We call (dA, dn) a multiple of (A, n). As P. Erdős observed, multiples of suresums are suresum. We call (A, n) prime if $\gcd(A, n)=1$ or, equivalently, (A, n) is a multiple only of itself. We call (A, n) a minimal suresum if there is no proper subset $B\subset A$ such that (B, n) is a suresum.

Theorem 1. *For every c there are a finite number of prime minimal suresum (B, q) with $|B|=c$.*

For suresum $(A, n)=(\{x_1, \ldots, x_c\}, n)$ we define

$$\mathcal{S}=\Big\{S\subseteqq\{1, \ldots, c\}\colon \sum_{i\in S} x_i = n\Big\}$$

as the *family* of (A, n). Let $\mathcal{S}$ be the family of some *minimal* $(\{x_1, \ldots, x_c\}, n)$. We shall show that all suresum (A, m) with family $\mathcal{S}$ are multiples of a single prime (B, q).

Consider the system of equations

$$\sum_{i\in S} y_i = n, \quad S\in\mathcal{S}. \tag{1}$$

This system has solution $(x_1, \ldots, x_c)$; suppose it has a different solution $(x_1', \ldots, x_c')$. Let $A^*=\{x_i\colon x_i=x_i'\}$ so $A^*\neq A$. By minimality we Red/Blue color A^* so that no monochromatic set sums to n. We extend this by coloring (and this is the critical step) $x_i\in A-A^*$ Red if $x_i>x_i'$; Blue if $x_i<x_i'$. If $\{x_i\colon i\in S\}$ is a monochromatic set with sum n, then $S\in\mathcal{S}$ so

$$\sum_{i\in S} x_i = n = \sum_{i\in S} x_i'.$$

As $S\not\subset A^*$ some $x_i\neq x_i'$. But then some $x_i<x_i'$ and some $x_i>x_i'$, giving Red and Blue points. This is a contradiction. Hence, $(x_1, \ldots, x_c)$ is the *unique* solution to (1).

Consider the system

$$\sum_{i\in S} z_i = 1, \quad S\in\mathcal{S}. \tag{2}$$

The solutions to (2) are merely the solutions to (1), multiplied by n^{-1}. Thus, (2) has a unique solution which depends on $\mathcal{S}$, not on n. The solution may be uniquely written

$$z_i = p_i/q, \quad 1\leqq i\leqq c$$

where $\gcd(q, p_1, \ldots, p_c)=1$. As $x_i=nz_i\in Z$, $q\,|\,n$ so that (A, n) is a multiple of $(\{p_1, \ldots, p_c\}, q)$.

For fixed c, there are a finite number of possible $\mathcal{S}$. Every $\mathcal{S}$ that is the family of some minimal suresum (A, n) is the family of exactly one prime minimal (B, q). Thus there are only a finite number of prime minimal (B, q). ∎

For every c there exists, in theory at least, a complete description of the suresum (A, n) with $|A|\leqq c$. There is a finite list of minimal prime (B, q) with $|B|\leqq c$. (The smallest is $(\{1, 2, 4, 5, 6, 7, 8, 9\}, 15)$.). All suresum (A, n) are multiples of these, plus possibly some extra elements.

Let $Q(c)$ denote the set of q such that there exists a minimal prime (B, q) with $|B|\leqq c$. Then $Q(c)$ is a calculatable finite set. There exists suresum (A, n) with $|A|\leqq c$ iff $q|n$ for some $q\in Q(c)$. Taking the contrapositive, and restricting n to be prime, allows a restatement in striking form: *For all c if n is a sufficiently large prime, any c integers $<n$ may be two-colored so that no monochromatic set sums to n.* In the notation of the introduction: Lim Sup $f(n)=+\infty$.

We indicate another proof of the above statement. Let $0<x_1, \ldots, x_c<n$. Set $\mathcal{S}=\{S\subseteq \{1, \ldots, c\}: \sum_{i\in S} x_i=n\}$. Let $y_1, \ldots, y_c$ satisfy

(i) $\sum_{i\in S} y_i = n$ for all $S\in\mathcal{S}$,

(ii) $y_i \neq x_i$ for all $1 \leqq i \leqq c$.

(The existence of $y_1, \ldots, y_c$ requires argument similar to the first proof.) Then color x_i Red if $x_i>y_i$ and Blue if $x_i<y_i$. Any $S\in\mathcal{S}$ will have elements of both colors.

2. Bounds of f(n)

If $q\in Q(c)$, there exists a family of sets $\mathcal{S}$ on $\{1, \ldots, d\}$ for some $d\leqq c$ so that (2) has unique solution $z_i=p_i/q$ where $\gcd(p_1, \ldots, p_d, q)=1$. (In addition, the z_i are distinct, $0<z_i<1$, and $\mathcal{S}$ is not 2-colorable, but we ignore these conditions.) Graver [3] discusses the "maximal depth problem" which is essentially finding the maximal q satisfying the above.

As system (2) has a unique solution, some d of the equations, say,

$$\sum_{i\in S_j} z_i = 1, \quad 1 \leqq j \leqq d \tag{3}$$

have the unique solution. By Cramer's Rule, we may solve

$$z_i = \alpha_i/\det(A)$$

where A is the coefficient matrix of (3) and $\alpha_i\in Z$ is another determinant. The common denominator q thus satisfies $q|\det(A)$ where A has size $\leqq c$ and coefficients (critically) 0 or 1.

The possible values for such $\det(A)$ are a matter of some conjecture. It is known that $\det(A)\leqq(c+1)^{(c+1)/2}2^{-c}$, the maximum achieved when A is derived from a Hadamard Matrix of order $(c+1)$. Thus, if q is prime and $q>(c+1)^{(c+1)/2}2^{-c}$, then $q\notin Q(c)$. As the primes are dense, inverting this function of c we find

$$f(n) > k \ln n/\ln\ln n.$$

We outline a relatively simple construction giving an upper bound on $f(n)$. Call a sequence $z_1, z_2, \ldots. z_m$ of positive integers a chain if for $i\geqq 3$, z_i may be expressed as the sum of previous z_j (allowing an arbitrary number of distinct summands). With initial conditions $z_1=1, z_2=2$ or $z_1=1, z_2=3$ or $z_2=2, z_3=3$, we construct such a chain with all $z_i<n/2$ (a technical point) and n expressible as a sum of z_i. Basically, we set $z_3=z_1+z_2$, $z_{3+i}=2^i z_3$ and "fill in". For example, if $n=1001$, the sequence 1, 2, 3, 6, 12, 24, 48, 96, 192, 384, 333 will do. In general, such a sequence S can be constructed with $|S|\leqq\log_2 n+O(1)$.

Let M be the union of the three sequences. $(M\cup(n-M), n)$ is suresum. For let $M\cup(n-M)$ be 2-colored. Suppose $\alpha_1, \dots, \alpha_r \in M$, $\alpha=\alpha_1+\dots+\alpha_r\in M$ and $\alpha_1, \dots, \alpha_r$ are colored Red. If α is Blue, then $\{\alpha_1, \dots, \alpha_r, n-\alpha\}$ or $\{\alpha, n-\alpha\}$ is monochromatic. Thus we assume α is Red. (We require $\alpha_i<n/2$ to be certain $n-\alpha\neq\alpha_i$.) Either 1, 2 or 1, 3 or 2, 3 is monochromatic. All cases give monochromatic chains which give n as a monochromatic sum. This construction yields

$$f(n) \leqq 6 \log_2 n+O(1).$$

Surprisingly, this construction does not seem to generalize to more than two colors. Even with two colors, we have not succeeded in finding a small $(=O(\ln n))$ suresum (A, n) without pairs $a, n-a\in A$.

3. More than two colors

Recall $f_r(n)$ denotes the minimal $|C|$ where $C\subseteqq\{1, \dots, n-1\}$ and if C is r-colored, there exists a monochromatic set with sum n. We let $P(X)$ denote the set of sums (allowing an arbitrary number of distinct summands) of X.

Theorem 2. $f_r(n)\leqq e^{c_r\sqrt{\ln n}}$.

For a lower bound, we have only $f_r(n)\geqq f(n)\geqq \ln n/\ln\ln n$. Thus a great gap remains in the evaluation of $f_r(n)$. We give the proof only for $r=3$. The construction itself is quite simple. Set

$$C = \{a_0+a_1D+\dots+a_tD^t+D^{t+1}\colon\ 0 \leqq a_i < 10\},$$

where we assume

(i) $10^{t+1} > 10^{20}Dt$,

(ii) $10!|D$ (a convenience),

(iii) D is "sufficiently large";

(iv) $D^{t+3} \leqq n \leqq (9D)^{t+1}$.

We shall show that if $C=X_1\cup X_2\cup X_3$, then $n\in P(X_i)$ for some i. This implies Theorem 2 as we may take $t\sim 50\sqrt{\ln n}$ and D satisfying (ii), (iv). (For $r>3$ the construction differs only in replacing $0\leqq a_i<10$ by $0\leqq a_i<K_r$ for appropriate K_r.) We make no attempts to find best possible constants. Assumption (iii) is made tacitly throughout the proof.

The result $n\in P(X_i)$ cannot be simply a density result on $|X_i|$. It is possible that for some small d, $d|x$ for all $x\in X_i$ and $d\nmid n$. We will show that if there are no such divisibility problems and $|X_i|$ is sufficiently large, then $n\in P(X_i)$.

Similar results for *infinite* X_i are given by P. Erdős [1] and J. Folkman [2].

Definition. A is *multiple* if for some $m, 2\leqq m\leqq 10$ and i, $0\leqq i<m$, $P(A)$ contains no $x\equiv i \mod m$. Otherwise A is non-multiple.

Lemma 1. *If A is multiple, $|A-dZ|<100$ for some $d, 2\leqq d\leqq 10$.*

Proof. Let m, i be given by the above definition. Set

$$R = \{j\colon\ 0 \leqq j < m,\ a \equiv j \mod m \text{ for at least } 10\ a \in A\}.$$

Set $d = \gcd(m, R)$. If $d=1$, there exist $j_1, \ldots, j_s \in R$; $n_1, \ldots, n_s \in Z$ so that

$$n_1 j_1 + \ldots + n_s j_s \equiv i \mod m.$$

We may find the above n_u with $0 \leqq n_u < m$ as the equation is $\bmod m$. A contains n_u elements $\equiv j_u \bmod m$ and these $n_1 + \ldots + n_s$ elements sum to $i \bmod m$. Thus $d > 1$. At most, 10 elements of $A - dZ$ lie in each residue class mod m so $|A - dZ| \leqq \leqq 10m \leqq 100$. ▮

Lemma 2. *If A is nonmultiple, there exists $M \subseteqq A$, M nonmultiple, $|M| \leqq 440$.*

Proof. It suffices to find, for each of the 44 (m, i), a set of $\leqq m \leqq 10$ elements with sum $\equiv i \bmod m$. Fixing (m, i), there exists a sum $a_1 + \ldots + a_r \equiv i \bmod m$. Assume $r \geqq m$. Set $s_u = a_1 + \ldots + a_u$. By the Pigeon-Hole Principle there exist $1 \leqq u < v \leqq r$ so that $s_u \equiv s_v \bmod p$. Then

$$a_1 + \ldots + a_u + a_{v+1} + \ldots + a_r \equiv i \mod m.$$

We may continue this reduction until $\leqq m$ summands remain. ▮

Of course, 100 and 440 are overestimates in the above lemmas but they suffice for our purpose.

Theorem 3. *If $A \subseteqq C$, $|A| \geqq 0.12|C|$, A nonmultiple, then*

$$P(A) \supseteqq [D^{t+3}, (9D)^{t+1}].$$

The proof proceeds in stages. First let $M \subseteqq A$, $|M| \leqq 440$, M nonmultiple and set $A_1 = A - M$ so that $|A_1| \geqq 0.11|C|$.

For $0 \leqq i \leqq t$, we split C into 10^t equivalence classes — two elements in the same class if they differ only in their i-th D-ary digit. Formally, $x \equiv y$ iff $|x-y| = = sD^i$ where $0 \leqq s < 10$. As $|A_1| \geqq 1.1 \cdot 10^t$ at least 0.01 of the classes have at least two elements of A_1 and thus, there are $0.001 \cdot 10^t$ disjoint pairs (a, a') where $a' - a = sD^i$ for some fixed s. As $0.001 \cdot 10^t > 10^{10} D(t+1)$, we find simultaneously in A_1 distinct elements a_{ij}, a'_{ij} for $0 \leqq i \leqq t$, $1 \leqq j \leqq 10^6 D$ so that

$$a'_{ij} - a_{ij} = s_i D^i$$

where $0 < s_i < 10$. The next lemma is the heart of the proof.

Lemma 3. *If $0 \leqq x \leqq 10^6 D^{t+1}$ and $s_0 | x$, there exist $n_0, n_1, \ldots, n_t$, $0 \leqq n_i \leqq 10^6 D$ so that*

$$x = \sum_{i=0}^{t} n_i (S_i D^i).$$

Proof. We find the n_i by reverse induction (beginning at $i = t$), letting n_i be as large as possible so that the partial sum does not exceed x (a greedy algorithm). At any point the "slack" $x - n_t(s_t D^t) - \ldots - n_{i+1}(s_{i+1} D^{i+1})$ is at most $s_{i+1} D^{i+1} < 10 D^{i+1}$ so may be made up by the $n_i(s_i D^i)$ term. At the last step, the slack is divisible by s_0, since $s_0 | x$ and $s_0 | D$ (here we use $10! | D$) so exact equality is achieved. ▮

Let

$$B_1 = \{a_{ij}\colon\ 0 \leqq i \leqq t,\ 1 \leqq j \leqq 10^6 D\},$$
$$B_2 = \{a'_{ij}\colon\ 0 \leqq i \leqq t,\ 1 \leqq j \leqq 10^6 D\},$$
$$K = \sum_{b \in B_1} b.$$

Since $D^{t+1} \leqq x \leqq 2D^{t+1}$ for all $x \in A$,

$$10^6(t+1)D^{t+2} \leqq K \leqq 2 \cdot 10^6(t+1)D^{t+2}.$$

Lemma 4. $P(B_1 \cup B_2) \supseteqq \{y\colon\ y \equiv K \mod s_0,\ K \leqq y \leqq K + 10^6 D^{t+1}\}$.

Proof. Applying Lemma 3, set

$$y - K = \sum_{i=0}^{t} n_i(s_i D^i).$$

Begin with the set B_1 and, for $0 \leqq i \leqq t$, replace exactly n_i of the a_{ij} by the corresponding a'_{ij}. The set obtained has sum y. ▮

Lemma 5. $P(M \cup B_1 \cup B_2) \supseteqq [K + 20D^{t+1},\ K + 10^6 D^{t+1}]$.

Proof. Let $K + 20D^{t+1} \leqq z \leqq K + 10^6 D^{t+1}$. We find, using Lemma 2, $a_1, \ldots, a_r \in M$, $r \leqq 10$ so that

$$z - K \equiv a_1 + \ldots + a_r \mod s_0.$$

Thus, $z - (a_1 + \ldots + a_r) \in P(B_1 \cup B_2)$ so $z \in P(M \cup B_1 \cup B_2)$. ▮

Proof of Theorem 3. Let $E = A - (M \cup B_1 \cup B_2)$. We have selected D, t so that $|M \cup B_1 \cup B_2| \ll |A|$ and $|E| \geqq 0.1\,|C|$. Order $E = \{e_1, e_2, \ldots\}$ arbitrarily. Let $D^{t+3} \leqq z \leqq (9D)^{t+1}$. Bound have been arranged with "room to spare" so that $z \leqq \sum_{e \in E} e$ and $K + 20D^{t+1} \leqq z$. The sequence $z, z - e_1, z - e_1 - e_2, \ldots, z - e_1 - \ldots - e_i, \ldots$ has gaps at most $2D^{t+1}$ so some

$$z - e_1 - \ldots - e_i \in [K + 20D^{t+1},\ K + 10^6 D^{t+1}] \subseteqq P(M \cup B_1 \cup B_2).$$

Whence $z \in P(M \cup B_1 \cup B_2 \cup E) = P(A)$. ▮

To show C is a sureset, we prove that if $C = X_1 \cup X_2 \cup X_3$, then one of the X_i meets the conditions of Theorem 3. Suppose $|X_1| \geqq |X_2| \geqq |X_3|$ and X_1, X_2 do not meet the conditions. As $|X_1| \geqq |C|/3$, $X_1 \subseteqq d_1 Z$ (except for 100 ignorable elements) with $d_1 \geqq 2$. Thus $|X_1| \leqq |C|/2$ so $|X_2| \geqq |C|/4$ so $X_2 \subseteqq d_2 Z$. But d_1, d_2 can cover at most 7 of the 10 residue classes (when $d_1 = 2, d_2 = 3$) leaving X_3 satisfying the conditions of Theorem 3 and $n \in P(X_3)$ as desired.

References

[1] P. Erdős, On the representation of large integers as sums of distinct summands taken from a fixed set, *Acta Arith.* **7** (1962), 345—354.

[2] J. Folkman, On the representation of integers as sums of distinct terms from a fixed sequence, *Canad. J. Math.* **18** (1966), 643—655.

[3] J. E. Graver, A survey of the maximum depth problem for indecomposible exact covers, *in: Infinite and Finite Sets* (A. Hajnal *et. al.*, eds.), *Colloq. Math. Soc. János Bolyai* **10**, North-Holland 1975, Vol. II, 731—744.