COLLOQUIUM MATHEMATICUM

VOL. 86 2000 NO. 2

PROBABILISTIC CONSTRUCTION OF SMALL STRONGLY SUM-FREE SETS VIA LARGE SIDON SETS

BY

ANDREAS BALTZ (KIEL), TOMASZ SCHOEN (KIEL AND POZNAŃ) AND ANAND SRIVASTAV (KIEL)

Abstract. We give simple randomized algorithms leading to new upper bounds for combinatorial problems of Choi and Erdős: For an arbitrary additive group G let $\mathcal{P}_n(G)$ denote the set of all subsets S of G with n elements having the property that 0 is not in $S+S$. Call a subset A of G admissible with respect to a set S from $\mathcal{P}_n(G)$ if the sum of each pair of distinct elements of A lies outside S. Suppose first that S is a subset of the positive integers in the interval $[2n, 4n)$. Denote by $f(S)$ the number of elements in a maximum subset of $[n, 2n)$ admissible with respect to S. Choi showed that $f(n) := \min\{|S| + f(S) \mid S \subseteq [2n, 4n)\} = \mathcal{O}(n^{3/4})$. We improve this bound to $\mathcal{O}((n \ln n)^{2/3})$. Turning to a problem of Erdős, suppose that S is an element of $\mathcal{P}_n(G)$, where G is an arbitrary additive group, and denote by $h(S)$ the maximum cardinality of a subset A of S admissible with respect to S. We show $h(n) := \min\{h(S) \mid G \text{ a group}, \ S \in \mathcal{P}_n(G)\} = \mathcal{O}((\ln n)^2)$.

Our approach relies on the existence of large Sidon sets.

1. Introduction. In this paper we are concerned with the following question of Erdős [2]:

Let $a_1, \ldots, a_n$ be distinct real numbers. A subset $a_{i_1}, \ldots, a_{i_k}$ is called *strongly sum-free* if $a_{i_j} + a_{i_l} \neq a_r$ for all $1 \leq j < l \leq k$, $1 \leq r \leq n$. Let $g(n)$ be the maximum cardinality of a strongly sum-free set. How large is $g(n)$?

The best known bounds so far have been given by Choi [1] who proved that

$$g(n) \geq \ln n$$

and, using sieve methods, showed

$$g(n) = \mathcal{O}(n^{2/5+\varepsilon}).$$

Moreover, Choi observed that in Erdős's problem it is enough to consider the case when all $a_1, \ldots, a_n$ are non-negative integers. Choi also considered the following variant of the problem:

2000 *Mathematics Subject Classification*: 05D05.

The first author is supported by the graduate school "Effiziente Algorithmen und Mehrskalenmethoden", Deutsche Forschungsgesellschaft.

Let us call a set A of non-negative integers *admissible* with respect to a set S of non-negative integers if the sum of each pair of distinct elements of A lies outside S. Let $n \in \mathbb{N}$, and suppose that S is a subset of the interval $[2n, 4n)$. Denote by $f(S)$ the number of elements in a maximum subset of $[n, 2n)$ admissible with respect to S, and define $f(n)$ by

$$f(n) := \min\{|S| + f(S) \mid S \subseteq [2n, 4n)\}.$$

How large is $f(n)$?

It is easy to see that $f(n) \geq \sqrt{n}$: Given $|S| < \sqrt{n}$ one can construct an admissible set A by successively selecting $a_i \in [n, 2n) \setminus D_i$, where $D_1 := \emptyset$ and $D_{i+1} := -a_i + S$. In each step we remove at most $|S|$ elements, so the procedure can be carried out at least $n/|S| > \sqrt{n}$ times yielding an admissible set of the claimed size.

For an upper bound Choi proved that $f(n) = \mathcal{O}(n^{3/4})$ and conjectured $f(n) = \mathcal{O}(n^{1/2+\varepsilon})$.

In this article we show that $f(n) = \mathcal{O}(n^{2/3} \ln^{2/3} n)$ improving the previous upper bound given by Choi (Theorem 2). As a consequence, the function $g(n)$ which appears in Erdős's problem is bounded from above by $\mathcal{O}(n^{2/5} \ln^{2/5} n)$ (Corollary 3). The probabilistic proof of this result is based on a deep theorem of Komlós, Sulyok, and Szemerédi [4] who showed that every set $A \subseteq \mathbb{N}$ contains a Sidon set of size $\Theta(\sqrt{|A|})$.

Finally, we study the following more general version of Erdős's problem (see [2] and [3]). Let G be an arbitrary additive group with at least n elements and let $\mathcal{P}_n(G)$ denote the set of all subsets S of G satisfying $|S| = n$ and $0 \notin S+S$. (The latter condition prevents us from taking S as a subgroup of G.) If the maximum cardinality of a subset A of $S \in \mathcal{P}_n(G)$ admissible with respect to S is $h(S)$, how large is

$$h(n) := \min\{h(S) \mid G \text{ a group},\ S \in \mathcal{P}_n(G)\}?$$

It is shown in [5] that $h(n) \geq 3$ for abelian groups. We estimate $h(n)$ from above by showing that $h(n) = \mathcal{O}(\ln^2 n)$.

NOTATIONS. As we consider only intervals of positive integers we abbreviate $[a, b] \cap \mathbb{N}$, $(a, b] \cap \mathbb{N}$, and $[a, b) \cap \mathbb{N}$ (for positive numbers a and b) by $[a, b]$, $(a, b]$, and $[a, b)$. If z is an integer and S, T are sets of integers we define:

- $z + S := \{z + s \mid s \in S\}$,
- $z - S := \{z - s \mid s \in S\}$,
- $z \cdot S := \{z \cdot s \mid s \in S\}$,
- $S + T := \{s + t \mid s \in S,\ t \in T\}$,
- $S \dot{+} T := \{s + t \mid s \in S,\ t \in T,\ s \neq t\}$.

In our approach Sidon sets play a key role.

A *Sidon set* is a set of integers with the property that all pairwise sums of its elements are distinct. For us the crucial property of a Sidon set S is

$$|S \dot{+} S| = \binom{|S|}{2}. \tag{1}$$

By c, c', c_1, c_2 we denote absolute constants, which depend neither on the size of the group G, nor on the choice of its subset S.

2. Strongly sum-free sets in $\mathbb{N}$. Komlós, Sulyok, and Szemerédi proved the following remarkable theorem generalizing the celebrated Erdős–Turán theorem that the size of a Sidon set in $[1,n]$ is $\Theta(\sqrt{n})$.

LEMMA 1 (Komlós, Sulyok and Szemerédi). *There is an absolute constant $c > 0$, such that each finite set A of positive integers contains a Sidon set with at least $c \cdot |A|^{1/2}$ elements.*

THEOREM 2. $f(n) = \mathcal{O}(n^{2/3} \ln^{2/3} n)$.

Proof. Choose a random subset $S \subseteq [2n, 4n)$ by picking each element independently with probability $p = ((\ln^2 n)/n)^{1/3}$. Let

$$r := \lceil 2(n \ln n)^{1/3} \rceil$$

and define

$$\mathcal{S}_r := \{R \subseteq [n, 2n) \mid R \text{ a Sidon set, } |R| = r\}.$$

For every $R \in \mathcal{S}_r$ we consider the indicator random variable

$$X_R := \begin{cases} 1 & \text{if } (R \dot{+} R) \cap S = \emptyset, \\ 0 & \text{otherwise.} \end{cases}$$

Then the random variable $X := \sum_{R \in \mathcal{S}_r} X_R$ counts the number of Sidon sets $R \subseteq [n, 2n)$ with $|R| = r$ and $(R \dot{+} R) \cap S = \emptyset$. We have

$$\begin{aligned} \mathbb{E}(X) &= \sum_{R \in \mathcal{S}_r} \mathbb{E}(X_R) = \sum_{R \in \mathcal{S}_r} \mathbb{P}((R \dot{+} R) \cap S = \emptyset) \\ &= \sum_{R \in \mathcal{S}_r} \mathbb{P}(a + b \notin S \text{ for all } a, b \in R \text{ where } a \neq b). \end{aligned}$$

As R is a Sidon set, all of the sums $a + b$ are distinct. Since due to (1) for each R we have $|R \dot{+} R| = \binom{|R|}{2} = (r^2 - r)/2$ independent events, the probability that none of the elements of $R \dot{+} R$ belongs to the random set S is equal to $(1-p)^{r(r-1)/2}$. This yields

$$\begin{aligned} \mathbb{E}(X) &= \sum_{R \in \mathcal{S}_r} (1-p)^{(r^2 - r)/2} \le \binom{n}{r} (1-p)^{(r^2 - r)/2} \\ &\le \left(\frac{en}{r}\right)^r [(1-p)^{1/p}]^{(r^2 - r)p/2} \end{aligned}$$

$$\leq \left(\frac{en}{re^{(rp-p)/2}}\right)^r \leq \left(\frac{en}{re^{rp/2}}\right)^r \leq \frac{en}{2(n\ln n)^{1/3}n}.$$

Since the above expression can be made arbitrarily small by choosing n large enough,

$$\mathbb{P}(|S| \geq 4(n\ln n)^{2/3}) + \mathbb{P}(X \geq 1) \leq 1/2 + \mathbb{E}(X) < 1.$$

Hence there exists $S \subseteq [2n, 4n)$ of size $\mathcal{O}(n^{2/3}\ln^{2/3} n)$ such that every Sidon set R of size *at least* r satisfies $(R \dotplus R) \cap S \neq \emptyset$.

Let A be a (maximum) subset of $[n, 2n)$ with $(A \dotplus A) \cap S = \emptyset$. From Lemma 1 we know that A contains a Sidon set R with cardinality $c \cdot \sqrt{|A|}$. Obviously, $(R \dotplus R) \cap S = \emptyset$ and thus

$$|A| = \frac{1}{c^2}|R| < \frac{1}{c^2}r^2 = \mathcal{O}(n^{2/3}\ln^{2/3} n).$$

We conclude that $f(n) \leq |S| + |A| = \mathcal{O}(n^{2/3}\ln^{2/3} n)$. ∎

COROLLARY 3. $g(n) = \mathcal{O}(n^{2/5}\ln^{2/5} n)$.

Proof. Let $m := \lfloor n^{3/5} \rfloor$. From Theorem 2 we know that there exists $S' \subseteq [2m, 4m)$ of size at most $c_1(m\ln m)^{2/3}$ such that any subset $A' \subseteq [m, 2m)$ admissible with respect to S' has no more than $c_2(m\ln m)^{2/3}$ elements. Obviously, for any $k \in \mathbb{N}$ the set $2^{k-1} \cdot S'$ has the property that no subset of $2^{k-1} \cdot [m, 2m)$ consisting of more than $c_2(m\ln m)^{2/3}$ elements is admissible with respect to S'.

Now choose

$$k := \frac{n - |S'|}{m}$$

and define

$$S := \Big(\bigcup_{i=1}^{k} 2^{i-1} \cdot [m, 2m)\Big) \cup 2^{k-1} \cdot S'.$$

We have

$$|S| = k \cdot m + |S'| = n.$$

Let $A \subseteq S$ be a set of maximum cardinality admissible with respect to S. Clearly, $2^{k-1} \cdot S' \subseteq A$. Further, A contains at most 2 elements from each set $2^{i-1} \cdot [m, 2m)$, $i \in \{1, \ldots, k-1\}$, and at most $c_2(m\ln m)^{2/3}$ elements from $2^{k-1} \cdot [m, 2m)$. Thus $|A| \leq 2(k-1) + (c_1 + c_2)(m\ln m)^{2/3} = \mathcal{O}(n^{2/5}\ln^{2/5} n)$. ∎

3. Strongly sum-free sets in $\mathbb{Z}_n$

THEOREM 4. $h(n) = \mathcal{O}(\ln^2 n)$.

Proof. We shall show a slightly stronger statement, proving that there exists $S \in \mathcal{P}_n(\mathbb{Z}_{2n+1})$ such that each $A \subseteq \mathbb{Z}_{2n+1}$ admissible with respect to S has no more than $\mathcal{O}(\ln^2 n)$ elements.

Choose a random subset $T \subseteq [1,n]$ by selecting each element with probability $p = 1/2$. Set

$$S := T \cup \{[n+1, 2n] \setminus (2n+1-T)\}.$$

Clearly, $0 \notin S+S$ and $|S| = |T| + (n - |T|) = n$.

Let X_r^1, X_r^2, X_r^3, and X_r^4 be random variables counting the number of Sidon sets R of size r in $[1, n/2]$, $(n/2, n]$, $(n, 3n/2]$ and $(3n/2, 2n]$ respectively, where R satisfies $(R \dotplus R) \cap S = \emptyset$. (Note that any such R is a Sidon set in $\mathbb{Z}_{2n+1}$ if and only if it is a Sidon set in $\mathbb{N}$.)

As in the proof of Theorem 2 we estimate

$$\mathbb{E}(X_r^i) \le \binom{n/2}{r}(1-p)^{\binom{r}{2}} \le \left(\frac{en}{2re^{(r-1)/4}}\right)^r, \quad i \in \{1,3\},$$

and

$$\mathbb{E}(X_r^i) \le \binom{n/2}{r}p^{\binom{r}{2}} \le \left(\frac{en}{2re^{(r-1)/4}}\right)^r, \quad i \in \{2,4\}.$$

Choosing

$$r := 4\ln(en)$$

we get

$$\mathbb{E}(X_r^i) \le \frac{e^{1/4}}{8\ln(en)} < \frac{1}{4}$$

and hence by Markov's inequality

$$\mathbb{P}(X_r^1 \ge 1) + \mathbb{P}(X_r^2 \ge 1) + \mathbb{P}(X_r^3 \ge 1) + \mathbb{P}(X_r^4 \ge 1) < 1.$$

Thus there exists $S \in \mathcal{P}_n(\mathbb{Z}_{2n+1})$ such that every Sidon set R in $[1, n/2]$, $(n/2, n]$, $(n, 3n/2]$ or $(3n/2, 2n]$ of size *at least* $4\ln(en)$ has the property $(R \dotplus R) \cap S \ne \emptyset$.

Let A be a subset of $[1, 2n]$ admissible with respect to S and let

$$A_1 := A \cap [1, n/2], \quad A_2 := A \cap (n/2, n],$$
$$A_3 := A \cap (n, 3n/2], \quad A_4 := A \cap (3n/2, 2n].$$

The pigeon-hole principle gives

$$|A_j| \ge |A|/4$$

for some $j \in \{1,2,3,4\}$. From Lemma 1, $c\sqrt{|A_j|}$ elements in A_j form a Sidon set, and we conclude that $|A| \le 4 \cdot |A_j| \le (4/c^2) \cdot r^2 = \mathcal{O}(\ln^2 n)$. ∎

REFERENCES

[1] S. L. G. Choi, *On a combinatorial problem in number theory*, Proc. London Math. Soc. (3) 23 (1971), 629–642.

[2] P. Erdős, *Extremal problems in number theory*, in: Proc. Sympos. Pure Math. 8, Amer. Math. Soc., Providence, RI, 1965, 181–189.
[3] R. F. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 1994, Problem C14, 128–129.
[4] J. Komlós, M. Sulyok and E. Szemerédi, *Linear problems in combinatorial number theory*, Acta Math. Acad. Sci. Hungar. 26 (1975), 113–121.
[5] T. Łuczak and T. Schoen, *On strongly sum-free subsets of abelian groups*, Colloq. Math. 71 (1996), 149–151.

Mathematisches Seminar
Christian-Albrechts-Universität zu Kiel
Ludewig-Meyn-Str. 4
D-24098 Kiel, Germany
E-mail: aba@numerik.uni-kiel.de
tos@numerik.uni-kiel.de
asr@numerik.uni-kiel.de

Department of Discrete Mathematics
Adam Mickiewicz University
60-769 Poznań, Poland

Received 4 May 1999;
revised version 1 December 1999
(3746)