Inf. Proc. Letters 49 (1994), 255-256.

Selection of a Large Sum-Free Subset in Polynomial Time

Mihail N. Kolountzakis

Department of Mathematics, Stanford University, Stanford, CA 94305

E-mail: kolount@cauchy.stanford.edu

July 1993; revised October 1993

Abstract

A set E of integers is called sum-free if $x + y \neq z$ for all $x, y, z \in E$. Given a set $A = \{n_1, \ldots, n_N\}$ of integers we show how to extract a sum-free subset E of A with $|E| > N/3$. The algorithm requires polynomial time in the size of the input.

Keywords: Algorithms, Combinatorial Problems, Additive Number Theory

A subset E of an additive group is called *sum-free* if $x + y \neq z$ for all $x, y, z \in E$. Erdős [3] and Alon and Kleitman [1] have proved that every set $A = \{n_1, \ldots, n_N\}$ of integers has a sum-free subset E, with $|E| > N/3$. The proof is probabilistic and in [1] the question was posed whether there exists a deterministic algorithm for the selection of such a subset E, which runs in time polynomial in the size of the problem, that is in $l = \sum_{j=1}^{N} \log_2 n_j$. We assume that l is large. The purpose of this note is to point out that, with a slight modification, the proof given in [1] can be transformed to such an algorithm. A similar algorithm was independently found by Alon, Kriz and Nešetřil [2].

Sum-free sets have been used to estimate Ramsey numbers from below [4, p. 125, 247]. Many lower bounds for Ramsey numbers have been found by decomposing a certain group into a small collection of sum-free subsets, so that an algorithm which extracts a large sum-free subset could conceivably be of great help.

For a prime p write $\mathbf{Z}_p = \{0, \ldots, p-1\}$ for the field of the integers mod p and $\mathbf{Z}_p^\times = \{1, \ldots, p-1\}$ for the multiplicative group of units in $\mathbf{Z}_p$.

Theorem 1 *Let $p = 3k + 2$ be a prime number and $w(x)$ a nonnegative function defined on $\mathbf{Z}_p^\times$. Define $w = \sum_{x \in \mathbf{Z}_p^\times} w(x)$ and assume $w > 0$. Then there is a sum-free subset E' of $\mathbf{Z}_p^\times$ for which*

$$\sum_{x \in E'} w(x) > \frac{1}{3} w. \qquad (1)$$

51

Proof: Write $S = \{k+1, \dots, 2k+1\}$ and observe that S is sum-free in $\mathbf{Z}_p$ and $|S| > (p-1)/3$. Let the random variable t be uniformly distributed in $\mathbf{Z}_p^\times$ and write

$$f(t) = \sum_{t \cdot x \in S} w(x).$$

(The product $t \cdot x$ is computed in $\mathbf{Z}_p$.) Since $\mathbf{Z}_p^\times$ is a multiplicative group we have $\mathbf{E}f(t) = \frac{|S|}{p-1} w > w/3$. Consequently there is a $t_0 \in \mathbf{Z}_p^\times$ for which $f(t_0) > w/3$. Define $E' = t_0^{-1} S$. It follows that E' is sum-free and (1) is true. **QED**

Observe that the number of prime factors of an integer x is at most $\log_2 x$. This means that the number of primes which appear in the factorization of any element of A is at most l. Thus (using, say, the Prime Number Theorem for arithmetic progressions) there is a prime $p = 3k+2$, not greater than $3l \log l$, which does not divide any member of A.

Define now $w(x) = |\{t \in A : t = x \bmod p\}|$. Since p does not divide any member of A we have $w = N$ and, using our Theorem 1, we find a sum-free $E' \subseteq \mathbf{Z}_p^\times$ for which the set $E = \{t \in A : t \bmod p \in E'\}$ has more than $N/3$ elements. But E is sum-free since $x + y = z$ for some $x, y, z \in E$ would imply $x + y = z \bmod p$ and E' would not be sum-free.

In summary the steps of our algorithm are the following.

1. Compute all primes up to $3l \log l$.
2. Find one such prime $p = 3k + 2$ which divides no element of A.
3. Compute the function $w(x)$ for all $x \in \mathbf{Z}_p^\times$.
4. Find by exhaustive search a $t_0 \in \mathbf{Z}_p^\times$ for which $f(t_0) > N/3$ and compute the set $E' = t_0^{-1} S$.
5. Construct the set $E = \{t \in A : t \bmod p \in E'\}$.

All the above can obviously be carried out in time polynomial in l.

References

[1] N. Alon and D. J. Kleitman, *Sum-free subsets*, in A. Baker, B. Bollobás, and A. Hajnál, eds., A Tribute to Paul Erdős, Cambridge University Press (1990), 13-26.

[2] N. Alon, I. Kriz and J. Nešetřil, *How to color shift hypergraphs*, to appear.

[3] P. Erdős, *Extremal problems in number theory*, Proceedings of the Symp. Pure Math., VIII, AMS (1965), 181-189.

[4] W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Lect. Notes Math. 292 (1972), Springer-Verlag, Berlin.

52