MARK CHAIMOVICH

New algorithm for dense subset-sum problem

Astérisque, tome 258 (1999), p. 363-373
<http://www.numdam.org/item?id=AST_1999__258__363_0>

Astérisque **258**, 1999, p. 363–373

NEW ALGORITHM FOR DENSE SUBSET-SUM PROBLEM

by

Mark Chaimovich

Abstract. — A new algorithm for the dense subset-sum problem is derived by using the structural characterization of the set of subset-sums obtained by analytical methods of additive number theory. The algorithm works for a large number of summands (m) with values that are bounded from above. The boundary (ℓ) moderately depends on m. The new algorithm has $O(m^{7/4}/\log^{3/4} m)$ time boundary that is faster than the previously known algorithms the best of which yields $O(m^2/\log^2 m)$.

1. Introduction

Consider the following subset-sum problem (see [**13**]). Let $A = \{a_1, \dots, a_m\}$, $a_i \in \mathbb{N}$. For $B \subseteq A$, let $S_B = \sum_{a_i \in B} a_i$ and let $A^* = \{S_B \mid B \subseteq A\}$. The problem is to find the maximal subset-sum $S^* \in A^*$ satisfying $S^* \leq M$ for a given target number $M \in \mathbb{N}$.

Although the problem is NP-hard (the partition problem is easily reduced to the SSP), its restriction can be solved in polynomial time. Denote $\ell = \max\{a_i \mid a_i \in A\}$. Introducing restriction $\ell \leq m^\alpha$ where α is some positive real number (or equivalently $m \geq \ell^{1/\alpha}$), one can easily solve problems from this restricted class in $O(m^2\ell)$ time using dynamic programming.

This work belongs to the school of thought that applies analytical methods of number theory to integer programming (see [**8**], [**2**]). It continues the application of a new approach, the main idea of which is as follows: analytical methods enable us to effectively characterize the set A^* of subset-sums as a collection of arithmetic progressions with a common difference (see [**7**], [**12**], [**1**], [**10**]). Once this characterization is obtained, it is quite easy to find the largest element of A^* that is not greater than the given M.

Efficient algorithms have recently been derived using the new approach. In almost linear time (with respect to the number m of summands) they solve the following class

1991 ***Mathematics Subject Classification.*** — Primary: 90C10 Alternate: 05A17, 11B25, 68Q25.
Key words and phrases. — Analytical Number Theory, Integer Programming, Subset Sum Problem.

of SSP: the target number M is within a wide range of the mid-point of the interval $[0, S_A]$ and $m > c\ell^{2/3}\log^{1/3}\ell$, $\ell > \ell_0$ when A is a set of distinct summands ([**9**], [**4**], [**6**], [**11**]) or $m > 6\ell\log\ell$ when A is an arbitrary multi-set without any limitation on the number of distinct summands ([**5**]). Here and further on $\ell_0, c, c_1, c_2, \dots$ denote some absolute positive constants.

The latest analytical result ([**10**]) allows one to apply the algorithm from [**9**] to problems with density $m > c_1(\ell\log\ell)^{1/2}$. The algorithm from [**11**] works for density $m > c_2\ell^{1/2}\log\ell$ which is almost the same as in [**10**]. For $m < \ell^{2/3}$, the time boundary for both algorithms is estimated as $O((\frac{\ell}{m})^2)$, i.e., $O(\frac{m^2}{\log^2 m})$ for the lowest density $(m \sim (\ell\log\ell)^{1/2})$.

This work refines the structural characterization of the set of subset-sums which allows us to use more efficient conditions in the process of determining the structure. These refinements are discussed in Section 2. They lead to the development of a new algorithm which is described in Section 3. It works in $O(m\log m + \min\{\frac{\ell^{5/4}\log^{1/2}\ell}{m^{3/4}}, (\frac{\ell}{m})^2\})$ time which improves [**9**] and [**11**] for $m \le \frac{\ell^{3/5}}{\log^{2/5}\ell}$ and yields $O(m^{7/4}/\log^{3/4} m)$ time for $m \sim (\ell\log\ell)^{1/2}$.

2. Refinement of the structural characterization of the set A^* of subset-sums

The following Theorem 2.1 [**10**] determines the structure of the set A^* of subset-sums for $m > c_1(\ell\log\ell)^{1/2}$ as a long segment of an arithmetic progression.

***Theorem 2.1* (G. Freiman).** — *Let $A = \{a_1, \dots, a_m\}$ be a set of m integers taken from the segment $[1, \ell]$. Assume that $m > c_1(\ell\log\ell)^{1/2}$ and $\ell > \ell_0$.*
(i) There is an integer d, $1 \le d \le \frac{3\ell}{m}$, such that

$$|A(0,d)| > m - d \tag{1}$$

and

$$\{M : M \equiv 0 (\operatorname{mod} d), |M - \tfrac{1}{2}S_{A(0,d)}| \le c_2 dm^2\} \subseteq A^*(0,d),$$

where $A(s,t) = \{a : a \equiv s(\operatorname{mod} t), a \in A\}$.
(ii) If for all prime numbers p, $2 \le p \le \frac{3\ell}{m}$,

$$|A(0,p)| \le m - \frac{3\ell}{m}, \tag{2}$$

then the assertion (i) of the Theorem holds true with $d = 1$.

Simple consideration shows that verification of condition (2) is crucial for the structural characterization of a set A^* of subset-sums. Algorithms from [**9**] and [**11**] use this condition directly ([**9**]) or indirectly ([**11**]). Our intention is to replace condition (2) by a condition (or a set of conditions), verification of which is easier in the sense that the number of required operations is smaller. To do this we introduce the notion of *d-full set.* We say that set A is d-full if A^* contains all classes of residues modulo d, i.e., in other words, $A^*(\operatorname{mod} d) = \{0, 1, \dots, d-1\}$.

Let us study some properties of d-full sets.

Define $S_{r(\mathrm{mod}\, d)} = \min\{s \in A^*, s \equiv r(\mathrm{mod}\, d)\}$.

Lemma 2.2. — *Let A be a set of integers taken from the segment $[1,\ell]$. Suppose that A is d-full. Then for each r, $0 < r < d$,*

$$S_{r(\mathrm{mod}\, d)} \leq d\ell. \tag{3}$$

Proof. — Assume that for some r condition (3) is not true, i.e., $S_{r(\mathrm{mod}\, d)} > d\ell$. This means that $S_{r(\mathrm{mod}\, d)} = a_{i_1} + a_{i_2} + \cdots + a_{i_k}$ for some $k > d$. Consider the sequence of subset-sums $T_s = \sum_{j=1}^{s} a_{i_j}$, $1 \leq s \leq k$. Obviously, at least two of these sums (assume T_s and T_q, $s < q$) belong to the same residue class modulo d (since $k > d$). Then $T_q - T_s \equiv 0(\mathrm{mod}\, d)$ and subset-sum $T_k - (T_q - T_s) = a_{i_1} + \cdots + a_{i_s} + a_{i_{q+1}} + \cdots + a_{i_k} \equiv r(\mathrm{mod}\, d)$ and this subset-sum is smaller than $S_{r(\mathrm{mod}\, d)}$. This fact contradicts the minimality of $S_{r(\mathrm{mod}\, d)}$. □

Lemma 2.3. — *Suppose that the set A is d-full. Then there is a d-full subset of A with cardinality less than d.*

Proof. — Let us assume that contrary to the Lemma the smallest d-full subset of A has more than $d-1$ elements. Denote this subset by $A' = \{a_1, \ldots, a_k\}$. In fact, $d \not| a_i$ for all i's.

Let B be the multi-set of non-zero residues modulo d in A', that is B is composed with $|A'(i,d)|$ times i for any $1 \leq i < d$. Naturally one has $B^* = (A')^*(\mathrm{mod}\, d)$. Then, as a multi-set, $|B| = \sum_{i=1}^{d-1} |A'(i,d)| \geq d$, by the assumption.

Define a sequence of multi-sets $B_0, B_1, \ldots, B_k$ as follows: B_0 is an empty set and $B_i = \{b_1, \ldots, b_i\}$ for $i > 0$. Note that $0 \in B_i^*$ (since it is the sum of an empty subset), and that

$$B_i^* = B_{i-1}^* + \{0, b_i\} = B_{i-1}^* \cup (B_{i-1}^* + b_i), 1 \leq i \leq k. \tag{4}$$

Thus, obviously, $|B_{i-1}^*| \leq |B_i^*|$.

Taking into account that $|B_0^*| = 1$ and that $|B| = k \geq d$, for some i we have $|B_{i-1}^*| = |B_i^*|$ implying that residue b_i (and element a_i respectively) does not add new residue classes, i.e., $(B \setminus b_i)^* = B^*$. Therefore, $A' \setminus a_i$ is d-full as well as A'. This fact contradicts the assumption that A' is the smallest d-full subset of A and proves the Lemma. □

The next lemma refines the second assertion (ii) of Theorem 2.1.

Lemma 2.4. — *Let A be a set of integers taken from the segment $[1,\ell]$. Assume that $|A| = m > c_1(\ell \log \ell)^{1/2}$, $\ell > \ell_0$, and suppose that A is q-full for each q, $2 \leq q \leq \frac{3\ell}{m}$. Then the assertion (i) of Theorem 2.1 holds with $d = 1$.*

Proof. — Assume that $d > 1$ in Theorem 2.1. By the theorem, a long segment of an arithmetic progression belongs to $A^*(0,d)$. On the other hand, A is d-full (since $d \leq \frac{3\ell}{m}$) and subset-sum $S_{r(\mathrm{mod}\, d)}$ exists for each r, $1 \leq r < d$. Combine a long segment of an arithmetic progression (with difference d) in interval

$$[\tfrac{1}{2} S_{A(0,d)} - c_2 dm^2, \tfrac{1}{2} S_{A(0,d)} + c_2 dm^2]$$

(belonging to $A^*(0,d)$) with subset-sums $S_{1(\bmod d)}, S_{2(\bmod d)}, \ldots, S_{d-1(\bmod d)}$ (these subset-sums are obtained without using elements of $A(0,d)$). Thus we obtain an interval

$$[\tfrac{1}{2}S_{A(0,d)} - c_2dm^2 + \max\{S_{r(\bmod d)} : 1 \le r < d\}, \tfrac{1}{2}S_{A(0,d)} + c_2dm^2],$$

all integers of which belong to A^*. In fact, if the length of this new interval is sufficiently large ($O(m^2)$, for example), we will obtain the result of Theorem 2.1 with $d' = 1$. Actually, since we are interested only in the case $d > 1$ and since $\max\{S_{r(\bmod d)} : 1 \le r < d\} < d\ell = O(dm^2/\log m)$, the length of the obtained interval is

$$O(dm^2 - \max\{S_{r(\bmod d)} : 1 \le r < d\}) = O(dm^2 - \frac{dm^2}{\log m}) = O(dm^2)$$

which completes the proof. □

The latest property (Lemma 2.4) shows that in order to obtain a structural characterization of A^*, it is sufficient to verify that set A is q-full for all q's, $2 \le q \le \frac{3\ell}{m}$. Clearly, the new condition is weaker than (2): A can be q-full even if $|A(0,q)| > m - \frac{3\ell}{m}$. However, from an algorithmic point of view this new condition is difficult to verify. To correct this we have to use some lemmas which determine different sufficient conditions implying that set A is q-full. We will also show that it is sufficient to verify the prime numbers only.

Lemma 2.5 ([**3**]). — *If p is prime and*

$$\sum_{i=1}^{p-1} |A(i,p)| \ge p - 1 \tag{5}$$

then A is p-full.

The proof of this lemma is presented here because of the difficulty in accessing of reference [**3**].

Proof. — Using the fact that all elements of $A(i,p), i \ne 0$, are relatively prime to p, introduce ring $\mathbb{Z}_p$ of residues mod p. In the following reasoning it is implied that all arithmetic operations, including the operations for computing subset-sums, are operations modulo p in $\mathbb{Z}_p$.

Put, as in the proof of Lemma 2.3, $B = \{b_1, b_2, \ldots, b_k\}$ for the multi-set of non-zero residues modulo p in A and define the sequence of multi-sets $B_0, B_1, \ldots, B_k$ where B_0 is an empty set and $B_i = \{b_1, \ldots, b_i\}$ for $i > 0$.

By the hypothesis, $|B| = \sum_{i=1}^{p-1} |A(i,p)| \ge p - 1$. If for all $i \le p-1, |B^*_{i-1}| < |B^*_i|$, then $|B^*_i| \ge |B^*_{i-1}| + 1 \ge |B^*_0| + i = i + 1$, i.e., $|B^*_{p-1}| \ge p$, which concludes the proof, since we are dealing with residues modulo p.

Otherwise, the fact that $|B^*_{i-1}| = |B^*_i|$ for some $i < p - 1$ implies that for any $c \in B^*_{i-1}$, $c + b_i$ also belongs to B^*_{i-1}. Continuing this reasoning we obtain $c + rb_i \in B^*_{i-1} \subseteq B^*$ for any r. Recalling that all operations are modulo p and that $\gcd(b_i, p) = 1$, one obtains that all residues modulo p are in B^*, i.e., A is p-full. □