Long Arithmetic Progressions in Sumsets and Subset Sums: Constructive Proofs and Efficient Witnesses

Lin Chen Yuchen Mao Guochuan Zhang

Abstract

Existence of long arithmetic progression in sumsets and subset sums has been studied extensively in the field of additive combinatorics. These additive combinatorics results play a central role in the recent progress of fundamental problems in theoretical computer science including Knapsack and Subset Sum. The non-constructiveness of relevant additive combinatorics results affects their application in algorithms. In particular, additive combinatorics-based algorithms for Subset Sum, including an $\tilde{O}(n)$-time algorithm for dense subset sum [Bringmann and Wellnitz '21] and an $\tilde{O}(n + \sqrt{a_{\max} t})$-time algorithm [Chen, Lian, Mao, and Zhang '24], work only for the decision version of the problem, but not for the search version. To find a solution, one has to spend a lot more time.

We provide constructive proofs for finite addition theorems [Sárközy'89 '94], which are fundamental results in additive combinatorics concerning the existence of long arithmetic progression in sumsets and subset sums. Our constructive proofs yield a near-linear time algorithm that returns an arithmetic progression explicitly, and moreover, for each term in the arithmetic progression, it also returns its representation as the sum of elements in the base set.

As an application, we can obtain an $\tilde{O}(n)$-time algorithm for the search version of dense subset sum now. Another application of our result is Unbounded Subset Sum, where each input integer can be used an infinite number of times. A classic result on the Frobenius problem [Erdös and Graham '72] implies that for all $t \geqslant 2a_{\max}^2/n$, the decision version can be solved trivially in linear time. It remains unknown whether the search version can be solved in the same time. Our result implies that for all $t \geqslant ca_{\max}^2/n$ for some constant c, a solution for Unbounded Subset Sum can be obtained in $O(n \log a_{\max})$ time.

The major technical challenge is that the original proofs for the above-mentioned additive combinatorics results heavily rely on two fundamental theorems, Mann's theorem and Kneser's theorem. These two theorems constitute the main non-constructive part. To bypass these two obstacles, we introduce two techniques.

- A new set operation called greedy sumset. Greedy sumset computes a moderately large subset of the traditional sumset, but enjoys the advantage that searching for a representation for elements in the greedy sumset can be done efficiently.
- A framework that can be used to iteratively augment an arithmetic progression. It plays the role of Kneser's theorem in the proof but enjoys the advantage that the representation of elements in the arithmetic progression can be efficiently traced.