

Fast  $n$ -fold Boolean Convolution via Additive Combinatorics\*Karl Bringmann<sup>†</sup> Vasileios Nakos<sup>‡</sup>**Abstract**

We consider the problem of computing the Boolean convolution (with wraparound) of  $n$  vectors of dimension  $m$ , or, equivalently, the problem of computing the sumset  $A_1 + A_2 + \dots + A_n$  for  $A_1, \dots, A_n \subseteq \mathbb{Z}_m$ . Boolean convolution formalizes the frequent task of combining two subproblems, where the whole problem has a solution of size  $k$  if for some  $i$  the first subproblem has a solution of size  $i$  and the second subproblem has a solution of size  $k - i$ . Our problem formalizes a natural generalization, namely combining solutions of  $n$  subproblems subject to a modular constraint. This simultaneously generalises Modular Subset Sum and Boolean Convolution (Sumset Computation). Although nearly optimal algorithms are known for special cases of this problem, not even tiny improvements are known for the general case.

We almost resolve the computational complexity of this problem, shaving essentially a factor of  $n$  from the running time of previous algorithms. Specifically, we present a *deterministic* algorithm running in *almost* linear time with respect to the input plus output size  $k$ . We also present a *Las Vegas* algorithm running in *nearly* linear expected time with respect to the input plus output size  $k$ . Previously, no deterministic or randomized  $o(nk)$  algorithm was known.

At the heart of our approach lies a careful usage of Kneser's theorem from Additive Combinatorics, and a new deterministic almost linear output-sensitive algorithm for non-negative sparse convolution. In total, our work builds a solid toolbox that could be of independent interest.

---

\*This work is part of the project TIPEA that has received funding from the European Research Council (ERC) under the European Unions Horizon 2020 research and innovation programme (grant agreement No. 850979).

<sup>†</sup>kbringma@mpi-inf.mpg.de Max Planck Institute for Informatics, Saarland Informatics Campus, Saarbrücken, Germany.

<sup>‡</sup>vnakos@mpi-inf.mpg.de, Max Planck Institute for Informatics, Saarland Informatics Campus, Saarbrücken, Germany.

# 1 Introduction

In this paper we study  $n$ -fold variants of the following fundamental 2-fold problems.

## 1.1 2-Fold Case

**Boolean Convolution and Sumset Computation.** In Boolean convolution we are given vectors  $A, B \in \{0, 1\}^m$  and the task is to compute the vector  $C = A \otimes B \in \{0, 1\}^m$  defined by  $C[k] = \bigvee_i A[i] \wedge B[k - i]$ . This formalizes a situation in which we split a computational problem into two subproblems, so that in total there is a solution of size  $k$  if and only if for some  $i$  there is a solution of the left subproblem of size  $i$  and there is a solution of the right subproblem of size  $k - i$ . This is a natural task that frequently arises in algorithm design. There are two variants of this problem: *Without wraparound* the  $\bigvee_i$ -quantifier goes over  $0 \leq i \leq k$ ; *with wraparound* the quantifier goes over all  $i \in [m]$  and the entry  $B[k - i]$  means  $B[(k - i) \bmod m]$ . Algorithmically the two variants are equivalent, and throughout this paper we study the latter variant.

An equivalent problem is *sumset computation*: Given sets  $A, B \subseteq \mathbb{Z}_m$ , compute their sumset  $A + B$ , which denotes the set of all sums  $a + b$  modulo  $m$  with  $a \in A, b \in B$ . This corresponds to Boolean convolution with wraparound<sup>1</sup>.

**Standard Convolution and Polynomial Multiplication.** In (standard) convolution we are given vectors  $A, B \in \mathbb{R}^m$  and the task is to compute the vector  $C = A \star B \in \mathbb{R}^m$  with  $C[k] = \sum_i A[i] \cdot B[k - i]$ . For instance, if  $A[i]$  and  $B[i]$  count the number of size- $i$  solutions of the left and right subproblem, then  $C[k]$  counts the number of size- $k$  solutions of the whole problem. Again one can consider variants with or without wraparound. A typical restriction are *non-negative* entries, which is well-motivated in case that  $A, B, C$  represent numbers of solutions.

This problem is equivalent to *polynomial multiplication*: Given the coefficients of polynomials  $P(X) = \sum_{i=0}^m A[i] \cdot X^i$  and  $Q(X) = \sum_{i=0}^m B[i] \cdot X^i$ , compute the coefficients of their product  $P \cdot Q$ .

**State of the Art.** Using Fast Fourier Transform (FFT), all of the above problems can be solved in time  $O(m \log m)$ . A long line of work has considered these problems in a sparse setting, called sparse convolution or sparse polynomial multiplication, see, e.g., [Mut95, CH02, Roc08, MP09, VDHL12, AR15, CL15, Roc18, Nak20, GGdC20, BFN21]. Here the task is to compute the convolution of two sparse vectors much faster than performing FFT, ideally in near-linear time in terms of the input plus output size (i.e., the number of non-zero entries of the input and output vectors). Near-linear in the input plus output size running time was achieved for vectors with non-negative entries by Cole and Hariharan [CH02] and for general vectors in [Nak20], see also [GGdC20] for additional  $\log m$  factors improvements. Very recently, a Monte Carlo  $O(k \log k)$ -time algorithm has been achieved in [BFN21] for non-negative convolution, where  $k$  is the input plus output size. Sparse convolution techniques are crucially used in [AKP07, AKPR14, ABP14, CL15, ABJ<sup>+</sup>19, BN20], and are also relevant to the study of sparse wildcard matching, a fundamental string problem [CS98, CH02].

However, all known algorithms for these sparse problems are randomized, and thus an open problem is to *close the gap between deterministic and randomized algorithms*. This was explicitly posed as an open problem in [CL15, Remark 8.2].

---

<sup>1</sup> By removing the modulo operation and thus working over  $\mathbb{Z}$  we can also pose a problem variant corresponding to Boolean convolution without wraparound. Again, algorithmically these variants are equivalent, since for any  $A, B \subseteq \{0, 1, \dots, m - 1\}$ , on the one hand computing  $A + B$  over  $\mathbb{Z}$  and taking the result modulo  $m$  yields  $A + B$  over  $\mathbb{Z}_m$ , and on the other hand computing  $A + B$  over  $\mathbb{Z}_{2m}$  yields  $A + B$  over  $\mathbb{Z}$ .

**Our Contribution to the 2-Fold Case.** We present a deterministic algorithm for convolution of non-negative vectors (and thus also for Boolean convolution) running in time  $k \cdot m^{o(1)}$ , where  $k$  is the input plus output size. This matches up to the  $m^{o(1)}$  term the best known algorithms in the randomized case [CH02]. Our algorithm heavily builds upon an algorithm by Chan and Lewenstein [CL15], which operates under the additional assumption that a small superset of the non-negative terms is known in advance. We remove their assumption by gradually building the sumset using calls to their algorithm.

**Theorem 1.1** (Deterministic Non-Negative Sparse Convolution, Section 6). *Denote by  $\|x\|_0$  the number of non-zero entries of a vector  $x$ . Given vectors  $A, B \in \mathbb{R}_{\geq 0}^m$ , we can compute their convolution  $A \star B$  (with wraparound) in time  $\|A \star B\|_0 \cdot m^{o(1)}$  by a deterministic algorithm. More precisely, the running time is  $\|A \star B\|_0 \cdot 2^{O(\sqrt{\log \|A \star B\|_0 \log \log m})}$ .*

Observe that  $\|A\|_0, \|B\|_0 \leq \|A \star B\|_0$ , and thus rather than bounding the running time in terms of the input plus output size  $\|A\|_0 + \|B\|_0 + \|A \star B\|_0$ , it suffices to bound the running time in terms of only the output size  $\|A \star B\|_0$ . Moreover, note that since  $\|A \star B\|_0 \leq m$  the above running time is bounded by  $m^{1+o(1)}$ . As an additional bonus, our approach gives a quite simple  $\|A \star B\|_0 \cdot \text{polylog}(m)$ -time Las Vegas algorithm for the 2-fold case of non-negative sparse convolution, see Theorem 6.3.

We leave it as an open problem whether similarly efficient deterministic algorithms exist under the presence of negative entries.

## 1.2 $n$ -Fold Case

The focus of this paper is on  $n$ -fold generalizations of the above problems. Indeed, in typical applications we do not only split a problem into two subproblems, but these subproblems are recursively split into further subproblems. If the recursion tree has  $n$  leaves, we therefore want to compute Boolean convolutions of the form  $A_1 \otimes \dots \otimes A_n$  for vectors  $A_1, \dots, A_n$ .

Note that now the “gold standard” would be linear running time in terms of the total input plus output size  $k = \|A_1\|_0 + \dots + \|A_n\|_0 + \|A_1 \otimes \dots \otimes A_n\|_0$ . Note that in contrast to the 2-fold case, the size of the output is incomparable to the size of the input.

**A Special Case: Modular Subset Sum** As an example, consider the Modular Subset Sum problem, where we are given  $x_1, \dots, x_n \in \mathbb{Z}_m$  and a target  $t$ , and the task is to decide whether for some subset  $I \subseteq [n]$  we have  $\sum_{i \in I} x_i \equiv t \pmod{m}$ . Observe that the sumset  $\{0, x_1\} + \dots + \{0, x_n\} \subseteq \mathbb{Z}_m$  denotes the set of all attainable subset sums modulo  $m$ , and thus Modular Subset Sum can be solved by a direct application of  $n$ -fold sumset computation, which is equivalent to  $n$ -fold Boolean convolution (with wraparound).

The state of the art for Modular Subset Sum is as follows. A standard dynamic programming approach solves the problem in time  $O(n \cdot m)$ . After the first improvements by Koiliaris and Xu [KX17], Axiotis et al. [ABJ<sup>+</sup>19] designed an algorithm running in time  $O((n+m) \text{polylog}(n+m))$ , which was further simplified, sped up and made deterministic in [ABB<sup>+</sup>21, CI21]. Those running times match a conditional lower bound based on the Strong Exponential Time Hypothesis [ABHS19, ABJ<sup>+</sup>19]. Moreover, all of the above algorithms can be analyzed to run in time  $O(k \text{polylog } m)$ , where  $k$  is the total input plus output size [ABJ<sup>+</sup>19].

In other words, for the special case  $|A_1| = \dots = |A_n| = 2$  of  $n$ -fold sumset computation near-optimal algorithms are known. Furthermore, the techniques crucially exploit the fact that all sets  $A_i$  have constant cardinality. The goal of this paper is to investigate the general case without any

restrictions on  $|A_i|$ . Can one move beyond the problem-specific techniques in [KX17, ABJ<sup>+</sup>19, ABB<sup>+</sup>21, CI21] which seem to apply solely to Modular Subset Sum?

**Naive Approach** As it is already known how to compute  $A \star B$  (and thus  $A \otimes B$ ) in time near-linear in the output size [CH02, Nak20, BFN21], is there an easy generalization to compute the  $n$ -fold Boolean convolution  $A_1 \otimes \dots \otimes A_n$ ? Naively, if we compute the  $n$ -fold convolution in a linear fashion as  $((A_1 \otimes A_2) \otimes A_3) \star \dots \otimes A_{n-1}) \otimes A_n$ , then each intermediate convolution has input plus output size at most  $k$ , so using [CH02] we can bound the total expected running time by  $O(nk \text{ polylog } m)$ . Unfortunately, this running time analysis is tight. The issue is that up to  $\tilde{\Omega}(n)$  intermediate results may have size  $\Omega(k)$ .

The same is true if we compute the  $n$ -fold convolution in a bottom-up tree-like fashion as  $((A_1 \otimes A_2) \otimes (A_3 \otimes A_4)) \otimes \dots$ , as shown by the following example. Pick  $b = \lfloor \frac{\log m}{\log \log m} \rfloor$  and  $\ell = \lceil \log_b(m) \rceil = \Theta(b)$ , and set  $A_i$  to the indicator vector of  $b^{i \bmod \ell} \cdot \{0, 1, 2, \dots, b-1\}$ . Then the Boolean convolution of any  $\ell$  consecutive  $A_i$ 's is the all-ones vector and thus has size  $m$ , and this holds for  $\Omega(n/\ell) = \Omega(n \frac{\log \log m}{\log m})$  intermediate convolutions. On the other hand, the input size is  $O(n \frac{\log m}{\log \log m})$  and the output size is  $O(m)$ .

Analyzing the time only in terms of  $n, m$ , the naive approach yields time  $O(nm \text{ polylog } m)$ . A simple algorithm using  $n - 1$  FFTs also yields time  $O(nm \log m)$ . Before this work it was open whether  $n$ -fold Boolean convolution can be solved in time close to linear in  $n + m$ , and close to linear in  $k$ , or whether the additional factor  $\tilde{\Theta}(n)$  of the naive approach is necessary.

**$n$ -Fold Boolean Convolution versus  $n$ -Fold Convolution.** We note that  $n$ -fold Boolean convolution is quite different from  $n$ -fold convolution, and we focus on the former in this paper. The reason is that  $n$ -fold convolution results in exponentially large entries. Indeed, assuming that  $A_1, \dots, A_n$  are non-negative integer vectors, each with at least two non-zero entries, one can check that  $\|A_1 \star \dots \star A_n\|_1 = \|A_1\|_1 \cdot \dots \cdot \|A_n\|_1 \geq 2^n$  (here  $\|x\|_1 = \sum_i |x[i]|$ ), and thus at least one output entry requires  $\Omega(n)$  bits to represent exactly. Possible ways to handle this situation are (1) to let  $k$  be the total number of input plus output *bits*, (2) assume that entries come from a finite field, or (3) relax to approximation. We leave these as open problems and focus on Boolean convolution in this paper.

**Our Contribution to  $n$ -Fold Boolean Convolution.** We show that the multiplicative factor  $n$  in the naive running times  $O(nk \text{ polylog } m)$  and  $O(s + nm \log m)$  is not necessary (here  $s$  is the size of the input). Specifically, our approach yields two new results for  $n$ -fold Boolean convolution: a randomized Las Vegas algorithm running in expected time  $O(k \cdot \text{polylog } m)$ , and a deterministic algorithm running in time  $k \cdot m^{o(1)}$ . Morally, we show that one can convolve  $n$  Boolean vectors in a much better way than doing  $n - 1$  FFTs. In particular, in terms of  $m, n$  and the size of the input  $s$ , the known algorithms would run in time  $\tilde{O}(s + mn)$ , whereas our approach yields time  $\tilde{O}(s + m)$ . Thus, in instances where the size of the input does not dominate (as in Modular Subset Sum where  $s = 2n$ ) our approach yields a substantial improvement.

Our algorithm falls in a line of research that tries to apply results from Additive Combinatorics in algorithm design, such as [GM91, CL15, AKKN16, BGNV17, MWW19, BN20]. Quite interestingly, this is the first time that such a connection has produced an (almost) optimal result. Previous algorithms [GM91, CL15, AKKN16, BGNV17, MWW19, BN20] had less clean running time bounds and are thus likely to be suboptimal, partly because of the Additive Combinatorics machinery used.

We now state our results more formally. The main result of this paper is the following.

**Theorem 1.2** (*n*-Fold Boolean Convolution). *Given vectors  $A_1, A_2, \dots, A_n \in \{0, 1\}^m$  we can compute their Boolean convolution with wrap-around  $A_1 \otimes A_2 \otimes \dots \otimes A_n$*

- (1) *by a randomized Las Vegas algorithm in  $O(k \cdot \text{polylog}(mk))$  expected time, or*
- (2) *by a deterministic algorithm in  $k \cdot 2^{O(\sqrt{\log k \cdot \log \log m})}$  time*

Here,  $k := \|A_1\|_0 + \dots + \|A_n\|_0 + \|A_1 \otimes A_2 \otimes \dots \otimes A_n\|_0$  is the total input plus output size.

**Remark 1.3.** *It might seem confusing that for very small  $k$ , specifically for  $k \leq \log^{O(1)} m$ , our deterministic time is faster than our randomized time. However, as we will discuss later, it is easy to solve the problem deterministically in time  $k^{O(1)}$ . In fact our time bounds are  $\min \{k^3, k \cdot \text{polylog}(mk)\}$  expected time, and  $\min \{k^3, k \cdot 2^{O(\sqrt{\log k \cdot \log \log m})} \cdot \text{polylog}(mk)\}$  deterministically; the latter can be simplified to the expression in Theorem 1.2.*

In order to employ Additive Combinatorics machinery, it will be convenient to phrase the problem in terms of sets and sumsets, making the connection more clear. To this end, we replace every vector  $A_i \in \{0, 1\}^m$  by a set  $A'_i \subseteq \mathbb{Z}_m$  such that  $x \in A'_i$  if and only the  $x$ -th entry of  $A_i$  is 1. Then, it can easily be seen that the Boolean convolution  $A_1 \otimes A_2 \otimes \dots \otimes A_n$  is equivalent to computing the sumset  $A'_1 + A'_2 + \dots + A'_n$ . Written in a more Additive-Combinatorics-friendly way, our main result can be rephrased in the following way.

**Theorem 1.4** (Theorem 1.2 restated, Section 5). *Given sets  $A_1, \dots, A_n \subseteq \mathbb{Z}_m$ , we can compute their sumset  $A_1 + A_2 + \dots + A_n$*

- (1) *by a randomized Las Vegas algorithm in  $O(k \cdot \text{polylog}(mk))$  expected time, or*
- (2) *by a deterministic algorithm in  $k \cdot 2^{O(\sqrt{\log k \cdot \log \log m})}$  time.*

Here,  $k := |A_1| + \dots + |A_n| + |A_1 + \dots + A_n|$  is the total input plus output size.

We remark that further improvements over Theorem 1.1 would directly improve Theorems 1.2 and 1.4. In particular, our factor  $m^{o(1)} = 2^{O(\sqrt{\log m \cdot \log \log m})}$  stems entirely from the application of Theorem 1.1, and thus indirectly from a tool called the FFT Lemma [CL15] that we use to prove Theorem 1.1.

We also remark that Theorem 1.4 is formulated for sumsets over  $\mathbb{Z}_m$ , but by setting  $m$  sufficiently large (like  $1 + \sum_i \max(A_i)$ ) we can also compute sumsets  $A_1 + \dots + A_n \subseteq \mathbb{Z}$  over the integers in time close to the input plus output size. However, this is a much simpler result that can also be achieved by elementary means, without any Additive Combinatorics.

## 2 Preliminaries and Technical Toolkit

For any positive integer  $m$ , we let  $\mathbb{Z}_m$  be the group of residues modulo  $m$ . For two sets  $A, B \subseteq \mathbb{Z}_m$ , we define  $A + B := \{x \mid \exists a \in A, b \in B: a + b = x\}$ . Unless explicitly stated otherwise, all sumsets throughout the paper are computed in the underlying group  $\mathbb{Z}_m$ , i.e.,  $A + B \subseteq \mathbb{Z}_m$ . We also write  $A \bmod q := \{a \bmod q \mid a \in A\}$ .

Throughout the paper we use the notation of sumset computation instead of the equivalent Boolean convolution.

## 2.1 Randomized Sumset Computation

Cole and Hariharan’s sparse convolution algorithm [CH02] implies that the sumset  $A + B$  can be computed in Las Vegas time  $O(|A + B| \cdot \log^2 m + \text{poly}(\log m))$ . Very recently, this was improved to  $O(|A + B| \cdot \log |A + B| + \text{poly}(\log m))$  [BFN21] with a Monte Carlo algorithm.

**Theorem 2.1** (Randomized Sumset Computation, [CH02], see also Section 6). *Given sets  $A, B \subseteq \mathbb{Z}_m$ , their sumset  $A + B$  can be computed in expected time  $O(|A + B| \text{poly}(\log m))$ .*

## 2.2 The Symmetry Group and its Properties

**Definition 2.2** (Symmetry group of a set). *Let  $A \subseteq \mathbb{Z}_m$ . We define the symmetry group of  $A$  as  $\text{Sym}(A) = \{h \in \mathbb{Z}_m \mid A + \{h\} = A\}$ .*

It is easy to check that  $\text{Sym}(A)$  satisfies the group properties with respect to addition, and thus  $\text{Sym}(A)$  is a subgroup of  $\mathbb{Z}_m$ . In particular, we have  $\text{Sym}(A) = d \cdot \mathbb{Z}_{m/d}$ , where  $d$  is the minimum non-zero element of  $\text{Sym}(A)$  (to see this, note that the minimum non-zero element of a cyclic subgroup is also a generator of it).

One can check that  $\text{Sym}(A) \subseteq \text{Sym}(A + B)$  holds for any sets  $A, B \subseteq \mathbb{Z}_m$ . This property will be of great importance to us. Moreover, for any non-empty set  $A$  and any  $x \in A$  we have  $\text{Sym}(A) \subseteq A + \{-x\}$ . This holds since any  $h \in \text{Sym}(A)$  maps  $x$  to some  $x' \in A$ , which means  $x' = x + h \pmod{m}$ , hence  $h = x' - x \pmod{m}$ . In particular, the symmetry group of a non-empty set  $A$  has size at most  $|A|$ .

We show that the symmetry group can be computed in linear time.

**Theorem 2.3** (Computing the Symmetry Group, Section 7). *Given a sorted non-empty set  $A \subseteq \mathbb{Z}_m$ , we can compute  $\text{Sym}(A)$  in time  $O(|A|)$ .*

## 2.3 Kneser’s Theorem

The following theorem lies at the core of our algorithms.

**Theorem 2.4** (Kneser’s Theorem, see, e.g., Theorem 5.5 in [TV06]). *Let  $A, B \subseteq \mathbb{Z}_m$  be non-empty. Then*

$$|A + B| \geq \min\{|A| + |B| - |\text{Sym}(A + B)|, m\}.$$

We will use the following simple corollary.

**Corollary 2.5.** *Let  $A, B \subseteq \mathbb{Z}_m$  be non-empty. If  $|A + B| < |A| + |B| - 1$  then  $|\text{Sym}(A + B)| > 1$ .*

*Proof.* For  $m = 1$  it cannot happen that  $|A + B| < |A| + |B| - 1$ , so assume  $m \geq 2$ .

If  $|A + B| = m$ , then  $A + B = \mathbb{Z}_m$ . This implies  $\text{Sym}(A + B) = \mathbb{Z}_m$  and thus  $|\text{Sym}(A + B)| = m > 1$ . Otherwise, if  $|A + B| < m$ , we can simplify the bound obtained from Kneser’s Theorem to

$$|A + B| \geq |A| + |B| - |\text{Sym}(A + B)|.$$

Together with  $|A + B| < |A| + |B| - 1$ , this implies  $|\text{Sym}(A + B)| > 1$ . □

### 3 Overview and Comparison with Previous Approaches

We start by giving a rough overview of our algorithm, leaving out several details. Our improvements are obtained by delving deeper into the additive structure of sumset computation over  $\mathbb{Z}_m$  than previous work. Our algorithms compute the sumset  $A_1 + \dots + A_n$  in a bottom-up tree-like fashion as  $((A_1 + A_2) + (A_3 + A_4)) + \dots$ . For any two sets  $X, Y$  for which we compute  $X + Y$  during the execution of this algorithm, we check whether  $|X + Y| < |X| + |Y| - 1$ . If this is the case, Kneser’s Theorem (specifically Corollary 2.5) implies that  $X + Y$  has a non-trivial symmetry group, and hence  $A_1 + \dots + A_n$  has a non-trivial symmetry group. A non-trivial symmetry group of a set  $Z = X + Y \subseteq \mathbb{Z}_m$  implies that the set is *periodic*: there exists a divisor  $d$  of  $m$  and a set  $Z' \subseteq \{0, \dots, d - 1\}$  such that  $Z = Z' + d \cdot \mathbb{Z}_{m/d} = Z' + \{0, d, 2d, \dots, m - d\}$ , i.e.,  $Z$  is a rotation (by multiples of  $d$ ) of a subset of  $\{0, \dots, d - 1\}$ . This allows us to reduce to the smaller universe  $\mathbb{Z}_d$ , which is progress (it might seem from this discussion that we require a factorization of  $m$ , but this is not the case: if we reduce to a smaller universe  $\mathbb{Z}_d$ , then  $d$  is a divisor of  $m$  that can be easily read off the sumset  $Z = X + Y$ , by computing the symmetry group  $Sym(X + Y)$  and taking its smallest non-zero element). It remains to argue about the situation in which every computed sumset satisfies  $|X + Y| \geq |X| + |Y| - 1$ . Using this inequality, we can control at any intermediate step of the algorithm the total size of all sumsets computed so far. When the computation arrives at the root, the running time that we spent on computing these sumsets is almost linear in the input plus output size.

**Why Previous Approaches Cannot Solve the Generalized Problem.** A natural question to ask is whether previous algorithms for Subset Sum or Modular Subset Sum were also able to tackle the more general problem of  $n$ -fold sumset computation. The techniques underlying the algorithms for Subset Sum in [Bri17, KX17, JW19] are inherently non-modular, and hence cannot facilitate  $n$ -fold sumset computation problem over the group  $\mathbb{Z}_m$ . More relevant is the Modular Subset Sum problem, which is a standard variant of Subset Sum, where one works over  $\mathbb{Z}_m$  rather than  $\mathbb{Z}$ . This problem has seen two interesting developments in the last few years.

The deterministic algorithm of Koiliaris and Xu [KX17] uses multiple interesting problem-specific tricks for Modular Subset Sum, but it is unclear how to generalize them to  $n$ -fold sumset computation. In fact, their algorithm can be viewed as a reduction from Modular Subset Sum to  $\min\{\sqrt{n}, m^{1/4}\}$ -fold sumset computation, which they then solve by the straightforward repeated Fast Fourier Transform. Hence, also for the general case of  $n$ -fold sumset computation their approach does not seem to yield time  $o(nm)$ .

All known algorithms for Modular Subset Sum [ABJ<sup>+</sup>19, ABB<sup>+</sup>21, CI21] compute the set of attainable subset sums  $\mathcal{S}(A) = \{0, a_1\} + \dots + \{0, a_n\} \subseteq \mathbb{Z}_m$  for  $A = \{a_1, \dots, a_n\}$ . The main idea is to compute  $\mathcal{S}(A)$  from  $\mathcal{S}(A \setminus \{a\})$  by forming the vector  $\mathbf{1}_{a+\mathcal{S}(A \setminus \{a\})} - \mathbf{1}_{\mathcal{S}(A \setminus \{a\})}$ . It can be easily seen that this vector consists of an equal number of positive and negative entries, and the positive entries correspond to the “new” sums  $\mathcal{S}(A) \setminus \mathcal{S}(A \setminus \{a\})$ . Using hashing-based arguments or appropriate data structures for string manipulation, they show how to recover the support of the aforementioned vector in near-linear output-sensitive time. A possibility to generalize this approach to  $n$ -fold sumset computation  $A_1 + \dots + A_n$  would be to consider the vector  $\sum_{a \in A_n} (\mathbf{1}_{a+A_1+\dots+A_{n-1}} - \mathbf{1}_{A_1+\dots+A_{n-1}})$ . However, measuring this vector would incur time  $\Omega(|A_n|)$ , and thus an immediate generalization of their approach would at least pay a factor  $\max_i |A_i|$  on top of the output size.

**Symmetry Manifestations in Higher Dimensions.** It would be interesting to understand whether the symmetry considerations of our algorithm manifest themselves in other abelian groups, most notably in  $\mathbb{Z}_m^D$ . The characterization of subgroups over  $\mathbb{Z}_m^D$  with  $D > 1$  is less convenient

---

**Algorithm 1**

---

```
1: procedure NFOLDSETINPRIMEUNIVERSE( $A_1, A_2, \dots, A_n, p$ )
2:                                      $\triangleright n$  is a power of 2;  $p$  is prime; non-empty sets  $A_1, \dots, A_n \subseteq \mathbb{Z}_p$ 
3:    $X_{0,i} \leftarrow A_i$ , for all  $i \in [n]$ 
4:   for  $r = 1$  to  $\log n$  do
5:     for  $i = 1$  to  $n/2^r$  do
6:        $X_{r,i} \leftarrow X_{r-1,2i-1} + X_{r-1,2i}$   $\triangleright$  sumset computation via Theorem 1.1
7:       if  $\sum_{j \leq i} |X_{r,j}| > p + i - 1$  then
8:         return  $\mathbb{Z}_p$ 
9:   return  $X_{\log n, 1}$ 
```

---

for our purposes than the characterization in the one-dimensional case, so it seems that a different treatment and notion of progress is needed in that case. We leave this to potential future work. Even if one does worry about the  $n$ -fold case and concentrates in the simplest case of  $n = 2$ , i.e. 2-fold  $d$ -dimensional sparse convolution, the best algorithm we are aware of solves the problem with a multiplicative  $2^d$  multiplicative factor on top of output size. We leave as an open question the problem of avoiding the exponential dependence of 2-fold  $d$ -dimensional sparse convolution.

## 4 Warmup: $n$ -Fold Sumset Computation over Prime Universe

As a warmup, we consider universe  $\mathbb{Z}_m = \mathbb{Z}_p$  for prime  $p$ . For simplicity, we analyze our algorithm only in terms of the input size and the universe size  $p$ , that is, we defer the output-sensitive analysis to the general algorithm in Section 5.

Suppose we are given sets  $A_1, \dots, A_n \subseteq \mathbb{Z}_p$ . We may assume that  $n$  is a power of 2, since otherwise we can add an appropriate number of sets  $A_i = \{0\}$  without affecting the sumset. Consider Algorithm 1. We compute  $A_1 + \dots + A_n$  in a tree-like bottom-up fashion, by first computing  $A_1 + A_2, A_3 + A_4, \dots$ , then computing  $A_1 + A_2 + A_3 + A_4, \dots$ , and so on. The intermediate sets in round  $r$  are called  $X_{r,1}, \dots, X_{r,n/2^r}$ . The termination criterion is that the sets that we computed so far in the current round  $r$  have total size significantly more than  $p$ , more precisely,  $\sum_{j \leq i} |X_{r,j}| > p + i - 1$ . If this criterion is satisfied, then we return the complete universe  $\mathbb{Z}_p$ . If the termination criterion is never satisfied, then in the end we return  $X_{\log n, 1}$ .

It remains to analyze correctness and running time of this algorithm. To analyze correctness of the termination criterion, we need the following lemma.

**Lemma 4.1.** *Let  $p$  be a prime, and let  $A_1, A_2, \dots, A_n \subseteq \mathbb{Z}_p$  be non-empty. If  $\sum_{j=1}^n |A_j| \geq p + n - 1$ , then  $A_1 + A_2 + \dots + A_n = \mathbb{Z}_p$ .*

*Proof.* Suppose that the symmetry group has size  $|Sym(A_1 + \dots + A_n)| > 1$ . Since  $\mathbb{Z}_p$  has no non-trivial subgroups, this yields  $Sym(A_1 + \dots + A_n) = \mathbb{Z}_p$ . Since  $|Sym(A)| \leq |A|$  holds for any set  $A$ , we obtain  $A_1 + \dots + A_n = \mathbb{Z}_p$ .

It remains to consider the case  $|Sym(A_1 + \dots + A_n)| = 1$ . Since  $Sym(A) \subseteq Sym(A + B)$  holds for any sets  $A, B$ , it follows that  $|Sym(A_1 + \dots + A_i)| = 1$  for all  $1 \leq i \leq n$ . We now inductively prove that  $|A_1 + \dots + A_i| \geq \min\{\sum_{j=1}^i |A_j| - i + 1, p\}$ , from which the corollary follows. The induction base for  $i = 1$  is trivial. For  $i > 1$ , we use Kneser's theorem on  $A := A_1 + \dots + A_{i-1}$  and  $B := A_i$  to obtain

$$|A_1 + \dots + A_i| \geq \min\{|A_1 + \dots + A_{i-1}| + |A_i| - |Sym(A_1 + \dots + A_i)|, p\}.$$



Plugging in  $|Sym(A_1 + \dots + A_i)| = 1$  and the induction hypothesis on  $|A_1 + \dots + A_{i-1}|$ , and simplifying  $\min\{\min\{a, p\} + b, p\}$  to  $\min\{a + b, p\}$ , yields

$$|A_1 + \dots + A_i| \geq \min \left\{ \left( \sum_{j=1}^{i-1} |A_j| - (i-1) + 1 \right) + |A_i| - 1, p \right\} = \min \left\{ \sum_{j=1}^i |A_j| - i + 1, p \right\},$$

which finishes the inductive proof.<sup>2</sup> □

**Lemma 4.2** (Analysis of Algorithm 1). *Given non-empty sets  $A_1, \dots, A_n \subseteq \mathbb{Z}_p$ , where  $p$  is prime and  $n$  is a power of 2, Algorithm 1 correctly computes  $A_1 + \dots + A_n$  and runs in deterministic time  $O((p+n)^{1+o(1)} + \sum_{i=1}^n |A_i|)$ .*

*Proof.* If the termination criterion  $\sum_{j \leq i} |X_{r,j}| > p + i - 1$  is satisfied, then Lemma 4.1 implies that  $X_{r,1} + \dots + X_{r,i} = \mathbb{Z}_p$ , and hence  $A_1 + \dots + A_n = \mathbb{Z}_p$ , so we correctly return  $\mathbb{Z}_p$ . Otherwise we reach the last line of Algorithm 1, and we correctly computed  $X_{\log n,1} = A_1 + \dots + A_n$ . This shows correctness.

To analyze the running time, let  $(r^*, i^*)$  be the values of  $r$  and  $i$  at the end of the execution of the algorithm. In particular, if  $r^* = \log n$  we have  $i^* = 1$ . By our use of Theorem 1.1, the total running time of the algorithm is

$$\sum_{r < r^*} \sum_{i=1}^{n/2^r} |X_{r,i}| \cdot p^{o(1)} + \sum_{i < i^*} |X_{r^*,i}| \cdot p^{o(1)}.$$

We use the fact that the termination criterion was not satisfied before step  $(r^*, i^*)$  to obtain:

$$\begin{aligned} \sum_{i=1}^{n/2^r} |X_{r,i}| &\leq p + \frac{n}{2^r} - 1 \quad \text{for any } r < r^*, \\ \sum_{i < i^*} |X_{r^*,i}| &\leq p + \frac{n}{2^{r^*}} - 1. \end{aligned}$$

Moreover, we have  $|X_{r^*,i^*}| \leq p$ . Combining these observations allows us to further bound the running time by

$$\left( \sum_{r < r^*} \left( p + \frac{n}{2^r} - 1 \right) + \left( p + \frac{n}{2^{r^*}} - 1 \right) + p \right) \cdot p^{o(1)} = (p \log n + n) \cdot p^{o(1)} = (p+n)^{1+o(1)}. \quad \square$$

## 5 Algorithm for $n$ -Fold Sumset Computation

This section proves Theorem 1.4. The main idea is that whenever we detect a non-trivial symmetry group we reduce to a problem over a smaller universe  $\mathbb{Z}_d$ , for a divisor  $d$  of  $m$ .

Consider Algorithm 2. Suppose we are given sets  $A_1, \dots, A_n \subseteq \mathbb{Z}_p$ . We may assume that  $n$  is a power of 2, since otherwise we can add an appropriate number of sets  $A_i = \{0\}$  without affecting the sumset. We maintain a guess  $s$  of the outputsize  $|A_1 + \dots + A_n|$ . Specifically,  $s$  loops over all

---

<sup>2</sup>We remark that for this lemma it would be sufficient to use the Cauchy-Davenport theorem (see, e.g., [TV06, Theorem 5.4]) instead of Kneser's theorem. Only for the generalization to non-prime  $m$  we need the more general theorem by Kneser.

---

**Algorithm 2**

---

```
1: procedure NFOLDSUMSET( $A_1, \dots, A_n, m$ )
2:                                      $\triangleright n$  is a power of 2; non-empty  $A_1, \dots, A_n \subseteq \mathbb{Z}_m$ 
3:   for  $s = 1, 2, 4, \dots, 2^{\lceil \log m \rceil}$  do
4:      $X_{0,i} \leftarrow A_i$ , for all  $i \in [n]$ 
5:     for  $r = 1$  to  $\log n$  do
6:       for  $i = 1$  to  $n/2^r$  do
7:          $X_{r,i} \leftarrow X_{r-1,2i-1} + X_{r-1,2i}$   $\triangleright$  sumset computation via Theorem 1.1 or 2.1
8:         if  $|X_{r,i}| < |X_{r-1,2i-1}| + |X_{r-1,2i}| - 1$  then
9:           Compute  $Sym(X_{r,i})$   $\triangleright$  symmetry group computation via Theorem 2.3
10:           $d \leftarrow m/|Sym(X_{r,i})|$   $\triangleright Sym(X_{r,i}) = d \cdot \mathbb{Z}_{m/d}$ 
11:           $A'_i \leftarrow A_i \bmod d$ , for all  $i \in [n]$ 
12:          return NFOLDSUMSET( $A'_1, \dots, A'_n, d$ ) +  $d \cdot \{0, 1, 2, \dots, m/d - 1\}$ 
13:        if  $\sum_{j \leq i} |X_{r,j}| \geq s + n/2^r$  then
14:           $X_{r,j} \leftarrow \{0\}$ , for all  $i < j \leq n/2^r$ 
15:          break
16:      if  $|X_{\log n,1}| \leq s$  then
17:        return  $X_{\log n,1}$ 
```

---

powers of 2 starting from  $2^0 = 1$ , and the algorithm returns the correct result once we reach the first iteration with  $s \geq |A_1 + \dots + A_n|$ . Thus, in iteration  $s$  we know that the output size is more than  $s/2$ , and our primary goal is to test whether  $|A_1 + \dots + A_n| \leq s$ . If this is true then we want to compute the set  $A_1 + \dots + A_n$ . We compute  $A_1 + \dots + A_n$  in a tree-like bottom-up fashion, by first computing  $A_1 + A_2, A_3 + A_4, \dots$ , then computing  $A_1 + A_2 + A_3 + A_4, \dots$ , and so on. The intermediate sets in round  $r$  are called  $X_{r,1}, \dots, X_{r,n/2^r}$ . Our two main ideas now are as follows.

First, due to the presence of non-trivial subgroups in  $\mathbb{Z}_m$  when  $m$  is not a prime, an intermediate set  $X_{r,i}$  can have a non-trivial symmetry group  $Sym(X_{r,i})$ . As a criterion for a non-trivial symmetry group we test whether  $|X_{r,i}| < |X_{r-1,2i}| + |X_{r-1,2i+1}| - 1$  (cf. Corollary 2.5 of Kneser's Theorem). Once we have found a non-trivial symmetry group  $Sym(X_{r,i})$ , then also  $Sym(A_1 + \dots + A_n) \supseteq Sym(X_{r,i})$  is non-trivial, and thus the output set  $A_1 + \dots + A_n$  is periodic, with period length  $d = m/|Sym(X_{r,i})|$ . It therefore suffices to compute  $A_1 + \dots + A_n$  modulo  $d$ . Hence, we reduce to a problem over a smaller universe  $\mathbb{Z}_d$ . This case is handled in lines 8-12. Note that  $d$  may not be the smallest period length for  $A_1 + A_2 + \dots + A_n$ , but since we only need to reduce the problem size, any period suffices for us.

Second, if the criterion  $|X_{r,i}| < |X_{r-1,2i}| + |X_{r-1,2i+1}| - 1$  is never satisfied, then we can use it to bound the output size. Specifically, we obtain a lower bound for  $|X_{\log n,1}|$  in terms of the total intermediate size  $\sum_j |X_{r,j}|$ . In particular, if the total intermediate size is much larger than  $s$ , then also the output size is more than  $s$ . However, we cannot move to the next guess  $2s$  yet, since we do not know whether the criterion  $|X_{r,i}| < |X_{r-1,2i}| + |X_{r-1,2i+1}| - 1$  will be satisfied in future rounds  $r' > r$ . Nevertheless, we argue that once we have intermediate set size  $\sum_{j \leq i} |X_{r,j}| \gg s$ , then we can ignore the remaining sets  $X_{r,j}$ ,  $j > i$ , by setting them to  $\{0\}$ , cf. lines 13-15. This allows us to bound the total size of all intermediate sets to be linear in the input plus output size.

We next prove correctness and then analyze the running time of Algorithm 2.

**Lemma 5.1** (Correctness of Algorithm 2). *Given non-empty sets  $A_1, \dots, A_n \subseteq \mathbb{Z}_m$ , where  $n$  is a power of 2, Algorithm 2 correctly computes  $A_1 + \dots + A_n$ .*

*Proof.* Note that without lines 13-15, we would compute the sumset in a straightforward bottom-up

tree-like fashion as  $((A_1 + A_2) + (A_3 + A_4)) + \dots$ , and thus the intermediate set  $X_{r,i}$  would be equal to  $A_x + A_{x+1} + \dots + A_y$  for  $x = (i-1)2^r + 1$  and  $y = i2^r$ . In the additional lines 13-15, we set some intermediate sets  $X_{r,i}$  to  $\{0\}$ . Thus, we may lose some summands, but any intermediate set  $X_{r,i}$  still corresponds to the sumset of a subset of its summands  $A_x, A_{x+1}, \dots, A_y$ . More precisely, the set  $X_{r,i}$  satisfies  $X_{r,i} = A_{z_1} + A_{z_2} + \dots + A_{z_\ell}$  for some  $\{z_1, \dots, z_\ell\} \subseteq \{x, x+1, \dots, y\}$ , with the understanding that  $X_{r,i} = \{0\}$  if  $\ell = 0$ . (This property holds initially in line 4 and it continues to hold when we set  $X_{r,i}$  in lines 7 and 14.) In particular, we always have

$$\text{Sym}(X_{r,i}) = \text{Sym}(A_{z_1} + A_{z_2} + \dots + A_{z_\ell}) \subseteq \text{Sym}(A_1 + \dots + A_n). \quad (1)$$

Moreover, we also infer

$$|X_{r,i}| = |A_{z_1} + A_{z_2} + \dots + A_{z_\ell}| \leq |A_1 + \dots + A_n|. \quad (2)$$

We shall perform induction on the universe size  $m$ . For the base case  $m = 1$ , the result is obvious. For larger  $m$ , we consider the following two cases.

**Case 1:** *At some point in the execution, the criterion  $|X_{r,i}| < |X_{r-1,2i-1}| + |X_{r-1,2i}| - 1$  in line 8 is satisfied.* Then by Corollary 2.5,  $\text{Sym}(X_{r,i})$  is non-trivial and hence  $\text{Sym}(A_1 + \dots + A_n) \supseteq \text{Sym}(X_{r,i})$  is also non-trivial. We make use of the fact that all subgroups of  $\mathbb{Z}_m$  are of the form  $d \cdot \mathbb{Z}_{m/d}$ , where  $d$  divides  $m$ . In particular,  $\text{Sym}(X_{r,i}) = d \cdot \mathbb{Z}_{m/d}$  for  $d := m/|\text{Sym}(X_{r,i})|$ . This means that  $A_1 + \dots + A_n$  is cyclic with period length  $d$ . It follows that for  $A'_i := A_i \bmod d$  we have (using the induction hypothesis on  $d$ )

$$A_1 + \dots + A_n = \text{nFOLDSET}(A'_1, \dots, A'_n, d) + d \cdot \{0, 1, \dots, \frac{m}{d} - 1\}.$$

This shows correctness of lines 8-12.

**Case 2:** *Lines 8-12 are never executed.* That is, for each computed set  $X_{r,i}$  in line 7 we have

$$|X_{r,i}| \geq |X_{r-1,2i-1}| + |X_{r-1,2i}| - 1. \quad (3)$$

We use inequality (3) to analyze line 13. Fix any  $s \in \{1, 2, 4, \dots, 2^{\lceil \log m \rceil}\}$ , and consider iteration  $s$ .

**Claim 5.2.** *In iteration  $s$ , we have  $|X_{\log n,1}| > s$  if and only if  $|A_1 + \dots + A_n| > s$ . Moreover, if  $|X_{\log n,1}| \leq s$  then  $X_{\log n,1} = A_1 + \dots + A_n$ .*

Comparing this claim with lines 16-17, we see that if our guess  $s$  for the output size is too small, i.e.,  $|A_1 + \dots + A_n| > s$ , then the algorithm proceeds with the next larger guess. Otherwise, the algorithm correctly computes  $X_{\log n,1} = A_1 + \dots + A_n$  and returns this set. It remains to prove the claim.

*Proof.* The ‘only if’ part follows from the bound  $|X_{\log n,1}| \leq |A_1 + \dots + A_n|$  by (2).

For the ‘if’ part, we consider two cases:

**Case A:** If the criterion  $\sum_{j \leq i} |X_{r,j}| \geq s + n/2^r$  in line 13 is never satisfied, then the algorithm computes  $X_{\log n,1} = A_1 + \dots + A_n$  in a straightforward manner, and thus  $|X_{\log n,1}| = |A_1 + \dots + A_n|$ .

**Case B:** If the criterion  $\sum_{j \leq i} |X_{r,j}| \geq s + n/2^r$  in line 13 is satisfied in some iteration  $r$ , then the following bound shows that it will also be satisfied in iteration  $r + 1$  for some value of  $i$ :

$$\sum_{j=1}^{n/2^{r+1}} |X_{r+1,j}| \stackrel{(3)}{\geq} \sum_{j=1}^{n/2^r} |X_{r,j}| - \frac{n}{2^{r+1}} \geq \left(s + \frac{n}{2^r}\right) - \frac{n}{2^{r+1}} = s + \frac{n}{2^{r+1}}.$$

This nearly proves that the criterion is satisfied in iteration  $r + 1$ , but it ignores that some of the sets  $X_{r+1,j}$  could be set to  $\{0\}$  by lines 13-15. However, when this happens then by the criterion in line 13 we nevertheless have  $\sum_{j=1}^{n/2^{r+1}} |X_{r+1,j}| \geq s + n/2^{r+1}$ .

Therefore, if the criterion in line 13 is satisfied in some iteration  $r$ , then it is also satisfied for  $r = \log n$ , which yields  $|X_{\log n,1}| \geq s + 1 > s$ .

In either case, we obtain  $|X_{\log n,1}| > s$  if  $|A_1 + \dots + A_n| > s$ . This proves the equivalence.

For the second claim, note that  $|X_{\log n,1}| \leq s$  only happens in Case A, and in this case we showed that  $X_{\log n,1} = A_1 + \dots + A_n$ .  $\square$

In summary, if at any point during the course of the algorithm the criterion  $|X_{r,i}| < |X_{r-1,2i-1}| + |X_{r-1,2i}| - 1$  in line 8 is satisfied (Case 1), then we have found a non-trivial symmetry group, and we can move to a problem over a smaller universe  $\mathbb{Z}_d$ , where  $d < m$  is a divisor of  $m$ . Correctness then follows by induction on  $m$ . If this never happens (Case 2), then the algorithm behaves as follows. We have an increasing guess  $s$  for the output size  $|A_1 + \dots + A_n|$ . When this guess is too small, at some point the criterion  $\sum_{j \leq i} |X_{r,j}| \geq s + n/2^r$  in line 13 is satisfied, from which point on we set some of the sets  $X_{r,i}$  to  $\{0\}$ , but we ensure that we end up with  $|X_{\log n,1}| > s$ . This allows us to conclude that our guess  $s$  was too small, so we increase it. When our guess  $s$  reaches the smallest power of 2 that is at least  $|A_1 + \dots + A_n|$ , then the algorithm correctly computes  $X_{\log n,1} = A_1 + \dots + A_n$  and returns this set.  $\square$

**Lemma 5.3** (Running Time of Algorithm 2). *Let  $k := |A_1| + \dots + |A_n| + |A_1 + \dots + A_n|$  be the total input plus output size. Depending on whether we use Theorem 1.1 or Theorem 2.1 for sumset computation, Algorithm 2 is*

1. *deterministic and runs in time  $k \cdot 2^{O(\sqrt{\log k \log \log m})} \cdot \log m$ , or*
2. *randomized and runs in expected time  $O(k \cdot \text{polylog}(mk))$ .*

*Proof.* Let  $T(k, m)$  be the running time of our algorithm. Note that we have at most one call to a recursive subproblem in line 12, incurring time  $T(k, d)$ , where  $d$  is a divisor of  $m$  and thus  $d \leq m/2$ .

Let  $s^*$  be the smallest power of 2 that is at least  $|A_1 + \dots + A_n|$ . Similarly as in the proof of correctness, we see that the algorithm only performs iterations  $s$  from 1 to at most  $s^*$ , since we return the correct output in iteration  $s^*$ , unless we call a recursive subproblem before that.

We bound the running time in iteration  $s$  as follows. For any iteration  $r$ , let  $X_{r,i(r)}$  be the last set that we computed in line 7. (That is, after computing  $X_{r,i(r)}$  we either move to a recursive call, or we set all remaining sets  $X_{r,j} \leftarrow \{0\}$ , for any  $j > i(r)$ .) Note that  $\sum_{j < i(r)} |X_{r,j}| < s + n/2^r$ , since otherwise we would have set  $X_{r,i(r)} \leftarrow \{0\}$  and not computed it in line 7. Moreover,  $|X_{r,i(r)}| \leq |A_1 + \dots + A_n| \leq k$  by (2). By Theorem 1.1, computing  $X_{r,i}$  takes time

$$|X_{r,i}| \cdot 2^{O(\sqrt{\log |X_{r,i}| \log \log m})} \leq |X_{r,i}| \cdot 2^{O(\sqrt{\log k \log \log m})}.$$

Therefore, the total time spent in iteration  $r$  is bounded by

$$\left(s + \frac{n}{2^r} + k\right) \cdot 2^{O(\sqrt{\log k \log \log m})} \leq k \cdot 2^{O(\sqrt{\log k \log \log m})},$$

for any  $1 \leq s \leq s^* = O(k)$ . Summing over all iterations  $r$  adds a factor  $\log n \leq \log k \leq 2^{O(\sqrt{\log k})}$ , which can be ignored. Summing over all iterations  $s$  adds a factor  $\log s^* = O(\log k)$ , which can also be ignored. Adding the potential recursive call, the total running time is

$$T(k, m) \leq k \cdot 2^{O(\sqrt{\log k \log \log m})} + T(k, m/2).$$

This solves to total time  $k \cdot 2^{O(\sqrt{\log k \log \log m})} \cdot \log(m)$ .

The analysis of the randomized variant is analogous.  $\square$

*Proof of Theorem 1.4.* Algorithm 2 almost proves the theorem, except that the deterministic running time shown in Lemma 5.3 is  $k \cdot 2^{O(\sqrt{\log k \log \log m})} \cdot \log m$  instead of the promised  $k \cdot 2^{O(\sqrt{\log k \log \log m})}$ . Note that the former can be bounded by the latter unless  $k \leq \log^c m$ , for some absolute constant  $c$ . In the case  $k \leq \log^c m$  we switch to a different algorithm. Specifically, we simply compute  $((A_1 + A_2) + A_3) + \dots + A_n$  in a linear fashion, in each step using a naive sumset computation that computes  $A + B$  in time  $\tilde{O}(|A| \cdot |B|)$ . Since each intermediate result has size at most  $k$ , each sumset computation takes time  $O(k^2)$ . Since  $n \leq k$ , in total this simple algorithm runs in time  $O(k^3)$ . Finally, since  $k \leq \log^c m$  we can bound  $O(k^3) \leq 2^{O(\sqrt{\log k \log \log m})}$ . This shows the promised running time also in case  $k \leq \log^c m$ . We obtain the promised guarantees even if we do not know  $k$ , by running both algorithms in parallel until the first one finishes.  $\square$

## 6 Output-sensitive Sumset Computation

Recall that in sumset computation we are given sets  $A, B \subseteq \mathbb{Z}_m$  and the task is to compute  $A + B$ . In this section we present a deterministic algorithm for sumset computation. We also show a generalization to convolution of non-negative vectors, proving Theorem 1.1.

Chan and Lewenstein [CL15] designed very efficient algorithms for sumset computation in a specialized setting, in which the input additionally contains a set  $T$  promised to be a superset of  $A + B$ . Their running time is close to linear in  $|T|$ . Specifically, they proved the following lemma.

**Lemma 6.1** (FFT Lemma from [CL15]). *Given sets  $A, B \subseteq \{0, 1, \dots, m-1\}$  and given a set  $T$  which is known to be a superset of  $A + B$ , we can compute  $A + B$  (over  $\mathbb{Z}$ )*

- (1) *by a randomized Las Vegas algorithm in  $O(|T| \text{polylog } m)$  expected time, or*
- (2) *by a deterministic algorithm in  $|T| \cdot 2^{O(\sqrt{\log |T| \log \log m})}$  time*

*The running time bounds are taken from [CL15, Section 8].*

Here we show a trick that yields the same time bounds in the standard setting (without the additional set  $T$ ). We note that it makes no significant difference whether we compute  $A + B$  over  $\mathbb{Z}_m$  or over  $\mathbb{Z}$ , as discussed also in the introduction. We choose to work over  $\mathbb{Z}_m$ , for consistency with the rest of this paper.

**Lemma 6.2.** *Given sets  $A, B \subseteq \mathbb{Z}_m$ , we can compute  $A + B$  (over  $\mathbb{Z}_m$ )*

- (1) *by a randomized Las Vegas algorithm in  $O(|A + B| \text{polylog } m)$  expected time, or*
- (2) *by a deterministic algorithm in  $|A + B| \cdot 2^{O(\sqrt{\log |A+B| \log \log m})}$  time.*

Note that bullet point (1) reproves Theorem 2.1 by Cole and Hariharan [CH02], and bullet point (2) answers an open problem by Chan and Lewenstein [CL15].

---

**Algorithm 3**

---

```
1: procedure DETERMINISTICSUMSET( $A, B, m$ )
2:                                      $\triangleright m$  is a power of 2; non-empty  $A, B \subseteq \mathbb{Z}_m$ ; computes  $A + B$  over  $\mathbb{Z}_m$ 
3:    $m' := m/2$ 
4:    $S \leftarrow$  DETERMINISTICSUMSET( $A \bmod m', B \bmod m', m'$ )
5:    $T \leftarrow S + \{0, m', 2m', 3m'\}$  over  $\mathbb{Z}$                                       $\triangleright T \supseteq A + B$  over  $\mathbb{Z}$ 
6:   Compute  $R := A + B$  over  $\mathbb{Z}$  via the FFT Lemma using additional input  $T$ 
7:   return  $R \bmod m$ 
```

---

*Proof.* First note that we can assume  $m$  to be a power of 2. Indeed, if  $m$  is not a power of 2, we let  $m'$  be the smallest power of 2 greater than  $2m$ . Given  $A, B \subseteq \{0, 1, \dots, m-1\}$  we compute  $A + B$  over  $\mathbb{Z}_{m'}$  and take the resulting set modulo  $m$  to obtain  $A + B$  over  $\mathbb{Z}_m$ . This assumption is not necessary, but shall make the exposition cleaner, avoiding using the ceil and floor functions.

So assume that  $m$  is a power of 2, and set  $m' := m/2$ . Let  $A' := A \bmod m'$  and  $B' := B \bmod m'$  and recursively compute  $S := A' + B'$  over  $\mathbb{Z}_{m'}$ . Then we have  $S = (A + B) \bmod m'$ . Thus, since  $\max(A) + \max(B) < 2m \leq 4m'$ , the set  $T := S + \{0, m', 2m', 3m'\}$  covers  $A + B$ . In other words,  $T$  is a superset of  $A + B$  over  $\mathbb{Z}$ . We can thus use the FFT Lemma to compute  $A + B$  over  $\mathbb{Z}$ . Reducing the resulting set modulo  $m$  yields  $A + B$  over  $\mathbb{Z}_m$ . This leads to the recursive Algorithm 3.

Since we can bound  $|T| \leq 4|S| \leq 4|A + B|$ , the expected running time of one recursive step is  $O(|A + B| \cdot \text{polylog } m)$ , and there are  $O(\log m)$  recursive steps. This yields the claimed randomized running time. For the deterministic variant we obtain running time  $|A + B| \cdot 2^{O(\sqrt{\log |A+B| \log \log m})}$ . polylog  $m$  from the FFT Lemma, times an additional  $\log m$  factor due to the recursion.

Now, to get rid of the additional  $\text{polylog}(m)$  factor and obtain the promised guarantee, we shall observe the following. If  $|A + B| \geq \log m$ , then this running time is bounded by the claimed  $|A + B| \cdot 2^{O(\sqrt{\log |A+B| \log \log m})}$ . If  $|A + B| < \log m$ , then the naive approach which computes  $A + B$  in time  $\tilde{O}(|A| \cdot |B|) = \tilde{O}(|A + B|^2) = 2^{O(\sqrt{\log |A+B| \log \log m})}$ . Running both algorithms in parallel until the first one finishes yields the claimed bound.  $\square$

A similar result also holds for convolution of non-negative vectors. We denote by  $\|x\|_0$  the number of non-zero entries of a vector  $x$ .

**Lemma 6.3.** *Given vectors  $A, B \in \mathbb{R}_{\geq 0}^m$ , we can compute their convolution  $A \star B$  (with wraparound)*

(1) *by a randomized Las Vegas algorithm in  $O(\|A \star B\|_0 \text{polylog } m)$  expected time, or*

(2) *by a deterministic algorithm in  $\|A \star B\|_0 \cdot 2^{O(\sqrt{\log \|A \star B\|_0 \log \log m})}$  time.*

Again bullet point (1) reproves a result by Cole and Hariharan [CH02], and bullet point (2) proves Theorem 1.1.

*Proof.* Denote by  $I$  and  $J$  the indicator vectors of the non-zero entries of  $A$  and  $B$ , respectively. Observe that  $|I + J| = \|A \star B\|_0$ . We can thus compute  $I + J$  in expected time  $O(\|A \star B\|_0 \text{polylog } m)$  by Lemma 6.2. We now make use of a variant of the FFT Lemma from [CL15, Remark 8.2], stating that if we know a superset  $T \supseteq I + J$  then we can compute  $A \star B$  in expected time  $O(|T| \text{polylog } m)$ . Using this for  $T = I + J$  yields expected time  $O(\|A \star B\|_0 \text{polylog } m)$ , or time  $\|A \star B\|_0 \cdot 2^{O(\sqrt{\log \|A \star B\|_0 \log \log m})} \cdot \text{poly}(\log m)$  for the deterministic variant. Now, we can get rid of the  $\text{polylog}(m)$  factors in the deterministic variant using the same argument as the one in Lemma 6.2.  $\square$

## 7 Computing the Symmetry Group

In this section, we show how to compute the symmetry group  $Sym(A)$  for any given non-empty set  $A \subseteq \mathbb{Z}_m$  in time  $O(|A|)$ , proving Theorem 2.3. Let  $n := |A|$  and denote by  $a_1 < a_2 < \dots < a_n$  the elements of  $A$ . For simplicity of notation, we set

$$a_{n+1} := a_1, \quad a_{n+2} := a_2, \quad \dots, \quad a_{2n} := a_n.$$

Note that for our applications of this Theorem,  $a_i$  correspond to residue classes modulo  $m$ . We construct a string  $P$  (the pattern) of length  $n$  by setting for any  $1 \leq i \leq n$ :

$$P_i := (a_{i+1} - a_i) \bmod m.$$

Similarly, we construct a string  $T$  (the text) of length  $2n - 1$  by setting for any  $1 \leq i \leq 2n - 1$ :

$$T_i := (a_{i+1} - a_i) \bmod m.$$

Note that the text is constructed by repeating the pattern twice and removing the last letter.

We say that there is a match of pattern  $P$  in text  $T$  at position  $i$  if  $P_j = T_{i-1+j}$  holds for any  $1 \leq j \leq n$ . The following lemma shows that the matches of  $P$  in  $T$  are in one-to-one correspondence with the symmetry group  $Sym(A)$ . Since all matches of  $P$  in  $T$  can be computed in time  $O(n)$  by the classic Knuth-Morris-Pratt pattern matching algorithm, this finishes the proof of Theorem 2.3.

**Lemma 7.1.** *If there is a match of  $P$  in  $T$  at position  $i$ , then  $a_i - a_1 \in Sym(A)$ . Moreover, for any  $x \in Sym(A)$ , we have  $x = a_i - a_1$  for some  $1 \leq i \leq n$  and there is a match of  $P$  in  $T$  at position  $i$ .*

*Proof.* Note that there is a match at position  $i$  if and only if for all  $1 \leq j \leq n$

$$a_{j+1} - a_j = a_{i+j} - a_{i+j-1} \pmod{m}.$$

Summing this equation in a telescoping sum over all  $j \in \{1, \dots, \ell - 1\}$ , for any fixed  $1 \leq \ell \leq n$ , yields

$$a_\ell - a_1 = a_{i+\ell-1} - a_i \pmod{m},$$

or, equivalently,

$$a_\ell + (a_i - a_1) = a_{i+\ell-1} \pmod{m}.$$

This establishes  $a_i - a_1 \in Sym(A)$ .

For the second part, recall that  $Sym(A) \subseteq A - \{a_1\}$ , as discussed in Section 2.2. Therefore for any  $x \in Sym(A)$  we have  $x = a_i - a_1$  for some  $i$ . Now consider the values  $a'_j := (a_j - x) \bmod m$  for  $1 \leq j \leq n$ . Observe that the sequence  $a'_1, \dots, a'_n$  is monotonically increasing up to some point, where the modulo operation reduces by an additional  $-m$ , and then is again monotonically increasing. In particular, for some  $1 \leq r \leq n$  we have

$$a'_r < a'_{r+1} < \dots < a'_{n-1} < a'_n < a'_1 < a'_2 < \dots < a'_{r-2} < a'_{r-1}.$$

Since  $x \in Sym(A)$  and  $Sym(A)$  is a group, also  $-x \in Sym(A)$ , and thus  $a'_j \in A$  for all  $j$ . Hence, the  $n$  different values  $a'_j$  must correspond to the elements of  $A$ . It follows that  $a'_{r-1+j} = a_j$  for all  $1 \leq j \leq n$ .

Observing that  $a'_i = a_i - x = a_i - (a_i - a_1) = a_1 \pmod{m}$ , we see that  $r = i$ . In other words, we have for all  $1 \leq j \leq n$

$$a_{i-1+j} - (a_i - a_1) = a_j \pmod{m}.$$

Subtracting this equation for  $j$  from this equation for  $j + 1$  yields, for any  $1 \leq j \leq n$ ,

$$a_{i+j} - a_{i+j-1} = a_{j+1} - a_j \pmod{m}.$$

As noted in the beginning of this proof, this means that there is a match of  $P$  in  $T$  at position  $i$ .  $\square$

## References

- [ABB<sup>+</sup>21] Kyriakos Axiotis, Arturs Backurs, Karl Bringmann, Ce Jin, Vasileios Nakos, Christos Tzamos, and Hongxun Wu. Fast and simple modular subset sum. In *Symposium on Simplicity in Algorithms (SOSA)*, pages 57–67. SIAM, 2021.
- [ABHS19] Amir Abboud, Karl Bringmann, Danny Hermelin, and Dvir Shabtay. Seth-based lower bounds for subset sum and bicriteria path. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 41–57. SIAM, 2019.
- [ABJ<sup>+</sup>19] Kyriakos Axiotis, Arturs Backurs, Ce Jin, Christos Tzamos, and Hongxun Wu. Fast modular subset sum using linear sketching. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 58–69. SIAM, 2019.
- [ABP14] Amihood Amir, Ayelet Butman, and Ely Porat. On the relationship between histogram indexing and block-mass indexing. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 372(2016):20130132, 2014.
- [AKKN16] Per Austrin, Petteri Kaski, Mikko Koivisto, and Jesper Nederlof. Dense Subset Sum may be the hardest. In *Proc. of the 33rd Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 13:1–13:14, 2016.
- [AKP07] Amihood Amir, Oren Kapah, and Ely Porat. Deterministic length reduction: Fast convolution in sparse data and applications. In *Combinatorial Pattern Matching, 18th Annual Symposium, CPM 2007, London, Canada, July 9-11, 2007, Proceedings*, pages 183–194, 2007.
- [AKPR14] Amihood Amir, Oren Kapah, Ely Porat, and Amir Rothschild. Polynomials: a new tool for length reduction in binary discrete convolutions. *CoRR*, 2014.
- [AR15] Andrew Arnold and Daniel S Roche. Output-sensitive algorithms for sumset and sparse polynomial multiplication. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, pages 29–36. ACM, 2015.
- [BFN21] Karl Bringmann, Nick Fischer, and Vasileios Nakos. Sparse nonnegative convolution is equivalent to dense nonnegative convolution. In *STOC 2021 (to appear)*. SIAM, 2021.
- [BGNV17] Nikhil Bansal, Shashwat Garg, Jesper Nederlof, and Nikhil Vyas. Faster space-efficient algorithms for Subset Sum,  $k$ -Sum and related problems. In *Proc. of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 198–209, 2017.
- [BN20] Karl Bringmann and Vasileios Nakos. Top- $k$ -convolution and the quest for near-linear output-sensitive subset sum. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 982–995, 2020.
- [Bri17] Karl Bringmann. A near-linear pseudopolynomial time algorithm for Subset Sum. In *Proc. of of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1073–1084, 2017.
- [CH02] Richard Cole and Ramesh Hariharan. Verifying candidate matches in sparse and wildcard matching. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing (STOC)*, pages 592–601. ACM, 2002.



- [CI21] Jean Cardinal and John Iacono. Modular subset sum, dynamic strings, and zero-sum sets. In *Symposium on Simplicity in Algorithms (SOSA)*, pages 45–56. SIAM, 2021.
- [CL15] Timothy M. Chan and Moshe Lewenstein. Clustered integer 3SUM via additive combinatorics. In *Proc. of the 47th Annual ACM Symposium on Theory of Computing (STOC)*, pages 31–40, 2015.
- [CS98] David E. Cardoze and Leonard J. Schulman. Pattern matching for spatial point sets. In *39th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 156–165, 1998.
- [GGdC20] Pascal Giorgi, Bruno Grenet, and Armelle Perret du Cray. Essentially optimal sparse polynomial multiplication. In *Proceeding of the 45th International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 202–209. ACM, 2020.
- [GM91] Zvi Galil and Oded Margalit. An almost linear-time algorithm for the dense Subset-Sum problem. *SIAM J. Comput.*, 20(6):1157–1189, 1991.
- [JW19] Ce Jin and Hongxun Wu. A simple near-linear pseudopolynomial time randomized algorithm for subset sum. In *2nd Symposium on Simplicity in Algorithms, SOSA@SODA 2019*, volume 69 of *OASICS*, pages 17:1–17:6, 2019.
- [KX17] Konstantinos Koiliaris and Chao Xu. A faster pseudopolynomial time algorithm for Subset Sum. In *Proc. of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1062–1072, 2017.
- [MP09] Michael Monagan and Roman Pearce. Parallel sparse polynomial multiplication using heaps. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 263–270. ACM, 2009.
- [Mut95] Shanmugavelayutham Muthukrishnan. New results and open problems related to non-standard stringology. In *Proceedings of the 6th Annual Symposium on Combinatorial Pattern Matching (CPM)*, volume 937, pages 298–317. Springer, 1995.
- [MWW19] Marcin Mucha, Karol Węgrzycki, and Michał Włodarczyk. A subquadratic approximation scheme for partition. In *Proceedings of the 30th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 70–88, 2019.
- [Nak20] Vasileios Nakos. Nearly optimal sparse polynomial multiplication. *IEEE Trans. Inf. Theory*, 66(11):7231–7236, 2020.
- [Roc08] Daniel S Roche. Adaptive polynomial multiplication. *Proc. Milestones in Computer Algebra (MICA’08)*, pages 65–72, 2008.
- [Roc18] Daniel S. Roche. What can (and can’t) we do with sparse polynomials? In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 25–30, 2018.
- [TV06] Terence Tao and Van H. Vu. *Additive Combinatorics*, volume 105. Cambridge University Press, 2006.
- [VDHL12] Joris Van Der Hoeven and Grégoire Lecerf. On the complexity of multivariate block-wise polynomial multiplication. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 211–218. ACM, 2012.