

# A Faster Pseudopolynomial Time Algorithm for Subset Sum

Konstantinos Koiliaris      Chao Xu

Department of Computer Science  
University of Illinois, Urbana-Champaign  
{koiliar2, chaoxu3}@illinois.edu

## Abstract

We introduce a faster pseudopolynomial time algorithm for the SUBSETSUM problem: deciding if there exists a subset of a given set  $S$  whose elements sum to a target number  $t$ , in  $\tilde{O}(\sqrt{n}t)$  time, where  $n$  is the size of  $S$ . In fact, we answer a more general question than that, we compute this for *all* target numbers  $t \leq u$  in  $\tilde{O}(\sqrt{n}u)$ . Our algorithm improves on the textbook  $O(nu)$  dynamic programming algorithm, and as far as we know, is the fastest general algorithm for the problem. Our approach is based on a fast Minkowski sum calculation that exploits the structure of subset sums of small intervals. Finally, we attempt to shed some light on the number of applications this problem and its variations have.

**Keywords:** subset sum, convolution, pseudopolynomial

## 1 Introduction

The SUBSETSUM problem is the problem of deciding given a set of  $n$  integers  $S$  and a target integer  $t$ , if there is a subset  $T$  of  $S$  such that  $\sum_{s \in T} s = t$ . A natural question that arises from it is: *What integers are sums of subsets of  $S$ ?*

Let  $S$  be a subset of  $[u - 1]$  with  $n$  elements<sup>1</sup>,  $u \in \mathbb{N}$ . We define  $\Sigma_u(S)$  to be the *subset sums* of  $S$  that are included in  $[u - 1]$ , formally:

$$\Sigma_u(S) = \left\{ \sum_{s \in T} s \mid T \subset S \right\} \cap [u - 1].$$

Here addition is defined in  $\mathbb{Z}$  or  $\mathbb{Z}_u$ , the default is  $\mathbb{Z}$  unless specified otherwise. In this work, our goal will be to compute  $\Sigma_u(S)$  in time depending on both  $u$  and  $n$ .

The SUBSETSUM problem is a well studied one: a standard  $O(nu)$  pseudopolynomial time dynamic programming algorithm [9] is being taught at every elementary algorithms class. Moreover, there are a number of other algorithms in the literature, including an FPTAS [20], an exact algorithm with space/time trade offs [1], a polynomial time algorithm for most low density sums [10], and a number of more specialized pseudopolynomial time algorithms with various properties [23, 15, 7, 27].

Interestingly enough, little is known about computing *all* subset sums up to an upper bound  $u$  despite the number of applications they have. All current known methods are based on the fact that dynamic programming algorithms for SUBSETSUM also output the table of subset sums [21]. Subset sums are helpful in the design of algorithms that prune the search space depending on the

---

<sup>1</sup> With  $[u]$  we denote the set  $\{0, 1, \dots, u\}$ , this notation is consistent throughout the paper.

computation table, for instance, rectangle packing [19]. Subset sums over  $\mathbb{Z}_u$  are also widely studied in additive combinatorics [30, 3, 17], however, there is little study around computing them.

We can get a variant of SUBSETSUM when we allow the elements in  $S$  to be used *any number of times* in the sums. Let  $S$  be a set of  $n$  elements.  $\Sigma^*(S)$  is defined as the set of sums of any sequence of elements using elements from  $S$ . Computing  $\Sigma^*(S)$  is much simpler than computing  $\Sigma_u(S)$ . In  $\mathbb{Z}_u$  we require the elements of  $\Sigma^*(S)$  to be in  $[u-1]$  and this is equivalent to computing the subgroup generated by  $S$ , denoted  $\langle S \rangle$ , which can be done in  $O(u \log^2 u)$  time. In  $\mathbb{N}$ , this is related to the Frobenius problem, and there exists an algorithm that runs in  $O(n \min S)$  time, to produce a data structure that answers questions of the form “does  $t \in \Sigma^*(S)$ ?” in constant time [5].

Another variant of SUBSETSUM is when we assume the input  $S$  is a *sequence* and  $\Sigma_u(S)$  is defined analogously but now includes *subsequence sums* instead. A similar dynamic programming algorithm can decide if  $t \in \Sigma_u(S)$  in time  $O(n'u)$ , where  $n'$  is the number of unique elements in  $S$  [14, 26]. If there is an algorithm that runs in  $\tilde{O}(f(n, u))^2$  time for  $\Sigma_u(S)$ , where  $f(n, u) = \Omega(n)$ , then we have an algorithm that computes  $\Sigma_u(T)$  in  $\tilde{O}(f(n', u))$  time, where  $T$  is a sequence with  $n'$  unique elements [21]. To us, the counting version of this problem is more interesting, because as we will see it is useful in the calculation of power indices in voting games [25, 29]. Let  $N_{u;S} : [u-1] \rightarrow \mathbb{N}$  be the function that counts the subsequence sums; i.e.,  $N_{u;S}(t)$  is the number of subsequences of  $S$  that sum up to  $t$ . Moreover, let  $N'_{u;S} : \mathbb{N} \times [u-1] \rightarrow \mathbb{N}$  be the length-restricted subsequence sum counting function:  $N'_{u;S}(\ell, t)$  is the number of subsequences of  $S$  of length  $\ell$  that sum to  $t$ .

Our results are summarized as follows.

- Let  $S$  be a *subset* of  $n$  elements in  $[u-1]$ . There exists an algorithm that computes:
  - $\Sigma_u(S)$  in time  $\tilde{O}(\sqrt{n}u)$ , when addition is over  $\mathbb{Z}$ , and
  - $\Sigma_u(S)$  in time  $\tilde{O}(\min\{n^{2/3}, u^{1/3}\}u)$  when addition is over  $\mathbb{Z}_u$ .
- Let  $S$  be a *sequence* of  $n$  elements in  $[u-1]$ . There exists an algorithm that computes:
  - $N_{u;S}$  in time  $\tilde{O}(\sqrt{n}u)$ .
  - $N'_{u;S}$  in time  $\tilde{O}(nu)$ .

Our results apply directly to improve the running time of a few known algorithms, especially, a faster pseudopolynomial time algorithm for the SUBSETSUM problem.

## 2 Preliminaries

Let  $[a..b]$  be the inclusive set  $[a, b] \cap \mathbb{Z}$  and  $[a]$  be the inclusive  $[0..a]$ . All logarithms denoted  $\log$  have base 2.  $\mathbb{Z}_u$  is the group on  $[u-1]$  with addition mod  $u$ . We use the following notation for arithmetic progression:  $r + d[\ell] = \{r, r+d, r+2d, \dots, r+\ell d\}$ . We denote  $A + B = \{a + b \mid a \in A, b \in B\}$  the *Minkowski sum* of  $A$  and  $B$ , which can be computed in  $O(u \log u)$  time if  $A, B \subset [u-1]$ . For a sequence  $S$ , we will denote with  $S'$  the set of distinct elements in  $S$ . For two sequences  $A = a_1, \dots, a_n$  and  $B = b_1, \dots, b_m$ ,  $AB$  is the *concatenation*  $a_1, \dots, a_n, b_1, \dots, b_m$ .

An immediate observation from the subset sum definition is the following.

**Proposition 1.** • If  $A$  and  $B$  are two sequences, then  $\Sigma_u(AB) = (\Sigma_u(A) + \Sigma_u(B)) \cap [u-1]$ .

• If  $A$  and  $B$  are disjoint sets, then  $\Sigma_u(A \cup B) = (\Sigma_u(A) + \Sigma_u(B)) \cap [u-1]$ .

---

<sup>2</sup> $g(n) = \tilde{O}(f(n))$  iff  $g(n) = O(f(n) \log^c n)$  for some constant  $c$ .

The standard dynamic programming algorithm for SUBSETSUM can be seen as using a special case of proposition [9]. It computes  $\Sigma_u(S)$  using the recursive relation  $\Sigma_u(S) = (\Sigma_u(S \setminus \{s\}) + \Sigma_u(\{s\})) \cap [u - 1]$  for some  $s \in S$ . This simple proposition implies the correctness of all divide-and-conquer algorithms: first partition the set, then solve the problem on each individual partition class and combine the results (using the Minkowski sum above).

A function  $h$  is  $S$ -perfect if  $h(a + b) = h(a) + h(b)$  for all  $a, b \in S$  and  $h$  is a injection. If  $h$  is  $S$ -perfect, then for any  $A, B \subset S$ ,  $A + B = h^{-1}(h(A) + h(B))$  [8].

**Lemma 1.** *Given  $\ell, k, d$ , if  $S = \bigcup_{i=1}^k id + [\ell - 1]$ ,  $\bar{S} = \bigcup_{i=1}^{2k} id + [2\ell - 1]$ . We can compute a  $S$ -perfect function  $h : \bar{S} \rightarrow [O(k\ell)]$  in  $O(1)$  time.*

### 3 Subset Sums

In this section, we consider the problem of computing  $\Sigma_u(S)$  when  $S$  is a *subset* of elements in  $[u - 1]$ . Some lemmas in this section are proven in the more general setting of subsequence sums, which also hold for subset sums.

The main idea here is to partition the input into smaller inputs, such that the subset sums of each smaller part span a small set with regular structure. Then we take advantage of the structure and combine the subset sums quickly.

The algorithm relies on the following crucial observation that speeds up the computation of Minkowski sums.

**Theorem 2.** *Let  $A$  and  $B$  be two sequences with total length  $n$ . All elements in  $A$  and  $B$  is in  $a + [\ell - 1]$ . If  $\Sigma_u(A)$  and  $\Sigma_u(B)$  are given, then we can compute  $\Sigma_u(AB) = (\Sigma_u(A) + \Sigma_u(B)) \cap [u - 1]$  in  $\tilde{O}(\min\{\ell k^2, u\})$  time, where  $k = \min\{n, u/a\}$ .*

This bound has three estimates, each of which is useful in its own right. When  $a$  is large, most sums lie outside  $[u - 1]$ , hence we can discard them and get the bound  $(u/a)^2 \ell$ . If  $a$  is small but there are only a few elements in the range, we use the bound  $n^2 \ell$ . Finally, the naive estimate  $u$  is only applied when the other bounds are significant overestimates.

#### 3.0.1 Combine Subroutine.

We first consider a subroutine `Combine`. See Algorithm 1. This subroutine takes a sequence of sets  $S_1, \dots, S_m$ , finds the Minkowski sum of adjacent sets and recurses. It utilizes Theorem 2.

---

**Algorithm 1:** `Combine`( $A_1, \dots, A_n$ )

---

```

1 if  $n = 1$  then
2   | return  $A_1$ 
3 for  $i$  in  $[1..n/2]$  do
4   |  $B_i \leftarrow (A_{2i-1} + A_{2i}) \cap [u - 1]$ 
5 return Combine( $B_1, \dots, B_{n/2}$ )

```

---

**Theorem 3.** *1. If the inputs of `Combine` are  $\Sigma_u(\{s_1\}), \dots, \Sigma_u(\{s_n\})$ ,  $a \leq s_1 \leq s_2 \leq \dots \leq s_n \leq a + \ell - 1$  and  $n \leq \ell\sqrt{u}$ , then the algorithm outputs  $\Sigma_u(s_1, \dots, s_n)$  in time*

$$\tilde{O}(\ell^{1/3} n^{2/3} u^{2/3}). \quad (1)$$

2. Let  $a \leq s_1 < s_2 < \dots < s_n \leq a + \ell - 1$ . If the inputs of *Combine* are  $s_1[\ell_1], \dots, s_n[\ell_n]$ , then the algorithm outputs  $s_1[\ell_1] + \dots + s_n[\ell_n]$  in time

$$\tilde{O}\left(\frac{u^2 \ell}{a^2}\right). \quad (2)$$

The second part of the theorem is more general than we need. For this section, we will only use the case when all  $\ell_i = 1$  because  $\Sigma_u(\{s\}) = s[1]$ .

### 3.0.2 The Algorithm.

Consider algorithm 2. Let  $k = \lceil \log \log n \rceil$ , we partition  $[u - 1]$  by cutting it into intervals  $[0..a_1 - 1], [a_1..a_2 - 1], \dots, [a_k..u - 1]$ , and find  $\Sigma_u(S \cap [a_i..a_{i+1} - 1])$  by using the *Combine* method.

---

#### Algorithm 2: $\text{SS}(S)$

---

```

1  $n \leftarrow |S|$ 
2  $a_0 \leftarrow 0$ 
3  $k \leftarrow \lceil \log \log n \rceil$ 
4 for  $i$  in  $[1..k]$  do
5    $a_i \leftarrow \left\lceil u/n^{(2^k - 2^i + 2)/2^{k+1}} \right\rceil$ 
6  $a_{k+1} \leftarrow u$ 
7 for  $i$  in  $[k]$  do
8    $s_1, \dots, s_t \leftarrow$  sorted list of all elements in  $S \cap [a_i..a_{i+1} - 1]$ 
9   for  $j$  in  $[1..t]$  do
10     $B_j \leftarrow \Sigma_u(\{s_j\})$ 
11   $A_i \leftarrow \text{Combine}(B_1, \dots, B_t)$ 
12 return  $(A_0 + A_1 + \dots + A_k + A_{k+1}) \cap [u - 1]$ 

```

---

We set  $a_i = \left\lceil u/n^{\frac{2^k - 2^i + 2}{2^{k+1}}} \right\rceil$ , for all  $1 \leq i \leq k$ ,  $a_0 = 0$  and  $a_{k+1} = u$ . When  $i = 0$ ,  $n \leq (u/\sqrt{n})\sqrt{u}$

because  $n$  is at most  $u$ . *Combine* applied on subset sums of singletons of  $S \cap [a_0..a_1 - 1]$  is  $\tilde{O}(\sqrt{n}u)$  by (1). For all other  $i \in [1..k]$ , we can apply the bound in (2) and get running time  $\tilde{O}(n^{1/2+1/2^k}u)$ . Because  $k$  is chosen so that  $n^{1/2^k} = n^{1/\log n} = 2$ , the total running time of *Combine* is  $\tilde{O}(\sqrt{n}u)$ . The rest of the algorithm is clearly  $\tilde{O}(u)$ .

When  $n$  is large, specifically  $n > u^{2/3}$ , we can make a small improvement to the above. Consider the same algorithm but this time let  $k = \lceil \log \log u^{1/3} \rceil$  and  $a_i = \lceil 2^{2^i - 1} u^{2/3} \rceil$  for all  $i \in [1..k]$ . Using (1) along with the fact that  $|S \cap [\ell - 1]| \leq \ell$ , we can compute  $\Sigma_u(S \cap [0..a_1 - 1])$  in  $\tilde{O}(u^{4/3})$  time. By applying (2) we can see that computing all other intervals can also be done in time  $\tilde{O}(u^{4/3})$ , yielding the overall running time. Notice this modification is specific only to the subset sums, and would not hold for sequences. All of the above is formally summed up in the following theorem.

**Theorem 4.** *Let  $S$  be a subset of  $n$  elements of  $[u - 1]$ . Then there exists an algorithm that computes  $\Sigma_u(S)$  in  $\tilde{O}(\min\{\sqrt{n}, u^{1/3}\}u)$  time.*

## 3.1 Applications

**Subset Sum.** As we mentioned in the introduction, our approach provides a faster algorithm for the SUBSETSUM problem. Although other faster pseudopolynomial time algorithms exist, they

all enforce some restrictions. Pisinger in [27] presented a  $O(n \max S)$  time algorithm that is fast if  $\max S$  is small, our algorithm surpasses it when  $\max S = \tilde{\Omega}(u/\sqrt{n})$ . There also exist a series of algorithms based on analytical number theory [15, 7] that have faster running time only when a list of technical properties are satisfied: first, they require the input to be dense, namely  $n = \tilde{\Omega}(\sqrt{\max S})$ , also they require the target value  $t$  to be within some interval close to  $\sum_{s_i \in S} s_i/2$ .

The following corollary is useful on its own right for applications that use subsequence sums, and for when the sum of all elements in the sequence is the measure of the running time.

**Corollary 1.** *Let  $S$  be a sequence of natural numbers that sums to  $u$ , then  $\Sigma_u(S)$  can be computed in  $\tilde{O}(u^{5/4})$  time.*

*Proof.* There are  $O(\sqrt{u})$  unique values in  $S$  because sum of  $2\sqrt{u}$  smallest natural number exceeds  $u$ . Hence, we can find  $\Sigma_u(S)$  in running time  $\tilde{O}(n'^{1/2}u) = \tilde{O}(u^{5/4})$ , where  $n'$  is the number of unique values in the sequence, by Theorem 4 and the fact that subsequence sums reduce to subset sums with only a polylog blowup with respect to the number of unique elements in the sequence.  $\square$

**Attack on Precise Query Protocols.** In an application for attacking Precise Query Protocols, one of the bottlenecks is generating all permissible regions for an attack [11]. This reduces to the problem of computing all  $\Sigma_n(S_x)$ , where  $S_x$  is  $S$  with a single entry  $x$  removed, of a given sequence  $S$  of positive integers that sum to  $n$ . This can be done in two steps. First, compute  $\Sigma_n(T)$ , where  $T$  is the sequence obtained from  $S$  by deleting one copy of  $S'$ . Corollary 1 gives us  $\tilde{O}(n^{5/4})$  running time. For each element  $x \in S'$ , compute  $\Sigma_n(S' - \{x\})$ . This can be done in  $\tilde{O}(n|S'|) = O(n^{3/2})$  time using a dynamic subset sum data structure [13]. Finally, use the fact  $\Sigma_n(S_x) = (\Sigma_n(T) + \Sigma(S' - \{x\})) \cap [n - 1]$  to compute the solutions in  $\tilde{O}(n|S'|)$  time. Hence we have a  $\tilde{O}(n^{3/2})$  running time algorithm, a improvement to the  $\tilde{O}(n^2)$  running time [11].

**Graph Partitioning.** In this section we assume  $G = (V, E)$  is a graph with  $n$  vertices and  $m$  edges. Subset sums arise naturally in graph algorithms that try to find bipartitions with restriction on the sizes of each cluster while satisfying certain properties [6, 12, 18, 22, 16].

One such problem is the *bottleneck graph partition* problem that asks for a cut where all the clusters are of equal size and the maximum edge weight across the cut is minimized. This problem can be reduced to solving  $O(\log n)$  subset sum problems: pick a weight, delete all edges with smaller weight, and decide if there exist an arrangement of components that satisfy the size requirement [18]. In [22] the question of whether there exists an algorithm with faster running time than  $O(m + n^{3/2} \log n)$  was left as an open problem. By Corollary 1 we answer this affirmatively, giving a  $\tilde{O}(m + n^{5/4})$  time algorithm.

Another example arises in finding the most balanced valid bipartition. If  $A, B$  is a partition of  $V$  and all edges goes across  $A$  and  $B$ , then it's called a valid bipartition. Define

$$b(G) = \min \{ \max \{ |A|, |B| \} \mid A, B \text{ is a valid bipartition} \}.$$

Intuitively,  $b(G)$  measures the bipartition of the graph, which we want to be as balanced as possible. Finding  $b(G)$  is an important subtask in computing zero-sum bipartite Ramsey numbers [6] and approximation algorithms for almost-perfect graph bisections [16]. This problem can be easily converted to a subsequence sums problem. Consider the case where  $G$  has  $k$  components and the  $i$ th component has bipartition of size  $a_i$  and  $b_i$ , where  $a_i \leq b_i$ . Create a subsequence sums instance by forming a sequence of  $n$  elements with the  $i$ th element  $c_i$  having size  $b_i - a_i$ . Finally, let  $a = \sum_i a_i$ , then

$$b(G) = \min_{x \in \Sigma_n(c_1, \dots, c_n)} \max \{ a + x, n - (a + x) \},$$

using Corollary 1, we get a running time of  $\tilde{O}(m + n^{5/4})$ .

## 4 Subset Sums in $\mathbb{Z}_u$

The main advantage in addition under  $\mathbb{Z}$  is that we throw away a large part of the subset sums that falls outside  $[u - 1]$ . Unfortunately, this is not the case in  $\mathbb{Z}_u$ . All possible sums need to stay in the group, and so must be accounted for. Furthermore, Theorem 2 does not hold in  $\mathbb{Z}_u$ , so we will use the  $O(u \log u)$  algorithm for Minkowski sums.

Fortunately though, if we partitioning the domain in a way that the output sizes remain small, then we can take advantage that there are subset sum algorithm with running time depending on the output size.

**Theorem 5** ([21]). *There is an algorithm  $\text{SSDP}(S)$  that computes  $\Sigma_u(S)$  in  $O(|S| |\Sigma_u(S)|)$  time.*

Let  $\mathbb{Z}_u^*$  be the set of units of  $\mathbb{Z}_u$ , i.e., the set of elements in  $\mathbb{Z}_u$  that are relatively prime to  $u$ . We first show how to handle the input when  $S \subset \mathbb{Z}_u^*$ .

### 4.1 Subset Sums of a Subset of $\mathbb{Z}_u^*$

The set  $x[\ell]$  is called a segment of length  $\ell$  with slope  $x$ . Assume  $\ell \geq 2$ . Observe that a subset of a segment always produces a small output: if  $S$  is a non-empty subset of  $x[\ell]$ , then  $\Sigma_u(S)$  has at most  $|S|\ell + 2 \leq 2|S|\ell$  elements.

The idea is to find a segment  $x[\ell]$  that covers a large portion of the input, compute the subset sums of  $S \cap x[\ell]$ , and repeat the process for  $S \setminus x[\ell]$ . Because  $\Sigma_u(S \cap x[\ell])$  is small, we can bound the running time with Theorem 5. However, it's not clear that there always exist a short segment that covers a large enough portion of  $S$ .

Consider a bipartite graph  $H_{S,\ell} = (A \cup B, E)$ .  $A = \{u_x | x \in \mathbb{Z}_u\}$ ,  $B = \{v_c | c \in S\}$ . If  $ix \equiv c \pmod{u}$  where  $x \in \mathbb{Z}_u$ ,  $c \in S$  and  $0 \leq i \leq \ell$ , then there is an edge  $u_x v_c$  in  $E$ . The neighborhood of  $u_x$  corresponds to  $x[\ell] \cap S$ . There always exists some  $u_x$ , such that its neighborhood contains more than  $\frac{n}{u}\ell/50 \log \log u$  elements, and can be constructed in  $O(n\ell + u)$  time. See Appendix A.3 for details.

---

#### Algorithm 3: $\text{SSCyclicunit}(S)$

---

**Input:** A set  $S$  of  $n$  elements.

```

1  $\ell \leftarrow u/n^{2/3}$ 
2  $d \leftarrow \ell/(50u \log \log u)$ 
3  $X \leftarrow \{0\}$ 
4  $i \leftarrow 1$ 
5 while  $d|S| \geq 1$  do
6    $m_i \leftarrow \lceil d|S| \rceil$ 
7    $x \leftarrow$  a value such that  $|S \cap x[\ell]| \geq m_i$ 
8    $S_i \leftarrow m_i$  elements in  $|S \cap x[\ell]|$ 
9    $S \leftarrow S \setminus S_i$ 
10   $Y \leftarrow \text{SSDP}(S_i)$ 
11   $X \leftarrow X + Y$ 
12   $i \leftarrow i + 1$ 
13 return  $X + \text{SSDP}(S)$ 
```

---

Recall we have now shown that there always exist a segment of length  $\ell$  that covers  $\tilde{O}(|S|/\ell)$  elements. We are ready to go through the algorithm. The algorithm is described formally in Algorithm 3. The running time for all parts except the while loop can be bounded by  $\tilde{O}(u)$ . In the while loop, we have to find  $x[\ell]$  that covers the at least  $d|S|$ , remove some elements from  $S$  and repeat. In order to support this operation, we implicitly represent  $S$  with the graph  $H_{S,\ell}$ . This allow us to find the  $x$  that maximizes  $|S \cap x[\ell]|$  quickly by picking the vertex in  $A$  with maximum degree. Computing  $S \setminus S_i$  is equivalent to removing vertices of  $S_i$  and corresponding edges in  $H_{S,\ell}$ . The running time is proportional to the number of edges and vertices removed. Hence the total amount of time spent between lines 6 and 9 is  $\tilde{O}(n\ell + u)$ .

At the  $i$ th iteration we have  $|S| \leq (1-d)^i n$ , and we removed

$$|S_i| = \lceil d|S| \rceil \leq \lceil d(1-d)^i n \rceil \leq d(1-d)^i n + 1,$$

elements. Because the algorithm executes an iteration only when  $d|S| \geq 1$ ,  $|S_i| \leq 2d(1-d)^i n$ . Knowing the size of  $|S_i|$  help us bounds all the time spent on SSDP.

$$\sum_{i=0}^k |S_i| |\Sigma_u(S_i)| \leq \sum_{i=0}^{\infty} 2(d(1-d)^i n + 1)^2 \ell = 8d^2 n^2 \ell \frac{1}{(2-d)d} = \tilde{O}(\ell^2 n^2 / u).$$

The number of time while loop executed is  $\tilde{O}(u/\ell)$ . See Appendix A.4. The final SSDP takes  $\tilde{O}(u^2/\ell)$  time, because  $d|S| < 1$  if and only if  $|S| < 50u \log \log u/\ell$ , hence  $|S|u = \tilde{O}(u^2/\ell)$ .

Aggregate all running time, we get

$$\tilde{O}(\ell^2 n^2 / u + u^2 / \ell + n\ell + u).$$

By setting  $\ell = u/n^{2/3}$ , the above expression simplifies to  $\tilde{O}(n^{2/3}u)$ .

We can further improve the running time when  $n$  is large, by using the following theorem from additive combinatorics.

**Theorem 6** (Theorem 1.1 [17]). *If  $Y \subset \mathbb{Z}_u^*$  and  $|Y| > 1 + 2\sqrt{u-4}$ , then  $\Sigma_u(Y) = \mathbb{Z}_u$ .*

We use it by editing the previous algorithm by adding a condition to just return  $\mathbb{Z}_u$  if  $|S_0| > 1 + 2\sqrt{u-4}$ , and continue with the computation otherwise. This guarantees we spend at most  $\tilde{O}(\sqrt{u}^{2/3} u) = \tilde{O}(u^{4/3})$  time.

This result is summed up in the following theorem.

**Theorem 7.** *Given a subset  $S \subset \mathbb{Z}_u^*$  of  $n$  elements, we can compute  $\Sigma_u(S)$  in  $\tilde{O}(\min\{n^{2/3}, u^{1/3}\}u)$  time.*

## 4.2 Subset Sums in $\mathbb{Z}_u$

Other than elements in  $S \cap \mathbb{Z}_u^*$ , all of the input can be divided by some prime factor of  $u$  and fall into smaller cyclic subgroups. The algorithm then solves them in each smaller subgroup, pulls them back and convolves them together.

Let's consider the recursive Algorithm 4.

Before partitioning all operations clearly take  $O(u)$  time. Partitioning and computing  $S' \cap \mathbb{Z}_u^*$  can be done in  $O(uk)$  time: divide each element by  $p_k, \dots, p_1$  successively, and add it to  $S_i$  if  $p_i$  is the first prime dividing it. If none of the elements divide it, we know it is in  $S_0$ . Since  $k = O(\log u)$ , this step takes  $O(u \log u)$  time. Once we are done with the partition, we run  $O(k)$  recursions, and spend  $O(u)$  time to project the sets to the input and lift from the output. The only time-consuming



---

**Algorithm 4:**  $\text{SSCyclic}(S, u)$ 

---

**Input:** A set  $S$  and a cyclic group of size  $u$ , where  $u$  has distinct prime factors

$p_1 < p_2 < \dots < p_k$ , and  $p_0 = 1$ .

```
1 if  $\min\{u, |S'|\} \leq 4$  then
2   | return  $\text{SSDP}(S)$ 
3 Partition  $S$  into  $S_0, S_1, \dots, S_k$  such that all elements in  $S_i$  are divisible by  $p_i$  but not  $p_j$  for
    $j > i$ .
4  $X_0 \leftarrow \text{SSCyclicunit}(S_0)$ 
5 for  $1 \leq i \leq k$  do
6   |  $X_i \leftarrow \text{SSCyclic}(S_i/p_i, u/p_i) \times p_i$ 
7 return  $X_0 + X_1 + \dots + X_k$ 
```

---

part is computing  $N_{u;S_0}$ , which takes at most  $\tilde{O}(\min\{n^{2/3}, u^{1/3}\}u)$  time. Finally, combining all the results with minkowski sums takes  $O(ku \log u) = O(u \log^2 u)$  time. Each call of  $\text{SSCyclic}$  spends  $\tilde{O}(\min\{n^{2/3}, u^{1/3}\}u)$  outside the recursion. The recursion doesn't contribute much, see Appendix A.5. Hence we conclude the following theorem.

**Theorem 8.** *Given a subset  $S$  of  $\mathbb{Z}_u$  of  $n$  elements, we can compute  $\Sigma_u(S)$  in  $\tilde{O}(\min\{n^{2/3}, u^{1/3}\}u)$  time.*

## 5 Computing $N_{u;S}$

This section extends the result in section 3 to both sequences and counting. Most results carry over without need of any proof.

### 5.1 Preliminaries

For a sequence  $S = s_1, \dots, s_n$ ,  $\chi_S(x) = |\{i \mid s_i = x\}|$  is the number of occurrences of  $x$  in  $S$ .

For finding  $N_{u;S}$ , we assume the Real RAM model [28, 4]. In the the Real RAM model all basic arithmetic operations on real numbers can be done in  $O(1)$  time. This model is chosen to account for the inherent exponential large numbers during counting, and for consistency with previous works [29]. All functions are non-negative. The support of a function is defined as  $\text{supp } f = \{x \mid f(x) > 0\}$ . Each function can be implemented as a dictionary data structure. For each  $x \in \text{supp } f$ , the dictionary stores  $x$  and  $f(x)$ , for instance consider a binary search tree. This allows every atomic operation to be completed in  $O(\log \text{supp } f)$  time.

Define the *discrete convolution* of two functions as follows:

- $f, g : [u-1] \rightarrow \mathbb{R}_{\geq 0}$  to be equal to

$$(f * g)(j) = \sum_{\substack{j-i, \\ i \in [u-1]}} f(j-i)g(i).$$

Where  $f * g$  can be computed in  $\tilde{O}(u)$  time using the fast fourier transformation [24].

- $f, g : \mathbb{N} \times [u-1] \rightarrow \mathbb{R}_{\geq 0}$  to be

$$(f * g)(a, j) = \sum_{\substack{(a-b, j-i), \\ (b, i) \in \mathbb{N} \times [u-1]}} f(a-b, j-i)g(b, i).$$



Where  $f * g$  can be computed in  $\tilde{O}(\max\{a \mid (a, i) \in \text{supp}(f * g)\} u)$  time using the fast fourier transformation [24].

$\text{Repeat}(x, m)$  computes  $N_{u;X}$ , where  $X$  is a sequence of  $x$  repeated  $m$  times. See Fig. 1. Let  $k = \min\{\lfloor u/x \rfloor, m\}$ . The list of binomial coefficients can be derived by the recurrence  $\binom{n}{i} = \frac{n-i}{i} \binom{n}{i-1}$  and as such takes  $O(k)$  time. The output is a function  $g$  with  $\text{supp } g = x[k]$ .

We introduce  $\text{Combine}'$  that operates by taking convolutions instead of Minkowski sums. See Fig. 1.

There is an analogue to Proposition 1, which also can be proved by definition.

**Proposition 2.** *Let  $A$  and  $B$  be two subsequences partitioning sequence  $S$ . Then  $N_{u;S} = N_{u;A} * N_{u;B}$  and  $N'_{u;S} = N'_{u;A} * N'_{u;B}$ .*

One can easily verify that  $\text{supp}(N_{u;A} * N_{u;B}) = (\Sigma_u(A) + \Sigma_u(B)) \cap [u-1]$  for all sequences  $A$  and  $B$ . In other words,  $\text{supp}$  is just a homomorphism between  $\{\Sigma_u(S) \mid S \text{ a sequence}\}$  under the Minkowski sum intersect  $[u-1]$  and  $\{N_{u;S} \mid S \text{ a sequence}\}$  under convolution.

If  $h$  is  $S$ -perfect function, define

$$f_h(x) = \begin{cases} (f \circ h^{-1})(x) & x \in S + S \\ 0 & \text{otherwise} \end{cases},$$

Note  $h^{-1}(x)$  is well defined if  $x \in S + S$ , because  $h$  is injective, and  $h(x)$  exists because  $h$  is  $S$ -perfect.

For any  $f, g$  such that  $\text{supp } f, \text{supp } g \subset S$ , we have

$$f * g = (f_h * g_h) \circ h.$$

This provides us with an analogue of the Minkowski sum theorems for convolutions. In particular, Theorem 2 and Theorem 3 generalize for convolutions as follows.

**Theorem 9.** *Let  $A$  and  $B$  be two sequences with total length  $n$  such that all values are in  $a + [\ell-1]$ . If  $N_{u;A}$  and  $N_{u;B}$  are given, then we can compute  $N_{u;A} * N_{u;B}$  in  $\tilde{O}(\min\{k^2\ell, u\})$  time, where  $k = \min\{n, u/a\}$ .*

**Theorem 10.** 1. *If the inputs of  $\text{Combine}'$  are  $N_{u;s_1}, \dots, N_{u;s_n}$ , where  $a \leq s_1 \leq s_2 \leq \dots \leq s_n \leq a + \ell - 1$  and  $n \leq \ell\sqrt{u}$ , then the algorithm outputs  $N_{u;s_1, \dots, s_n}$  in time  $\tilde{O}(\ell^{1/3} n^{2/3} u^{2/3})$ .*

2. *Let  $a \leq s_1 < s_2 < \dots < s_n \leq a + \ell - 1$ . If the inputs of  $\text{Combine}'$  are  $f_1, \dots, f_n$  such that  $\text{supp } f_i = s_i[\ell_i]$  for some  $\ell_i$ , then the algorithm outputs  $f_1 * \dots * f_n$  in time  $\tilde{O}\left(\frac{u^2\ell}{a^2}\right)$ .*

The proof for the convolution variants are almost identical to original theorems, hence omitted.

## 5.2 Counting Subsequence Sums

In this section, we consider the problem of computing  $N_{u;S}$  when  $S$  is a *sequence* of elements in  $[u-1]$ . Our algorithm for subset sums can be applied directly to the counting sum problem with only a few small modification.

<b>: Combine'(<math>f_1, \dots, f_n</math>)</b>	<b>: Repeat(<math>x, m</math>)</b>
1 <b>if</b> $n = 1$ <b>then</b>	1 $g$ is an all 0 function
2   <b>return</b> $f_1$	2 $k \leftarrow \min\{\lfloor u/x \rfloor, m\}$
3 <b>for</b> $i$ <b>in</b> $[1..n/2]$ <b>do</b>	3 <b>for</b> $i \in [k]$ <b>do</b>
4   $g_i \leftarrow f_{2i-1} * f_{2i}$	4   $g(ix) \leftarrow \binom{m}{i}$
5 <b>return</b> <b>Combine'</b> ( $g_1, \dots, g_{n/2}$ )	5 <b>return</b> $g$

Figure 1: Combine' and Repeat.

<b>Algorithm 5: SSCount(<math>S</math>)</b>
1 $n \leftarrow  S $
2 $v \leftarrow \min(n, u)$
3 $k \leftarrow \lceil \log \log v \rceil$
4 <b>for</b> $s \in S'$ <b>do</b>
5   $g_s \leftarrow \text{Repeat}(s, \chi_S(s))$
6 <b>for</b> $j$ <b>in</b> $[1..k]$ <b>do</b>
7   $a_j \leftarrow \lceil u/v^{(2^k - 2^j + 2)/2^{k+1}} \rceil$
8 $a_{k+1} \leftarrow u$
9 <b>if</b> $n \leq u$ <b>then</b>
10   $s_1, \dots, s_t \leftarrow$ sorted list of all elements of $S$ in $[0..a_1]$
11   <b>for</b> $i$ <b>in</b> $[1..t]$ <b>do</b>
12     $h_i \leftarrow N_{u; s_i}$
13   $f_0 \leftarrow \text{Combine}'(h_1, \dots, h_t)$
14 <b>else</b>
15   $s_1, \dots, s_t \leftarrow$ sorted list of $S' \cap [0..a_1]$
16   $f_0 \leftarrow \text{Combine}'(g_{s_1}, \dots, g_{s_t})$
17 <b>for</b> $j$ <b>in</b> $[1..k]$ <b>do</b>
18   $s_1, \dots, s_t \leftarrow$ sorted list of $S' \cap [a_j..a_{j+1} - 1]$
19   $f_j \leftarrow \text{Combine}'(g_{s_1}, \dots, g_{s_t})$
20 <b>return</b> $f_0 * f_1 * \dots * f_{k+1}$

**Counting Algorithm.** We are ready to present Algorithm 5. Contrast the algorithm SSCount with SS. Almost all run time analysis carries over with Theorem 9.

When  $n \leq u$ , we have  $n \leq (u/\sqrt{n})\sqrt{u}$  using the first bound of Theorem 10. The time for computing  $f_0$  is therefore  $\tilde{O}(\sqrt{nu})$ . When  $n > u$ ,  $f_0$  is computed through  $O(\sqrt{u})$  convolutions, and each convolution takes  $\tilde{O}(u)$  time. Either way, the running time is  $\tilde{O}(\sqrt{nu})$ .

Second part of Theorem 10 bounds the running time for computing all  $f_i$  where  $1 \leq i \leq k+1$  by  $\tilde{O}(n'^{1/2+1/2^k}u)$ , where  $n'$  is the number of unique elements in  $S$ . Because  $n'^{1/2^k} \leq \min\{n, u\}^{1/2^k} = 2$ , it simplifies to  $\tilde{O}(\sqrt{n'}u) = \tilde{O}(\sqrt{nu})$ .

The total time spent over all Repeat is  $\tilde{O}(u)$  because  $\sum_{x \in [1..u-1]} u/x = O(u \log u)$ , which is dominated by  $\tilde{O}(\sqrt{nu})$ . We summarize this as a theorem.

**Theorem 11.** *There exist an algorithm to compute  $N_{u;S}$  in  $\tilde{O}(\sqrt{nu})$  time.*

### 5.3 Counting Length Restricted Subsequence Sums

One can use a similar technique as in this section to compute the table  $N'_{u;S}$  in  $\tilde{O}(nu)$  time.

Let  $A = a_1, \dots, a_n$ ,  $B = b_1, \dots, b_m$ , then the convolution  $N'_{u;A} * N'_{u;B}$  takes  $\tilde{O}((n+m)u)$  time, as there is no subsequence of  $A, B$  with length more than  $n+m$ . Applying  $\text{Combine}(N'_{u;s_1}, \dots, N'_{u;s_n})$  we get the desired result in time  $\tilde{O}\left(\sum_{i=0}^{\log n} \sum_{j=1}^{n/2^i} 2^i u\right) = \tilde{O}(nu)$ .

### 5.4 Applications

The counting variants of SUBSETSUM are prominent in computing power indices for voting games with  $n$  voters and cutoff value of  $u$ .

In particular, given voters  $V = \{v_1, \dots, v_n\}$  with weight function  $w : V \rightarrow \mathbb{N}$ , a subset  $S$  is called *winning* if  $\sum_{v \in S} w(v) \geq u$ , and *losing*, otherwise. Let  $\mathcal{P}_v$  be all the sets  $S$  such that  $S$  is winning and  $S \setminus \{v\}$  is losing. We offer two algorithms that outperform the current best known algorithms.

**Banzhaf Index.** The *Banzhaf index* of a player  $v$  is the probability a random set is in  $\mathcal{P}_v$ , defined  $BZ(v) = \frac{1}{2^n} |\mathcal{P}_v|$ . The algorithm for computing  $N_{u;S}$  can be directly applied to compute the Banzhaf index. The previously best known pseudopolynomial time algorithm has running time of  $O(nu)$  [29]. Our truncated subsequence sum result improves the running time to  $\tilde{O}(\sqrt{n}u)$ .

**Shapley-Shubik Index.** The *Shapley-Shubik index* adds a weight  $(|S| - 1)!(n - |S|)!$  to each set, and subsequently asks for the weighted sum. Formally it is defined as:  $SS(v) = \frac{1}{n!} \sum_{S \in \mathcal{P}_v} (|S| - 1)!(n - |S|)!$ . After computing  $N'_{u;S}$ , the Shapley-Shubik index can be calculated easily by reading all the values in  $N'_{u;S}$  in  $O(nu)$  time. Our  $\tilde{O}(nu)$  time algorithm is a significant improvement to the previously known fastest algorithm, which ran in  $O(n^2u)$  time [29].

## References

- [1] P. Austrin, P. Kaski, M. Koivisto, and J. Mtt. Spacetime tradeoffs for subset sum: An improved worst case algorithm. In F. Fomin, R. Freivalds, M. Kwiatkowska, and D. Peleg, editors, *Automata, Languages, and Programming*, volume 7965 of *Lecture Notes in Computer Science*, pages 45–56. Springer Berlin Heidelberg, 2013.
- [2] E. Bach and J. Shallit. *Algorithmic Number Theory: Efficient algorithms*. Number v. 1 in Algorithmic Number Theory. MIT Press, 1996.
- [3] E. Balandraud, B. Girard, S. Griffiths, and Y. Hamidoune. Subset sums in abelian groups. *European Journal of Combinatorics*, 34(8):1269 – 1286, 2013. Special Issue in memory of Yahya Ould Hamidoune.
- [4] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bull. Amer. Math. Soc. (N.S.)*, 21(1):1–46, 1989.
- [5] S. Bocker and Z. Liptak. A fast and simple algorithm for the money changing problem. *Algorithmica*, 48(4):413–432, 2007.

- [6] Y. Caro and R. Yuster. The characterization of zero-sum (mod 2) bipartite ramsey numbers. *Journal of Graph Theory*, 29(3):151–166, 1998.
- [7] M. Chaimovich. New algorithm for dense subset-sum problem. *Astrisque*, (258):363–373, 1999.
- [8] T. M. Chan and M. Lewenstein. Clustered integer 3sum via additive combinatorics. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, STOC ’15, pages 31–40, New York, NY, USA, 2015. ACM.
- [9] T. Cormen, C. Leiserson, R. Rivest, and C. Stein. *Introduction to Algorithms*. The MIT Press, 3rd edition, 2014.
- [10] M. Coster, A. Joux, B. LaMacchia, A. Odlyzko, C.-P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *computational complexity*, 2(2):111–128, 1992.
- [11] J. L. Dautrich, Jr. and C. V. Ravishankar. Compromising privacy in precise query protocols. In *Proceedings of the 16th International Conference on Extending Database Technology*, EDBT ’13, pages 155–166, New York, NY, USA, 2013. ACM.
- [12] J. Diaz, F. Grandoni, and A. Spaccamela. Balanced cut approximation in random geometric graphs. In T. Asano, editor, *Algorithms and Computation*, volume 4288 of *Lecture Notes in Computer Science*, pages 527–536. Springer Berlin Heidelberg, 2006.
- [13] D. Eppstein. Minimum range balanced cuts via dynamic subset sums. *Journal of Algorithms*, 23(2):375 – 385, 1997.
- [14] B. Faaland. Solution of the value-independent knapsack problem by partitioning. *Operations Research*, 21(1):pp. 332–337, 1973.
- [15] Z. Galil and O. Margalit. An almost linear-time algorithm for the dense subset-sum problem. *SIAM J. Comput.*, 20(6):1157–1189, Dec. 1991.
- [16] V. Guruswami, Y. Makarychev, P. Raghavendra, D. Steurer, and Y. Zhou. Finding almost-perfect graph bisections. In *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 7-9, 2011. Proceedings*, pages 321–337, 2011.
- [17] Y. Hamidoune, A. Llad, and O. Serra. On complete subsets of the cyclic group. *Journal of Combinatorial Theory, Series A*, 115(7):1279 – 1285, 2008.
- [18] D. S. Hochbaum and A. Pathria. The bottleneck graph partition problem. *Networks*, 28(4):221–225, 1996.
- [19] E. Huang and R. E. Korf. Optimal rectangle packing: An absolute placement approach. *J. Artif. Intell. Res. (JAIR)*, 46:47–87, 2013.
- [20] O. H. Ibarra and C. E. Kim. Fast approximation algorithms for the knapsack and sum of subset problems. *J. ACM*, 22(4):463–468, Oct. 1975.
- [21] H. Kellerer, U. Pferschy, and D. Pisinger. *Knapsack Problems*. Springer, 2004.
- [22] B. Klinz and G. J. Woeginger. A note on the bottleneck graph partition problem. *Networks*, 33(3):189–191, 1999.

- [23] D. Lokshtanov and J. Nederlof. Saving space by algebraization. In *Proceedings of the Forty-second ACM Symposium on Theory of Computing*, STOC '10, pages 321–330, New York, NY, USA, 2010. ACM.
- [24] V. Madisetti. *The Digital Signal Processing Handbook*. Electrical Engineering Handbook. Taylor & Francis, 1997.
- [25] T. Matsui and Y. Matsui. A survey of algorithms for calculating power indices of weighted majority games. *J. Oper. Res. Soc. Japan*, 43:71–86, 2000.
- [26] U. Pferschy. Dynamic programming revisited: Improving knapsack algorithms. *Computing*, 63(4):419–430, 1999.
- [27] D. Pisinger. Linear time algorithms for knapsack problems with bounded weights. *Journal of Algorithms*, 33(1):1 – 14, 1999.
- [28] M. Shamos. *Computational Geometry*. PhD thesis, Yale University, may 1978.
- [29] T. Uno. Efficient computation of power indices for weighted majority games. In K.-M. Chao, T.-s. Hsu, and D.-T. Lee, editors, *Algorithms and Computation*, volume 7676 of *Lecture Notes in Computer Science*, pages 679–689. Springer Berlin Heidelberg, 2012.
- [30] V. Vu. A structural approach to subset-sum problems. In M. Grtschel, G. Katona, and G. Sgi, editors, *Building Bridges*, volume 19 of *Bolyai Society Mathematical Studies*, pages 525–545. Springer Berlin Heidelberg, 2008.

## A Appendix: Omitted Proofs

### A.1 Proof of Lemma 1

If  $d \geq 2\ell$ , then for every element  $x \in \bar{S}$ , let  $q(x)$  and  $r(x)$  to be defined as the unique solution such that  $x = q(x)d + r(x)$  and  $0 \leq r(x) \leq d - 1$ . In fact, if  $x \in S$  then  $r(x) \leq \ell - 1$ .

If  $d < 2\ell$ , then we define  $q(x) = 0$ , and  $r(x) = x$ , then  $r(x) \leq 2kd + 4kl < 8kl$ .

The function we desire is the following

$$h(x) = 2\ell q(x) + r(x).$$

If  $a, b \in S$ , then  $a + b \in \bar{S}$ . Therefore  $a + b = (q(a) + q(b))d + r(a) + r(b) = q(a + b)d + r(a + b)$ . It is easy to verify  $h$  is injective, and  $h(x) \in [4k\ell]$  when  $d \geq 2\ell$ , and  $h(x) \in [8k\ell]$  otherwise.

### A.2 Proof of Theorem 2

The following lemma shows that the set of subsequence sums of an sequence with elements from an interval is small and has nice structure.

**Lemma 12.** *Let  $S$  be a sequence of length  $n$ , where each element is in  $a + [\ell - 1]$ . Then*

$$\Sigma_u(S) \setminus \{0\} \subset \bigcup_{i=1}^k ia + [k(\ell - 1)]$$

and

$$|\Sigma_u(S) \setminus \{0\}| \leq \min\{u, k^2\ell\},$$

where  $k = \min\{n, u/a\}$ .

*Proof.* Sum of any  $i$  elements is at most  $ia + i(\ell - 1)$ , and at least  $ia$ . Hence

$$\Sigma_u(S) \setminus \{0\} \subset \bigcup_{i=1}^k ia + [i(\ell - 1)] \subset \bigcup_{i=1}^k ia + [k(\ell - 1)].$$

Here  $k = \min\{n, u/a\}$ , since we can't sum more than  $n$  elements, and summing more than  $u/a$  elements pushes the value above  $u$ . The size of the set is clearly at most  $k^2\ell$ .  $\square$

If  $\ell k^2 \geq u$ , then we apply the standard Minkowski sum algorithm and get a  $\tilde{O}(u)$  time algorithm.

Otherwise, let  $S = \bigcup_{i=1}^k ia + [\ell k]$  and  $\bar{S} = \bigcup_{i=1}^{2k} ia + [2\ell k]$ . By Lemma 12,  $\Sigma_u(A) \setminus \{0\}, \Sigma_u(B) \setminus \{0\} \subset S$ . Apply Lemma 1 to find a  $S$ -perfect function  $h : \bar{S} \rightarrow [O(k^2\ell)]$ .

The algorithm compute  $h(\Sigma_u(A) \setminus \{0\}) + h(\Sigma_u(B) \setminus \{0\})$ . This is done in  $\tilde{O}(k^2\ell)$  time since both  $h(\Sigma_u(A) \setminus \{0\})$  and  $h(\Sigma_u(B) \setminus \{0\})$  lie in  $[O(k^2\ell)]$ . Finally, apply  $h^{-1}$  to the result and get a set  $C$ . Note that  $\Sigma_u(AB) = C \cup \Sigma_u(A) \cup \Sigma_u(B)$ , which can found in nearly linear time with respect to the size of the sets, which we know is  $O(k^2\ell)$ . The total running time is  $\tilde{O}(k^2\ell)$ .

### A.3 Property of $H_{S,\ell}$

**Theorem 13.** *Given  $b \in \mathbb{Z}_u^*$  and  $u > 3$ ,*

$$|\{x \mid 0 \leq i \leq \ell, ix \equiv b \pmod{u}\}| > \ell / (50 \log \log u).$$

*Proof.* For fixed  $i \in \mathbb{Z}_u$  and  $b \in \mathbb{Z}_u^*$ , there is a solution to  $ix \equiv b \pmod{u}$  if and only if  $\gcd(i, u) = 1$ . Moreover, the solution is unique. Hence, the total number of solutions are

$$\begin{aligned} \sum_{\substack{1 \leq i \leq \ell \\ \gcd(i, u) = 1}} 1 &= \sum_{d|u} \mu(d) \left\lfloor \frac{\ell}{d} \right\rfloor \geq \sum_{d|u} \mu(d) \left( \frac{\ell}{d} - 1 \right) = \ell \sum_{d|u} \mu(d) - \sum_{d|u} \mu(d) = \ell \frac{\phi(u)}{u} \\ &> \frac{\ell}{e^\gamma \log \log u + \frac{3}{\log \log u}} > \frac{\ell}{50 \log \log u}. \end{aligned}$$

Recall  $u > 3$ . Here  $\gamma$  is the *Euler-Mascheroni* constant,  $\phi(u)$  is the *Euler totient* function,  $\mu(u)$  is the *Möbius* function. The last few steps are standard equalities and bounds in number theory [2].  $\square$

**Corollary 2.** *Let  $S \subset \mathbb{Z}_u^*$  of size  $n$ . There exists an  $x \in \mathbb{Z}_u$  such that  $|x[l] \cap S| > \frac{n}{u} \frac{\ell}{50 \log \log u}$ .*

*Proof.* Consider  $H_{S,\ell}$ , every vertex in  $B$  has degree  $> \frac{\ell}{50 \log \log u}$ , since  $ix \equiv b \pmod{u}$  has at least  $\ell / 50 \log \log u$  solutions with different  $x$ 's (by Theorem 13). On average the degree of the vertices in  $A$  is at least  $\frac{n}{u} \frac{\ell}{50 \log \log u}$ , so there exist vertices that achieve the required bound.  $\square$

Construction of  $H_{S,\ell}$  is easy. First, spend  $O(u)$  time to preprocess for all modular inverses. For every  $b \in S$  and  $0 \leq i \leq \ell$  and  $\gcd(i, u) = 1$ , we compute  $x$  such that  $ix \equiv b \pmod{u}$  using the inverse. This computation takes  $O(1)$  time. Hence, the  $O(n\ell + u)$  running time.

#### A.4 Number of while loop

Let  $T(i)$  be the total number of elements in  $S$  at the  $i$ th iteration of the while loop, then we get the recurrence  $T(0) = n$  and

$$T(i) \geq T(i-1) + (d(n - T(i-1))) .$$

Solving the recurrence shows it is sufficient for  $k$  to satisfy

$$n - T(k) \leq n(1 - d)^k \leq ne^{-kd} \leq 1 .$$

Some algebra shows  $k = O(u \log n \log \log u / \ell) = \tilde{O}(u/\ell)$ . Hence we applied  $\tilde{O}(u/\ell)$  convolutions.

#### A.5 Analysis: Algorithm 4

Consider the function  $W(k, n, u)$  to give the worst case running time of `SSCyclic`, when we work in  $\mathbb{Z}_u$ , and the input set of elements cannot be divided by any prime factor of  $u$  except the first  $k$  smallest ones.  $W(0, n, u)$  is the running time when the input comes from  $\mathbb{Z}_u^*$ , let  $W(0, n, u) = uf(n, u)$ .

$$\begin{aligned} W(n, k, u) &\leq \max_{\sum_{i=0}^k n_i = n} \left\{ \sum_{j=0}^k W(j, n_j, u/p_j) \right\} \\ &\leq \sum_{j=0}^k W(j, n, u/p_j) , \end{aligned}$$

where  $p_0 = 1, p_1 < \dots < p_k$  are the  $k$  smallest prime factors of  $u$  and  $n_j$  is the number of elements divisible by  $p_j$  but not any  $p_i$ , where  $i > j$ . Consider the function  $T_k(u)$ , with  $T_0(u) = u$  and

$$T_k(u) = \sum_{j=0}^k T_j \left( \frac{u}{j+1} \right) .$$

A simple induction can show that that  $W(k, n, u) \leq T_k(u)f(n, u)$  for all  $n, u \geq 1$ . Indeed,  $W(0, n, u) = T_0(u)f(n, u)$ , and

$$\begin{aligned} \sum_{j=0}^k W(j, n, u/p_j) &\leq \sum_{j=0}^k W(j, n, u/(j+1)) \\ &\leq \sum_{j=0}^k T_j(u/(j+1))f(n, u) \\ &= T_k(u)f(n, u) . \end{aligned}$$

Hence we are interested in bounding  $T_k(u)$ . Again, another simple induction argument gives:

$$T_k(u) = (k+1)u .$$



The base case  $k = 0$  is trivial, as for the inductive step:

$$\begin{aligned}
T_k(u) &= \sum_{j=0}^k T_j \left( \frac{u}{j+1} \right) \\
&= \sum_{j=0}^{k-1} \sum_{i=0}^{\infty} T_j \left( \frac{u}{(j+1)(k+1)^i} \right) \\
&= \sum_{j=0}^{k-1} \sum_{i=0}^{\infty} (j+1) \frac{u}{(j+1)(k+1)^i} \\
&= u \sum_{j=0}^{k-1} \frac{k+1}{k} \\
&= (k+1)u.
\end{aligned}$$

Since  $k$  is at most  $\log u$ , the running time for the algorithm is therefore bounded by  $\tilde{O}(n^{2/3}u)$ .

## A.6 Proof of Theorem 3

Assume, for simplicity,  $n$  is a power of 2. We can see that `Combine` gets called  $\log n$  times. At the  $i$ th iteration, it computes  $n/2^i$  Minkowski sums. We will bound the running time of `Combine` when the input is from  $a + [\ell - 1]$ .

Assuming the input elements are  $\Sigma_u(\{s_1\}), \dots, \Sigma_u(\{s_n\})$ , and  $s_i \leq s_{i+1}$ . Applying Theorem 2, the total running time (up to polylog factors) can be bounded by

$$\begin{aligned}
\sum_{i=0}^{\log n} \sum_{j=1}^{n/2^i} \min \{ (s_{j2^i} - s_{(j-1)2^i} + 1)(2^i)^2, u \} &\leq \sum_{i=0}^{\log n} \min \{ \ell(2^i)^2 + 2^i n, n/2^i u \} \\
&\leq \sum_{i=0}^{\frac{1}{3} \log(\frac{nu}{\ell})} (\ell(2^i)^2 + 2^i n) + \sum_{i=\frac{1}{3} \log(\frac{nu}{\ell})+1}^{\log n} nu/2^i \\
&= O \left( \ell^{1/3} n^{2/3} u^{2/3} + \ell^{-1/3} n^{4/3} u^{1/3} \right).
\end{aligned}$$

If  $n \leq \ell\sqrt{u}$ , then  $\tilde{O}(\ell^{1/3}n^{2/3}u^{2/3})$ .

Assuming the input is the sequence  $s_1[l_1], \dots, s_n[l_n]$ , and  $s_i < s_{i+1}$ . Applying Theorem 2, the total running time (up to polylog factors) can be bounded by

$$\begin{aligned}
\sum_{i=0}^{\log n} \sum_{j=1}^{n/2^i} (s_{j2^i} - s_{(j-1)2^i} + 1)(u/(s_{(j-1)2^i}))^2 &\leq \sum_{i=0}^{\log n} \sum_{j=1}^{n/2^i} (s_{j2^i} - s_{(j-1)2^i} + 1)(u/a)^2 \\
&\leq (u/a)^2 \sum_{i=0}^{\log n} \sum_{j=1}^{n/2^i} (s_{j2^i} - s_{(j-1)2^i} + 1) \\
&\leq (u/a)^2 \sum_{i=0}^{\log n} \ell + n/2^i \\
&\leq O(u^2 \ell \log n / a^2 + u^2 n / a^2).
\end{aligned}$$

All the  $s_i$  are unique, therefore  $n \leq \ell$ . We get the bound  $\tilde{O}\left(\frac{u^2 \ell}{a^2}\right)$ . □