

Algorithms for Solving Some Inverse Problems from Combinatorial Number Theory

Elias Abboud

Faculty of education, Beit Berl College, Doar Beit Berl 44905, Israel
eabboud@beitberl.ac.il

December 10, 2016

Abstract

In this paper we use the characteristic property of sumsets which states that there exists a proper subset tiling the set by translates to solve by an algorithmic methods, for finite sets, some inverse problems in combinatorial number theory.

Keywords: translation, sumset, decomposable set, tiling a set, maximal covering

Mathematics subject Classification: 11B13, 11B75

1 Introduction

Ruzsa in his booklet "Sumsets and structure" [6] gave a brief description of the topic of additive systems and its combinatorial theory; "In classical additive number theory we start with a given set, say of primes, and try to understand how an integer can be expressed as a sum of elements of this set. In combinatorial (or inverse) theory we do the opposite: given an additive assumption about a set, say that it has few or many sums, we try to understand its structure".

Given a finite set of integers C , do there exist sets A and B with $|A| \geq 2$ and $|B| \geq 2$ such that $A + B = C$? Beginning with an example, let $A = \{1, 2\}$ and $B = \{3, 4, 5\}$ then taking all the paired sums of an element of A and an element of B gives $A + B = \{1, 2\} + \{3, 4, 5\} = \{4, 5, 6, 7\}$. This was quite easy since we had A and B and then computed C . What if we have C and we want to find sets A and B such that $A + B = C$? Letting $C = \{6, 7, 8, 9\}$ then, by trial and error one can find $C = \{6, 7, 8, 9\} = \{3, 5\} + \{3, 4\}$. But, is there a *systematic method* to find A and B whenever they exist!

To clarify the point, if $C = \{6, 7, 8, 9\}$ then we may write $A = \{x, y\}$ and

$B = \{z, w\}$ and solve the system of equations

$$\begin{cases} x + z = 6 \\ x + w = 7 \\ y + z = 8 \\ y + w = 9 \end{cases}.$$

In this case there are an infinite number of integral solutions, namely:

$$(x, y, z, w) = (6, 8, 0, 1) + z(-1, -1, 1, 1).$$

Table 1 shows some few solutions:

z	A	B
1	$\{5, 7\}$	$\{1, 2\}$
2	$\{4, 6\}$	$\{2, 3\}$
3	$\{3, 5\}$	$\{3, 4\}$
4	$\{2, 4\}$	$\{4, 5\}$
5	$\{1, 3\}$	$\{5, 6\}$
6	$\{0, 2\}$	$\{6, 7\}$

Table 1: Some solutions

Another way of looking at the case $z = 6$, notice that $C = A + B = (0 + B) \cup (2 + B)$ where $B \subset C$. This means that there exists a subset which "tiles" C by translates.

Nathanson [4], posed a list of 7 inverse problems from combinatorial number theory. These problems are open and hard to solve in general. On the other hand, for **finite sets** we can give an affirmative answer in a systematic method to some of these problems, namely:

Problem 1 *Do there exist sets A and B with $|A| \geq 2$ and $|B| \geq 2$ such that $A + B = C$?*

Problem 2 *Do there exist sets A and B with $|A| \geq 2$ and $|B| \geq 2$ such that $A + B \subseteq C$ and $C \setminus (A + B)$ is "small"?*

Problem 3 *Does there exist a set A with $|A| \geq 2$ and $A + A = C$?*

Problem 4 *Does there exist a set A with $|A| \geq 2$ such that $A + A \subseteq C$ and $C \setminus (A + A)$ is "small"?*

These problems are related to Freiman's theorem [2] and other inverse problems in additive number theory ([5],[7]), and will be the core of our discussion.

2 Definitions and notations

Let $\mathbb{Z}$ be the set of integers. For integers a and b with $a < b$, define the *intervals of integers* $[a, b] = \{n \in \mathbb{Z} | a \leq n \leq b\}$ and $[a, b) = \{n \in \mathbb{Z} | a \leq n < b\}$. For $A \subseteq \mathbb{Z}$ and $g \in \mathbb{Z}$ the *translation* of the set A by g is the set $g + A = \{g + a | a \in A\}$. Let A and B be two sets of integers then their *sumset* is the set $C = A + B = \{a + b | a \in A \text{ and } b \in B\}$. In this case, A and B are called *factors* of C .

If every element of C has a unique representation in the form $a + b$ where $a \in A$ and $b \in B$ then $\{A, B\}$ is called a *unique representation system* for C and we denote $C = A \oplus B$.

A set C of integers is called *decomposable* if there exist sets A and B such that $|A| \geq 2, |B| \geq 2$ and $C = A \oplus B$.

A set $K, |K| \geq 2$, *tiles* C by translates if $C = \bigcup_{\alpha \in I} (\alpha + K)$ for some set of integers $I, |I| \geq 2$. If $\bigcup_{\alpha \in I} (\alpha + K) \subseteq C$ for some set of integers I , where $|K| \geq 2, |I| \geq 2$, and $C \setminus \bigcup_{\alpha \in I} (\alpha + K)$ is minimal, we say that $\bigcup_{\alpha \in I} (\alpha + K)$ is a *maximal K -covering* of C . Set C is a *double addition* of set A provided $C = A + A$.

The term "tiling the integers" was used by Tijdeman [8] and Coven and Meyerowitz [1] in a different manner: "set A tiles the integers if and only if the set of integers can be written as a disjoint union of translates of A ". We use the term "tiling" in a more general context, namely: a set $K, |K| \geq 2$, *tiles* C by translates if $C = \bigcup_{\alpha \in I} (\alpha + K)$ for some set of integers $I, |I| \geq 2$. Hence, our definition refers to any subset C of the integers and the set of translates $\{\alpha + K\}_{\alpha \in I}$ need not be disjoint.

3 Sumsets and decomposable sets

The following lemma characterizes sumsets and decomposable sets by showing that there exists a proper subset tiling the set by translates.

Lemma 1 *Let $C \subseteq \mathbb{Z}$. Then $C = A + B$, where A and B are sets of integers, $|A| \geq 2, |B| \geq 2$, if and only if there exists a set of integers $K \subset C, |K| \geq 2$ and a set of integers $I, \{0\} \subset I \subseteq \mathbb{Z}, |I| \geq 2$, such that;*

$$C = \bigcup_{\alpha \in I} (\alpha + K)$$

Moreover, C is decomposable with factors $A = I$ and $B = K$ if and only if the sets $\{\alpha + K\}_{\alpha \in I}$ are pairwise disjoint.

Proof. We have to consider two directions.

($\Leftarrow$) Clearly, if $C = \bigcup_{\alpha \in I} (\alpha + K), \{0\} \subset I \subset C, |I| \geq 2$, then we may take $A = I$ and $B = K$ so that $C = A + B$.

($\Rightarrow$) Suppose there are sets A and B , $|A| \geq 2, |B| \geq 2$ such that $C = A + B$. We use the following properties which are direct conclusions from the definition of sumsets. If

$$C = A + B$$

then for any integer α , we have:

- $\alpha + C = (\alpha + A) + B = A + (\alpha + B)$.
- $C = (-\alpha + A) + (\alpha + B)$.
- $B \subseteq (-\alpha + C) \Leftrightarrow (\alpha + B) \subseteq C$.

We proceed by considering two cases;

I. $0 \in A \cup B$. In this case, $0 \in A$ or $0 \in B$. If $0 \in A$ then take $I = A$ and $K = B$. If $0 \in B$ then take the opposite option $I = B$ and $K = A$. Hence, the result follows.

II. $0 \notin A \cup B$. If we take any element $a \in A$ then $0 \in (-a + A)$ and

$$-a + C = (-a + A) + B.$$

Therefore, $B \subseteq (-a + C)$ which implies $(a + B) \subseteq C$. On the other hand,

$$C = (-a + A) + (a + B).$$

Hence, we may take $I = (-a + A)$ and $K = (a + B)$. Obviously, $K = (a + B) \subseteq C$ and we have

$$C = \bigcup_{\alpha \in I} (\alpha + K),$$

where $0 \in I = (-a + A)$, $|I| = |(-a + A)| = |A| \geq 2$, and $|K| = |(a + B)| = |B| \geq 2$.

Finally, if the sets $\{\alpha + K\}_{\alpha \in I}$ are pairwise disjoint then $C = A \oplus B$, because then each element of C belongs only to one set $\alpha + K, \alpha \in I$, and therefore can be represented uniquely as a sum of an element of A and an element of B . ■

Example 1 Let $C = \{1, 2, 4, 5, 7, 8\}$. If we take $K = \{1, 4\}$ then $1 + K = \{2, 5\}$, $3 + K = \{4, 7\}$ and $4 + K = \{5, 8\}$. Hence, $A = \{0, 1, 3, 4\}$, $B = K = \{1, 4\}$ and $C = A + K$.

On the other hand if we take $K' = \{1, 2\}$ then $3 + K' = \{4, 5\}$ and $6 + K' = \{7, 8\}$. Therefore, C is decomposable with factors $A' = \{0, 3, 6\}$, $K' = \{1, 2\}$ and we have $C = A' \oplus K'$.

4 Covering finite sets

Let C be a finite set. Denote by m_C and M_C to be the minimal and the maximal elements of C , respectively.

4.1 Maximal K -covering

Concerning Problems 1- 2, take a proper subset $K \subset C, |K| \geq 2$ and search first for a maximal K -covering of elements of C . Thus we need the following result.

Theorem 1 *Given a finite set C and a proper subset $K \subset C, |K| \geq 2$, then a maximal K -covering of C can be found as follows: Let $c_1 < c_2 < \dots < c_n$ be the elements of C .*

I. For $\alpha \in [m_C - M_K, M_C - m_K]$ let $\{\alpha + K\}_{\alpha \in I_K}$ be all the translations of K such that each covers a $|K|$ number of elements of C :

$$|(\alpha + K) \cap C| = |K|, \alpha \in I_K.$$

II. If $|I_K| = 1$ then there is no maximal K -covering of C . If $|I_K| \geq 2$ then a maximal K -covering of C is obtained:

$$\bigcup_{\alpha \in I_K} (\alpha + K).$$

Proof. For each $\alpha \in [m_C - M_K, M_C - m_K]$ the translation $\alpha + K$ covers at least one element of the set $[m_C, M_C]$. Since $|(\alpha + K)| = |K|$ and $|(\alpha + K) \cap C| = |K|$ then for each $\alpha \in I_K$ we have $\alpha + K \subseteq C$. Hence,

$$\bigcup_{\alpha \in I_K} (\alpha + K) \subseteq C.$$

Since, $\{\alpha + K\}_{\alpha \in I_K}$ are all the translations of K , each of which covers exactly a $|K|$ number of elements of C , it follows that $\bigcup_{\alpha \in I_K} (\alpha + K)$ is indeed a maximal K -covering of C . If $|I_K| = 1$ then there is no maximal K -covering of C , since by definition the subset K must cover a $|K|$ number of elements of C at least twice. ■

Example 2 *Let $C = \{2, 3, 4, 5, 7, 8, 9, 11\}$, $K = \{2, 3, 4\}$. Then $m_C = 2, M_C = 11, m_K = 2$ and $M_K = 4$. Therefore, $m_C - M_K = -2, M_C - m_K = 9$ and $-2 \leq \alpha \leq 9$. Table 2 shows all the possible translations, each of which covers at least one element of the set $[m_C, M_C] = [2, 11]$.*

α	$\alpha + K$	$ (\alpha + K) \cap C = K $
-2	$\{0, 1, 2\}$	
-1	$\{1, 2, 3\}$	
0	$\{2, 3, 4\}$	$\leftarrow$
1	$\{3, 4, 5\}$	$\leftarrow$
2	$\{4, 5, 6\}$	
3	$\{5, 6, 7\}$	
4	$\{6, 7, 8\}$	
5	$\{7, 8, 9\}$	$\leftarrow$
6	$\{8, 9, 10\}$	
7	$\{9, 10, 11\}$	
8	$\{10, 11, 12\}$	
9	$\{11, 12, 13\}$	

Table 2: The possible translations

Thus we have $I_K = \{0, 1, 5\}$, and a maximal K -covering of C is obtained:

$$K \cup (1 + K) \cup (5 + K) \subseteq C.$$

4.2 Algorithm for solving problems 1-2

The next theorem solves Problems 1-2 for finite sets.

Theorem 2 *Given a finite set C , the following algorithm describes how to find sets A and B with $|A| \geq 2$ and $|B| \geq 2$ such that $A + B \subseteq C$ and $C \setminus (A + B)$ is minimal.*

- I. Start with any proper subset $K \subset C, |K| \geq 2$.
- II. Search for a maximal K -covering of elements of $C : T_K = \bigcup_{\alpha \in I_K} (\alpha + K)$.
- III. Do I. and II. for all proper subsets $K \subset C, |K| \geq 2$.
- IV. If $|I_K| = 1$ for all subsets $K \subset C, |K| \geq 2$, then the algorithm ends and there is no solution to problem 2. Otherwise,
- V. Let T_{K_0} be a maximal K -covering for which

$$\min_{K \subset C, |K| \geq 2} |C \setminus T_K| = |C \setminus T_{K_0}|,$$

and define $A = \{\alpha | \alpha \in I_{K_0}\}$ and $B = K_0$.

VII. If

$$\min_{K \subset C, |K| \geq 2} |C \setminus T_K| = |C \setminus T_{K_0}| = 0,$$

then C is the sumset of A and K_0 . Moreover, if the sets $\{\alpha + K_0\}_{\alpha \in I_{K_0}}$ are pairwise disjoint then C is decomposable with factors A and K_0 .

Proof. Since T_K is a maximal K -covering of C we have $T_K \subset C$. Hence,

$$\min_{K \subset C, |K| \geq 2} |C \setminus T_K|$$

is defined. Let T_{K_0} be a maximal covering for which this minimum is achieved. Since $T_{K_0} = \bigcup_{\alpha \in I_{K_0}} (\alpha + K)$ then clearly $T_{K_0} = A + B$, where $A = \{\alpha | \alpha \in I_{K_0}\}$ and $B = K_0$.

On the other hand, if A and B are sets with $|A| \geq 2$ and $|B| \geq 2$ such that $A + B \subseteq C$ then choose $A + B$ to have a maximal number of elements of C (and therefore $C \setminus (A + B)$ is minimal). By Lemma 1, there exists a proper subset $K \subseteq A + B \subseteq C$ such that $A + B = T_K = \bigcup_{\alpha \in I_K} (\alpha + K)$ is a maximal K -covering of C . Thus the algorithm covers all the possibilities and results in a solution to problem 2.

Now, if

$$\min_{K \subset C, |K| \geq 2} |C \setminus T_K| = |C \setminus T_{K_0}| = 0,$$

then T_{K_0} provides a solution to problem 1, and if the sets $\{\alpha + K_0\}_{\alpha \in I_{K_0}}$ are pairwise disjoint then C is decomposable with factors A and K_0 . ■

5 Double additions

Concerning Problems 3 and 4 we shall see that it is sufficient to consider all maximal K -coverings T_K of the set C , where $K \subset C, |K| \geq 2$, and check if one of them is a double addition of some set A : $T_K = A + A, |A| \geq 2$.

Therefore, we need the following algorithm which finds out whether a finite set T is a double addition of a set A or not and thus solving Problem 3.

Theorem 3 *Given a finite set of integers T , let E be the subset of T which contains all the even numbers $e, e \in T$.*

The following algorithm describes how to find a double addition which equals T , i.e., $T = A + A, |A| \geq 2$.

I. If $E = \phi$ (empty set), then the algorithm ends and T is not a double addition of any set.

II. If $E \neq \phi$, then for each subset $L \subseteq E, 2 \leq |L| \leq \frac{1}{2}|T| + \frac{1}{2}$ check whether $T = \frac{1}{2}L + \frac{1}{2}L$, where $\frac{1}{2}L = \{\frac{l}{2} \mid l \in L\}$. If the answer is positive then take $A = \frac{1}{2}L$.

III. If there is no subset L for which $L \subseteq E, 2 \leq |L| \leq \frac{1}{2}|T| + \frac{1}{2}$ and $T = \frac{1}{2}L + \frac{1}{2}L$, then the algorithm ends and T is not a double addition of any set.

Proof. If $T = A + A$, where $A = \{a_1, a_2, \dots, a_n\}, n \geq 2$, then for each $i, 1 \leq i \leq n$, we have $2a_i \in T$. Hence, T must contain even numbers. Moreover, $A = \frac{1}{2}L$, where $L = \{2a_1, 2a_2, \dots, 2a_n\} \subseteq E$. Now, $|A| = |L| \leq \frac{1}{2}|T| + \frac{1}{2}$ since, otherwise, if $|A| > \frac{1}{2}|T| + \frac{1}{2}$ then;

$$|T| = |A + A| > |A| + |A| - 1 > \frac{1}{2}|T| + \frac{1}{2} + \frac{1}{2}|T| + \frac{1}{2} - 1 = |T|,$$

which is a contradiction. ■

We used the elementary fact from additive theory that (see [3]):

$$|A + B| \geq |A| + |B| - 1.$$

Example 3 Let $T = \{2, 4, 5, 6, 7, 8, 9, 10, 12\}$. Then $E = \{2, 4, 6, 8, 10, 12\}$. We have to consider subsets $L \subseteq E$, where $2 \leq |L| \leq 5$. Since,

$$|A + A| \leq \frac{1}{2} |A| (|A| + 1),$$

the only relevant cases are $|L| = 4$ or 5 . Now, L must contain the numbers 2 and 12, hence the following table shows all the possible cases:

$ L $	L	$A = \frac{1}{2}L$	$A + A$
4	$\{2, 4, 6, 12\}$	$\{1, 2, 3, 6\}$	T
4	$\{2, 4, 8, 12\}$	$\{1, 2, 4, 6\}$	
4	$\{2, 4, 10, 12\}$	$\{1, 2, 5, 6\}$	
4	$\{2, 6, 8, 12\}$	$\{1, 3, 4, 6\}$	
4	$\{2, 6, 10, 12\}$	$\{1, 3, 5, 6\}$	
4	$\{2, 8, 10, 12\}$	$\{1, 4, 5, 6\}$	
5	$\{2, 4, 6, 8, 12\}$	$\{1, 2, 3, 4, 6\}$	
5	$\{2, 4, 6, 10, 12\}$	$\{1, 2, 3, 5, 6\}$	
5	$\{2, 6, 8, 10, 12\}$	$\{1, 3, 4, 5, 6\}$	

Table 3: The possible cases

Therefore, $T = A + A$ is a double addition of $A = \{1, 3, 4, 6\}$.

Now, we are ready to answer Problem 4.

Theorem 4 Given a finite set of integers C , the following algorithm describes how to check whether there is a set $A, |A| \geq 2$ such that $A + A \subseteq C$ and $C \setminus (A + A)$ is minimal;

- I. consider all maximal K -coverings T_K of the set C , where $K \subset C, |K| \geq 2$.
- II. For each T_K check whether it is equal to a double addition of some set $A : T_K = A + A, |A| \geq 2$.
- III. If there is no maximal K -covering T_K of C , which is a double addition of some set $A, |A| \geq 2$, then the algorithm ends and there is no solution to the problem.
- IV. From among all the possible sets A for which $T_K = A + A \subseteq C, |A| \geq 2$ choose one for which $C \setminus (A + A)$ is minimal.

Proof. If $A + A \subseteq C, |A| \geq 2$, then by Lemma 1 there exist sets K and I such that $A + A = \bigcup_{\alpha \in I} (\alpha + K) \subseteq C$ and $K \subseteq A + A \subseteq C$. Therefore, it is sufficient to consider all maximal K -coverings T_K of the set C , where $K \subset C, |K| \geq 2$. For that we use Algorithm 1, then we check by Algorithm 3 whether one of them is equal to a double addition of some set $A : T_K = A + A, |A| \geq 2$. Since C is finite we ought to consider only a finite number of possibilities. Therefore, from among all the possible sets A for which $T_K = A + A \subseteq C, |A| \geq 2$ we may choose one for which $C \setminus (A + A)$ is minimal. ■

6 Concluding remarks

The characterization of sumsets and decomposable sets allowed us to search for a maximal K -covering by which a complete and affirmative answers were given, in the case of finite sets, to Problems 1-2. Concerning Problems 3 and 4 we considered all maximal K -coverings T_K of a set C , where $K \subset C$, $|K| \geq 2$, and checked whether or not one of them is a double addition of some set A : $T_K = A + A$, $|A| \geq 2$. Then, from among all the possible sets A for which $T_K = A + A \subseteq C$, $|A| \geq 2$ we chose one for which $C \setminus (A + A)$ is minimal. Thus, the notion of maximal K -covering plays an important rule in solving the proposed problems as we have seen in Theorems 2 and 4.

Finally, other problems, which were posed by Nathanson, can be addressed by similar methods. For more details we refer the reader to [4].

Acknowledgement This research was supported by Beit Berl College.

References

- [1] Coven E., Meyerowitz A., Tiling the integers with translates of one finite set, *Journal of Algebra* **212** (1999) 161-174.
- [2] Freiman G. A., *Foundation of a Structural Theory of Set Addition*, Translations of Mathematical Monographs, Vol. 37, American Mathematical Society, Providence, RI, 1973.
- [3] Geroldinger, A. ; Ruzsa, I.Z., *Combinatorial number theory and additive group theory*. Advanced Courses in Mathematics CRM, Barcelona, 2009.
- [4] Nathanson M. B., Additive systems and a theorem of de Bruijn. *The American Mathematical Monthly* **121** (2014) 5-17.
- [5] Nathanson, M. B., *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, New York, 1996.
- [6] Ruzsa, I. Z., *Sumsets and structure (Combinatorial number theory and additive group theory)*, Advanced courses in mathematics, Birkhäuser, CRM Barcelona, 2009, 87-210.
- [7] Tao T., Vu V., *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2006.
- [8] Tijdeman R., Decomposition of the integers as a direct sum of two subsets, in *Number Theory (Paris, 1992 -1993)*, Cambridge Univ. Press, Cambridge, 1995, 261-276.