Generalized Difference Sets on an Infinite Cyclic Semigroup

Otokar Grošek
Department of Mathematics
Slovak Technical University
Bratislava, 812 19, Ilkovičova 3
Czechoslovakia
grosek@elf.stuba.cs

Robert Jajcay
Department of Mathematics
University of Nebraska
Lincoln, NE 68588-0323
jajcay@helios.unl.edu

Abstract

Generalized difference sets are difference sets with prescribed (and possibly different) multiplicities for every element. In this paper, constructions will be given for generalized difference sets on the semigroup of positive integers for almost every possible multiplicity function (sequence of multiplicities).

Difference sets appear in various areas of mathematics. The purpose of this paper is to study a generalization of this notion to an infinite cyclic semigroup. Every such semigroup is isomorphic to the additive semigroup of all positive integers. Generalized difference sets on this semigroup are also related to the notion of an A-ideal introduced in [1]. All the following results can be proved for the infinite cyclic group as well, which is done at the end of our paper.

Definition 1 *Let S be an abelian semigroup and G be a nonempty subset of S such that for every $s \in S$ there exists an element $g \in G$ such that $sg \in G$. Then G is called an* A-ideal *of the semigroup S.*

JCMCC 13 (1993), pp. 167-174

Definition 2 ([2]) *Let A be an abelian group of order v. A set D of k different elements from A is called a (v, k, λ)-group difference set if the following condition hold: For every $d \in A$, different from the unit element, there are exactly λ ordered pairs (a_i, a_j), $a_i, a_j \in D$, such that $a_i a_j^{-1} = d$.*

The following examples clarify the difference between these two notions.

Example 1. Let $S = \mathcal{Z}_7$, the additive group modulo 7. Then the set $G_1 = \{1, 2, 4\}$ forms an A-ideal. It is at the same time a (7,3,1)-difference set.

It is easy to show that every difference set on a semigroup is also an A-ideal of this semigroup. The converse, as we shall see in the next example, is not true.

Example 2. Take the group S and the set G_1 from the preceding example. Let $G_2 = G_1 \cup \{3\} = \{1, 2, 3, 4\}$. Although G_2 is not a difference set, it is an A-ideal of S. Unlike the set G_1, where we had for a given $s \in \mathcal{Z}_7$, $s \neq 0$, precisely one solution for every equation $s + g_1 = g_2$, in terms of elements g_1, g_2 from G_1, the same task for G_2 leads to the following result:

$1 + g_1 = g_2$ has 3 solutions (g_1, g_2): (1,2),(2,3),(3,4)

$2 + g_1 = g_2$ has 2 solutions (g_1, g_2): (1,3),(2,4)

etc. for 3, 4, 5 and 6, which leads to a multiset of differences of elements of G_2: $(1^3, 2^2, 3^1, 4^1, 5^2, 6^3)$.

We will call G_1 the generalized difference set of type (1,1,1,1,1,1), while G_2 is of type (3,2,1,1,2,3). In contrast, note the fact that while the group $\mathcal{Z}_6$ contains no difference sets (except of the trivial one), it does contain A-ideals.

Let us now proceed to the notion of a generalized difference set on the additive semigroup $S = \{1, 2, 3, \ldots\}$ of positive integers.

Definition 3 *Let S be the additive semigroup of positive integers and let $\{\lambda_1, \lambda_2, \lambda_3, \ldots\}$ be an infinite sequence of positive integers. We say that a subset G is a* generalized difference set of type $\{\lambda_1, \lambda_2, \lambda_3, \ldots\}$ *on the semigroup S if for every element $i \in S$ we have precisely λ_i solutions of the equation $i + g_1 = g_2$, with $g_1, g_2 \in G$ (i. e. every positive integer i can be expressed exactly λ_i times as a difference $g_2 - g_1$ of elements of G).*

We begin by focusing on a special case, the sequence $\{1, 1, 1, \ldots\}$, which plays an important role in helping to understand the general problem.

Given a subset M of the set S of positive integers, let $D(M)$ denote the multiset of all possible differences of elements from M, i. e. $D(M) = \{m_i - m_j | m_i, m_j \in M, m_i > m_j\}$.

Now we can introduce the following recursive definition of an infinite sequence of subsets of S:

(i) Let m_0 be an arbitrary element of S and let $N_1 = \{m_0, m_0 + 1\}$.

(ii) Having the set N_i we define the set N_{i+1} as follows:

$$N_{i+1} = N_i \cup \{2(k+1), 2(k+1) + j\}$$

where j is the smallest element of the set $S \setminus D(N_i)$, and k is the maximal element of N_i.

Before stating the theorem proper, let us mention the fact that the sequence $\{N_i\}_{i=1}^{\infty}$ is well defined. For, given any $i > 1$, the set N_i is a union of two finite sets, and is hence finite. Any N_i, therefore, contains a maximal element k. This also forces $D(N_i)$ to be finite and thereby $S \setminus D(N_i)$ is both nonempty and contains a smallest element.

Theorem 1 *The set $G = \bigcup\{N_i | i \in S\}$ is a generalized difference set of type $\{1, 1, 1, \ldots\}$ on the semigroup S.*

Proof. To prove the theorem we have to show that $D(G)$ contains every positive integer exactly once.

Let us start by showing that $D(G)$ contains every element of S. Suppose the opposite, i. e. suppose that $D(G)$ is a proper subset of S. Then there exists an element n_0 which is the smallest element of $S \setminus D(G)$. It follows that n_0 does not belong to N_i for any $i \in S$. On the other hand, the finite set $\{m | m < n_0\}$ belongs to $D(G)$ and, since $\{D(N_i)\}_{i=1}^{\infty}$ is an increasing sequence, there exists a smallest index l such that $\{m | m < n_0\} \subset D(N_l)$. Then clearly $N_{l+1} = N_l \cup \{2(k+1), 2(k+1) + n_0\}$, where k is the maximal element of N_l. Since $n_0 = 2(k+1) + n_0 - 2(k+1) \in D(N_{l+1})$, we have a contradiction with the way n_0 was chosen. Hence $D(G)$ contains every element of S at least once.

To prove that $D(G)$ contains no positive integers more than once, notice that if any n appears in $D(G)$ more than once then, for i sufficiently large, $D(N_i)$'s contain n more than once. Therefore it suffices to prove that none of the multisets $D(N_i)$ contains any n more than once. Again,

Since all the possible cases for a repeated appearance of any positive integer force a contradiction, we can conclude that $D(G)$ contains every positive integer exactly once. This proves the assertion. □

Example 3. Here are the first few elements of G, when starting with $m_0 = 1$:

$$1, 2, 6, 8, 18, 21, 44, 52, 106, 115, 232, 243, \ldots$$

Having solved the special case for the sequence $\{1, 1, 1, \ldots\}$, we can proceed to the general case for an arbitrary multiplicity sequence $\{\lambda_i\}_{i=1}^{\infty}$. The following construction works for every sequence $\{\lambda_i\}_{i=1}^{\infty}$ of positive integers greater than one (i. e. $\lambda_i \geq 2$ for all $i \in S$).

Let $\{\lambda_i\}_{i=1}^{\infty}$ be a sequence with the required property. Define a sequence of subsets of S as follows:

(i) $M_1 = \{m_0, m_0 + 1\}$, where m_0 is an arbitrary element of S .

(ii) Having the set M_i we define the set M_{i+1} by setting

$$M_{i+1} = M_i \cup \{2(k+1), 2(k+1) + j\}$$

where k is the maximal element of M_i and j is the smallest positive integer which appears in $D(M_i)$ fewer than λ_j -times.

The sequence $\{M_i\}_{i=1}^{\infty}$ is well defined , and we can state:

Theorem 2 *Let $\{\lambda_i\}_{i=1}^{\infty}$ be a sequence of positive integers such that $\lambda_i \geq 2$ for all $i \in S$. Then $G = \bigcup\{M_i | i \in S\}$, the union of all sets M_i constructed by our recursive definition, is the generalized difference set of type $\{\lambda_i\}_{i=1}^{\infty}$ on the additive semigroup of positive integers.*

Proof. The proof of the fact that the multiplicity of every positive integer n in $D(G)$ is at least λ_n proceeds exactly in the same way as the proof of the appearance of every positive integer in the preceding proof. It remains only to prove that no positive integer n appears in $D(G)$ more than λ_n -times.

Suppose the contrary: let n_0, M_{i_0} be the smallest positive integer appearing in $D(G)$ more than λ_{n_0} -times together with the first set M_{i_0} satisfying the condition that $D(M_{i_0})$ contains n_0 more than λ_{n_0} -times. This time we have four possibilities to consider. Each of them gives rise to a contradiction:

suppose the opposite. Let n_0 be a positive integer appearing at least twice in $D(G)$, and let i_0 be the smallest number for which $D(N_{i_0})$ contains n_0 at least twice. Then the preceding multiset $D(N_{i_0-1})$ contains n_0 at most once. We have to deal with three possible cases for n_0:

- *n_0 is the smallest element of $S \setminus D(N_{i_0-1})$ (i. e. it is the smallest element, and must be included)*

  Then by the recursive definition of N_{i_0}, we get $N_{i_0} = N_{i_0-1} \cup \{2(k+1), 2(k+1)+n_0\}$, where k is the maximal element of N_{i_0-1}. Since n_0 does not belong to $D(N_{i_0-1})$, the only possible appearance of n_0 in $D(N_{i_0})$ (except as the difference $n_0 = 2(k+1)+n_0-2(k+1)$) must be of the form $n_0 = 2(k+1) - m$ or $n_0 = 2(k+1) + n_0 - m$, for some $m \in N_{i_0-1}$. By the definition of $D(N_{i_0-1})$ it is obvious that $l < k$ for every $l \in D(N_{i_0-1})$, and since n_0 is the smallest number not contained in $D(N_{i_0-1})$ we must have $n_0 \leq k$. On the other hand, both of these two possible expressions for repeated appearances of n_0 are strictly greater than k ; therefore, n_0 cannot appear in $D(N_{i_0})$ more than once. This is a contradiction to the assumption of a multiple appearance of n_0 in $D(N_{i_0})$.

- *n_0 does not belong to $D(N_{i_0-1})$, but it is not the smallest number with this condition (i. e. it will not be added to N_{i_0-1}).*

  For the same reasons as in the preceding case, the only possibilities for an appearance of n_0 in $D(N_{i_0})$ are the differences $2(k+1)+j-m_1$ or $2(k+1) - m_2$, for some $m_1, m_2 \in N_{i_0-1}$. If n_0 appears in $D(N_{i_0})$ at least twice, then $2(k+1) + j - m_1 = 2(k+1) - m_2 = n_0$, where obviously $m_1 > m_2$. Since j does not belong to $D(N_{i_0-1})$, we get that $j \neq m_1 - m_2$. Hence, after subtracting our two expressions for n_0, we get the contradiction:

$$0 = 2(k+1) + j - m_1 - 2(k+1) + m_2 = j - (m_1 - m_2).$$

- $n_0 \in D(N_{i_0-1})$

  Once again, the only possible repeated appearance of n_0 in N_{i_0} can be of the form $2(k+1) + j - m_1$ or $2(k+1) - m_2$, for some $m_1, m_2 \in N_{i_0-1}$. Again, in exactly the same manner as the first case, we can show that n_0 must simultaneously be strictly greater than k and smaller than k, which gives a contradiction.

- *n_0 is the smallest positive integer not contained in $D(M_{i_0-1})$ exactly λ_{n_0} -times (i. e. it will be included)*

  By the definition of our sets, $M_{i_0} = M_{i_0-1} \cup \{2(k+1), 2(k+1) + n_0\}$. Using the same arguments as in the first case of the preceding proof we can show that $D(M_{i_0})$ contains n_0 exactly once more than $D(M_{i_0-1})$. As $D(M_{i_0-1})$ contains n_0 fewer than λ_{n_0} -times, $D(M_{i_0})$ contains n_0 at most λ_{n_0} -times, which is a contradiction.

- *n_0 appears in $D(M_{i_0-1})$, but it does so fewer than λ_{n_0} -times and n_0 is not the smallest element with this property (i. e. we will not include it in the next step)*

  Repeating the procedure from the second case of the preceding proof, we can show that the multiplicity of n_0 in $D(M_{i_0})$ increases by at most one, and hence is not greater than λ_{n_0}, which is a contradiction.

- *n_0 does not appear in $D(M_{i_0-1})$, but it is greater than the smallest number not expressed sufficiently many times in $D(M_{i_0-1})$*

  This is the only truly different case. The set M_{i_0} is by definition equal to $M_{i_0-1} \cup \{2(k+1), 2(k+1) + j\}$. As n_0 does not belong to $D(M_{i_0-1})$, the only possible differences which can create n_0 are of the form $2(k+1) - m_1$ or $2(k+1) + j - m_2$, for some $m_1, m_2 \in M_{i_0-1}$. This time we cannot exclude either of these two possibilities, but as the multiplicity of n_0 in $D(M_{i_0-1})$ was zero, the multiplicity of n_0 in the set $D(M_{i_0})$ increases by at most two, which is not greater than λ_{n_0} by our assumptions about the sequence $\{\lambda_i\}_{i=1}^{\infty}$.

- *n_0 appears in $D(M_{i_0-1})$ exactly λ_{n_0} -times.*

  For this case we can show, as in the third part of the proof of Theorem 1, that there are no additional appearances of n_0 in the set $D(M_{i_0})$ according to the multiplicity in the preceding multiset, and get the same contradiction.

By exhausting all possible cases we have proved that there are no positive integers, which appear in $D(G)$ more than λ_i -times. This completes the proof. □

Example 4. Here are the first elements of the generalized difference set G of type $\{2, 2, 2, 2, \ldots\}$ when starting with $m_0 = 1$:

$1, 2, 6, 7, 16, 18, 38, 40, 82, 85, 172, 175, 350, 354, 710, 716 \ldots$

As the reader may have realized, the condition $\lambda_i > 1$, for all $i \in S$, was crucial for our proof. The following example shows that, in some sense, this condition cannot be "weakened".

Example 5. Let $\{\lambda_i\}_{i=1}^{\infty}$ be a sequence $\{1, 1, \ldots, 1, 3, 1, 1, \ldots\}$ which posseses exactly one "3" on the i -th place (i. e. $\lambda_i = 3$), and is equal to "1" otherwise ($\lambda_j = 1$, for $j \neq i$). Then there is no generalized difference set of this type on the additive semigroup of positive integers. The proof of this claim is based on the fact that the three different expressions for i force the existence of another positive integer different from i with multiplicity at least 2. It is an easy combinatorial exercise to show this, and we leave it to the reader.

Theorem 2 can be extended to the more general

Theorem 3 *Let $\{\lambda_i\}_{i=1}^{\infty}$ be a sequence of positive integers such that $\lambda_i = 1$ for only finitely many i from S. Then there exists a generalized difference set of the additive semigroup of positive integers of type $\{\lambda_i\}_{i=1}^{\infty}$.*

Proof. We can construct the set G using our second recursive definition by making the "starting" m_0 greater than the largest index of an element equal to 1. Choosing m_0 in this way, we cannot "accidentally" create two differences when we need only one. The details are left to the reader. □

All the results achieved for the infinite cyclic semigroup can be shown to be true for the infinite cyclic group as well.

Definition 4 *Let S be the additive group of integers, and let $\lambda = \{\ldots, \lambda_{-3}, \lambda_{-2}, \lambda_{-1}, \lambda_1, \lambda_2, \lambda_3, \ldots\}$ be a doubly infinite sequence of positive integers. We say that a subset G is a* generalized difference set of type λ *on the group S if for every element $i \in S, i \neq 0$, we have precisely λ_i solutions of the equation $i + g_1 = g_2$, with $g_1, g_2 \in G$ (i. e. every integer i can be expressed exactly λ_i -times as a difference $g_2 - g_1$ of elements of G).*

Obviously, $\lambda_i = \lambda_{-i}$, for all i, is a necessary condition for the existence of a generalized difference set of the type λ. Hence, λ is completely determined by the sequence $\{\lambda_1, \lambda_2, \lambda_3, \ldots\}$. Each of the above three theorems, therefore, remains true after replacing the infinite cyclic semigroup by the infinite cyclic group.

Remark. The generalized difference set G constructed in Theorem 1 is also a minimal A-ideal of the infinite cyclic semigroup. It is different from both of the known examples of such an A-ideal, which are presented in [1] and [3].

References

[1] O.Grošek and L.Satko,*A new notion in the theory of semigroups*, Semigroup Forum **20**, (1980), 233-240.

[2] M.Hall,*Combinatorial Theory*, Blaisdell Publ. Comp., 1967, 120-166.

[3] R.Šulka,*The Minimal Right A-Ideal of The Free Semigroup on a Countable Set*, Math.Slovaca **32**, (1982), 3, 301-304.