

## Direct Sum Decomposition of the Integers

Yuji ITO

*Keio University*

### §1. Introduction.

In this paper we shall be concerned with the direct sum decomposition  $Z = A \oplus B$  of the set  $Z$  of all integers, where both subsets  $A$  and  $B$  are infinite subsets. Recently, a very interesting connection between such a decomposition of  $Z$  (and of  $N$ ) and properties of infinite measure preserving ergodic transformations was discovered, and exploiting this connection, a number of significant results have been obtained characterizing the nature of the summands that appear in such a decomposition, see [2], [3], [4] and [5].

While it is well-known and is not difficult to characterize the infinite subsets that appear as direct summands of the decomposition  $N = A \oplus B$ , see, for example [1], [6], the situation is very different for the case of the direct sum decomposition of  $Z$ , where it seems to be very difficult to give a reasonable characterization of summands in general, see Proposition 2.2 below. On the other hand, if one fixes one of the summands of such a decomposition to be a "reasonable set" in some sense, then one can give some interesting characterizations for infinite subsets of  $Z$  that can be a complement of this set in the decomposition of  $Z$ . If we let the set  $A$  to be one of the sets that appear as a direct summand of the decomposition of  $N$ , for example, it follows from the known result mentioned above that there exists a unique subset  $B$  such that  $N = A \oplus B$  and it is not difficult to show that for this  $B$ ,  $A \oplus (-B) = Z$  holds, and furthermore, one can construct by starting with this  $B$  many other complements of  $A$  in  $Z$ , see Proposition 2.3 below. In fact, in [3] and [4], it was shown by using ergodic theory that such a set  $A$  always has uncountably many distinct complements in  $Z$ , some of which can be of very different nature from those described in Proposition 2.3.

So, in this paper, we shall take  $A$  to be one of the sets that can appear as a direct summand of the decomposition of  $N$ ; in fact, for the sake of simplicity, we take  $A$  to be the simplest of such sets, namely, let  $A$  consist of 0 and all finite sums of distinct odd powers of 2, and give a characterization of sets  $C$  that can appear as a complement of this  $A$  in the direct sum decomposition of  $Z$ . For this set  $A$ , S. Eigen, A. Hajian and

S. Kakutani gave in [5] a very interesting characterization for a *finite* subset  $F$  of  $Z$  in order for it to be extendable to a complement of  $A$  in  $Z$ . We will prove in §3 a theorem related to this result giving a necessary and sufficient condition for an *infinite* subset  $C$  to be a complement of  $A$  in  $Z$ . This theorem would indicate that a little more general theorem, which we will state as a conjecture in §4, might be true, although we do not have a proof for it at present. Also in §4, we will give an example, which indicates that in a sense one cannot hope to have a stronger theorem than this conjecture.

Although our results will be stated specifically for the simplest  $A$  mentioned above, the results can be generalized for any summand  $A$  appearing in the direct sum decomposition of  $N$  without much difficulty.

The author would like to thank Profs. S. Eigen, A. Hajian, S. Kakutani and R. Tijdeman for enlightening discussions on the topic of this paper. He is grateful also to the referee for pointing out that the representation of  $Z$  as a subset of  $Z_2$  will shorten the original proof of the Claim made in §4 considerably and make it much clearer.

## §2. Definitions and preparatory remarks.

For a pair  $E, F$  of subsets of  $Z$  or  $N$ , we denote the difference set  $\{e-f \mid e \in E, f \in F\}$  by  $E-F$  and the sum set  $\{e+f \mid e \in E, f \in F\}$  by  $E+F$ . The sum  $E+F$  is said to be a *direct sum* and is denoted by  $E \oplus F$ , if every  $n$  in  $E+F$  is represented uniquely as  $n=e+f$  with  $e \in E$ , and  $f \in F$ . It is easy to see that  $E+F=E \oplus F$  if and only if  $(E-E) \cap (F-F) = \{0\}$ .

In the sequel we shall call the pair of sets  $A, B$  a *complementing  $N$ -pair* or a *complementing  $Z$ -pair*, according as  $A \oplus B = N$  or  $A \oplus B = Z$ , respectively. In this paper we shall always assume that  $0 \in N$ .

Concerning infinite complementing  $N$ -pairs, the following was proved in [1] (see also [6]):

**PROPOSITION 2.1** (de Bruijn). *Infinite subsets  $A$  and  $B$  of  $N$  give an  $N$ -pair if and only if there exists an infinite sequence of integers  $\{m_i \mid i \geq 1\}$  with  $m_i \geq 2$  for all  $i$ , such that*

$$A = \text{the set of all finite sums of the form } \sum_{i \geq 0} x_{2i+1} M_{2i+1},$$

$$B = \text{the set of all finite sums of the form } \sum_{i \geq 0} x_{2i} M_{2i},$$

where  $0 \leq x_i < m_{i+1}$  for  $i \geq 0$  and  $M_0 = 1$  and  $M_i = \prod_{j=1}^i m_j$  for  $i \geq 1$ .

The simplest pair  $A, B$  satisfying the conditions of this proposition is given when  $m_j = 2$  for all  $j \geq 1$ , and in this case,  $A$  consists of 0 and all finite sums of distinct odd powers of 2, and  $B$  consists of 0 and all finite sums of distinct even powers of 2.

Infinite complementing  $Z$ -pairs, on the other hand, are much more complicated and it is difficult to give a reasonable description as the following Proposition indicates.

PROPOSITION 2.2. *Let  $E$  and  $F$  be any pair of finite subsets of  $\mathbf{Z}$  satisfying the condition  $(E-E) \cap (F-F) = \{0\}$ . Then, there exists an infinite complementing  $\mathbf{Z}$ -pair  $C, D$  such that  $C \supset E$  and  $D \supset F$ .*

PROOF. First we note that if  $(E-E) \cap (F-F) = \{0\}$  and if  $p$  is any number not belonging to  $E+F$ , then one can always find  $e$  and  $f$  in  $\mathbf{Z}$  so that  $p = e+f$  and  $(E'-E') \cap (F'-F') = \{0\}$ , where  $E' = E \cup \{e\}$  and  $F' = F \cup \{f\}$ . To see this, let us enumerate elements of  $E$  in increasing order as  $e_1 < e_2 < \dots < e_n$ , and those of  $F$  in decreasing order as  $f_1 > f_2 > \dots > f_m$ , and fix an integer  $q$  satisfying

$$(2.1) \quad q > (f_1 - f_m + e_n) \vee (e_n - e_1 + p - f_m).$$

If we then let  $e = q$  and  $f = p - q$ , it is easy to check that they satisfy the desired properties.

To complete the proof of the proposition, let  $p_1$  be the number not in  $E \oplus F$  having the smallest absolute value, and find, by using the remark made above, two numbers  $e$  and  $f$  so that  $e + f = p_1$ , and  $E_1 = E \cup \{e\}$  and  $F_1 = F \cup \{f\}$  satisfy  $E_1 + F_1 = E_1 \oplus F_1$ . Next, we let  $p_2$  be the number not in  $E_1 \oplus F_1$  having the smallest absolute value, and enlarge  $E_1$  and  $F_1$  to  $E_2$  and  $F_2$ , respectively, by the same method so that  $E_2 + F_2 = E_2 \oplus F_2$  and  $p_2 \in E_2 \oplus F_2$ . Continuing in this way, we get increasing sequences of sets  $\{E_n\}$  and  $\{F_n\}$ , and if we let  $C = \bigcup_{n=1}^{\infty} E_n$ , and  $D = \bigcup_{n=1}^{\infty} F_n$ , then they satisfy the assertion of the proposition.

Proposition 2.1 shows that when one of the summands in the direct sum decomposition of  $N$  is given, its complement in  $N$  is uniquely determined. However, the situation is very different in the case of the direct sum decomposition of  $\mathbf{Z}$ . When the pair  $A, B$  is an infinite complementing  $N$ -pair, for example, it is well-known and is not difficult to prove that  $A$  and  $-B$  give a complementing  $\mathbf{Z}$ -pair, but there are many subsets of  $\mathbf{Z}$  different from  $-B$ , which are complements of  $A$  in  $\mathbf{Z}$ . This can be shown for any  $A$ , which is a summand in the direct sum decomposition of  $N$ , but in order to simplify the arguments, we shall consider from now on, only the case of  $A$  consisting of 0 and all finite sums of distinct odd powers of 2.

So, let us take

$$(2.2) \quad A = \left\{ \sum_{i \geq 0} \alpha_i 2^{2i+1} \mid \alpha_i = 1 \text{ for finitely many } i\text{'s and } = 0 \text{ for all other } i\text{'s} \right\},$$

$$(2.3) \quad B = \left\{ \sum_{i \geq 0} \beta_i 2^{2i} \mid \beta_i = 1 \text{ for finitely many } i\text{'s and } = 0 \text{ for all other } i\text{'s} \right\}.$$

We also let

$$(2.4) \quad \Omega = \{ \omega = (\omega_1, \omega_2, \dots, \omega_n, \dots) \mid \omega_n = -1 \text{ or } +1 \text{ for every } n \},$$

$$(2.5) \quad \Omega^- = \{ \omega = (\omega_1, \omega_2, \dots, \omega_n, \dots) \in \Omega \mid \omega_n = -1 \text{ for infinitely many } n\text{'s} \}$$

and for an  $\omega \in \Omega$  write

$$(2.6) \quad B_\omega = \left\{ \sum_{i \geq 0} \beta_i \omega_i 2^{2i} \mid \beta_i = 1 \text{ for finitely many } i\text{'s and } = 0 \text{ for all other } i\text{'s} \right\}.$$

Note that if  $\omega = (-1, -1, -1, \dots)$ , then  $B_\omega = -B$ .

**PROPOSITION 2.3.** *Let  $A$  be as defined in (2.2). Then for any  $\omega \in \Omega^-$ ,  $A \oplus B_\omega = \mathbf{Z}$ , where  $\Omega^-$  and  $B_\omega$  are as defined in (2.5) and (2.6), respectively.*

**PROOF.** Since for any  $\omega \in \Omega$ ,  $B_\omega - B_\omega = B - B$ , it is clear that  $A + B_\omega = A \oplus B_\omega$ . Next, for each fixed  $n \geq 1$ , define

$$(2.7) \quad K_n = \left\{ \sum_{i=0}^n (\alpha_i 2^{2i+1} + \beta_i \omega_i 2^{2i}) \mid \alpha_i \text{ and } \beta_i \text{ are 0 or 1 for each } 0 \leq i \leq n \right\}.$$

All the numbers appearing in the definition of this set  $K_n$  are distinct, and there are  $2^{2n+2}$  numbers. The largest number  $p_n$  appearing in  $K_n$  is obviously

$$\sum_{i=0}^n 2^{2i+1} + \sum_{i \in I_1} 2^{2i}$$

where  $I_1 = \{i \mid 0 \leq i \leq n \text{ and } \omega_i = +1\}$ , and the smallest number  $q_n$  in  $K_n$  is

$$- \sum_{i \in I_2} 2^{2i}$$

where  $I_2 = \{i \mid 0 \leq i \leq n \text{ and } \omega_i = -1\}$ .

There are exactly

$$\sum_{i=0}^n 2^{2i+1} + \sum_{i \in I_1} 2^{2i} + \sum_{i \in I_2} 2^{2i} + 1 = \sum_{i=0}^{2n+1} 2^i + 1 = 2^{2n+2}$$

numbers  $k$  satisfying  $q_n \leq k \leq p_n$ , and therefore, all the consecutive numbers between  $q_n$  and  $p_n$  are represented in  $K_n$ .

Obviously, as  $n \uparrow \infty$ ,  $p_n \uparrow \infty$ , and  $q_n \downarrow -\infty$ , since  $\omega_n = -1$  for infinitely many  $n$ 's. Thus, we see that  $A \oplus B_\omega = \bigcup_{n=1}^{\infty} K_n = \mathbf{Z}$ .

In [3] and [4] it was shown by using ergodic theoretic ideas that  $A$  considered above has uncountably many complements  $C$  in  $\mathbf{Z}$ , some of which have properties not shared by any of the  $B_\omega$ 's considered above; for example,  $C - C \neq B - B$ , or  $C$  having even nastier properties.

### §3. The main theorem.

Throughout the remainder of this paper, we shall assume that the sets  $A$  and  $B$  we consider are those defined in (2.2) and (2.3), respectively. We will be concerned with the problem of characterizing the complements of the set  $A$  in  $\mathbf{Z}$ . We note that if a set

$C$  is a complement of  $A$  in  $\mathbf{Z}$ , then so is any translate  $C+k$  for any  $k$ , so we shall assume that complements  $C$  of  $A$  in  $\mathbf{Z}$  which we consider always contain 0. Now, let us denote by  $\mathfrak{C}(A)$  the set of all complements  $C$  (containing 0) of  $A$  in  $\mathbf{Z}$ . Namely,

$$(3.1) \quad \mathfrak{C}(A) = \{C \subset \mathbf{Z} \mid 0 \in C \text{ and } A \oplus C = \mathbf{Z}\}.$$

For  $n \in \mathbf{Z}$ , we define  $ord_2(n)$  to be equal to  $k$  if  $2^k$  divides  $n$  but  $2^{k+1}$  does not. In [5], the following result was obtained:

**THEOREM 3.1** (Eigen, Hajian and Kakutani). *If  $F$  is a finite subset of  $\mathbf{Z}$ , then there exists a  $C \in \mathfrak{C}(A)$  such that  $C \supset F$  if and only if every number belonging to the difference set  $F-F$  is of even  $ord_2$ .*

The following theorem, which is the main result of this paper, gives a characterization for infinite subsets  $C$  belonging to  $\mathfrak{C}(A)$ .

**THEOREM 3.2.** *Suppose  $C$  is an infinite subset of  $\mathbf{Z}$  containing 0. Then,  $C \in \mathfrak{C}(A)$  if and only if all of the following conditions are satisfied:*

- (i) Every number in  $C-C$  is of even  $ord_2$ ,
- (ii)  $C$  is maximal with respect to the property (i),
- (iii) there exists an  $\omega$  in  $\Omega^-$  such that  $A \oplus C \supset B_\omega$ , where  $\Omega^-$  and  $B_\omega$  are as defined in (2.5) and (2.6), respectively.

**PROOF.** The necessity of the condition (i) follows from the theorem of Eigen, Hajian and Kakutani mentioned above, and (ii) and (iii) are obvious. To prove the sufficiency of these conditions, we need a few lemmas. Note that since every number in  $A-A$  is of odd  $ord_2$ , the condition (i) implies that  $(A-A) \cap (C-C) = \{0\}$ , and hence  $A+C = A \oplus C$ .

**LEMMA 3.1.** *Suppose a set  $C$  satisfies the condition (i) of the theorem. If for some  $k > 0$ ,  $n$  and  $n+2^{2k}$  both belong to the set  $A \oplus C$ , then  $n+2^{2k-1}$  also belongs to  $A \oplus C$ .*

**PROOF.** If both  $n$  and  $n+2^{2k}$  belong to  $A \oplus C$ , then one can write  $n = \sum_{i \geq 0} \alpha_i 2^{2i+1} + c_1$ , and  $n+2^{2k} = \sum_{i \geq 0} \rho_i 2^{2i+1} + c_2$  for some  $c_1$  and  $c_2$  in  $C$ , where  $\alpha_i$  and  $\rho_i$  are as in (2.2). Then we have

$$2^{2k} = \sum_{i \geq 0} (\rho_i - \alpha_i) 2^{2i+1} + (c_2 - c_1).$$

Since  $c_2 - c_1$  is of even  $ord_2$ , we must have  $\alpha_i = \rho_i$  for  $0 \leq i \leq k-1$ . Thus, we can write

$$(3.2) \quad n = \sum_{i=0}^{k-1} \alpha_i 2^{2i+1} + \sum_{i \geq k} \alpha_i 2^{2i+1} + c_1,$$

$$(3.3) \quad n + 2^{2k} = \sum_{i=0}^{k-1} \alpha_i 2^{2i+1} + \sum_{i \geq k} \rho_i 2^{2i+1} + c_2.$$

If  $\alpha_{k-1} = 0$ , we see from (3.2)  $n + 2^{2k-1} \in A \oplus C$ , while if  $\alpha_{k-1} = 1$ , then from (3.3) we also get  $n + 2^{2k-1} \in A \oplus C$ .

LEMMA 3.2. *Suppose a set  $C$  satisfies the conditions (i) and (ii) of the theorem. If for every  $k \geq 0$ ,  $n - 2^{2k-1} \in A \oplus C$  holds, then  $n$  itself belongs to  $A \oplus C$ .*

PROOF. If  $n - c$  has even  $\text{ord}_2$  for every  $c \in C$ , then since  $C$  is maximal with respect to the condition (i),  $n$  must belong to  $C$  and hence to  $A \oplus C$ . So, suppose for some  $c$  in  $C$ ,  $n - c$  has an odd  $\text{ord}_2$ . Then, one can write

$$(3.4) \quad n - c = \pm(2^{2k+1} + p),$$

where  $p$  is either 0 or a positive number with  $\text{ord}_2(p) \geq 2k + 2$ . By hypothesis,  $n - 2^{2k+1}$  belongs to  $A \oplus C$ , so there exist  $a$  in  $A$  and  $c^*$  in  $C$  such that

$$(3.5) \quad n - 2^{2k+1} = a + c^*.$$

From (3.4) and (3.5), we then get that  $c - c^*$  equals either  $-p + a$  or  $2^{2k+2} + p + a$ , depending on the sign for  $n - c$  in (3.4). Since  $c - c^*$  has even  $\text{ord}_2$ , and since  $\text{ord}_2(p) \geq 2k + 2$  if  $p$  is not 0, we conclude that in either case  $\text{ord}_2(a) \geq 2k + 3$  must hold, and therefore, that  $a + 2^{2k+1} \in A$ . From (3.5) it now follows that  $n$  belongs to  $A \oplus C$ .

LEMMA 3.3. *Suppose a set  $C$  satisfies the conditions (i) and (iii) of the theorem. Then, we have  $-N \subset A \oplus C$ .*

PROOF. By (iii) there exists an  $\omega$  in  $\Omega^-$  such that  $A \oplus C \supset B_\omega$ . Since  $A \oplus B_\omega = \mathbf{Z}$ , as was shown in Proposition 2.3, we can represent any negative integer  $n$  uniquely as the sum  $a + b$ , with  $a$  in  $A$  and  $b$  in  $B_\omega$ . Let us define for each  $k \geq 0$ ,

$$A_k = \left\{ a = \sum_{i \geq 0} \alpha_i 2^{2i+1} \mid \text{the number of } i\text{'s for which } \alpha_i = 1 \text{ is exactly } k \right\}.$$

Then, clearly,  $-N \subset \bigcup_{k \geq 0} (A_k \oplus B_\omega)$ . We will show by induction on  $k$  that any negative number in the set  $A_k \oplus B_\omega$  belongs to the set  $A \oplus C$ . Since  $A_0 = \{0\}$ , this is clear when  $k = 0$ , because of the hypothesis (iii). So, suppose that for each  $0 \leq j \leq k$  every negative integer in the set  $A_j \oplus B_\omega$  belongs to  $A \oplus C$ , and let  $n$  be a negative integer in  $A_{k+1} \oplus B_\omega$ . Then, we can write  $n = \sum_{i=0}^{p-1} \alpha_i 2^{2i+1} + 2^{2p+1} + \sum_{i \geq 0} \beta_i \omega_i 2^{2i}$ , where  $\beta_i$ 's are 1 for finitely many  $i$ 's and 0 for all other  $i$ 's. Since  $n$  is negative, the largest index, say  $q$ , for which  $\beta_q = 1$  must be greater than  $p$ , and for this  $q$ ,  $\omega_q$  must be  $-1$ . Thus we can write

$$(3.6) \quad n = a + 2^{2p+1} + \sum_{i=0}^{q-1} \beta_i \omega_i 2^{2i} - 2^{2q},$$

where  $a = \sum_{i=0}^{p-1} \alpha_i 2^{2i+1} \in A_k$ . Then, we see by the induction hypothesis that  $n - 2^{2p+1} \in A \oplus C$ . We also have

$$(3.7) \quad n + 2^{2p+1} = a + 2^{2p+2} + \sum_{i=0}^{q-1} \beta_i \omega_i 2^{2i} - 2^{2q}.$$

Now there are two cases to consider depending on the possible combinations of the values of  $\beta_{p+1}$  and  $\omega_{p+1}$ .

In case  $(I_1)$ , we suppose that either  $\beta_{p+1}=1$  and  $\omega_{p+1}=-1$ , or  $\beta_{p+1}=0$  and  $\omega_{p+1}=+1$ . In this case we see that  $2^{2p+2} + \sum_{i=0}^{q-1} \beta_i \omega_i 2^{2i} - 2^{2q}$  belongs to  $B_\omega$ , so we get from (3.7) and the induction hypothesis that  $n + 2^{2p+1}$  belongs to  $A \oplus C$ . Using Lemma 3.1, we then conclude that  $n \in A \oplus C$ .

In case  $(II_1)$ , we suppose that either  $\beta_{p+1}=0$  and  $\omega_{p+1}=-1$ , or  $\beta_{p+1}=1$  and  $\omega_{p+1}=+1$ . In this case, we let  $n_1 = n + 2^{2p+1}$ , and note that

$$(3.8) \quad n_1 = a + 2^{2p+3} - 2^{2p+2} + \sum_{i=0}^{q-1} \beta_i \omega_i 2^{2i} - 2^{2q}.$$

Under the combinations considered for case  $(II_1)$ , we see that  $-2^{2p+2} + \sum_{i=0}^{q-1} \beta_i \omega_i 2^{2i} - 2^{2q}$  (call this number  $b$ ) belongs to  $B_\omega$ , and therefore, from (3.8) it follows that  $n_1 - 2^{2p+3} \in A \oplus C$ . We also have  $n_1 + 2^{2p+3} = a + 2^{2p+4} + b$ , and again we consider two separate cases:

Case  $(I_2)$ , where either  $\beta_{p+2}=1$  and  $\omega_{p+2}=-1$ , or  $\beta_{p+2}=0$  and  $\omega_{p+2}=1$ , and Case  $(II_2)$ , where either  $\beta_{p+2}=0$  and  $\omega_{p+2}=-1$ , or  $\beta_{p+2}=1$  and  $\omega_{p+2}=+1$ .

In case  $(I_2)$  we see that  $2^{2p+4} + b$  belongs to  $B_\omega$  so that  $n_1 + 2^{2p+3}$  belongs to  $A \oplus B_\omega$  by the induction hypothesis. By using Lemma 3.1 again we get that  $n_1 = n + 2^{2p+1} \in A \oplus C$ . Since we already know that  $n - 2^{2p+1} \in A \oplus C$ , we conclude that  $n \in A \oplus C$  in case  $(I_2)$ .

In case  $(II_2)$ , we let  $n_2 = n_1 + 2^{2p+3}$ , and repeat the same argument as before. We then see that  $n_2 - 2^{2p+5}$  belongs to  $A \oplus C$ , and for  $n_2 + 2^{2p+5}$ , two further cases have to be considered. In the first case (case  $(I_3)$ )  $n_2 + 2^{2p+5}$  also belongs to  $A \oplus C$ , in which case,  $n_2 = n_1 + 2^{2p+3} \in A \oplus C$ , and hence  $n_1$  and finally  $n$  itself belongs to  $A \oplus C$ .

In the second (case  $(II_3)$ ), we let  $n_3 = n_2 + 2^{2p+5}$ , and repeat the argument.

Since for the largest index  $q$ , for which  $\beta_q=1$ , we have  $\omega_q=-1$ , we see that after at most  $q-p$  steps we end up with case  $(I)$ , and we conclude that each  $n_j$  considered in these steps must belong to  $A \oplus C$ , and hence  $n$  must belong to  $A \oplus C$  also in all cases.

This completes the proof of the lemma, since 0 obviously belongs to  $A \oplus C$ .

**PROOF OF SUFFICIENCY OF THE CONDITIONS OF THEOREM 3.2.** Let us define  $n$  to be the largest integer with the property that  $j \in A \oplus C$  for every  $j \leq n$ . We know from Lemma 3.3 that  $n > 0$ . We have to show that  $n = \infty$ . So, suppose  $n < \infty$ . Then, we must have that  $n+1$  does not belong to the set  $A \oplus C$ . But from the definition of  $n$  it follows that for each  $k \geq 0$ ,  $n+1 - 2^{2k+1} \in A \oplus C$ . Lemma 3.2 then implies that  $n+1$  must belong to  $A \oplus C$ . The contradiction implies that  $n$  must equal  $\infty$ , and therefore,  $A \oplus C = \mathbb{Z}$ .

#### §4. Remarks and examples.

The fact that conditions (i) and (ii) of Theorem 3.2 are not enough to guarantee

that  $C$  belongs to  $\mathfrak{C}(A)$  is easily seen from the fact that the set  $B$  as defined in (2.3) satisfies both of these conditions and yet  $A \oplus B = N$  and not  $Z$ . What is wrong with  $B$  is that no negative numbers are in  $B$ , so you might wonder if in addition to the conditions (i) and (ii), the following condition is satisfied by  $C$ , then this would guarantee that  $C \in \mathfrak{C}(A)$ :

(iv)  $C$  is unbounded below, i.e.,  $C$  contains arbitrarily large negative numbers.

However, the following example shows that the conditions (i), (ii) and (iv) are still not sufficient for  $C$  to be in  $\mathfrak{C}(A)$ .

EXAMPLE 4.1. Let

$$B^* = \{b \mid b \in B \text{ and } b \text{ is odd}\} \cup \{-b \mid b \in B \text{ and } b \text{ is even}\}.$$

Clearly,  $B^*$  satisfies (iv) and it is easy to check that every number in  $B^* - B^*$  has even  $\text{ord}_2$ , so it satisfies (i) as well. Since  $B^*$  is the union of disjoint sets  $4B+1$  and  $-4B$ , where  $4B = \{4b \mid b \in B\}$ , we also get, using the fact that  $A = 2B$ ,

$$\begin{aligned} A \oplus B^* &= (A + 4B + 1) \cup (A - 4B) \quad (\text{disj.}) \\ &= \{2(B + A) + 1\} \cup \{2(B - A)\} \quad (\text{disj.}) \\ &= (2N + 1) \cup 2Z, \end{aligned}$$

which says that  $A \oplus B^*$  contains no negative odd numbers, and therefore,  $B^*$  does not belong to  $\mathfrak{C}(A)$ . Furthermore, this shows that only number that can be adjoined to  $B^*$  without destroying the property (i) must be a negative odd integer, but it is easy to check that for any negative odd integer  $n$  there exists a number  $b$  in  $B^*$  such that  $b - n$  has odd  $\text{ord}_2$ . Therefore,  $B^*$  satisfies (ii) as well.

REMARK 4.1. The fact that an additional condition like (iii) in Theorem 3.2 would guarantee that  $C \in \mathfrak{C}(A)$  was first noticed by R. Tijdeman in [7], where he proved that if  $C$  satisfies (i) and (ii) and the following condition (iii)', then  $C \in \mathfrak{C}(A)$ .

(iii)'  $A \oplus C \supset B$ .

His proof of this assertion is quite different from ours, and it is not easy to see how to extend his arguments to give a proof of our theorem.

We note that for every  $\omega \in \Omega^-$ ,  $B_\omega \in \mathfrak{C}(A)$ , so it seems reasonable to extend our Theorem 3.2 to the following form, which we state as a conjecture.

CONJECTURE. *Suppose  $C$  is an infinite subset of  $Z$  containing 0. Then,  $C \in \mathfrak{C}(A)$  if and only if all of the following conditions are satisfied:*

- (i) *Every numbers in  $C - C$  is of even  $\text{ord}_2$ ,*
- (ii)  *$C$  is maximal with respect to the property (i),*
- (iii)" *there exists a set  $D$  in  $\mathfrak{C}(A)$  such that  $A \oplus C \supset D$ .*

Finally, we give an example, which is a modification of one given earlier by Eigen for somewhat different purposes, to show that in some sense one cannot improve on this conjecture.

EXAMPLE 4.2. Let for each  $k \geq 0$ ,

$$E_k = -2^{2k}B = \{-2^{2k}b \mid b \in B\}$$

and let

$$(4.1) \quad C_1 = E_1 \quad \text{and} \quad C_k = E_k + p_k \quad \text{for each } k \geq 2,$$

where  $p_k = \sum_{i=0}^{k-2} 2^{2i}$ . Define  $C^*$  to be the set  $\bigcup_{k \geq 1} C_k$ .

One can then show the following facts for  $C^*$ :

(a)  $C^*$  satisfies the conditions (i) and (ii) of Theorem 3.2.

(b) For each  $D \in \mathfrak{C}(A)$ , the set  $A \oplus C^*$  misses exactly one number from  $D$ .

The fact that  $C^*$  satisfies the condition (i) can be checked easily, by considering three cases:

(1) If both  $c_1$  and  $c_2$  belong to the same  $C_k$ , then  $c_1 - c_2 \in 2^{2k}(B - B)$ , and this set consists only of even  $ord_2$  numbers.

(2) If  $c_1 \in C_1$ , and  $c_2 \in C_k$  for some  $k > 1$ , then  $c_1 - c_2$  is an odd integer, and therefore, has even  $ord_2$ .

(3) If  $c_1 \in C_k$ , and  $c_2 \in C_l$  for  $k > l > 1$ , then  $c_1 - c_2 \in 2^{2l}B - 2^{2k}B + (p_l - p_k)$ , and since any non-zero element in the set  $2^{2l}B - 2^{2k}B$  has an  $ord_2$  at least equal to  $2l$ , while the  $ord_2(p_l - p_k) = 2(l - 1)$ , the latter is the  $ord_2(c_1 - c_2)$ , which is even.

The fact that  $C^*$  satisfies the condition (ii) and the statement (b) above will follow if we can establish the following claim:

**CLAIM.** *The set of numbers missing from the set  $A \oplus C^*$  coincides with the set  $-A - 1 = \{-a - 1 \mid a \in A\}$ .*

Indeed, the assertion (b) follows immediately from this claim since if  $D \in \mathfrak{C}(A)$ , then  $-1$  has a unique representation  $-1 = a + d$  with  $a \in A$  and  $d \in D$ , so that  $n = -1 - a = d$  is the unique number in the set  $D \cap (-A - 1)$ .

Also, it is clear from the claim above that only possible number that can be adjoined to  $C^*$  without destroying the property (i) must come from the set  $(-A - 1)$ , but for any  $a$  in  $A$ , one can show, as we indicate below, that there exists a number  $c$  in  $C^*$  such that  $c - (-a - 1) = c + a + 1$  has an odd  $ord_2$ , and therefore,  $C^*$  satisfies the condition (ii) as well.

To show the existence of such a  $c$ , let  $a$  be any number in  $A$ . Then

$$a = \sum_{i=0}^{k-1} 2^{2i+1} + \sum_{i>k} \alpha_i 2^{2i+1}$$

where  $k$  is the smallest index for which  $\alpha_k = 0$ . Now, the number  $c = p_{k+2} = \sum_{i=0}^k 2^{2i}$  belongs to the set  $C_{k+2}$  and hence to  $C^*$ , and we have

$$c + a + 1 = \sum_{j=0}^{2k} 2^j + 1 + \sum_{i>k} \alpha_i 2^{2i+1}$$

$$= 2^{2k+1} + \sum_{i>k} \alpha_i 2^{2i+1},$$

which shows that  $c+a+1$  has an odd  $\text{ord}_2$ .

So, it remains now to establish the claim above. We shall do this by proving a series of lemmas.

LEMMA 4.1. *Let for each  $k \geq 1$ ,*

$$A^k = \left\{ a = \sum_{j \geq 0} \alpha_j 2^{2j+1} \in A \mid \alpha_j = 0 \text{ for all } j \geq k-1 \right\}.$$

*Then, for each  $k$ ,  $A$  is the union of disjoint sets  $\{2^{2k-1}B+a\}$ , where  $a$  runs over the set  $A^k$ , i.e.,*

$$A = \bigcup_{a \in A^k} \{2^{2k-1}B+a\} \quad (\text{disj}).$$

PROOF. We will prove this by induction on  $k$ . Since  $A^1 = \{0\}$  and  $A = 2B$ , this is obvious for  $k=1$ . It is easy to see that

$$B = (2^2B) \cup (2^2B+1) \quad (\text{disj}),$$

and therefore, for each  $k$ ,

$$2^{2k-1}B+a = (2^{2k+1}B+a) \cup (2^{2k+1}B+2^{2k-1}+a) \quad (\text{disj})$$

holds. Since it is clear that  $A^{k+1} = A^k \cup (A^k + 2^{2k-1})$  (disj.), we see that if the assertion is valid for  $k$ , then

$$A = \bigcup_{a \in A^{k+1}} \{2^{2k+1}B+a\} \quad (\text{disj}),$$

which completes the induction.

Let us denote for each  $k \geq 1$ ,  $\overline{C}_k = A \oplus C_k$ , where  $C_k$  is as defined in (4.1). Then we have

LEMMA 4.2. *For each  $k$ ,*

$$\overline{C}_k = \bigcup_{a \in A^k} \{2^{2k-1}Z+p_k+a\} \quad (\text{disj}),$$

where  $p_1 = 0$  and  $p_k = \sum_{i=0}^{k-2} 2^{2i}$  for  $k \geq 2$ .

PROOF. By using the definition of  $C_k$  and Lemma 4.1, we see that

$$(4.2) \quad \begin{aligned} \overline{C}_k &= A \oplus (-2^{2k}B+p_k) \\ &= \bigcup_{a \in A^k} \{2^{2k-1}B-2^{2k}B+p_k+a\} \quad (\text{disj}). \end{aligned}$$

But since  $B - 2B = B - A = \mathbf{Z}$ , the assertion of the lemma follows from (4.2).

For the rest of the argument, it is convenient to represent  $\mathbf{Z}$  as a subset of  $\mathbf{Z}_2$ , the set of 2-adic integers, which is the completion of  $\mathbf{Z}$  with respect to the 2-adic valuation. Specifically, we can write

$$\mathbf{Z}_2 = \left\{ \sum_{i \geq 0} c_i 2^i \mid c_i = 0 \text{ or } 1 \text{ for all } i \geq 0 \right\}$$

and

$$\mathbf{Z}^+ = \left\{ \sum_{i \geq 0} c_i 2^i \in \mathbf{Z}_2 \mid c_i = 0 \text{ for all but finitely many } i \text{'s} \right\},$$

$$\mathbf{Z}^- = \left\{ \sum_{i \geq 0} c_i 2^i \in \mathbf{Z}_2 \mid c_i = 1 \text{ for all but finitely many } i \text{'s} \right\},$$

and see that  $\mathbf{Z}^+$  and  $\mathbf{Z}^-$  represent the set of all non-negative and all negative elements of  $\mathbf{Z}$  in  $\mathbf{Z}_2$ , respectively. Furthermore, we note that if we define for  $n = \sum_{i \geq 0} c_i 2^i \in \mathbf{Z}$

$$\tilde{n} = \sum_{i \geq 0} (1 - c_i) 2^i$$

then  $\tilde{n}$  also belongs to  $\mathbf{Z}$ , and satisfies  $n + \tilde{n} = -1$  for all  $n \in \mathbf{Z}$ . Therefore, if we denote for any subset  $E$  of  $\mathbf{Z}$ ,  $\tilde{E} = \{\tilde{n} \mid n \in E\}$ , then the set  $-E - 1 = \{-n - 1 \mid n \in E\}$  equals the set  $\tilde{E}$ .

With these representations, we see that due to Lemma 4.2 we can write

$$\overline{C_1} = 2\mathbf{Z} = \left\{ \sum_{i \geq 0} c_i 2^i \mid c_0 = 0 \right\}$$

and

$$\overline{C_k} = \left\{ \sum_{i \geq 0} c_i 2^i \in \mathbf{Z} \mid c_{2j} = 1 \text{ for } 0 \leq j \leq k-2 \text{ and } c_{2k-2} = 0 \right\}$$

for  $k \geq 2$ .

Now it is easy to see that for each  $k \geq 1$  a number  $n = \sum_{i \geq 0} c_i 2^i \in \mathbf{Z}$  does not belong to the set  $\bigcup_{1 \leq j \leq k} \overline{C_j}$  if and only if  $c_{2j} = 1$  for  $0 \leq j \leq k-1$ .

Since  $A \oplus C^* = \bigcup_{m=1}^{\infty} \overline{C_m}$ , we conclude that  $n = \sum_{i \geq 0} c_i 2^i \in \mathbf{Z}$  will not belong to the set  $A \oplus C^*$  if and only if  $c_{2j} = 1$  for all  $j \geq 0$ . But since

$$\left\{ n = \sum_{i \geq 0} c_i 2^i \in \mathbf{Z} \mid c_{2j} = 1 \text{ for all } j \geq 0 \right\} = \tilde{A} = -A - 1$$

this completes the proof of the claim.

REMARK 4.2. Since the set  $C_k$  contains  $p_k$ , which tends to  $\infty$ , as  $k \rightarrow \infty$ , the set  $C^*$  is unbounded above. However, if we define for each  $k \geq 1$ ,  $G_k$  to be  $C_k - 2^{2k-1}$ , and

let  $G^* = \bigcup_{k=1}^{\infty} G_k$ , then  $G^*$  does not contain any positive number, and one can show that  $G^*$  satisfies the conditions (i) and (ii) of Theorem 3.2. Furthermore, since  $\overline{C_k + 2^{2k-1}s} = \overline{C_k}$  for any  $s \in \mathbb{Z}$ , which is obvious from Lemma 4.2, we see that for each  $k \geq 1$ ,  $\overline{G_k} = \overline{C_k}$ , and hence  $A \oplus G^* = A \oplus C^*$ . Thus,  $G^*$  also fails to be in  $\mathfrak{C}(A)$ .

In [7] it was mentioned that the following condition (v) together with (i) and (ii) might be sufficient for a set  $C$  to be in  $\mathfrak{C}(A)$ :

(v)  $C$  is bounded above.

However, the set  $G^*$  mentioned above satisfies (i), (ii) and (v) and yet fails to be in  $\mathfrak{C}(A)$ , so the assertion in [7] is false.

### References

- [ 1 ] N. G. DE BRUIJN, On bases for sets of integers, *Publ. Math. Debrecen* **1** (1950), 232–242.
- [ 2 ] S. EIGEN and A. HAJIAN, A characterization of exhaustive weakly wandering sequences for nonsingular transformations, *Comment. Math. Univ. St. Paul.* **36** (1987), 227–233.
- [ 3 ] S. EIGEN and A. HAJIAN, Sequences of integers and ergodic transformations, *Adv. Math.* **73** (1989), 256–262.
- [ 4 ] S. EIGEN, A. HAJIAN and S. KALIKOW, Ergodic transformations and sequences of integers, *Israel J. Math.* **75** (1991), 119–128.
- [ 5 ] S. EIGEN, A. HAJIAN and S. KAKUTANI, Complementing sets of integers—A result from ergodic theory, *Japanese J. Math.* **18** (1992), 205–211.
- [ 6 ] C. T. LONG, Addition theorems for sets of integers, *Pacific J. Math.* **23** (1967), 107–112.
- [ 7 ] R. TUJEMAN, Decomposition of the integers as a direct sum of two subsets, Technical Report, Math. Inst., Univ. of Leiden **W 91-14** (1991), 1–16.

*Present Address:*

DEPARTMENT OF MATHEMATICS, KEIO UNIVERSITY,  
HIYOSHI, KOHOKU-KU, YOKOHAMA, 223 JAPAN.