AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **53** (2012), Pages 135–139

Some results on near factorizations of boolean groups

G.R. Vijayakumar

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road, Colaba, Mumbai 400 005
India
vijay@math.tifr.res.in

Abstract

A group in which every element is its own inverse is called a *boolean* group. We show that if G is an infinite boolean group, then there exist subsets A, B of G such that $|A| = |B| = |G|$ and $G \setminus \{0\}$ is the direct sum of A and B, i.e., for each $(a, b) \in A \times B$, $a + b \neq 0$ and for each nonzero element $g \in G$, there exists a unique pair $(a, b) \in A \times B$ such that $g = a + b$. A variant of this result also is derived: any infinite boolean group G has subsets A, B such that $\min\{|A|, |B|\} = \aleph_0$ and $G \setminus \{0\}$ is the direct sum of A and B. In [S. Grüter et al., *Australas. J. Combin.* 49 (2011), 245–254] and [P.N. Balister et al., *European J. Combin.* 32 (2011), 533–537], by using different methods, it has been shown that if A, B are subsets of a finite nontrivial boolean group G such that $G \setminus \{0\}$ is the direct sum of A and B, then $|A|$ or $|B|$ is 1. In this note we present a simple proof for this result and extend this result to infinite boolean groups.

Let G be an additive group; let A, B be two subsets of G; the set $\{a + b : a \in A \text{ and } b \in B\}$ is called the *sum* of A and B and denoted by $A + B$; if for each g in this set, there is only one pair $(a, b) \in A \times B$ such that $g = a + b$, then this set is called the *direct sum* of A and B and denoted by $A \oplus B$. For any $g \in G$, in place of $\{g\} + A$, we simply write $g + A$. If for every $g \in G$, $g + g = 0$, then G is called a *boolean group.* A well known easily provable fact is that any boolean group is abelian. If A, B are subsets of a boolean group, it is easy to see that $0 \notin A + B \iff A \cap B = \emptyset$.

Remark 1. Let G be a group; let A, B be subsets of G such that $A + B = A \oplus B$. Then it can be verified easily that for any $P \subset A$, $P + B = P \oplus B$ and for any $\alpha \in G$, $(\alpha + A) + B = (\alpha + A) \oplus B$. If $\{B_i : i \in I\}$ is a collection of subsets of G such that for each $i \in I$, $A + B_i = A \oplus B_i$ and for all distinct $i, j \in I$, $(A + B_i) \cap (A + B_j) = \emptyset$, then it can be verified that $\cup_{i \in I}(A + B_i) = A \oplus (\cup_{i \in I} B_i)$.

This note concerns the question of finding subsets A, B of a nontrivial boolean group G such that $G \setminus \{0\} = A \oplus B$. Choosing a subset of G which is a singleton and its complement in G is an obvious solution. In [4], it has been conjectured that if G is finite, then there is no other solution. (The terminology used in [4] for stating this conjecture is quite different.) In [1] and [3], by using different methods, this conjecture has been settled. An objective of this note is to present a simple short proof for the result of [1, 3] obtained in this regard, and generalize this result to infinite boolean groups. Let $\mathbb{N}$ denote the set of all natural numbers. The main objective of this article is to show in an infinite boolean group G, the existence of subsets A, B, P and Q such that $|A| = |B| = |G|$, $\min\{|P|, |Q|\} = |\mathbb{N}|$ and $G \setminus \{0\} = A \oplus B = P \oplus Q$.

Proposition 2. *Let G be a finite nontrivial boolean group and A, B be subsets of G such that $G \setminus \{0\} = A \oplus B$. Then $|A|$ or $|B|$ is* 1.

Proof. First note that $|G| - 1 = |A||B|$. Suppose that $|A| \neq 1 \neq |B|$; then $(|A| - 1)(|B| - 1) > 0$; therefore $|A| + |B| < 1 + |A||B| = |G|$ whence we can find some $\alpha \in G \setminus (A \cup B)$. Now, let $P = \alpha + A$ and $Q = \alpha + B$. It is easy to verify that $G \setminus \{0\} = P \oplus Q$. Note that $0 \notin P \cup Q$. Now, let $p \in P$. Let us show that there is exactly one element $v \in P$ such that $p + v \in Q$. Since $p \neq 0$, for some $p' \in P$ and $q \in Q$, $p = p' + q$ whence $p + p' = q$. Suppose that $p'' \in P$ and $r \in Q$ such that $p + p'' = r$. Then $p' + q = p = p'' + r$ whence $p' = p''$. Therefore for each $p \in P$, there is a unique $p^\star \in P$ such that $p + p^\star \in Q$. Since for each $p \in P$, $p^\star \neq p$ (because $0 \notin Q$) and $(p^\star)^\star = p$, we find that $\big\{\{p, p^\star\} : p \in P\big\}$ is a partition of P into subsets of order 2. Therefore $|P|$ is even. Since $|G| = 1 + |P||Q|$, it follows that $|G|$ is odd—a contradiction. □

Theorem 3. *Suppose that the set of all nonzero elements of a nontrivial boolean group G is the direct sum of some subsets A, B of G. Then either one of the sets A, B is a singleton or both are infinite.*

Proof. We can assume that $|A| < \infty$ and $|B| \geqslant 2$. Let b_1, b_2 be distinct elements of B. Let H be the subgroup generated by $A \cup \{b_1, b_2\}$. [For any nonempty finite subset X of G, let $\sigma(X)$ denote the sum of all elements in X; let $\sigma(\emptyset) = 0$; note that for any finite subsets X, Y of G, $\sigma(X) + \sigma(Y) = \sigma(X \Delta Y)$. Therefore for any $S \subset G$, $\{\sigma(X) : X \subseteq S \text{ and } |X| < \infty\}$ is a subgroup of G, known as the group *generated* by S.] Since $A \cup \{b_1, b_2\}$ is finite, H also is finite. Let g be a nonzero element of H; then for some $a \in A$ and $b \in B$, $g = a + b$ whence $b = g + a \in H$. Therefore $H \setminus \{0\} = A + (H \cap B)$ whence by Remark 1, $H \setminus \{0\} = A \oplus (H \cap B)$. Since $|H \cap B| \geqslant 2$, by Proposition 2, it follows that $|A| = 1$. □

Let G be a nontrivial group and g be an element of G. If A, B are subsets of G such that $G \setminus \{g\}$ is the direct sum of A and B, then the pair (A, B) is called a *near factorization* of G. (For some basic results on this notion, see [2]; in [6, 7] by using this notion, an important class of graphs known as 'partitionable graphs' has been studied.) A near factorization (X, Y) is called *trivial* if $\min\{|X|, |Y|\} = 1$; in this case, note that for some $a, b \in G$, $\{X, Y\} = \{\{a\}, G \setminus \{b\}\}$. If G is boolean and (A, B) is a near factorization of G, then $G \setminus \{0\} = (\alpha + A) \oplus B$ where α is the element which does not belong to $A + B$; from this observation and Proposition 2, we have the following.

Corollary 4. *Let G be a finite nontrivial boolean group; then any near factorization of G is trivial.*

A natural question in connection with the above result is the following. Is there an infinite boolean group that admits a nontrivial near factorization? This is answered by Theorem 7; to derive this result, we need the following two set theoretic results. (A proof for the first one, a basic result in set theory, is given in [5].)

Theorem 5. *If A is an infinite set and B is a non-empty set, then $|A \times B| = |A \cup B| = \max\{|A|, |B|\}$.*

Lemma 6. *Any non-empty set X can be endowed with a well ordering $\preccurlyeq$ such that for all $a \in X$, $|\{x \in X : x \prec a\}| < |X|$.* (For any $x, y \in X$, when we write $x \prec y$ we mean that $x \neq y$ and $x \preccurlyeq y$.)

Proof. Let $\preccurlyeq$ be a well ordering of X. For any $a \in X$, let $S_a = \{x \in X : x \prec a\}$. If for each $a \in X$, $|S_a| < |X|$, then $\preccurlyeq$ has the required property; so assume that $\{a \in X : |S_a| = |X|\}$ is non-empty. Let m be the smallest element of this set. Since $|S_m| = |X|$, there is a bijection $\theta : X \to S_m$. Now define a relation $\preccurlyeq'$ on X as follows: for any $x, y \in X$, $x \preccurlyeq' y \iff \theta(x) \preccurlyeq \theta(y)$. It is easy to verify that $\preccurlyeq'$ is a well ordering of X with the required property. □

Theorem 7. *Let G be an infinite boolean group. Then there exist subsets A, B of G such that $|A| = |B| = |G|$ and $G \setminus \{0\} = A \oplus B$.*

Proof. Let $H = G \setminus \{0\}$. Let $\preccurlyeq$ be a well ordering of H having the property mentioned in the statement of Lemma 6. By using transfinite induction, let us construct two maps from H to itself such that for each $g \in H$ the following hold. (For any $x \in H$, its images under these mappings are denoted by x' and x'', respectively.)

(1) $g \in \{x' : x \preccurlyeq g\} + \{x'' : x \preccurlyeq g\}$.

(2) $\{x' : x \preccurlyeq g\} \cap \{x'' : x \preccurlyeq g\} = \emptyset$.

(3) For each a in H such that $a \prec g$, $a' \neq g'$ and $a'' \neq g''$.

(4) $\{x' : x \preccurlyeq g\} + \{x'' : x \preccurlyeq g\} = \{x' : x \preccurlyeq g\} \oplus \{x'' : x \preccurlyeq g\}$.

Let f be the first element of $(H, \preccurlyeq)$. Choose f', f'' arbitrarily such that $f = f' + f''$. Obviously, (1), (2), (3) and (4) hold when $g = f$; now, let h be any element in $H \setminus \{f\}$. Assume that $\{x', x'' : x \prec h\}$ is known and for each $g \in \{x \in H : x \prec h\}$, (1), (2), (3) and (4) hold.

Let $X = \{x', x'' : x \prec h\} \cup \{0, h\}$ and $Y = X + X + X + X$. Since $|\{x \in H : x \prec h\}| < |H|$, by Theorem 5, $|X| < |H|$ whence we have $|Y| \leqslant |X \times X \times X \times X| < |H|$ also, by Theorem 5. Therefore we can find some $h' \in (H \setminus Y)$. If $h \notin \{x' + y'' : x \prec h \text{ and } y \prec h\}$, taking $h'' = h + h'$, it can be verified that when $g = h$, (1), (2), (3) and (4) hold; so, suppose that for some $p, q \in \{x \in H : x \prec h\}$, $p' + q'' = h$. Now let $P = \{x', x'' : x \prec h\} \cup \{h'\}$ and $Q = P + P + P$. Using Theorem 5, it is easy to verify that $|Q| < |H|$; so, let h'' be any element in $H \setminus Q$. It is easy to verify that when $g = h$, (1), (2), (3) and (4) hold.

Thus by transfinite induction, we obtain two subsets $A := \{g' : g \in H\}$ and $B := \{g'' : g \in H\}$ of H such that for each $g \in H$, (1), (2), (3) and (4) hold. Since for every $g \in H$, (3) holds, the maps obtained are injective; therefore $|A| = |B| = |G|$. Since (2) holds for all $g \in H$, $A \cap B = \emptyset$; therefore $0 \notin A + B$. Since (1) holds for each $g \in H$, $H \subseteq A + B$. Now from the fact that (4) holds for each $g \in H$, it follows that $H = A \oplus B$. □

A result [8] on $\mathbb{Z}$, the set of all integers, which Theorems 7 and 8 are somewhat reminiscent of, is the following: *If A, B are finite subsets of $\mathbb{Z}$ such that $0 \in A \cap B$ and $A + B = A \oplus B$, then there exist infinite subsets P, Q of $\mathbb{Z}$ such that $A \subset P$, $B \subset Q$ and $\mathbb{Z} = P \oplus Q$.*

Let A, B be subsets of a boolean group G such that $|A| \geqslant |B| > 1$ and $G \setminus \{0\} = A \oplus B$. By Theorem 3, $|B| \geqslant |\mathbb{N}|$ whence it is natural to ask whether this lower bound for $|B|$ can be attained. The following result answers this question affirmatively.

Theorem 8. *Any infinite boolean group G has subsets A, B such that $\min\{|A|, |B|\} = |\mathbb{N}|$ and $G \setminus \{0\} = A \oplus B$.*

Proof. Let $H = \{0, h_1, h_2, \ldots\}$ be a countably infinite subgroup of G. (Let S be a countably infinite subset of G and $\mathfrak{F}$ be the collection of all finite subsets of S; it is a well known fact that such a collection is countable; it is easy to show that there exists a surjective map from $\mathfrak{F}$ to the subgroup generated by S; therefore this subgroup also is countable; we can take H to be this subgroup.) By using induction, let us construct three sequences $(A_n)_{n=1}^{\infty}$, $(X_n)_{n=1}^{\infty}$ and $(Y_n)_{n=1}^{\infty}$ whose terms are finite subsets of H such that for each $k \in \mathbb{N}$, $A_k \subset A_{k+1}$, $X_k \subset X_{k+1}$ and $Y_k \subset Y_{k+1}$ and (1) and (2) given below hold. Let $A_1 = \{0\}$, $X_1 = \{0, h_1\}$ and $Y_1 = \{h_1, h_2\}$. It is easy to verify that (1) and (2) given below hold when $k = 1$. Let us suppose that for some $n \in \mathbb{N}$, chains $A_1 \subset A_2 \subset \cdots \subset A_n$, $X_1 \subset X_2 \subset \cdots \subset X_n$ and $Y_1 \subset Y_2 \subset \cdots \subset Y_n$ whose terms are finite subsets of H are known such that for each $k \in \{1, 2, \ldots, n\}$, the following hold.

(1) $h_k \in A_k + X_k = A_k \oplus X_k$.

(2) $0 \notin A_k + Y_k$ and $h_k \in A_k + Y_k = A_k \oplus Y_k$.

Let us construct A_{n+1}, X_{n+1} and Y_{n+1} as follows. Let $P = Q + Q + Q + Q$ where $Q = A_n \cup X_n \cup Y_n \cup \{h_{n+1}\}$. Let a be any element in $H \setminus P$; let $A_{n+1} = A_n \cup \{a\}$. If $h_{n+1} \in A_n + X_n$, let $X_{n+1} = X_n$; otherwise let $X_{n+1} = X_n \cup \{a + h_{n+1}\}$. If $h_{n+1} \in A_n + Y_n$, let $Y_{n+1} = Y_n$; otherwise let $Y_{n+1} = Y_n \cup \{a + h_{n+1}\}$. It can be verified that (1) and (2) hold when $k = n + 1$.

Therefore by induction, we get the desired three sequences. Now let $A = \cup_{i=1}^{\infty} A_i$, $X = \cup_{i=1}^{\infty} X_i$ and $Y = \cup_{i=1}^{\infty} Y_i$. Since $0 \in A_1 + X_1$ and (1) holds for each $k \in \mathbb{N}$, it follows that $H = A \oplus X$; since (2) holds for each $k \in \mathbb{N}$, it follows that $H \setminus \{0\} = A \oplus Y$. Now let J be a subset of G such that $\{H + \alpha : \alpha \in J\}$ is the collection of all cosets of H, other than H itself. Let $B = Y \cup [\cup_{\alpha \in J}(X + \alpha)]$. Since for each $\alpha \in J$, $H + \alpha = A \oplus (X + \alpha)$ and $(H \setminus \{0\}) \cap (H + \alpha) = \emptyset$ and for any two distinct $\alpha, \beta \in J$, $(H + \alpha) \cap (H + \beta) = \emptyset$, by Remark 1 (taking $\{Y\} \cup \{X + \alpha : \alpha \in J\}$ in place of $\{B_i : i \in I\}$) we get $(A + Y) \cup [\cup_{\alpha \in J}(A + (X + \alpha))] = A \oplus B$; i.e., $(H \setminus \{0\}) \cup [\cup_{\alpha}(H + \alpha)] = A \oplus B$; i.e., $G \setminus \{0\} = A \oplus B$. By construction itself, A is infinite whereas the fact that $|Y_1| = 2$ and Theorem 3 imply that Y is infinite whence $\min\{|A|, |B|\} = |\mathbb{N}|$. □

Acknowledgements

The author is quite grateful to the referee for giving information about some related work, for pointing out some minor errors and for making some suggestions to enhance the presentation of this note.

References

[1] P. N. Balister, E. Györi and R. H. Schelp, Coloring vertices and edges of a graph by nonempty subsets of a set, *European J. Combin.* **32** (4) (2011), 533–537.

[2] D. de Caen, D. A. Gregory, I. G. Hughes and D. L. Kreher, Near-factors of finite groups, *Ars Combin.* **29** (1990), 53–63.

[3] S. Grüter, A. Holtkamp and M. Surmacs, On set colorings of complete bipartite graphs, *Australas. J. Combin.* **49** (2011), 245–254.

[4] S. M. Hegde, Set colorings of graphs, *European J. Combin.* **30** (4) (2009), 986–995.

[5] I. Kaplansky, *Set Theory and Metric Spaces*, Reprint of Second Ed., Chelsea Pub. Co., U.S.A. (2001).

[6] A. Pêcher, Partitionable graphs arising from near-factorizations of finite groups, *Discrete Math.* **269** (1–3) (2003), 191–218.

[7] A. Pêcher, Cayley partitionable graphs and near-factorizations of finite groups, 6^{th} Int. Conf. Graph Theory, *Discrete Math.* **276** (1–3) (2004), 295–311.

[8] C. Swenson, Direct sum subset decompositions of Z, *Pacific J. Math.* **53** (2) (1974), 629–633.

(Received 29 July 2011; revised 9 Dec 2011)