Distinct Matroid Base Weights and Additive Theory

Y. O. Hamidoune* I.P. da Silva†

Abstract

Let $M$ be a matroid on a set $E$ and let $w : E \to G$ be a weight function, where $G$ is a cyclic group. Assuming that $w(E)$ satisfies the Pollard’s Condition (i.e. Every non-zero element of $w(E) - w(E)$ generates $G$), we obtain a formulae for the number of distinct base weights. If $|G|$ is a prime, our result coincides with a result Schrijver and Seymour.

We also describe Equality cases in this formulae. In the prime case, our result generalizes Vosper’s Theorem.

1 Introduction

Let $G$ be a finite cyclic group and let $A, B$ be nonempty subsets of $G$. The starting point of Minkowski set sum estimation is the inequality $|A + B| \geq \min(|G|, |A| + |B| - 1)$, where $|G|$ is a prime, proved by Cauchy [2] and rediscovered by Davenport [4]. The first generalization of this result, due to Chowla [3], states that $|A + B| \geq \min(|G|, |A| + |B| - 1)$, if there is a $b \in B$ such that every non-zero element of $B - b$ generates $G$. In order to generalize his extension of the Cauchy-Davenport Theorem [11] to composite moduli, Pollard introduced in [12] the following more sophisticated Chowla type condition: Every non-zero element of $B - b$ generates $G$.

Equality cases of the Cauchy-Davenport were determined by Vosper in [16, 17]. Vosper’s Theorem was generalized by Kemperman [9]. We need only a light form of Kemperman’s result stated in the beginning of Kemperman’s paper.

We need the following combination of Chowla and Kemperman results:

**Theorem A** (Chowla [3], Kemperman [9]) Let $A, B$ be non-empty subsets of a cyclic group $G$ with $|A|, |B| \geq 2$ such that for some $b \in B$, every non-zero element of $B - b$ generates $G$. Then $|A + B| \geq |A| + |B| - 1$.

Moreover $|A + B| = |A| + |B| - 1$ if and only if $A + B$ is an arithmetic progression.

A shortly proved generalization of this result to non-abelian groups is obtained in [8].

---

*Université Pierre et Marie Curie, E. Combinatoire, Case 189, 4 Place Jussieu, 75005 Paris, France.
yha@ccr.jussieu.fr
†CELC/Universidade de Lisboa, Faculdade de Ciências, Campo Grande, edifício C6 - Piso 2, 1749-016 Lisboa, Portugal.isilva@cii.fc.ul.pt
Zero-sum problems form another developing area in Additive Combinatorics having several applications. The Erdős-Ginzburg-Ziv Theorem [6] was the starting point of this area. This result states that a sequence of elements of an abelian group $G$ with length $\geq 2|G| - 1$ contains a zero-sum subsequence of length $= |G|$.

The reader may find some details on these two areas of Additive Combinatorics in the textbooks: Nathanson [10], Geroldinger-Halter-Koch [7] and Tao-Vu [15]. More specific questions may be found in Caro’s survey paper [1].

The notion of a matroid was introduced by Whitney in 1935 as a generalization of a matrix. Two pioneer works connecting matroids and Additive Combinatorics are due to Schrijver-Seymour [14], Dias da Silva-Nathanson [5]. Recently, in [13], orientability of matroids is naturally related with an open problem on Bernoulli matrices.

Stating the first result requires some vocabulary:

Let $E$ be a finite set. The set of the subsets of $E$ will be denoted by $2^E$.

A matroid over $E$ is an ordered pair $(E, B)$ where $B \subseteq 2^E$ satisfies the following axioms:

(B1) $B \neq \emptyset$.

(B2) For all $B, B' \in B$, if $B \subseteq B'$ then $B = B'$.

(B3) For all $B, B' \in B$ and $x \in B \setminus B'$, there is a $y \in B' \setminus B$ such that $(B \setminus \{x\}) \cup \{y\} \in B$.

A set belonging to $B$ is called a basis of the matroid $M$.

The rank of a subset $A \subseteq E$ is by definition $r_M(A) := \max\{|B \cap A| : B \text{ is a basis of } M\}$. We write $r(M) = r(E)$. The reference to $M$ could be omitted. A hyperplane of the matroid $M$ is a maximal subset of $E$ with rank $= r(M) - 1$.

The uniform matroid of rank $r$ on a set $E$ is by definition $U_r(E) = (E, \binom{E}{r})$, where $\binom{E}{r}$ is the set of all $r$-subsets of $E$. Let $M$ be a matroid on $E$ and let $N$ be a matroid on $F$. We define the direct sum:

$$M \oplus N = (E \times \{0\} \cup F \times \{1\}, \{B \times \{0\} \cup C \times \{1\} : B \text{ is a base of } M \text{ and } C \text{ is a base of } N\}.$$  

Let $w : E \longrightarrow G$ be a weight function, where $G$ is an abelian group. The weight of a subset $X$ is by definition

$$X^w = \sum_{x \in X} w(x).$$

The set of distinct base weights is

$$M^w = \{B^w : B \text{ is a basis of } M\}.$$  

Suppose now $|G| = p$ is a prime number. Schrijver and Seymour proved that $|M^w| \geq \min(p, \sum_{g \in G} r(w^{-1}(g)) - r(M) + 1)$. Let $A$ and $B$ be subsets of $G$. Define $w : A \times \{0\} \cup B \times \{1\}$,
by the relation \( w(x, y) = x \). Then
\[
(U_1(A) \oplus U_1(B))^w = A + B.
\]
Applying their result to this matroid, Schrijver and Seymour obtained the Cauchy-Davenport Theorem.

Let \( x_1, \ldots, x_{2p-1} \in G \). Consider the uniform matroid \( M = U_p(E) \), of rank \( p \) over the set \( E = \{1, \ldots, 2p - 1\} \), with weight function \( w(i) = x_i \). In order to prove the Erdős-Ginzburg-Ziv Theorem \([6]\), one may clearly assume that no element is repeated \( p \) times. In particular for every \( g \in G \), \( r(w^{-1}(g)) = |w^{-1}(g)| \). Applying Schrijver and Seymour to this matroid we have:
\[
|M^w| \geq \min(|G|, \sum_{g \in G} r(w^{-1}(g)) - r(M) + 1) = \min(p, \sum_{g \in G} |w^{-1}(g)| - p + 1) = p.
\]
Thus Schrijver-Seymour result also implies the Erdős-Ginzburg-Ziv Theorem \([6]\) in a prime order.

In the present work, we prove the following result:

**Theorem 1** Let \( G \) be a cyclic group, \( M \) be a matroid on a finite set \( E \) with \( r(M) \geq 1 \) and let \( w : E \to G \) be a weight function. Assume moreover that every non-zero element of \( w(E) - w(E) \) generates \( G \). Then
\[
|M^w| \geq \min(|G|, \sum_{g \in G} r(w^{-1}(g)) - r(M) + 1),
\]
where \( M^w \) denotes the set of distinct base weights. Moreover, if Equality holds in (1) then one of the following conditions holds:

(i) \( r(M) = 1 \) or \( M^w \) is an arithmetic progression.

(ii) There is a hyperplane \( H \) of \( M \) such that \( M^w = g + (M/H)^w \), for some \( g \in G \).

If \( G \) has a prime order, then the condition on \( w(E) - w(E) \) holds trivially. In this case (1) reduces to the result of Schrijver-Seymour.

## 2 Terminology and Preliminaries

Let \( M \) be a matroid on a finite set \( E \). One may see easily from the definitions that all bases a matroid have the same cardinality. A circuit of \( M \) is a minimal set not contained in a base. A loop is an element \( x \) such that \( \{x\} \) is a circuit. By the definition bases contain no loop. The closure of a subset \( A \subseteq E \) is by definition
\[
cl(A) = \{x \in A : r(A \cup x) = r(A)\}.
\]
Note that an element \( x \in cl(A) \) if and only if \( x \in A \), or there is circuit \( C \) such \( x \in C \) and \( C \setminus \{x\} \subseteq A \).
Given a matroid $M$ on a set $E$ and a subset $A \subseteq E$. Then $B/A := \{J \setminus A : J$ is a basis of $M$ with $|B \cap A| = r(A)\}$. One may see easily that $M/A = (E \setminus A, B/A)$ is a matroid on $E \setminus A$. We say that this matroid is obtained from $M$ contracting $A$. Notice that $r_{M/A}(X) = r_M(X \cup A) - r_M(A)$.

Recall the following easy lemma:

**Lemma 2** Let $M$ be a matroid on a finite set $E$ and let $U, V$ be disjoint subsets of $E$. Then

- $M/U$ and $M/\text{cl}(U)$ have the same bases. In particular, $(M/U)^w = (M/\text{cl}(U))^w$.
- $(M/U)/V = M/(U \cup V)$.

For more details on matroids, the reader may refer to one of the text books: Welsh [18] or White [19].

For $u \in E$, we put $G_u := \{g \in G : u \in \text{cl}(w^{-1}(g))\}$.

We recall the following lemma proved by Schrijver and Seymour in [14]:

**Lemma B** Let $M$ be a matroid on a finite set $E$ and let $w : E \rightarrow G$ be a weight function. Then for every non-loop element $u \in E$,

$$(M/u)^w + G_u \subseteq M^w.$$  

**Proof.** Take a basis $B$ of $M/u$ and an element $g \in G_u$. If $g = w(u)$ then, by definition of contraction, $B \cup \{u\}$ is a basis of $M$ and $B^w + w(u) \in M^w$. If $g \neq w(u)$, there is a circuit $C$ containing $u$ such that $\emptyset \neq C \setminus \{u\} \subseteq w^{-1}(g)$. For some $v \in C \setminus \{u\}$ the subset $B \cup \{v\}$ must be a basis of $M$ otherwise $C \setminus \{v\} \subseteq \text{cl}(B)$, implying that $u \in \text{cl}(B)$, in contradiction with the assumption that $B$ is a basis of $M/u$. Therefore $(B \cup \{v\})^w = B^w + g \in M^w$. $\blacksquare$

## 3 Proof of the main result

We shall now prove our result:

**Proof of Theorem**

We first prove $\blacksquare$ by induction on the rank of $M$. The result holds trivially if $r(M) = 1$. Since $r(M) \geq 1$, $M$ contains a non-loop element. Take an arbitrary non-loop element $y$.

$$|M^w| \geq |(M/y)^w + G_y| \geq |(M/y)^w| + |G_y| - 1 \geq \sum_{g \in G} r(w^{-1}(g)) - r(M) + 1. \quad (2)$$
The first inequality follows from Lemma \[\text{a}\] the second follows by Theorem \[\text{A}\] and the third is a direct consequence of the definitions of \(M/u\) and \(G_u\). This proves the first part of the theorem.

Suppose now that Equality holds in \(\text{(1)}\) and that Condition (i) is not satisfied. In particular \(r(M) \geq 2\). Also \(|M^w| \geq 2\), otherwise \(M^w\) is a progression, a contradiction.

We claim that there exists a non-loop element \(u \in E\) such that \(|(M/u)^w| \geq 2\). Assume on the contrary that for every non-loop element \(u \in E\) we have \(|(M/u)^w| = 1\). Then every pair of bases \(B_1, B_2\) of \(M\) with \(B_1^w \neq B_2^w\) satisfies \(B_1 \cap B_2 = \emptyset\) otherwise for every \(z \in B_1 \cap B_2\), \(|(M/z)^w| \geq 2\). Now, for every \(z \in B_1\), there is \(z' \in B_2\) such that \(C = (B_1 \setminus \{z\}) \cup \{z'\}\) is a base of \(M\). For such a base \(C, B_1 \cap C \neq \emptyset, B_2 \cap C \neq \emptyset\), and we must have \(B_1^w = C^w = B_2^w\), a contradiction.

Applying the chain of inequalities proving \(\text{(2)}\) with \(y = u\). We have

\[|M^w| = |(M/u)^w + G_u| = |(M/u)^w| + |G_u| - 1.\] \(\text{(3)}\)

Note that \(w(E \setminus \{u\}) \subset w(E)\), clearly verifies the Pollard condition. If \(|G_u| \geq 2\) Theorem \(\text{A}\) implies that \(M^w\) is a progression and thus \(M\) satisfies Condition (i) of the theorem, contradicting our assumption on \(M\). We must have \(|G_u| = 1\).

Thus \(G_u = \{w(u)\}\) and \(M^w = w(u) + (M/u)^w\).

Since the translate of a progression is a progression, \(M/u\) is not a progression. By Lemma \(\text{2}\) \((M/u)\) and \(M/\text{cl}(u)\) have the same bases and thus the result holds if \(r(M) = 2\). If \(r(M) > 2\), then by the Induction hypothesis there is a hyperplane \(H\) of \(M/u\) such that \((M/u)^w = (M/u/H)^w = (M/(\text{cl}(\{u\}) \cup H))^w\), and (ii) holds. \(\blacksquare\)

**Corollary 3** \((\text{Vosper’s Theorem } \text{[16,17]})\) Let \(p\) be a prime and let \(A, B\) be subsets of \(\mathbb{Z}_p\) such that \(|A|, |B| \geq 2\).

If \(|A + B| = |A| + |B| - 1 < p\) then one of the following holds:

(i) \(c - A = (\mathbb{Z}_p \setminus B)\).

(ii) \(A\) and \(B\) are arithmetic progressions with a same difference.

**Proof.** Consider the matroid \(N = (\mathcal{U}_1(A) \oplus \mathcal{U}_1(B))\) and its weight function \(w\) defined in the Introduction. \(H = A \times \{0\}\) and \(H' = B \times \{1\}\) are the hyperplanes of \(N\) and we have \(N^w = A + B\).

If \(|N^w| = |A| + |B| - 1\) then Theorem \(\text{A}\) says that \(N\) must satisfy one of its conditions (i) or (ii). Since by hypothesis \(|A|, |B| \geq 2\) we have \(|N^w| > \max(|A|, |B|) \geq |(N/H)^w|, |(N/H')^w|\) and we conclude that \(N^w\) must be an arithmetic progression with difference \(d\). Without loss of generality we may take \(d = 1\).
Case 1. $|A + B| = p - 1$. Put $\{c\} = \mathbb{Z}_p \setminus (A + B)$. We have $c - A \subset (\mathbb{Z}_p \setminus B)$. Since these sets have the same cardinality we have $c - A = (\mathbb{Z}_p \setminus B)$.

Case 2. $|A + B| < p - 1$.

We have $|A + B + \{0, 1\}| = |A + B| + 1 = |A| + |B| < p$.

We must have $|A + \{0, 1\}| = |A| + 1$, since otherwise by the Cauchy-Davenport Theorem,

$$|A + B| + 1 = |A + B + \{0, 1\}| = |A + \{0, 1\} + B| \geq (|A| + 2) + |B| - 1 = |A| + |B| + 1,$$

a contradiction. It follows that $A$ is an arithmetic progression with difference 1. Similarly $B$ is an arithmetic progression with difference 1. ■

References

[1] Caro, Yair Zero-sum problems, a survey. *Discrete Math.* 152 (1996), no. 1-3, 93–113.

[2] A. L. Cauchy, Recherches sur les nombres, *J. Ecole Polytechnique* 9 (1813), 99–116.

[3] I. Chowla, A theorem on the addition of residue classes: applications to the number $\Gamma(k)$ in Waring’s problem, *Proc. Indian Acad. Sc.* , Section A, no. 1 (1935) 242–243.

[4] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* 10(1935), 30–32.

[5] J.A. Dias da Silva and M.B. Nathanson, "Maximal Sidon sets and matroids", *Discrete Math.* to appear.

[6] P. Erdős, A. Ginzburg and A. Ziv, A theorem in additive number theory, *Bull Res. Council Israel 10F* (1961), 41-43.

[7] A. Geroldinger, F. Halter-Koch, *Non-unique factorizations. Algebraic, combinatorial and analytic theory. Pure and Applied Mathematics (Boca Raton)*, 278. Chapman & Hall/CRC, Boca Raton, FL, 2006. xxii+700 pp.

[8] Y.O. Hamidoune, An isoperimetric method in additive theory. *J. Algebra* 179 (1996), no. 2, 622–630.

[9] J. H. B. Kemperman, On small sumsets in abeliangroups, *Acta Math.* 103 (1960), 66–88.

[10] M. B. Nathanson, *Additive Number Theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math. 165, Springer, 1996.

[11] J. M. Pollard, A generalisation of the theorem of Cauchy and Davenport, *J. London Math. Soc.* (2) 8 (1974), 460–462.

[12] J. M. Pollard, Addition properties of residue classes, *J. London Math. Soc.* (2) 11 (1975), no. 2, 147–152.
[13] I. P. F. da Silva, Orientability of Cubes, *Discrete Math.* 308 (2008), 3574-3585.

[14] A. Schrijver, P.D. Seymour, Spanning trees of different weights. *Polyhedral combinatorics* (Morristown, NJ, 1989), 281–288, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 1, Amer. Math. Soc., Providence, RI, 1990.

[15] T. Tao and V.H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105 (2006), Cambridge Press University.

[16] G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* 31 (1956), 200–205.

[17] G. Vosper, Addendum to "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* 31 (1956), 280–282.

[18] Welsh, D.J.A., *Matroid Theory*, Academic Press, London, 1976.

[19] White, N. (ed), *Theory of Matroids*, Cambridge University Press, 1986.