PLÜNNECKE'S INEQUALITY FOR DIFFERENT SUMMANDS

KATALIN GYARMATI, MÁTÉ MATOLCSI, AND IMRE Z. RUZSA

Abstract. The aim of this paper is to prove a general version of Plünnecke's inequality. Namely, assume that for finite sets A, $B_1, \dots B_k$ we have information on the size of the sumsets $A + B_{i_1} + \dots + B_{i_l}$ for all choices of indices $i_1, \dots i_l$. Then we prove the existence of a non-empty subset X of A such that we have 'good control' over the size of the sumset $X + B_1 + \dots + B_k$. As an application of this result we generalize an inequality of [1] concerning the submultiplicativity of cardinalities of sumsets.

1. Introduction

Plünnecke [4] developed a graph-theoretic method to estimate the density of sumsets $A + B$, where A has a positive density and B is a basis. The third author published a simplified version of his proof [5, 6]. Accounts of this method can be found in Malouf [2], Nathanson [3], Tao and Vu [7].

The simplest instance of Plünnecke's inequality for finite sets goes as follows.

Theorem 1.1. *Let $l < k$ be integers, A, B sets in a commutative group and write $|A| = m$, $|A + lB| = \alpha m$. There exists an $X \subset A$, $X \neq \emptyset$ such that*

$$|X + kB| \le \alpha^{k/l} |X|. \tag{1.1}$$

In [5] the case $l = 1$ of Theorem 1.1 is extended to the addition of different sets as follows.

Theorem 1.2. *Let A, $B_1, \dots, B_k$ be finite sets in a commutative group and write $|A| = m$, $|A + B_i| = \alpha_i m$, for $1 \le i \le h$. There exists an $X \subset A$, $X \neq \emptyset$ such that*

$$|X + B_1 + \dots + B_k| \le \alpha_1 \alpha_2 \dots \alpha_k |X|. \tag{1.2}$$

The aim of this paper is to give a similar extension of the general case. This extension will then be applied in Section 5 to prove a conjecture from our paper [1].

Theorem 1.3. *Let $l < k$ be integers, and let A, $B_1, \dots, B_k$ be finite sets in a commutative group G. Let $K = \{1, 2, \dots, k\}$, and for any $I \subset K$ put*

$$B_I = \sum_{i \in I} B_i,$$

$$|A| = m, \quad |A + B_I| = \alpha_I m.$$

1991 *Mathematics Subject Classification.* 11B50, 11B75, 11P70.

Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 43631, T 43623, T 49693.

Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. PF-64061, T-049301, T-047276.

Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 43623, T 42750, K 61908.

(This is compatible with the previous notation if we identify a one-element subset of K with its element.) Write

$$\beta = \left(\prod_{L \subset K, |L|=l} \alpha_L \right)^{(l-1)!(k-l)!/(k-1)!} . \tag{1.3}$$

There exists an $X \subset A$, $X \neq \emptyset$ such that

$$|X + B_K| \leq \beta |X|. \tag{1.4}$$

The following result gives estimates for the size of this set X and a more general property than (1.4), but it is weaker by a constant. We do not make any effort to estimate this constant; an estimate could be derived from the proof, but we feel it is probably much weaker than the truth.

Theorem 1.4. *Let $l < k$ be positive integers, and let A, $B_1, \dots, B_k$ be finite sets in a commutative group G. Let $K = \{1, 2, \dots, k\}$, and for any $I \subset K$ put*

$$B_I = \sum_{i \in I} B_i,$$

$$|A| = m, \quad |A + B_I| = \alpha_I m.$$

For any $J \subset K$ such that $l < j = |J| \leq k$ define

$$\beta_J = \left(\prod_{L \subset J, |L|=l} \alpha_L \right)^{(l-1)!(j-l)!/(j-1)!} . \tag{1.5}$$

(Observe that $\beta_K = \beta$ of (1.3).) Let furthermore a number ε be given, $0 < \varepsilon < 1$. There exists an $X \subset A$, $|X| > (1 - \varepsilon)m$ such that

$$|X + B_J| \leq c \beta_J |X| \tag{1.6}$$

for every $J \subset K$, $|J| \geq l$. Here c is a constant that depends on k, l and ε.

2. The case $k = l + 1$

First we prove the case $k = l + 1$ of Theorem 1.3 in a form which is weaker by a constant.

Lemma 2.1. *Let l be a positive integer, $k = l + 1$, and let A, $B_1, \dots, B_k$ be finite sets in a commutative group G. Let $K = \{1, 2, \dots, k\}$, and for any $I \subset K$ put*

$$B_I = \sum_{i \in I} B_i,$$

$$|A| = m, \quad |A + B_I| = \alpha_I m.$$

Write

$$\beta = \left(\prod_{L \subset K, |L|=l} \alpha_L \right)^{1/l} .$$

(Observe that this is the same as β of (1.3) in this particular case.) There exists an $X \subset A$, $X \neq \emptyset$ such that

$$|X + B_K| \leq c_k \beta |X| \tag{2.1}$$

with a constant c_k depending on k.

Proof. Let $H_1, \dots H_k$ be cyclic groups of order $n_1, \dots n_k$, respectively, let $H = H_1 \times H_2 \times \dots \times H_k$, and consider the group $G' = G \times H = G \times H_1 \times \dots \times H_k$. Introduce the notation $B_i' = B_i \times \{0\} \times \dots \times \{0\} \times H_i \times \{0\} \times \dots \times \{0\}$ which will be abbreviated as $B_i' = B_i \times H_i$, in the same manner as $A \times \{0\} \times \dots \times \{0\}$ will still be denoted by A.

We introduce the notation $i^* = K \setminus \{i\} = \{1, \dots, i-1, i+1, \dots, k\}$ which gives naturally $B_{i^*} = \sum_{j \neq i} B_j$ and, correspondingly, $\alpha_{i^*} = \alpha_{\{1,2,\dots,i-1,i+1,\dots k\}}$. Note that we have $\prod \alpha_{i^*} = \beta^l$.

Similarly, let $H_{i^*} = H_1 \times \dots \times H_{i-1} \times \{0\} \times H_{i+1} \times \dots \times H_k$, and $B_{i^*}' = \sum_{j \neq i} B_i' = B_{i^*} \times H_{i^*}$.

Let q be a positive integer (which should be thought of as a large number), and let $n_i = \alpha_{i^*} q$. We restrict q to values for which these are integers; such values exist, since the numbers α_L are rational. Then $|H| = n = \prod n_i = \beta^l q^k$ and $|H_{i^*}| = n/n_i = (\beta q)^l / \alpha_{i^*}$. Hence $|A + B_{i^*}'| = |A + B_{i^*}|\,|H_{i^*}| = m(\beta q)^l$ independently of i.

Now, let $B' = \bigcup_{i=1}^k B_i'$, and consider the cardinality of the set $A + (k-1)B'$. The point is that the main part of this cardinality comes from terms where the summands B_i' are all different, i.e. from terms of the form $A + B_{i^*}'$, $i = 1, 2, \dots, k$. There are k such terms, so their cardinality altogether is not greater than

$$km(\beta q)^l. \tag{2.2}$$

The rest of the terms all contain some equal summands, e.g. $A + B_1' + B_1' + B_2' + B_3' \dots + B_{k-2}'$, containing two copies of B_1', etc. The number of such terms is less than k^k, and each of them has 'small' cardinality for the simple reason that $H_i + H_i = H_i$. For instance, in the example above we have $|A + B_1' + B_1' + B_2' + B_3' \dots + B_{k-2}'| \le m|B_1|(\prod_{j=1}^{k-2} |B_j| n_j) \le c(A, B_1, \dots B_k) q^{k-2}$ where $c(A, B_1, \dots B_k)$ is a constant depending on the sets $A, B_1, \dots B_k$ but not on q. Therefore the cardinality of the terms containing some equal summands is not greater than

$$k^k c(A, B_1, \dots B_k) q^{k-2} = c(k, A, B_1, \dots B_k) q^{k-2} = o(q^l) \tag{2.3}$$

Therefore, combining (2.2)and (2.3) we conclude that

$$|A + (k-1)B'| \le 2km(\beta q)^l \tag{2.4}$$

if q is chosen large enough.

Finally, we apply Theorem 1.1 to the sets A and B' in G'. We conclude by (2.4) that there exists a subset $X \subset A$ such that

$$|X + kB'| \le |X| \left(2k(\beta q)^l\right)^{k/l} = c_k |X| (\beta q)^k. \tag{2.5}$$

Also, observe that $X + (B_K \times H) \subset X + kB'$, and $|X + (B_K \times H)| = n|X + B_K|$. From these facts and (2.5) we obtain

$$|X + B_K| \le c_k |X| (\beta q)^k / n = c_k \beta \, |X|$$

as desired. □

3. The general case

In this section we prove Theorem 1.4.

As a first step we add a bound on $|X|$ to Lemma 2.1.

Lemma 3.1. *Let $k = l + 1$, and let A, B_i, B_I, α_I and β be as in Lemma 2.1. Let a number ε be given, $0 < \varepsilon < 1$. There exists an $X \subset A$, $|X| > (1 - \varepsilon)m$ such that*

$$|X + B_K| \le c(k, \varepsilon)\beta\, |X| \tag{3.1}$$

with a constant $c(k, \varepsilon) = c_k \varepsilon^{-\frac{k}{k-1}}$ depending on k and ε.

Proof. Take the largest $X \subset A$ for which (3.1) holds. If $|X| > (1 - \varepsilon)m$, we are done. Assume this is not the case. Put $A' = A \setminus X$, and apply Lemma 2.1 with A' in the place of A. We know that $|A'| \ge \varepsilon m$. The assumptions will hold with

$$\alpha'_I = |A' + B_i| \,/\, |A'| \le |A + B_i| \,/\, |A'| \le \alpha_I/\varepsilon$$

in the place of α_I. We get a nonempty $X' \subset A'$ such that

$$|X' + B_K| \le c_k \beta' |X'|$$

with

$$\beta' = \left(\prod_{L \subset K, |L| = l} \alpha'_L \right)^{1/(k-1)} \le \beta \varepsilon^{-\frac{k}{k-1}}.$$

Then $X \cup X'$ would be a larger set, a contradiction. □

Now we turn to the general case.

Lemma 3.2. *Let $J_1, \dots, J_n$ be a list of all subsets of K satisfying $l < |J| \le k$ arranged in an increasing order of cardinality (so that $J_n = K$); within a given cardinality the order of the sets may be arbitrary.*

Let A, B_i, B_I, α_I and β_I be as in Theorem 1.4, and let the numbers $0 < \varepsilon < 1$ and $1 \le r \le n$ be given. There exists an $X \subset A$, $|X| > (1 - \varepsilon)m$ such that

$$|X + B_J| \le c(k, l, r, \varepsilon)\beta_J\, |X| \tag{3.2}$$

for every $J = J_1, \dots, J_r$ with a constant $c(k, l, r, \varepsilon)$ depending on k, l, r and ε.

Theorem 1.4 is the case $r = n$.

Proof. We shall prove the statement by induction on r. Since the sets are in increasing order of size, we have $|J_1| = l + 1$, and the claim for $r = 1$ follows from Lemma 3.1.

Now assume we know the statement for $r - 1$. We apply it with $\varepsilon/2$ in the place of ε, so we have a set $X \subset A$, $|X| > (1 - \varepsilon/2)m$ such that (3.2) holds for $J = J_1, \dots, J_{r-1}$ with $c(k, l, r - 1, \varepsilon/2)$. Write $A' = X$. This set satisfies the assumptions with

$$\alpha'_I = \alpha_I/(1 - \varepsilon/2).$$

We have $|J_r| = k'$ with some k', $l < k' \le k$. We are going to apply Lemma 3.1 with A', k' in the place of A, k and $\varepsilon/2$ in the place of ε. To this end we need bounds for $|A' + B_L|$ for every L such that $|L| = l' = k' - 1$. By the inductive assumption we know

$$|A' + B_L| \le c(k, l, r - 1, \varepsilon/2)\beta_L\, |A'|\,.$$

Lemma 3.1 gives us a set $X' \subset A'$ such that

$$|X'| > (1 - \varepsilon/2)\, |A'| > (1 - \varepsilon)m$$

and

$$|X' + B_{J_r}| \le c(l', \varepsilon/2)\beta'\, |X'|\,,$$

where

$$\beta' = \left(\prod_{L \subset J_r, |L|=l'} c(k,l,r-1,\varepsilon/2)\beta_L \right)^{1/l} = c(k,l,r-1,\varepsilon/2)\beta_{J_r}.$$

In the last step we used an identity among the quantities β_J which easily follows from their definition (1.5).

The desired set X will be this X', and the value of the constant is

$$c(k,l,r,\varepsilon) = c(l',\varepsilon/2)c(k,l,r-1,\varepsilon/2).$$

□

4. Removing the constant

In this section we prove Theorem 1.3. This is done with the help of Theorem 1.4 and the standard technique of taking direct powers of the appearing groups, sets, and corresponding digraphs. The details are as follows:

Proof of Theorem 1.3. Consider the following bipartite digraph $\mathcal{G}^1$. The first collection of vertices V_1 are the elements of set A, and the second collection of vertices V_2 are the elements of set $A + B_K$ (where V_1 and V_2 are considered disjoint; if the same element appears in both A and $A + B_K$ then we consider them in two different copies; a formal description is easy to give by introducing a further coordinate, 1 or 2, to each element, which describes the location of the element as in V_1 or V_2, but we do not want to obscure the notations). There is an edge in $\mathcal{G}^1$ from $v_1 = a_1 \in V_1$ to $v_2 = a_2 + b_{1,2} + \dots b_{k,2} \in V_2$ if and only if there exist elements $b_{1,1}, \dots b_{k,1}$ such that $a_1 + b_{1,1} + \dots b_{k,1} = a_2 + b_{1,2} + \dots b_{k,2}$. The image of a set $Z \subset V_1$ is the set $imZ \subset V_2$ reachable from Z via edges. The *magnification ratio* γ of the the graph $\mathcal{G}^1$ is $\min\{\frac{|imZ|}{|Z|}, Z \subset V_1\}$. The statement of Theorem 1.3 in these terms is that $\gamma \le \beta$, with β as defined in the theorem.

Consider now the direct power $\mathcal{G}^r = \mathcal{G}^1 \times \mathcal{G}^1 \times \cdots \times \mathcal{G}^1$ with collections of edges $V_1^r = V_1 \times \cdots \times V_1$ and $V_2^r = V_2 \times \cdots \times V_2$, and edges from $(v_1^1, v_2^1, \dots, v_r^1) \in V_1^r$ to $(v_1^2, v_2^2, \dots v_r^2) \in V_2^r$ if and only if there exist $\mathcal{G}^1$-edges in each of the coordinates. Observe that the digraph $\mathcal{G}^r$ corresponds exactly to the sets A^r and $A^r + (B_1^r + \cdots + B_k^r)$ in the direct power group G^r. Applying Theorem 1.4 in the group G^r to the sets $A^r, B_1^r, \dots B_k^r$ with any fixed ε, say $\varepsilon = 1/2$, we obtain that the magnification ration γ_r of $\mathcal{G}^r$ is not greater than $c\beta^r$. On the other hand, the magnification ratio is multiplicative (see [5] or [3]), so that we have $\gamma_r = \gamma^r$. Therefore we conclude that $\gamma \le \sqrt[r]{c}\beta$ and, in the limit, $\gamma \le \beta$ as desired. □

5. An application to restricted sums

We prove the following result, which was conjectured in [1].

Theorem 5.1. *Let $A, B_1, \dots B_k$ be finite sets in a commutative group, and $S \subset B_1 + \cdots + B_k$. We have*

$$|S + A|^k \le |S| \prod_{i=1}^{k} |A + B_1 + \cdots + B_{i-1} + B_{i+1} + \cdots + B_k| \ . \qquad (5.1)$$

Two particular cases were established in [1]; the case when S is the complete sum $B_1 + \cdots + B_k$, and the case $k = 2$. The proof in the sequel is similar to the proof of the case $k = 2$, the main difference being that we use the above generalized Plünnecke inequality, while for $k = 2$ the original was sufficient.

Proof. Let us use the notation $|A| = m$, $s = \prod_{i=1}^{k} |A+B_1+\cdots+B_{i-1}+B_{i+1}+\cdots+B_k|$. Observe that if $|S| \le (s/m^k)^{\frac{1}{k-1}}$ then

$$|S+A| \le |S||A| = |S|^{\frac{1}{k}}|S|^{\frac{k-1}{k}}m \le (|S|s)^{\frac{1}{k}} \tag{5.2}$$

and we are done.

If $|S| > (s/m^k)^{\frac{1}{k-1}}$ then we will need to use an improved version of Lemma 3.1 implied by Theorem 1.3 as follows.

Let an integer a be given, $1 \le a \le m$. We show that there exists an $X \subset A$, $|X| \ge a$ such that

$$|X+B_K| \le \frac{s^{\frac{1}{k-1}}}{m^{\frac{k}{k-1}}} + \frac{s^{\frac{1}{k-1}}}{(m-1)^{\frac{k}{k-1}}} + \cdots + \frac{s^{\frac{1}{k-1}}}{(m-a+1)^{\frac{k}{k-1}}} + (|X|-a)\frac{s^{\frac{1}{k-1}}}{(m-a+1)^{\frac{k}{k-1}}}. \tag{5.3}$$

We use induction on a. The case $a = 1$ is Theorem 1.3. Assume we know it for a; we prove it for $a+1$. The assumption gives us a set X, $|X| \ge a$ with a bound on $|X+B|$ as given by (5.3). We want to find a set X' with $|X'| \ge a+1$ and

$$|X'+B_K| \le \frac{s^{\frac{1}{k-1}}}{m^{\frac{k}{k-1}}} + \frac{s^{\frac{1}{k-1}}}{(m-1)^{\frac{k}{k-1}}} + \cdots + \frac{s^{\frac{1}{k-1}}}{(m-a)^{\frac{k}{k-1}}} + (|X'|-a-1)\frac{s^{\frac{1}{k-1}}}{(m-a)^{\frac{k}{k-1}}}. \tag{5.4}$$

If $|X| \ge a+1$, we can put $X' = X$. If $|X| = a$, we apply Theorem 1.3 to the sets $A \setminus X$, $B_1, \ldots, B_k$. This yields a set $Y \subset A \setminus X$ such that

$$|Y+B_K| \le \left(\frac{s}{(m-a)^k}\right)^{\frac{1}{k-1}} |Y|$$

and we can put $X' = X \cup Y$. This concludes the induction.

It will be useful in the sequel to have a similar statement for any real number t, $0 \le t < m$, instead of just integers a. Therefore we now show that for all $0 \le t < m$ there exists an $X \subset A$, $|X| > t$ such that

$$|X+B_K| \le (k-1)s^{\frac{1}{k-1}}\left((m-t)^{-\frac{1}{k-1}} - m^{-\frac{1}{k-1}}\right) + (|X|-t)\left(\frac{s}{(m-t)^k}\right)^{\frac{1}{k-1}}. \tag{5.5}$$

Indeed, we simply apply (5.3) with $a = [t]+1$. The right side of (5.5) can be written as $s^{\frac{1}{k-1}} \int_0^{|X|} f(x)\,dx$, where $f(x) = (m-x)^{-\frac{k}{k-1}}$ for $0 \le x \le t$, and $f(x) = (m-t)^{-\frac{k}{k-1}}$ for $t < x \le |X|$. Since f is increasing, the integral is $\ge f(0)+f(1)+\cdots+f(|X|-1)$. This exceeds the right side of (5.3) by a termwise comparison.

Let us now take $t = m - \left(\frac{s}{|S|^{k-1}}\right)^{1/k}$. Then there exists a set $X \subset A$ such that $|X| = r > t$ and (5.5) holds. For such an X we have

$$|S+X| \le |B_K+X| \le (k-1)s^{\frac{1}{k-1}}\left((m-t)^{-\frac{1}{k-1}} - m^{-\frac{1}{k-1}}\right) + (r-t)\left(\frac{s}{(m-t)^k}\right)^{\frac{1}{k-1}} \tag{5.6}$$

and the trivial bound

$$|S+(A \setminus X)| \le |S||A \setminus X| = |S|(m-r). \tag{5.7}$$

We conclude that

$$|S+A| \le |S+X| + |S+(A\setminus X)| \le (k-1)s^{\frac{1}{k-1}}\left((m-t)^{-\frac{1}{k-1}} - m^{-\frac{1}{k-1}}\right) + \tag{5.8}$$

$$(r-t)\left(\frac{s}{(m-t)^k}\right)^{\frac{1}{k-1}} + |S|((m-t)-(r-t)) = ks^{1/k}|S|^{1/k} - (k-1)\left(\frac{s}{m}\right)^{\frac{1}{k-1}} \le k(s|S|)^{1/k}$$

This inequality is nearly the required one, except for the factor k on the right hand side. We can dispose of this factor as follows (once again, the technique of direct powers). Consider the sets $A' = A^r$, $B'_j = B^r_j$ $(j = 1, \dots k)$, and $S' = S^r$ in the r'th direct power of the original group. Applying equation (5.8) to A', etc., we obtain

$$|S' + A'| \le k(s'|S'|)^{1/k}. \tag{5.9}$$

Since $|S' + A'| = |S + A|^r$, $s' = s^r$ and $|S'| = |S|^r$, we get

$$|S + A| \le k^{1/r}(s|S|)^{1/k}. \tag{5.10}$$

Taking the limit as $r \to \infty$ we obtain the desired inequality

$$|S + A| \le (s|S|)^{1/k}. \tag{5.11}$$

□

References

[1] K. Gyarmati, M.Matolcsi, I. Z. Ruzsa, *A superadditivity and submultiplicativity property for cardinalities of sumsets*, preprint, arXiv:0707.2707v1

[2] J. L. Malouf, *On a theorem of Plünnecke concerning the sum of a basis and a set of positive density*, J. Number Theory **54**.

[3] M. B. Nathanson, *Additive number theory: Inverse problems and the geometry of sumsets*, Springer, 1996.

[4] H. Plünnecke, *Eine zahlentheoretische anwendung der graphtheorie*, J. Reine Angew. Math. **243** (1970), 171–183.

[5] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Scientia, Ser. A **3** (1989), 97–109.

[6] ———, *Addendum to: An application of graph theory to additive number theory*, Scientia, Ser. A **4** (1990/91), 93–94.

[7] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, 2006.

Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364 Hungary
E-mail address: gykati@cs.elte.hu

Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364 Hungary
E-mail address: matomate@renyi.hu

Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364 Hungary
E-mail address: ruzsa@renyi.hu
E-mail address: To all authors: triola@renyi.hu