#A42 INTEGERS 15 (2015)

THE RELATIVE SIZES OF SUMSETS AND DIFFERENCE SETS

Merlijn Staps
Department of Mathematics, Utrecht University, Utrecht, The Netherlands
M.Staps@uu.nl

Received: 10/9/14, Revised: 8/23/15, Accepted: 9/26/15, Published: 10/13/15

Abstract

Let A be a finite subset of a commutative additive group Z. The sumset and difference set of A are defined as the sets of pairwise sums and differences of elements of A, respectively. The well-known inequality $\sigma(A)^{1/2} \leq \delta(A) \leq \sigma(A)^2$, where $\sigma(A) = \frac{|A+A|}{|A|}$ is the doubling constant of A and $\delta(A) = \frac{|A-A|}{|A|}$ is the difference constant of A, relates the relative sizes of the sumset and difference set of A. The exponent 2 in this inequality is known to be optimal. For the exponent $\frac{1}{2}$ this is unknown. Here, we determine the equality case of both inequalities. For both inequalities we find that equality holds if and only if A is a coset of some finite subgroup of Z or, equivalently, if and only if both the doubling constant and difference constant are equal to 1. This is a necessary condition for possible improvement of the exponent $\frac{1}{2}$. We then use the derived methods to show that Plünnecke's inequality is strict when the doubling constant is larger than 1.

1. Introduction

Let $(Z, +)$ be a commutative group. We will consider finite non-empty subsets of Z. The sumset $A + A$ and difference set $A - A$ of such a set A are defined by $A + A = \{a + b : a, b \in A\}$ and $A - A = \{a - b : a, b \in A\}$. More generally, we define

$$nA - mA = \{a_1 + \cdots + a_n - b_1 - \cdots - b_m : a_1, \ldots, a_n, b_1, \ldots, b_m \in A\}$$

for integers $m, n \geq 0$. Furthermore, we define the the doubling constant $\sigma(A) = \frac{|A+A|}{|A|}$ and difference constant $\delta(A) = \frac{|A-A|}{|A|}$ of A. It is immediately clear that $\sigma(A) \geq 1$ and $\delta(A) \geq 1$. Of interest are those sets A for which $\sigma(A)$ or $\delta(A)$ are "small". When $\sigma(A) = 1$ or $\delta(A) = 1$ we have the following result that is easily proven (for instance, see [8]):

Proposition 1. *We have $\sigma(A) = 1$ if and only if $\delta(A) = 1$ if and only if A is a coset of some finite subgroup of Z.*

It is a general result that sets with a small sumset also have a small difference set and vice versa. In particular, it turns out that the following inequality

$$\sigma(A)^{1/2} \leq \delta(A) \leq \sigma(A)^2, \tag{1}$$

relates the doubling constant $\sigma(A)$ and difference constant $\delta(A)$ of any set A [8].

The bounds in (1) are the best known bounds of this type. The exponent 2 in the upper bound cannot be improved at all [2]. Whether the exponent $\frac{1}{2}$ in the lower bound can be improved is not known. Here, we determine the equality case for both inequalities in (1). The main result of the paper is the following theorem.

Theorem 1. *We have $\sigma(A) = \delta(A)^2$ or $\delta(A) = \sigma(A)^2$ if and only if A is a coset of a finite subgroup of Z, i.e. if and only if $\sigma(A) = \delta(A) = 1$.*

In Section 2 we prove the known inequality $\delta(A) \leq \sigma(A)^2$, the upper bound in (1). This bound easily follows from Ruzsa's triangle inequality [6]. We show that equality holds if and only if $\sigma(A) = \delta(A) = 1$ (Theorem 2).

In Section 3 we determine the equality case of the lower bound in (1). We first derive an equality condition for a lemma of Petridis [1, 4] that can be used to prove the lower bound. We then determine that equality holds in the lower bound of (1) if and only if $\sigma(A) = \delta(A) = 1$ (Theorem 3). The fact that equality holds only in this case is a necessary condition for a possible improvement of the exponent $\frac{1}{2}$ in (1).

Petridis' lemma can also be used to derive Plünnecke's inequality [4]. This inequality states $|nA| \leq \sigma(A)^n|A|$ and thus gives an upper bound on the size of sumsets of the form $A + A + \cdots + A$ [5]. In Section 4 we use the results derived in section 3 to show that Plünnecke's inequality is strict unless $\sigma(A) = 1$.

We will use the symbols $\subset$, $\subsetneq$ and $\sqcup$ for inclusion, strict (proper) inclusion, and disjoint union, respectively.

2. Sets With Few Sums and Many Differences

First, we consider the inequality $\delta(A) \leq \sigma(A)^2$. Careful analysis of the standard proof using the Ruzsa triangle inequality [6] shows that the equality case of this inequality is given by those sets A for which $\delta(A) = \sigma(A) = 1$.

Theorem 2. *We have $\delta(A) \leq \sigma(A)^2$ with equality if and only if $\sigma(A) = 1$.*

Proof. The inequality $\delta(A) \leq \sigma(A)^2$ is a special case of a more general inequality

$$|K||J - L| \leq |J - K||K - L|$$

which is known as the Ruzsa triangle inequality [6]. The inequality is proven by constructing an injective map $K \times (J - L) \to (J - K) \times (K - L)$. We construct this map in the special case $(J, K, L) = (A, -A, A)$, thereby proving $|A||A - A| \leq |A + A|^2$. The obvious map $A^2 \to A - A$ given by $(a, b) \mapsto a - b$ is surjective by definition. We choose $\psi : A - A \to A^2$ to be a one-sided inverse of this map, such that we have $u - v = w$ when $\psi(w) = (u, v)$. Now consider the map $\phi : A \times (A - A) \to (A + A)^2$ defined by $\phi(a, u) = (a + b, a + c)$, where $(b, c) = \psi(u)$. This map ϕ is easily proven to be injective.

We have equality in $\delta(A) \leq \sigma(A)^2$ if and only if ϕ is also surjective. Suppose ϕ is surjective. Then for each $k \in A + A$ there exists a pair $(a, u) \in A \times (A - A)$ with $\phi(a, u) = (k, k)$. It follows that $u = 0$ and $a = k - b$, where b is the first coordinate of $\psi(0)$. We conclude that $A + A$ is contained in $b + A$, hence $|A + A| \leq |b + A| = |A|$ and $\sigma(A) \leq 1$. It follows that $\sigma(A) = 1$. Since if $\sigma(A) = 1$ we also have $\sigma(A)^2 = 1 = \delta(A)$, and the proof is complete. □

3. Sets With Few Differences and Many Sums

Now, we state and prove the lemma that is used to prove the lower bound in (1).

Lemma 1 (Petridis, [4]). *Let $K \geq 1$ and let A and X be finite subsets of Z such that $|A + X| = K|X|$ and $|A + X'| \geq K|X'|$ for all subsets X' of X. Then we have $|A + X + C| \leq K|X + C|$ for all finite subsets C of Z.*

Proof. Write $C = \{c_1, \dots, c_m\}$ and let $C_k = \{c_1, \dots, c_k\}$ for $1 \leq k \leq m$. We prove $|A + X + C_k| \leq K|X + C_k|$ by induction on k, the base case $k = 1$ being trivial. Notice that

$$A + X + C_k = (A + X + C_{k-1}) \cup ((A + X + c_k) \backslash (A + X_k + c_k)) \tag{2}$$

where $X_k = \{x \in X : A + x + c_k \subset A + X + C_{k-1}\}$. Since $A + X_k + c_k \subset A + X + C_k$, we have

$$\begin{aligned} |A + X + C_k| &\leq |A + X + C_{k-1}| + |A + X + c_k| - |A + X_k + c_k| \\ &= |A + X + C_{k-1}| + |A + X| - |A + X_k|, \end{aligned}$$

with equality if and only if the union in (2) is disjoint. Using the induction hypothesis we now find $|A + X + C_k| \leq K(|X + C_{k-1}| + |X| - |X_k|)$. Here we also used that $|A + X_k| \geq K|X_k|$, which follows from the fact that X_k is a subset of X. Notice that $X + C_k = (X + C_{k-1}) \sqcup ((X + c_k) \backslash (Y_k + c_k))$ where $Y_k = \{x \in X : x + c_k \in X + C_{k-1}\}$. Because $Y_k \subset X_k$, it follows that $|X + C_k| = |X + C_{k-1}| + |X| - |Y_k| \geq |X + C_{k-1}| + |X| - |X_k|$. Hence

$$|A + X + C_k| \leq K(|X + C_{k-1}| + |X| - |X_k|) \leq K|X + C_k|,$$

completing the induction step. □

We will next formulate conditions for a set C to satisfy $|A+X+C| = K|X+C|$ in the above lemma. In order to do so, we will strengthen the assumption $|A+X'| \geq K|X'|$ to $|A+X'| > K|X'|$ when X' is a non-empty proper subset of X. In practice, this means that one will have to replace X by the smallest non-empty subset X' of X satisfying $\frac{|A+X'|}{|X'|} = \frac{|A+X|}{|X|}$ before applying the lemma.

We will call two sets A and B *independent* if the sums $a+b$ with $a \in A$ and $b \in B$ are all different, i.e., when $|A+B| = |A||B|$. It then turns out that for a set C equality holds in Lemma 1 if and only if C contains a set Q such that $A+X$ and Q are independent and $X+C = X+Q$. Loosely speaking, this means that some elements of C (the ones in Q) introduce only new elements on both sides of $|A+X+C| = K|X+C|$, whereas the other elements of C introduce no new elements on either side of this equality. The set Q is not necessarily unique.

Lemma 2 (Equality case of Lemma 1). *Let $K \geq 1$ and let A and X be finite subsets of Z such that $|A+X| = K|X|$ and $|A+X'| > K|X'|$ for all proper non-empty subsets X' of X. Then we have $|A+X+C| \leq K|X+C|$ for all finite subsets C of Z, with equality if and only if there exists a subset Q of C such that $X+C = X+Q$ and such that $A+X$ and Q are independent.*

Proof. First suppose $X+C = X+Q$ and $A+X$ and Q are independent. This implies that X and Q are independent as well and that $A+X+C = A+X+Q$. We now have $|A+X+C| = |A+X+Q| = |A+X||Q| = K|X||Q| = K|X+Q| = K|X+C|$.

Now suppose $|A+X+C| = K|X+C|$. Then we have equality in Lemma 1, and thus for each $1 \leq k \leq m$ the following conditions are satisfied:

- we have $(A+X+C_{k-1}) \cap ((A+X+c_k) \setminus (A+X_k+c_k)) = \emptyset$ (since the union in (2) is disjoint);
- we have $X_k = \emptyset$ or $X_k = X$ (since we have equality in $|A+X_k| \geq K|X_k|$);
- we have $Y_k = X_k$ (since we have equality in $|Y_k| \leq |X_k|$).

When $X_k = \emptyset$ it follows from the first condition that $(A+X+C_{k-1}) \cap (A+X+c_k) = \emptyset$, hence $A+X+C_k = (A+X+C_{k-1}) \sqcup (A+X+c_k)$ and $(X+C_k) = (X+C_{k-1}) \sqcup (X+c_k)$. When $X_k = X$ we have $Y_k = X$, hence $X+c_k \subset X+C_{k-1}$. It now follows that $X+C_k = X+C_{k-1}$ and $A+X+C_k = A+X+C_{k-1}$. Let Q be the subset of C consisting of those c_k for which $X_k = \emptyset$. Then we have $X+C = \bigsqcup_{q \in Q}(X+q)$, and thus $X+C = X+Q$. Furthermore, we have

$$|A+X+Q| = |A+X+C| = \left| \bigsqcup_{q \in Q} (A+X+q) \right| = |A+X||Q|,$$

showing that $A+X$ and Q are independent. $\square$

We are now ready to prove the inequality $\sigma(A) \leq \delta(A)^2$ and to determine the equality case.

Theorem 3. *We have $\sigma(A) \leq \delta(A)^2$ with equality if and only if $\sigma(A) = 1$.*

Proof. Choose the smallest possible non-empty subset $X \subset -A$ minimizing $\frac{|A+X|}{|X|}$. Let $K = \frac{|A+X|}{|X|} \leq \frac{|A-A|}{|-A|} = \delta(A)$. Then the condition of lemma 2 is satisfied, hence for $C = A$ we have $|2A| \leq |2A + X| \leq K|X + A| = K^2|X| \leq K^2|A| \leq \delta(A)^2|A|$, showing that $\sigma(A) \leq \delta(A)^2$. We have equality if there exists a subset $Q \subset A$ such that $X + A = X + Q$ and such that $A + X$ and Q are independent. In that case, it follows that $\delta(A)|X + A| = K|X + A| = |2A + X| = |A + X + Q| = |A + X||Q|$; hence $|Q| = \delta(A)$. Since $A + X$ and Q are independent, the sets A and Q are independent. Since Q is a subset of A, this implies that $|Q| = 1$. Thus we have $\delta(A) = |Q| = 1$, implying that $\sigma(A) = 1$ as well (Proposition 1). When $\sigma(A) = 1$ we have $\sigma(A) = 1 = \delta(A)^2$. □

It remains unknown whether the inequality $\sigma(A) \leq \delta(A)^C$ is true for some exponent $C < 2$. Using explicit constructions, Penman and Wells have shown that C cannot be decreased below $\frac{\log(32/5)}{\log(26/5)} = 1.12594$ [3].

4. A Strict Version of Plünnecke's inequality

Lemma 1 can be used to prove Plünnecke's Inequality [4, 7]. Here we use lemma 2 to show that Plünnecke's inequality is strict except when $\sigma(A) = 1$.

Theorem 4 (Strict Plünnecke inequality). *Suppose that $\sigma(A) > 1$. Then we have $|nA| < \sigma(A)^n|A|$ for all $n \geq 1$.*

Proof. The statement is trivially true for $n = 1$, so suppose that $n \geq 2$. Choose the smallest possible non-empty subset $X \subset A$ minimizing $\frac{|A+X|}{|X|}$. Then we have $K = \frac{|A+X|}{|X|} \leq \frac{|A+A|}{|A|} \leq \sigma(A)$. Applying lemma 2 with $C = (n-1)A$, we find that

$$|nA + X| \leq K|(n-1)A + X|.$$

Applying lemma 2 repeatedly, it follows that $|nA + X| \leq K^n|X|$. This yields

$$|nA| \leq |nA + X| \leq K^n|X| \leq K^n|A| \leq \sigma(A)^n|A|.$$

Let us show that we cannot have equality. If we would have equality, we would have equality in $|2A + X| \leq K|A + X|$. This in turn implies the existence of a $Q \subset A$ such that $|2A + X| = |A + X + Q| = |A + X||Q|$, hence $|Q| = K$. Furthermore, we have $|Q| = 1$ since $A + X$ and Q are independent. It follows that $\sigma(A) = K = 1$, contradicting the assumption $\sigma(A) > 1$. □

In other words, equality holds in Plünnecke's inequality if and only if A is a coset of some finite subgroup of Z.

Acknowledgment. I would like to thank Prof. Gunther Cornelissen for helpful discussions and suggestions.

References

[1] Gowers, T. A new way of proving sumset estimates (2011). `http://gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/`.

[2] Hennecart, F., Robert, G., and Yudin, A. On the number of sums and differences. Structure theory of set addition. *Asterisque* **258** (1999), 173-178.

[3] Penman, D., and Wells, M. On sets with more restricted sums than differences. *Integers* **13** (2013), A57.

[4] Petridis, G. New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica* **32** (2011), 721-733.

[5] Plünnecke, H. *Eigenschaften und Abschätzungen von Wirkingsfunktionen*, BMwF-GMD-22 Gesellschaft für Mathematik und Datenverarbeitung, Bonn (1969).

[6] Ruzsa, I.Z. Sums of finite sets. In: *Number Theory: New York Seminar*. Chudnovsky, D.V., Chudnovsky, G.V., and Nathanson, M.B. Springer-Verlag (1996), 281-293.

[7] Sanders, T. The structure theory of set addition revisited. *Bull. Amer. Math. Soc.* **50** (2013), 93-127.

[8] Tao, T. and Vu, V. *Additive Combinatorics*. Cambridge University Press (2006).