DENSITY AND SUM SETS

R.C. VAUGHAN

This is an exposition of two of the standard theorems on density and sum sets, namely the Cauchy–Davenport–Chowla theorem and Mann's theorem. There are various proofs of these theorems and their many variations in the literature. The purpose here is to give short and simple proofs of both theorems the core of which are based on a common and generic idea. This is that one or more elements can be removed from one of the sets and their translates added to the other in such a way that the orginal sum set is contained in the new sum set, and so an induction on the number of elements of one of the sets can be established.

Given a positive integer q and a collection $\mathcal{A}$ of residue classes modulo q, its local density $\rho = \rho(\mathcal{A})$ modulo q is defined by $\rho = q^{-1}\mathrm{card}(\mathcal{A})$.

Theorem 1 (Cauchy–Davenport–Chowla)**.** *Suppose that q is a positive integer, that $\mathcal{A}$ and $\mathcal{B}$ are sets of residue classes modulo q of local density modulo q, α and β respectively, that $0 \in \mathcal{B}$ and that every non–zero residue class in $\mathcal{B}$ is a reduced residue class modulo q. Then*

$$\rho(\mathcal{A}+\mathcal{B}) \geq \min(1, \alpha+\beta-1/q).$$

This is best possible, as is seen by the example $\mathcal{A} = \{0, 1, \dots, r-1\}$, $\mathcal{B} = \{0, 1, \dots, s-1\}$, $\mathcal{A}+\mathcal{B} = \{0, 1, \dots, r+s-2\}$ when $r+s-1 \leq q$ with q prime.

Proof. If $\alpha = 1$, then the conclusion is trivial. Thus we may suppose that $r = q\alpha = \mathrm{card}(\mathcal{A}) <$ q. We now proceed by induction on $s = q\beta = \mathrm{card}(\mathcal{B})$. When $s = 1$ the conclusion is immediate. Thus it remains to consider the case $s > 1$ (and $\alpha < 1$), and we may assume the conclusion holds for *all* α when $card\mathcal{B} < s$. When $b \in \mathcal{B}\backslash\{0\}$ we cannot have $a + b \in \mathcal{A}$ for every $a \in \mathcal{A}$, for otherwise

$$\sum_{a\in\mathcal{A}} a + br \equiv \sum_{a'\in\mathcal{A}} a' \pmod q \tag{0.1}$$

whence $br \equiv 0 \pmod q$ and it would follow that $(b, q) > 1$. Hence there are $a_0 \in \mathcal{A}$, $b_0 \in \mathcal{B}$ such that $a_0 + b_0 \notin \mathcal{A}$.

Let

$$\mathcal{A}' = \mathcal{A} \cup \{a_0 + b : b \in \mathcal{B}, a_0 + b \notin \mathcal{A}\} \tag{0.2}$$

and

$$\mathcal{B}' = \{b : b \in \mathcal{B}, a_0 + b \in \mathcal{A}\}. \tag{0.3}$$

Then $\mathrm{card}(\mathcal{A}') + \mathrm{card}(\mathcal{B}') = \mathrm{card}(\mathcal{A}) + \mathrm{card}(\mathcal{B}) = \mathrm{r} + \mathrm{s}$ and $1 \leq \mathrm{card}(\mathcal{B}') \leq \mathrm{s} - 1$. Hence, by the inductive hypothesis

$$\rho(\mathcal{A}'+\mathcal{B}') \geq \min\big(1, \rho(\mathcal{A}') + \rho(\mathcal{B}') - 1/q\big) = \min(1, \alpha+\beta-1/q). \tag{0.4}$$

Suppose that $a' \in \mathcal{A}'$ and $b' \in \mathcal{B}'$. When $a' \in \mathcal{A}$ we have $a' + b' \in \mathcal{A} + \mathcal{B}$. When $a' \notin \mathcal{A}$ there is a $b" \in \mathcal{B}$ such that $a' = a_0 + b"$ and so $a' + b' = a_0 + b" + b' = a_0 + b' + b"$. Moreover $a_0 + b' \in \mathcal{A}$, so $a' + b' \in \mathcal{A} + \mathcal{B}$ in this case also. Hence $\mathcal{A}' + \mathcal{B}' \subset \mathcal{A} + \mathcal{B}$ and the theorem follows. □

For convenience, given $\mathcal{A} \subset \mathbb{Z}$ we define

$$A(n) = \mathrm{card}\{\mathrm{a} \in \mathcal{A} : 1 \le \mathrm{a} \le \mathrm{n}\}. \tag{0.5}$$

Then the Schnirel'man density $\sigma(\mathcal{A})$ of a set of integers $\mathcal{A}$ is given by

$$\sigma(\mathcal{A}) = \inf_{n \ge 1} n^{-1} A(n) \tag{0.6}$$

Theorem 2 (Mann)**.** *Suppose that $\mathcal{A}$ and $\mathcal{B}$ are sets of integers of Schnirel'man density α and β respectively and that $0 \in \mathcal{A} \cap \mathcal{B}$. Then*

$$\sigma(\mathcal{A} + \mathcal{B}) \ge \min(1, \alpha + \beta).$$

Proof. The case $\alpha + \beta \ge 1$ can be disposed of by a simple box argument. For a given $n \in \mathbb{N}$ consider the $A(n) + B(n) + 2$ numbers objects a with $0 \le a \le n$ and $a \in \mathcal{A}$ and $n - b$ with $0 \le b \le n$ and $b \in \mathcal{B}$. Since $A(n) + B(n) + 2 \ge \alpha n + \beta n + 2 \ge n + 2$, one of the $n + 1$ numbers m with $0 \le m \le n$ must be both an a and an $n - b$. Hence $n = a + b$. Thus $\mathbb{N} \subset \mathcal{A} + \mathcal{B}$ and the theorem follows.

Henceforward we suppose that

$$\alpha + \beta < 1 \tag{0.7}$$

If $\alpha\beta = 0$, then the conclusion follows from the observation that $\mathcal{A} \subset \mathcal{A}+\mathcal{B}$ and $\mathcal{B} \subset \mathcal{A}+\mathcal{B}$. Hence we may suppose that $\alpha\beta > 0$ and therefore

$$1 \in \mathcal{A} \cap \mathcal{B}. \tag{0.8}$$

It suffices to prove that for $n \in \mathbb{N}$ we have

$$\mathrm{card}\{\mathrm{m} : 1 \le \mathrm{m} \le \mathrm{n}, \mathrm{m} \in \mathcal{A} + \mathcal{B}\} \ge \mathrm{A(n)} + \mathrm{B(n)}. \tag{0.9}$$

Suppose first that $a + b \in \mathcal{A}$ whenever $a \in \mathcal{A}$, $b \in \mathcal{B}$ and $a + b \le n$. Then for $m = 1, 2, ..., n - 1$ we have $1 \in \mathcal{A}$ and if $m \in \mathcal{A}$, then $m + 1 \in \mathcal{A}$. Hence $A(n) = n$ and since $\mathcal{A} \subset \mathcal{A} + \mathcal{B}$ the desired result follows.

Thus we may suppose that there are $a_0 \in \mathcal{A}$, $b_0 \in \mathcal{B}$ such that $a_0 \ge 1$, $b_0 \ge 1$, $a_0+b_0 \le n$ and $a_0 + b_0 \notin \mathcal{A}$. Let

$$s = B(n). \tag{0.10}$$

Then by (0.8) we may assume that $s \ge 1$. We proceed by induction on $s = 1, \dots, n$.

Let

$$\mathcal{A}' = \mathcal{A} + \{a_0 + b : b \in \mathcal{B}, a_0 + b \le n, a_0 + b \notin \mathcal{A}\} \tag{0.11}$$

$$\mathcal{B}' = \mathcal{B} \backslash \{b \in \mathcal{B} : a_0 + b \le n \text{ and } a_0 + b \notin \mathcal{A}\}. \tag{0.12}$$

Suppose that $a' \in \mathcal{A}'$ and $b' \in \mathcal{B}'$. When $a' \in \mathcal{A}$ we have $a' + b' \in \mathcal{A} + \mathcal{B}$. When $a' \notin \mathcal{A}$ there is a $b" \in \mathcal{B}$ such that $a' = a_0 + b"$ and so $a' + b' = a_0 + b" + b' = a_0 + b' + b"$. Moreover $a_0 + b' \in \mathcal{A}$, so $a' + b' \in \mathcal{A} + \mathcal{B}$ in this case also. Hence

$$A'(n) + B'(n) = A(n) + B(n), \tag{0.13}$$

$\mathcal{A}' + \mathcal{B}' \subset \mathcal{A} + \mathcal{B}$ and

$$\mathrm{card}\{\mathrm{m} : 1 \leq \mathrm{m} \leq \mathrm{n}, \mathrm{m} \in \mathcal{A} + \mathcal{B}\} \geq \mathrm{card}\{\mathrm{m} : 1 \leq \mathrm{m} \leq \mathrm{n}, \mathrm{m} \in \mathcal{A}' + \mathcal{B}'\} \tag{0.14}$$

We also have $B'(n) \leq s - 1$. If $B'(n) = 0$ (and this includes the case $s = 1$, the initial case of the inductive argument), then $\mathrm{card}\{\mathrm{m} : 1 \leq \mathrm{m} \leq \mathrm{n}, \mathrm{m} \in \mathcal{A}' + \mathcal{B}'\} = \mathrm{card}\{\mathrm{m} : 1 \leq \mathrm{m} \leq \mathrm{n}, \mathrm{m} \in \mathcal{A}'\} \geq \mathrm{A}'(\mathrm{n}) = \mathrm{A}'(\mathrm{n}) + \mathrm{B}'(\mathrm{n})$ and with (0.13) completes the proof in this case.

If $B'(n) \geq 1$, then on the inductive hypothesis for s we have

$$\mathrm{card}\{\mathrm{m} : 1 \leq \mathrm{m} \leq \mathrm{n}, \mathrm{m} \in \mathcal{A}' + \mathrm{B}'\} \geq \mathrm{A}'(\mathrm{n}) + \mathrm{B}'(\mathrm{n}) \tag{0.15}$$

once more and again with (0.13) this completes the proof.

□

Halberstam, H. & Roth, K. F. [1966], *Sequences*, Oxford University Press, Oxford, 1966

RCV: Department of Mathematics, McAllister Building, Pennsylvania State University, University Park, PA 16802-6401, U.S.A.

E-mail address: rvaughan@math.psu.edu