ACTA ARITHMETICA
164.2 (2014)

On the sum of dilations of a set

by

Antal Balog (Budapest) and George Shakan (Laramie, WY)

1. Introduction. Let A and B be finite sets of real numbers. The *sumset* and the *product set* of A and B are defined by

$$A+B=\{a+b : a\in A,\, b\in B\}, \qquad A\cdot B=\{ab : a\in A,\, b\in B\}.$$

For $d>0$ the *dilation* of A by d is defined by

$$d\cdot A=\{d\}\cdot A=\{da : a\in A\},$$

while for any real number x, the *translation* of A by x is defined by

$$x+A=\{x\}+A=\{x+a : a\in A\}.$$

The Erdős–Szemerédi sum-product conjecture [7] claims that for any finite subset of the positive integers, either the sumset $A+A$ or the product set $A\cdot A$ must be big; more precisely

$$\max\{|A+A|,|A\cdot A|\}\gg |A|^{2-\epsilon}$$

for any $\epsilon>0$. The best result in this direction, due to Solymosi [11], is the above bound with the weaker exponent $4/3-\epsilon$. Another realization of this phenomenon is that if an expression of sets uses both addition and multiplication, then it produces a big set. For example,

$$|A\cdot A+A|\gg |A|^{3/2}, \qquad |(A+A)\cdot A|\gg |A|^{3/2}$$

both come from the method of Elekes [6] using incidence geometry, notably the Szemerédi–Trotter Theorem (see the book of Tao and Vu [12]). Improving the exponent in these bounds is a challenging problem, and $2-\epsilon$ is certainly expected. The problem seems easier for more variables, for example

$$|A\cdot A+A\cdot A+A\cdot A+A\cdot A|\geq \tfrac{1}{2}|A|^2,$$

as proved by the first author [1]. Changing the role of addition and multiplication in most of these expressions does not change the results or our expectation dramatically.

2010 *Mathematics Subject Classification*: 11B13, 05B10, 11B30.
Key words and phrases: additive combinatorics, sumset estimates.

DOI: 10.4064/aa164-2-5

However, the two-variable expressions $A\cdot(1+A)$ and $p\cdot A+q\cdot A$ are exceptions, because translation seriously alters multiplicative behavior, while dilation seems rather harmless. It is a beautiful consequence of the incidence geometry that $A\cdot(1+A)$ is big; for example, Jones and Roche-Newton [9] proved

$$|A\cdot(1+A)|\gg|A|^{24/19-\epsilon}.$$

On the other hand, for $q>p\geq 1$ relatively prime integers and $X=\{1,\dots,|X|\}$, obviously $p\cdot X+q\cdot X\subset\{p+q,\dots,(p+q)|X|\}$, that is,

$$|p\cdot X+q\cdot X|\leq(p+q)|X|-(p+q-1). \tag{1}$$

Bukh [2] proved that for coprime integers $\lambda_1,\dots,\lambda_k$ one has

$$|\lambda_1\cdot A+\cdots+\lambda_k\cdot A|\geq(\lambda_1+\cdots+\lambda_k)|A|-o(|A|).$$

Our main result says $|p\cdot A+q\cdot A|\geq(p+q)|A|-C_{p,q}$. Cilleruelo, Hamidoune and Serra showed this for $p=1$ and q prime, and this result was extended by Du, Cao, and Sun [5] when q is a prime power or the product of two primes. Hamidoune and Rué [8] solved the case of $p=2$ and q prime, and this result was extended by Ljujic [10] to $p=2$ and q a power of an odd prime or the product of two odd primes. While it is certainly plausible that $|\lambda_1\cdot A+\cdots+\lambda_k\cdot A|\geq(\lambda_1+\cdots+\lambda_k)|A|-C$ for some C that only depends on $\lambda_1,\dots,\lambda_k$, our method seems to only handle the case where $k=2$.

We will confine ourselves to sets of integers. Transforming our result to the case when p, q are rational and also $A\subset\mathbb{Q}$ is an obvious task by clearing denominators. As Sean Eberhard pointed out, there is a "Freiman isomorphism" (see [12, Definition 5.21]) of arbitrarily large order from any finite set of real numbers to a finite set of integers (see [12, Lemma 5.25]), implying our result for $1\leq p<q$ being integers, and A being a finite set of reals. To estimate $|A+\alpha\cdot A|$ is a more subtle question when $\alpha>1$ is a real number. If α is algebraic then the linear behavior is still true, but the best multiplicative constant is not known. If α is transcendental then $|A+\alpha\cdot A|$ grows faster than linearly.

THEOREM 1.1. *For any relatively prime integers $1\leq p<q$ and for any finite $A\subset\mathbb{Z}$ one has*

$$|p\cdot A+q\cdot A|\geq(p+q)|A|-(pq)^{(p+q-3)(p+q)+1}.$$

Note that the multiplicative constant $p+q$ is best possible as the above example (1) shows. On the other hand we do not attempt to get the best additive constant, and improvements in that respect are very probable. For example, our method gives $q2^{(q-2)(q+1)}$ for the case $p=1$, or simply $q!$ for the case $p=1$, q a prime. We cannot even decide the true size of the best additive constant. The following example shows that, even in the special case $p=1$, the additive constant is not polynomial in q. It also suggests that

possibly a better constant can be proved for all sufficiently large sets A, avoiding such pathological cases.

For t a positive integer and $0 \le a < q/2$ also an integer, let

$$A := \{a_0 + a_1 q + a_2 q^2 + \cdots + a_t q^t : 0 \le a_i < a,\ a_i \in \mathbb{Z}\}.$$

If we set $a = \lfloor \sqrt{q} \rfloor$ and $t = \lfloor \log_2 \sqrt{q} \rfloor$, it is easy to see that $|A| = a^{t+1}$ and $|A + q \cdot A| = a^2(2a-1)^t \le a 2^t |A| \le q|A|$. Thus $|A + q \cdot A| \le (q+1)|A| - (\sqrt{q}-1)^{\log_2(\sqrt{q}-1)}$. The authors are thankful to Imre Ruzsa for drawing their attention to the present problem, as well as for pointing out this example.

It is obvious that the condition $(p, q) = 1$ cannot be dropped from Theorem 1.1 without modifying the multiplicative constant $p+q$ to $(p+q)/(p, q)$, however its use in the proof is somewhat hidden; we will emphasise it in due course.

2. Preliminaries. For nonempty finite subsets of the real numbers $A = \{a_1 < \cdots < a_r\}$ and $B = \{b_1 < \cdots < b_s\}$, we see that

$$|A + B| \ge |A| + |B| - 1 \tag{2}$$

by observing that

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_r + b_1 < a_r + b_2 < \cdots < a_r + b_s.$$

We extend this argument in the following lemma.

LEMMA 2.1. *Let A be a nonempty subset of the real numbers and $q > p \ge 1$. Then*

$$|p \cdot A + q \cdot A| \ge 3|A| - 2.$$

Proof. Let $A = \{a_1, \ldots, a_n\}$ where $a_1 < \cdots < a_n$. Then

$$\begin{aligned} pa_1 + qa_1 < pa_2 + qa_1 < pa_1 + qa_2 < pa_2 + qa_2 < pa_3 + qa_2 < \cdots \\ < pa_{n-1} + qa_n < pa_n + qa_n. \end{aligned}$$

For each $1 \le i \le n-1$ there are three elements in the previous list, $pa_i + qa_i < pa_{i+1} + qa_i < pa_i + qa_{i+1}$, and one more element $pa_n + qa_n$. So $|p \cdot A + q \cdot A| \ge 3(n-1) + 1 = 3|A| - 2$. ∎

It is worth noting that this gives $|A + 2 \cdot A| \ge 3|A| - 2$, which settles Theorem 1.1 in the case $p = 1$, $q = 2$. This is best possible by (1).

The main purpose of this section is to give a short proof of $|A + 3 \cdot A| \ge 4|A| - 4$ in order to introduce some of the main ideas of the proof of the general theorem. This was proved by Cilleruelo, Silva, and Vinuesa [4] using different methods, and they were able to classify the sets where equality holds. The method we use requires A to be a set of integers, and can be extended to a general lower bound for all cases with $q \ge 3$, though we leave this extension to the interested reader. The bound $4|A| - 4$ is also best possible, as follows from the next construction. Let $0 \le d < q \le n$ be integers

and let $X := \{i + xq : 0 \le i \le d,\ 0 \le x < n\}$. Note that $|X| = (d+1)n$. It is easy to check that $X + q \cdot X$ is precisely the set of integers in the interval $[0, \dots, (q+1)(d+(n-1)q)]$ that are equivalent to one of $\{0, \dots, d\}$ modulo q. It follows that $|X + q \cdot X| = (q+1)|X| - (d+1)(q-d)$, and the optimal choice $d = \lfloor (q-1)/2 \rfloor$ gives $|X + q \cdot X| = (q+1)|X| - \lfloor \frac{q+1}{2} \rfloor \lceil \frac{q+1}{2} \rceil$.

We remark that one can use Theorem 1.1 and the methods of [3] to show that for $|A| \ge (q-1)^2 q^{q^2-q+1}$, one has $|A + q \cdot A| \ge (q+1)|A| - \lfloor \frac{q+1}{2} \rfloor \lceil \frac{q+1}{2} \rceil$. Furthermore, these methods can be used to show X is a unique set, up to an affine transformation, where equality holds.

THEOREM 2.2. *Let A be a finite subset of the integers. Then $|A + 3 \cdot A| \ge 4|A| - 4$.*

Proof. If $|A| = 1$ the result is trivial. If $|A| = 2$ the result follows from Lemma 2.1. We use induction on the size of $|A|$. Assume that $|A| > 2$ and $|X + 3 \cdot X| \ge 4|X| - 4$ for any proper subsets X of A.

Translation and dilation do not change $|A + 3 \cdot A|$, so we may translate A so that 0 is the smallest element and then dilate A until it intersects at least two residue classes modulo 3. Let

$$A = \bigcup_{j=1}^{r} A_j, \qquad A_j = a_j + 3 \cdot B_j, \qquad B_j \ne \emptyset,\ 0 \le a_j < 3.$$

This union is disjoint and moreover the sets $A_j + 3 \cdot A$ are disjoint. Thus from the obvious fact (2) it follows that

$$|A + 3 \cdot A| = \sum_{j=1}^{r} |A_j + 3 \cdot A| \ge \sum_{j=1}^{r} (|A_j| + |A| - 1) = (r+1)|A| - r. \tag{3}$$

We say that A is *fully distributed modulo* 3 (FD mod 3) if A intersects all three residue classes modulo 3. By (3), if A is FD mod 3 then $|A + q \cdot A| \ge 4|A| - 3 > 4|A| - 4$, and the theorem follows.

Thus we may assume that A intersects exactly two residue classes modulo 3, so $A = A_1 \cup A_2$. Then

$$A + 3 \cdot A = (A_1 + 3 \cdot A) \cup (A_2 + 3 \cdot A)$$

where the union is disjoint and

$$|A_1 + 3 \cdot A| = |A_1 + 3 \cdot A_1| + |(A_1 + 3 \cdot A_2) \setminus (A_1 + 3 \cdot A_1)|,$$
$$|A_2 + 3 \cdot A| = |A_2 + 3 \cdot A_2| + |(A_2 + 3 \cdot A_1) \setminus (A_2 + 3 \cdot A_2)|.$$

Suppose now that

$$|(A_1 + 3 \cdot A_2) \setminus (A_1 + 3 \cdot A_1)| < |A_2|.$$

After a translation by $-a_1$, dilation by $\frac{1}{3}$, and another translation by $-a_1$,

we obtain

$$|(a_2 - a_1 + B_1 + 3 \cdot B_2) \setminus (B_1 + 3 \cdot B_1)| < |B_2|.$$

Therefore for any $x \in B_1$, there is a $y \in B_2$ such that $a_2 - a_1 + x + 3y \in B_1 + 3 \cdot B_1$ and so there is an $x' \in B_1$ such that $a_2 - a_1 + x \equiv x' \pmod 3$. We may repeat this for x' in place of x, so there is an $x'' \in B_1$ such that $a_2 - a_1 + x' \equiv x'' \pmod 3$. Since $(a_2 - a_1, 3) = 1$, we see that x, x', x'' are incongruent modulo 3. Thus B_1 is FD mod 3 and it follows from (3) that

$$|A_1 + 3 \cdot A_1| = |B_1 + 3 \cdot B_1| \geq 4|B_1| - 3 = 4|A_1| - 3.$$

A symmetric argument shows that if $|(A_2 + 3 \cdot A_1) \setminus (A_2 + 3 \cdot A_2)| < |A_1|$ then B_2 is FD mod 3 and $|A_2 + 3 \cdot A_2| \geq 4|A_2| - 3$.

Case 1: *B_1 and B_2 are both FD mod 3.* We can always find two more elements in the (disjoint) union of $(A_1 + 3 \cdot A_2) \setminus (A_1 + 3 \cdot A_1)$ and $(A_2 + 3 \cdot A_1) \setminus (A_2 + 3 \cdot A_2)$. Consider the maximum element of A; let it be in A_2 and call it M. Let $u \in A_1$ be maximal. Then it is clear that $u + 3M \in (A_1 + 3 \cdot A_2) \setminus (A_1 + 3A_1)$. A symmetric argument works if $M \in A_1$. Call this new element z_1. Similarly let $m \in A$ be minimal and assume $m \in A_1$. Then let $v \in A_2$ be minimal. It is clear that $v + 3m \in (A_2 + 3 \cdot A_1) \setminus (A_2 + 3 \cdot A_2)$. A symmetric argument works if $m \in A_2$. Call this new element z_2. Since $v + 3m \leq M + 3m < m + 3M \leq u + 3M$, we have $z_1 \neq z_2$ and

$$\{z_1, z_2\} \subset (A_1 + 3 \cdot A_2) \setminus (A_1 + 3 \cdot A_1) \cup (A_2 + 3 \cdot A_1) \setminus (A_2 + 3 \cdot A_2).$$

Then, by (3),

$$\begin{aligned} |A + 3 \cdot A| &\geq |A_1 + 3 \cdot A_1| + |A_2 + 3 \cdot A_2| + |\{z_1, z_2\}| \\ &\geq 4|A_1| - 3 + 4|A_2| - 3 + 2 = 4|A| - 4. \end{aligned}$$

Case 2: *B_1 and B_2 are both non-FD mod 3.* Then $|(A_1 + 3 \cdot A_2) \setminus (A_1 + 3 \cdot A_1)| \geq |A_2|$ and $|(A_2 + 3 \cdot A_1) \setminus (A_2 + 3 \cdot A_2)| \geq |A_1|$ and we see from Lemma 2.1 that

$$\begin{aligned} |A + 3 \cdot A| &= |A_1 + 3 \cdot A| + |A_2 + 3 \cdot A| \\ &\geq 3|A_1| - 2 + |A_2| + 3|A_2| - 2 + |A_1| = 4|A| - 4. \end{aligned}$$

Case 3: *One of B_1 and B_2 is FD mod 3 and the other is not.* We may assume, without loss of generality, that B_1 is FD mod 3 while B_2 is not. This is the only case when we use the induction hypothesis. Since B_1 is FD mod 3 we have $|A_1| \geq 3$, and since B_2 is not FD mod 3 we have $|(A_2 + 3 \cdot A_1) \setminus (A_2 + 3 \cdot A_2)| \geq |A_1| \geq 3$. By induction and (3),

$$|A + 3 \cdot A| = |A_1 + 3 \cdot A| + |A_2 + 3 \cdot A| \geq 4|A_1| - 3 + 4|A_2| - 4 + |A_1| \geq 4|A| - 4.$$

In all cases we obtain $|A + 3 \cdot A| \geq 4|A| - 4$, thus completing the induction. ∎

3. Proof of Theorem 1.1. Translation and dilation do not change $|p \cdot A + q \cdot A|$.

Suppose the residue classes modulo p that intersect A are $p_1, \dots, p_r$, and the residue classes modulo q that intersect A are $q_1, \dots, q_s$. For $1 \le i \le r$ and $1 \le j \le s$, consider the greatest common divisors

$$d_{p,i} = (p_1 - p_i, p_2 - p_i, \dots, p_r - p_i, p), \qquad d_{q,j} = (q_1 - q_j, q_2 - q_j, \dots, q_s - q_j, q).$$

Note that the set $(A - q_j)/d_{q,j}$ still consists of integers. If there is a $d_{q,j} > 1$, then change A to $(A - q_j)/d_{q,j}$. Similarly if there is a $d_{p,i} > 1$, then change A to $(A - p_i)/d_{p,i}$. Note that such a change redefines the residue classes p_i, q_j as well as r and s.

Repeat this process as many times as possible. If $|A| \ge 2$ then the process must stop after finitely many steps since each reduction decreases the distance between the minimal and maximal elements of A.

We say that A is *reduced* if both of the following hold for any $1 \le i \le r$ and $1 \le j \le s$:

$$(p_1 - p_i, p_2 - p_i, \dots, p_r - p_i, p) = 1, \tag{4}$$

$$(q_1 - q_j, q_2 - q_j, \dots, q_s - q_j, q) = 1. \tag{5}$$

Observe that any reduced set must have at least two residue classes modulo q and modulo p when $p > 1$.

We will assume A satisfies (4) and (5). We split A into residue classes modulo p and modulo q as follows:

$$A = \bigcup_{i=1}^{r} P_i, \qquad P_i = p_i + p \cdot P_i', \ P_i \neq \emptyset, \ 0 \le p_i < p,$$

$$A = \bigcup_{j=1}^{s} Q_j, \qquad Q_j = q_j + q \cdot Q_j', \ Q_j \neq \emptyset, \ 0 \le q_j < q.$$

We remark here that the proof is simpler when $p = 1$, since (4) is vacuous and we do not need to split A into residue classes modulo p.

Note that

$$p \cdot A + q \cdot A = \bigcup_{i=1}^{r} (p \cdot A + q \cdot P_i) = \bigcup_{j=1}^{s} (p \cdot Q_j + q \cdot A)$$
$$= \bigcup_{i=1}^{r} \bigcup_{j=1}^{s} (p \cdot Q_j + q \cdot P_i)$$

where the unions are disjoint. Indeed, for any $1 \le i \le r$ and $1 \le j \le s$, any element of $p \cdot Q_j + q \cdot P_i$ is equivalent to pq_j modulo q and qp_i modulo p, and since $(p, q) = 1$, the $p \cdot Q_j + q \cdot P_i$ are pairwise disjoint. This is not true

for, say, $A + A + q \cdot A$, and the extension of our method to three or more terms does not seem straightforward.

Utilizing (2), we obtain

$$|p \cdot A + q \cdot A| = \sum_{i=1}^{r} \sum_{j=1}^{s} |p \cdot Q_j + q \cdot P_i| \tag{6}$$
$$\geq \sum_{i=1}^{r} \sum_{j=1}^{s} (|Q_j| + |P_i| - 1) = (r+s)|A| - rs.$$

We will say that A is *fully distributed modulo* p (FD mod p) if A intersects every residue class modulo p, and A is *fully distributed modulo* q (FD mod q) if A intersects every residue class modulo q. Thus A is FD mod p and/or FD mod q if and only if $r = p$ and/or $s = q$.

LEMMA 3.1. *For any fixed* $1 \leq j \leq s$, *either* Q'_j *is FD mod* q *or*

$$|p \cdot Q_j + q \cdot A| \geq |p \cdot Q_j + q \cdot Q_j| + \min_{1 \leq m \leq s} |Q_m|.$$

Similarly, for any fixed $1 \leq i \leq r$, *either* P'_i *is FD mod* p *or*

$$|p \cdot A + q \cdot P_i| \geq |p \cdot P_i + q \cdot P_i| + \min_{1 \leq k \leq r} |P_k|.$$

Proof. We only prove the first statement; the second is obtained by a symmetric argument. Suppose $|p \cdot Q_j + q \cdot A| < |p \cdot Q_j + q \cdot Q_j| + \min_{1 \leq m \leq s} |Q_m|$. Then for any $1 \leq m \leq s$, we have

$$|Q'_m| = |Q_m| > |(p \cdot Q_j + q \cdot Q_m) \setminus (p \cdot Q_j + q \cdot Q_j)|$$
$$= |(q_m - q_j + p \cdot Q'_j + q \cdot Q'_m) \setminus (p \cdot Q'_j + q \cdot Q'_j)|.$$

It follows that for every $x \in p \cdot Q'_j$ there is a $y \in Q'_m$ such that $q_m - q_j + x + qy \in p \cdot Q'_j + q \cdot Q'_j$, and so there is an $x' \in p \cdot Q'_j$ such that $q_m - q_j + x \equiv x' \pmod{q}$. We may repeat this argument with x' in place of x, and so on, and we may repeat it for all m so that eventually we infer for any $x \in p \cdot Q'_j$ and any $z = u_1(q_1 - q_j) + \cdots + u_s(q_s - q_j)$, where $u_1, \ldots, u_s$ are arbitrary integers, that there is an $x' \in p \cdot Q'_j$ with $z + x \equiv x' \pmod{q}$. Since A is reduced, the set of z describes all residues modulo q by (5). It follows that $p \cdot Q'_j$ is FD mod q, and since $(p, q) = 1$, Q'_j is FD mod q. ∎

The previous lemma will be useful in finding new elements if no P'_i is FD mod p or if no Q'_j is FD mod q. For convenience, set $A_{ij} := P_i \cap Q_j$, where some of these sets may be empty. Then

$$A = \bigcup_{i=1}^{r} \bigcup_{j=1}^{s} A_{ij},$$

$$A_{ij} = a_{ij} + pq \cdot A'_{ij},\ 0 \leq a_{ij} < pq,\ a_{ij} \equiv p_i \pmod{p},\ a_{ij} \equiv q_j \pmod{q}.$$

The fact that we may write $A_{ij} = a_{ij} + pq \cdot A'_{ij}$ is precisely the Chinese remainder theorem. The condition $(p,q) = 1$ is essentially used here. We have

$$|A| = \sum_{i=1}^{r} \sum_{j=1}^{s} |A_{ij}|, \tag{7}$$

where some of the summands are possibly zero.

LEMMA 3.2. *Fix $1 \le i \le r$ and $1 \le j \le s$. Suppose P'_i is FD mod p. Then either A'_{ij} is FD mod p or*

$$|p \cdot Q_j + q \cdot P_i| \ge |p \cdot A_{ij} + q \cdot A_{ij}| + |A_{ij}|.$$

Similarly, suppose Q'_j is FD mod q. Then either A'_{ij} is FD mod q or

$$|p \cdot Q_j + q \cdot P_i| \ge |p \cdot A_{ij} + q \cdot A_{ij}| + |A_{ij}|.$$

Proof. We prove the first statement; the second follows by a symmetric argument. The result is trivial for $A_{ij} = \emptyset$. For $A_{ij} \neq \emptyset$, we analyze

$$|p \cdot A_{ij} + q \cdot P_i| = |p \cdot A_{ij} + q \cdot A_{ij}| + |(p \cdot A_{ij} + q \cdot P_i) \setminus (p \cdot A_{ij} + q \cdot A_{ij})|.$$

An easy calculation reveals that

$$|(p \cdot A_{ij} + q \cdot P_i) \setminus (p \cdot A_{ij} + q \cdot A_{ij})| = \left| \left(\frac{p_i - a_{ij}}{p} + p \cdot A'_{ij} + P'_i \right) \setminus (p \cdot A'_{ij} + q \cdot A'_{ij}) \right|.$$

Note that $(p_i - a_{ij})/p \in \mathbb{Z}$. Suppose this is smaller than $|A_{ij}| = |A'_{ij}|$. Then for every $x \in P'_i$ there is a $y \in A'_{ij}$ such that $(p_i - a_{ij})/p + py + x \in p \cdot A'_{ij} + q \cdot A'_{ij}$. This means that for every $x \in P'_i$ there is an $x' \in q \cdot A'_{ij}$ such that $(p_i - a_{ij})/p + x \equiv x' \pmod p$. Since P'_i is FD mod p, we see that $q \cdot A'_{ij}$ is FD mod p. But $(p,q) = 1$, so A'_{ij} is FD mod p. ∎

We are now ready to prove Theorem 1.1. Our strategy is simple: we start from Lemma 2.1 and gradually improve it in an iterative way.

PROPOSITION 3.3. *Let $q > p \ge 1$ be relatively prime integers. For every integer $3(p+q) \le m \le (p+q)^2$ and for all finite sets A of integers, we have*

$$|p \cdot A + q \cdot A| \ge \frac{m}{p+q}|A| - (pq)^{m+1-3(p+q)}.$$

Proof. Observe that the case $m = (p+q)^2$ is precisely Theorem 1.1. We proceed by induction on m. For $m = 3(p+q)$, we claim $|p \cdot A + q \cdot A| \ge 3|A| - pq$, which is even true with $3|A| - 2$ by Lemma 2.1.

Suppose now that the conclusion is true for a fixed $3(q+p) \le m < (p+q)^2$. For simplicity, we write

$$C_m = (pq)^{m+1-3(p+q)}.$$

First, assume there is $1 \le i \le r$ such that $|P_i| \le \frac{1}{p+q}|A|$. Then by the induction hypothesis, (2), and $m \le (p+q)^2$, we obtain

$$\begin{aligned}|p\cdot A + q\cdot A| &\ge |p\cdot A + q\cdot P_i| + |p\cdot(A\setminus P_i) + q\cdot(A\setminus P_i)|\\ &\ge |P_i| + |A| - 1 + \frac{m}{p+q}(|A| - |P_i|) - C_m \ge \frac{m+1}{p+q}|A| - C_{m+1},\end{aligned}$$

since $C_{m+1} \ge C_m + 1$. A symmetric argument completes the induction step if $|Q_j| \le \frac{1}{p+q}|A|$ for some $1 \le j \le s$. Thus we may assume that every P_i and Q_j has more than $\frac{1}{p+q}|A|$ elements. If there is $1 \le i \le r$ such that P_i' is not FD mod p then by Lemma 3.1 and the induction hypothesis we have

$$\begin{aligned}|p\cdot A + q\cdot A| &\ge |p\cdot A + q\cdot P_i| + |p\cdot(A\setminus P_i) + q\cdot(A\setminus P_i)|\\ &\ge |p\cdot P_i + q\cdot P_i| + \min_{1\le k\le r}|P_k| + \frac{m}{p+q}(|A| - |P_i|) - C_m\\ &\ge \frac{m}{p+q}|P_i| - C_m + \frac{1}{p+q}|A| + \frac{m}{p+q}(|A| - |P_i|) - C_m\\ &\ge \frac{m+1}{p+q}|A| - C_{m+1},\end{aligned}$$

since $C_{m+1} \ge 2C_m$. A symmetric argument works if there is $1 \le j \le s$ such that Q_j' is not FD mod q. Thus we may assume that every P_i' is FD mod p and every Q_j' is FD mod q.

Fix $1 \le i \le r$ and $1 \le j \le s$. Then using both parts of Lemma 3.2 we deduce that either

$$|p\cdot Q_j + q\cdot P_i| \ge |p\cdot A_{ij} + q\cdot A_{ij}| + |A_{ij}| \ge \frac{m+1}{p+q}|A_{ij}| - C_m$$

by the induction hypothesis, or A_{ij}' is FD mod p and FD mod q. In the latter case, by (6),

$$|p\cdot A_{ij} + q\cdot A_{ij}| = |p\cdot A_{ij}' + q\cdot A_{ij}'| \ge (p+q)|A_{ij}| - pq \ge \frac{m+1}{p+q}|A_{ij}| - C_m,$$

since $C_m \ge pq$ and $p+q \ge \frac{m+1}{p+q}$. Note that this is the point which blocks us from gradually improving the lower bound beyond $(p+q)|A|$.

In either case $|p\cdot Q_j + q\cdot P_i| \ge \frac{m+1}{p+q}|A_{ij}| - C_m$. By (7), it follows that

$$\begin{aligned}|p\cdot A + q\cdot A| &= \sum_{i=1}^{r}\sum_{j=1}^{s}|p\cdot Q_j + q\cdot P_i|\\ &\ge \sum_{i=1}^{r}\sum_{j=1}^{s}\left(\frac{m+1}{p+q}|A_{ij}| - C_m\right) \ge \frac{m+1}{p+q}|A| - C_{m+1},\end{aligned}$$

since $C_{m+1} = pqC_m$. ∎

Acknowledgements. The first author's research was supported by the Hungarian National Science Foundation Grants K81658 and K104183.

References

[1] A. Balog, *A note on sum-product estimates*, Publ. Math. Debrecen 79 (2011), 283–289.
[2] B. Bukh, *Sums of dilates*, Combin. Probab. Comput. 17 (2008), 627–639.
[3] J. Cilleruelo, Y. Hamidoune and O. Serra, *On sums of dilates*, Combin. Probab. Comput. 18 (2009), 871–880.
[4] J. Cilleruelo, M. Silva and C. Vinuesa, *A sumset problem*, J. Combin. Number Theory 2 (2010), 79–89.
[5] S. Du, H. Cao and Z. Sun, *On a sumset problem for integers*, Electron. J. Combin. 21 (2014), no. 1, #P1.13.
[6] Gy. Elekes, *On the number of sums and products*, Acta Arith. 81 (1997), 365–367.
[7] P. Erdős and E. Szemerédi, *On sums and products of integers*, in: Studies in Pure Mathematics, L. Alpár et al. (eds.), Birkhäuser, Basel, 1983, 213–218.
[8] Y. Hamidoune and J. Rué, *A lower bound for the size of a Minkowski sum of dilates*, Combin. Probab. Comput. 20 (2011), 249–256.
[9] T. G. F. Jones and O. Roche-Newton, *Improved bounds on the set $A(A+1)$*, J. Combin. Theory Ser. A 120 (2013), 515–526.
[10] Ž. Ljujić, *A lower bound for the size of a sum of dilates*, J. Combin. Number Theory 5 (2013), 31–51.
[11] J. Solymosi, *Bounding multiplicative energy by the sumset*, Adv. Math. 222 (2009), 402–408.
[12] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math. 105, Cambridge Univ. Press, Cambridge, 2006.

Antal Balog
Alfréd Rényi Institute of Mathematics
P.O. Box 127
1364 Budapest, Hungary
E-mail: balog@renyi.mta.hu

George Shakan
Department of Mathematics
University of Wyoming
Laramie, WY 82072, U.S.A.
E-mail: gshakan@uwyo.edu

Received on 3.9.2013
and in revised form on 12.2.2014 (7570)