New upper bound for sums of dilates

Albert Bush Yi Zhao*

Department of Mathematics and Statistics
Georgia State University
Atlanta, GA 30303, USA

albertbush@gmail.com yzhao6@gsu.edu

Submitted: Nov 2, 2016; Accepted: Aug 16, 2017; Published: Aug 25, 2017
Mathematics Subject Classifications: 11P70, 11B13, 05C70

Abstract

For $\lambda \in \mathbb{Z}$, let $\lambda \cdot A = \{\lambda a : a \in A\}$. Suppose $r, h \in \mathbb{Z}$ are sufficiently large and comparable to each other. We prove that if $|A + A| \leqslant K|A|$ and $\lambda_1, \ldots, \lambda_h \leqslant 2^r$, then

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{7rh/\ln(r+h)}|A|.$$

This improves upon a result of Bukh who shows that

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{O(rh)}|A|.$$

Our main technique is to combine Bukh's idea of considering the binary expansion of λ_i with a result on biclique decompositions of bipartite graphs.

Keywords: sumsets; dilates; Plünnecke–Ruzsa inequality; graph decomposition; biclique partition

1 Introduction

Let A and B be nonempty subsets of an abelian group, and define the *sumset* of A and B and the *h-fold sumset* of A as

$$A + B := \{a + b : a \in A, b \in B\} \text{ and } hA := \{a_1 + \ldots + a_h : a_i \in A\},$$

respectively. When the set A is implicitly understood, we will reserve the letter K to denote the doubling constant of A; that is, $K := |A + A|/|A|$. A classical result of Plünnecke bounds the cardinality of hA in terms of K and $|A|$.

*Partially supported by NSF grant DMS-1400073.

Theorem 1 (Plünnecke's inequality [5]). *For any set A and for any nonnegative integers ℓ and m, if $|A+A| = K|A|$, then*

$$|\ell A - mA| \leqslant K^{\ell+m}|A|.$$

See the survey of Ruzsa [6] for variations, generalizations, and a graph theoretic proof of Theorem 1; see Petridis [4] for a new inductive proof.

Given $\lambda \in \mathbb{Z}$, define a *dilate* of A as

$$\lambda \cdot A := \{\lambda a : a \in A\}.$$

Suppose $\lambda_1, \ldots, \lambda_h$ are nonzero integers. Since $\lambda_i \cdot A \subseteq \lambda_i A$, one can apply Theorem 1 to conclude that

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{\sum_i |\lambda_i|}|A|.$$

Bukh [1] significantly improved this by considering the binary expansion of λ_i and using Ruzsa's covering lemma and triangle inequality.

Theorem 2 (Bukh [1]). *For any set A, if $\lambda_1, \ldots, \lambda_h \in \mathbb{Z} \setminus \{0\}$ and $|A+A| = K|A|$, then*

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{7+12\sum_{i=1}^{h} \log_2(1+|\lambda_i|)}|A|.$$

If $|\lambda_i| \leqslant 2^r$ for all i, then Theorem 2 yields that

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{O(rh)}|A|. \tag{1}$$

In this paper we prove a bound that improves (1) when r and h are sufficiently large and comparable to each other. Throughout the paper ln stands for the natural logarithm.

Theorem 3. *Suppose $r, h \in \mathbb{Z}$ are sufficiently large and*

$$\min\{r+1, h\} \geqslant 10\left(\ln \max\{r+1, h\}\right)^2. \tag{2}$$

Given a set A and nonzero integers $\lambda_1, \ldots, \lambda_h$ such that $|\lambda_i| \leqslant 2^r$, if $|A+A| = K|A|$, then

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{7rh/\ln(r+h)}|A|. \tag{3}$$

The proof of Theorem 3 relies on Theorem 2 as well as a result of Tuza [8] on decomposing bipartite graphs into bicliques (complete bipartite subgraphs). The key idea is to connect Bukh's technique of considering the binary expansion of λ_i to the graph decomposition problem that allows us to efficiently group certain powers of 2.

We remark here that in all of the above theorems, the condition $|A+A| = K|A|$ can be replaced with $|A-A| = K|A|$ with no change to the conclusion. It is likely that Theorem 3 is not best possible – we discuss this in the last section.

2 Basic Tools

We need the following analogue of Ruzsa's triangle inequality, see [6, Theorem 1.8.7].

Theorem 4 (Ruzsa [6])**.** *For any sets X, Y, and Z,*

$$|X+Y| \leqslant \frac{|X+Z||Z+Y|}{|Z|}.$$

A useful corollary of Theorem 4 is as follows.

Corollary 5. *For any sets A and B, if p_1 and p_2 are nonnegative integers and $|A+A| \leqslant K|A|$, then*

$$|B+p_1A-p_2A| \leqslant K^{p_1+p_2+1}|B+A|.$$

Proof. Apply Theorem 4 with $X=B$, $Y=p_1A-p_2A$, and $Z=A$, then apply Plünnecke's inequality (Theorem 1). □

We can use Corollary 5 to prove the following proposition that we will use in the proof of Theorem 3.

Proposition 6. *If $k_1, \ell_1, \ldots, k_q, \ell_q$ are nonnegative integers, $K>0$, and $A_1, \ldots, A_q, C$ are sets such that $|A_i+A_i| \leqslant K|A_i|$, then*

$$|C+k_1A_1-\ell_1A_1+\ldots+k_qA_q-\ell_qA_q| \leqslant |C+A_1+\ldots+A_q| \cdot K^{q+\sum_{i=1}^{q}(k_i+\ell_i)}. \tag{4}$$

In particular,

$$|k_1A_1-\ell_1A_1+\ldots+k_qA_q-\ell_qA_q| \leqslant |A_1+\ldots+A_q| \cdot K^{q+\sum_{i=1}^{q}(k_i+\ell_i)}. \tag{5}$$

Proof. (5) follows from (4) by taking C to be a set with a single element so it suffices to prove (4). We proceed by induction on q. The case $q=1$ follows from Corollary 5 immediately. When $q>1$, suppose the statement holds for any positive integer less than q. Applying Corollary 5 with $B=C+k_1A_1-\ell_1A_1+\ldots+k_{q-1}A_{q-1}-\ell_{q-1}A_{q-1}$ and $A=A_q$, we obtain that

$$\begin{aligned}&|C+k_1A_1-\ell_1A_1+\ldots+k_qA_q-\ell_qA_q|\\ \leqslant\ & K^{k_q+\ell_q+1}|C+k_1A_1-\ell_1A_1+\ldots+k_{q-1}A_{q-1}-\ell_{q-1}A_{q-1}+A_q|.\end{aligned} \tag{6}$$

Now, let $C'=C+A_q$ and apply the induction hypothesis to conclude that

$$\begin{aligned}&|C'+k_1A_1-\ell_1A_1+\ldots+k_{q-1}A_{q-1}-\ell_{q-1}A_{q-1}|\\ \leqslant\ & |C'+A_1+\ldots+A_{q-1}| \cdot K^{q-1+\sum_{i=1}^{q-1}(k_i+\ell_i)}\end{aligned} \tag{7}$$

Combining (6) with (7) gives the desired inequality:

$$|C+k_1A_1-\ell_1A_1+\ldots+k_qA_q-\ell_qA_q| \leqslant |C+A_1+\ldots+A_q| \cdot K^{q+\sum_{i=1}^{q}(k_i+\ell_i)}. \qquad \square$$

3 Proof of Theorem 3

Given $\lambda_1, \ldots, \lambda_h \in \mathbb{Z} \setminus \{0\}$, we define

$$r := \max_i \lfloor \log_2 |\lambda_i| \rfloor \tag{8}$$

and write the binary expansion of λ_i as

$$\lambda_i = \epsilon_i \sum_{j=0}^{r} \lambda_{i,j} 2^j, \text{ where } \lambda_{i,j} \in \{0,1\} \text{ and } \epsilon_i \in \{-1,1\}. \tag{9}$$

Bukh's proof of Theorem 2 actually gives the following stronger statement.

Theorem 7 ([1])**.** *If $\lambda_1, \ldots, \lambda_h \in \mathbb{Z} \setminus \{0\}$ and $|A+A| = K|A|$, then*

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{7+10r+2\sum_i \sum_j \lambda_{i,j}} |A|.$$

In his proof of Theorem 2, the first step is to observe that

$$\lambda_1 \cdot A + \ldots + \lambda_h \cdot A \subseteq \sum_{j=0}^{r} (\lambda_{1,j} 2^j) \cdot A + \ldots + \sum_{j=0}^{r} (\lambda_{h,j} 2^j) \cdot A.$$

In our proof, we also consider the binary expansion of λ_i, but we do the above step more efficiently by first grouping together λ_i that have shared binary digits. In order to do this systematically, we view the problem as a graph theoretic problem and apply the following result of Tuza [8].

Theorem 8 (Tuza [8])**.** *There exists n_0 such that the following holds for any integers $m \geqslant n \geqslant n_0$ such that $n \geqslant 10(\ln m)^2$. Every bipartite graph G on two parts of size m and n can be decomposed into edge-disjoint complete bipartite subgraphs $H_1, \ldots, H_q$ such that $E(G) = \cup_i E(H_i)$ and*

$$\sum_{i=1}^{q} |V(H_i)| \leqslant \frac{3mn}{\ln m}. \tag{10}$$

Tuza stated this result [8, Theorem 4] for the *covers* of G, where a *cover* of G is a collection of subgraphs of G such that every edge of G is contained in at least one of these subgraphs. However, the cover provided in his proof is indeed a decomposition. Furthermore, the assumption $n \geqslant 10(\ln m)^2$ was not stated in [8, Theorem 4] but such kind of assumption is needed.[1] Indeed, (10) becomes false when $n = o(\ln m)$ because $\sum_{i=1}^{q} |V(H_i)| \geqslant m + n$ for any cover $H_1, \ldots, H_q$ of G if G has no isolated vertices.

Note that (10) is tight up to a constant factor. Indeed, Tuza [8] provided a bipartite graph G with two parts of size $n \leqslant m$ such that every biclique *cover* $H_1, \ldots, H_q$ of G satisfies $\sum_{i=1}^{q} |V(H_i)| \geqslant mn/(e^2 \ln m)$, where $e = 2.718\ldots$.

[1] In his proof, copies of $K_{q,q}$ were repeatedly removed from G, where $q = \lfloor \ln m / \ln j \rfloor$ for $2 \leqslant j \leqslant (\ln m) \ln \ln m$. By a well-known bound on the Zarankiewicz problem, every bipartite graph G with parts of size m and n contains a copy of $K_{q,q}$ if $|E(G| \geqslant (q-1)^{1/q}(n-q+1)m^{1-1/q} + (q-1)m$. A simplified bound $|E(G| \geqslant (1+o(1))nm^{1-1/q}$ was used in [8] but it requires that $qm^{1/q} = o(n)$.

Proof of Theorem 3. Let $r, h \in \mathbb{Z}$ be sufficiently large and satisfy (2). Given nonzero integers $\lambda_1, \ldots, \lambda_h$, define r and $\lambda_{i,j}$ as in (8) and (9). We define a bipartite graph $G = (X, Y, E)$ as follows: let $X = \{\lambda_1, \ldots, \lambda_h\}$, $Y = \{2^0, \ldots, 2^r\}$, and $E = \{(\lambda_i, 2^j) : \lambda_{i,j} = 1\}$. In other words, λ_i is connected to the powers of 2 that are present in its binary expansion.

We apply Theorem 8 to G and obtain a biclique decomposition $H_1, \ldots, H_q$ of G. Assume $H_i := (X_i, Y_i, E_i)$ where $X_i \subseteq X$, $Y_i \subseteq Y$. We have $E_i = \{(u, v) : u \in X_i, v \in Y_i\}$ and

$$\sum_{i=1}^{q} (|X_i| + |Y_i|) \leqslant \frac{3(r+1)h}{\ln \max\{r+1, h\}}. \tag{11}$$

Now, we connect this biclique decomposition to the sum of dilates $\lambda_1 \cdot A + \ldots + \lambda_h \cdot A$. Since the elements of X and Y are integers, we can perform arithmetic operations with them. For $j = 1, \ldots, q$, let

$$\gamma_j := \sum_{y \in Y_j} y,$$

and since $\mathcal{H}$ is a biclique decomposition, for $i = 1, \ldots, h$, we have

$$\lambda_i = \epsilon_i \sum_{j : \lambda_i \in X_j} \gamma_j.$$

Applying the above to each λ_i along with the fact that $B + (\alpha + \beta) \cdot A \subseteq B + \alpha \cdot A + \beta \cdot A$ results in

$$\lambda_1 \cdot A + \ldots + \lambda_h \cdot A \subseteq \epsilon_1 \sum_{j : \lambda_1 \in X_j} (\gamma_j \cdot A) + \ldots + \epsilon_h \sum_{j : \lambda_h \in X_j} (\gamma_j \cdot A). \tag{12}$$

Let $k_j := |\{\lambda_i \in X_j : \lambda_i > 0\}|$, $\ell_j := |\{\lambda_i \in X_j : \lambda_i < 0\}|$, and note that $k_j + \ell_j = |X_j|$. By regrouping the terms in (12), we have

$$\begin{aligned} &\epsilon_1 \sum_{j : \lambda_1 \in X_j} \gamma_j \cdot A + \ldots + \epsilon_h \sum_{j : \lambda_h \in X_j} \gamma_j \cdot A \\ &= k_1(\gamma_1 \cdot A) - \ell_1(\gamma_1 \cdot A) + \ldots + k_q(\gamma_q \cdot A) - \ell_q(\gamma_q \cdot A). \end{aligned}$$

Since $|\gamma_j \cdot A + \gamma_j \cdot A| = |A + A| \leqslant K|A| = K|\gamma_j \cdot A|$, we can apply Proposition 6 to conclude that

$$\begin{aligned} &|k_1(\gamma_1 \cdot A) - \ell_1(\gamma_1 \cdot A) + \ldots + k_q(\gamma_q \cdot A) - \ell_q(\gamma_q \cdot A)| \\ &\leqslant |\gamma_1 \cdot A + \ldots + \gamma_q \cdot A| \cdot K^{q + \sum_{i=1}^{q} k_i + \ell_i} \leqslant |\gamma_1 \cdot A + \ldots + \gamma_q \cdot A| \cdot K^{2 \sum_{i=1}^{q} |X_i|}. \end{aligned} \tag{13}$$

For $1 \leqslant i \leqslant q$ and $0 \leqslant j \leqslant r$, let $\gamma_{i,j} = 1$ if 2^j is in the binary expansion of γ_i and 0 otherwise. Observe that

$$\max_j \lfloor \log_2 \gamma_j \rfloor \leqslant \max_i \lfloor \log_2 |\lambda_i| \rfloor = r \quad \text{and} \quad \sum_{j=0}^{r} \gamma_{i,j} = |Y_i|.$$

Hence, by Theorem 7,

$$|\gamma_1 \cdot A + \ldots + \gamma_q \cdot A| \leqslant K^{7+10r+2\sum_{i=1}^{q}\sum_{j=0}^{r}\gamma_{i,j}}|A| = K^{7+10r+2\sum_{i=1}^{q}|Y_i|}|A|. \tag{14}$$

Combining (13) and (14) with (11) results in

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{7+10r+2\sum_{i=1}^{q}(|X_i|+|Y_i|)}|A| \leqslant K^{7+10r+\frac{6(r+1)h}{\ln\max\{r+1,h\}}}|A|.$$

We have $7 + 10r = o((r+1)h/\ln\max\{r+1,h\})$ because of (2) and the assumption that r, h are sufficiently large. Together with

$$\ln\max\{r+1,h\} \geqslant \ln\frac{r+1+h}{2} \geqslant (1-o(1))\ln(r+h),$$

this implies that $|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{7rh/\ln(r+h)}|A|$, as desired. □

4 Concluding Remarks

Instead of Theorem 8, in an earlier version of the paper we applied a result of Chung, Erdős, and Spencer [2], which states that every graph on n vertices has a biclique decomposition $H_1, \ldots, H_q$ such that $\sum_{i=1}^{q}|V(H_i)| \leqslant (1+o(1))n^2/(2\ln n)$. Instead of (3), we obtained that

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{O((r+h)^2/\ln(r+h))}|A|.$$

This bound is equivalent to (3) when $r = \Theta(h)$ but weaker than Bukh's bound (1) when r and h are not close to each other.

Although the assumption (2) may not be optimal, Theorem 3 is not true without any assumption on r and h. For example, when r is large and $h = o(\ln r)$, (3) becomes $|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{o(r)}|A|$, which is false when $A = \{1, \ldots, n\}$.

If each of $\lambda_1, \ldots, \lambda_r$ has $O(1)$ digits in its binary expansion, then Theorem 2 yields that $|\lambda_1 \cdot A + \ldots + \lambda_r \cdot A| \leqslant K^{O(r)}|A|$. Bukh asked if this bound holds whenever $\lambda_i \leqslant 2^r$:

Question 9 (Bukh [1])**.** For any set A and for any $\lambda_1, \ldots, \lambda_r \in \mathbb{Z}\setminus\{0\}$, if $|A+A| = K|A|$ and $0 < \lambda_i \leqslant 2^r$, then

$$|\lambda_1 \cdot A + \ldots + \lambda_r \cdot A| \leqslant K^{O(r)}|A|.$$

In light of Question 9, one can view Theorem 3 as providing modest progress by proving a subquadratic bound of quality $O(r^2/\ln r)$ whereas Theorem 2 shows that the exponent is $O(r^2)$.

Generalized arithmetic progressions give supporting evidence for Question 9. A *generalized arithmetic progression* P is a set of the form

$$P := \{d + x_1 d_1 + \ldots + x_k d_k : 0 \leqslant x_i < L_i\}.$$

Moreover, P is said to be *proper* if $|P| = L_1 \cdot \ldots \cdot L_k$. One can calculate that if P is proper, then

$$|P+P| \leqslant (2L_i - 1)^k \leqslant 2^k|P| =: K|P|.$$

Additionally, one can calculate that for any $\lambda_1, \dots, \lambda_h \in \mathbb{Z}^+$, if $\lambda_i \leqslant 2^r$ then

$$|\lambda_1 \cdot P + \ldots + \lambda_h \cdot P| \leqslant (\lambda_1 + \ldots + \lambda_h)^k |P| = 2^{k \log_2(\lambda_1 + \ldots + \lambda_h)} |P| = K^{r + \log_2 h} |P|.$$

Freiman's theorem [3] says that, roughly speaking, sets with small doubling are contained in generalized arithmetic progressions with bounded dimension. Using this line of reasoning, Schoen and Shkredov [7, Theorem 6.2] proved that

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant e^{O(\log_2^6(2K) \log_2 \log_2(4K))(h + \log_2 \sum_i |\lambda_i|)} |A|.$$

This naturally leads us to ask a more precise version of Question 9.

Question 10. If $|A + A| = K|A|$, then is

$$|\lambda_1 \cdot A + \ldots + \lambda_h \cdot A| \leqslant K^{O(h + \ln \sum_i |\lambda_i|)} |A|?$$

Acknowledgment

We thank Boris Bukh and Giorgis Petridis for reading an earlier version of this paper and giving valuable comments. We also thank an anonymous referee for suggesting [8] as well as other helpful comments.

References

[1] B. Bukh. Sums of dilates. *Combinatorics, Probability and Computing*, 17(05):627–639, 2008.

[2] F. Chung, P. Erdős, and J. Spencer. On the decomposition of graphs into complete bipartite subgraphs. In *Studies in Pure Mathematics*, pages 95–101. Springer, 1983.

[3] G. A. Freĭman. *Foundations of a structural theory of set addition*. American Mathematical Society, Providence, R. I., 1973. Translated from the Russian, Translations of Mathematical Monographs, Vol 37.

[4] G. Petridis. New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica*, 32(6):721–733, 2012.

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

[6] I. Z. Ruzsa. Sumsets and structure. In *Combinatorial Number Theory and Additive Group Theory*, pages 87–210, 2009.

[7] T. Schoen and I. D. Shkredov. Additive dimension and a theorem of Sanders. *J. Aust. Math. Soc.*, 100(1):124–144, 2016.

[8] Z. Tuza. Covering of graphs by complete bipartite subgraphs: complexity of 0-1 matrices. *Combinatorica*, 4(1):111–116, 1984.